International Telecommunication Union

ITU-T Y.4805

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(08/2017)

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 – Identification and security

Identifier service requirements for the interoperability of smart city applications

Recommendation ITU-T Y.4805

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.4805

Identifier service requirements for the interoperability of smart city applications

Summary

Recommendation ITU-T Y.4805 specifies a set of requirements for identifier services in smart city applications with a view to ensure that such systems are interoperable and secure. This set of requirements may additionally serve as guidelines for developing new identifier services for smart cities. It includes security features for service integrity and data confidentiality. The Recommendation defines a full list of identifier service requirements, including security requirements, for the identifier service.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4805	2017-08-22	20	11.1002/1000/13267

Keywords

Data confidentiality, identifier, service integrity, smart city.

---

* 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.4805

Identifier service requirements for the interoperability of smart city applications

1 Scope

This Recommendation specifies a set of requirements for identifier services in smart city applications with a view to ensure that such systems are interoperable and secure. This set of requirements may additionally serve as guidelines for developing new identifier services for smart cities. The Recommendation includes security features for service integrity and data confidentiality. The Recommendation defines a full list of identifier service requirements, including security requirements, for the identifier service.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2261]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

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 identifier resolution [b-ITU-T Y.4108]: A function to resolve an identifier into associated information and vice versa.

3.1.4 Internet of things (IoT) [b-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.

3.1.5 interoperability [b-ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 identifier administration: The ability to carry out functions to support life-cycle management of identifiers and identifier attributes. These functions include the registration of new identifiers, the removal of existing identifier, the amendment and update of any information

associated with the identifier and any other related administrative functions as defined within a specific identifier scheme as per definition 3.1.2 above.

3.2.2 identifier service: A network information service operated over the Internet which carries out identifier resolution as per definition 3.1.3 and identifier administration as per definition 3.2.1 above.

3.2.3 root service of identifier service: A root service is the key component at the apex of a hierarchical identifier or naming service. For example, DNS defines its root service as the collection of root name servers and data at the apex of the Internet naming system.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ID Identifier

IoT Internet of Things

TTL Time-To-Live

UTF-8 8-bit Unicode Transformation Format

5 Conventions

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

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

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

In this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Identifier services for smart city applications

Identifier (ID) services for smart city applications are discussed in terms of its service, data and operation models. The service model explores the service structure of the identifier service to better support smart city applications, including its service components and the relationship among these components. The data model defines necessary data structure that will be needed to support identifier attributes in smart city applications, as well as to security and management operations upon identifiers and identifier attributes. The operation model discusses essential operations that should be provided by the identifier service, as well as crucial features to allow cohesive, transparent and trustworthy operations among different identifier service components, as appropriate.

6.1 Service model

The identifier service for smart city applications must support applications operated from different cities, and managed by different organizations and/or service providers. A distributed service model can enable such identifier service.

The service model of the identifier service refers to the service structure of the identifier service, in terms of its service components, under a distributed networking environment.

The identifier service for smart city applications may consist of many service components, where each one is managed by different organizations and/or service providers. Each component of the identifier service may be responsible for a local domain of identifiers used in smart city applications. These service components must work cooperatively to allow identification of any smart city entity in terms of a global unique identifier, and to allow resolution and real-time update of information associated with the identifier.

On the other hand, a service component of the identifier service may be operated and managed by individual organizations independently from others. Any disruption of one component should not disrupt the service from other components. Administration of identifier and identifier information may be performed by an individual identifier service component, without reliance on the others.

6.2 Data model

The data model of the identifier service refers to data structures necessary to support resolution and administration of its identifiers. The data structure should be flexible enough to support existing smart city applications, and to allow backward compatibility.

An identifier in the smart city identifier service not only provides identification of the smart city entity, but also serves as a reference to information associated to the identified subject. The data model of the identifier service should define a data structure that allows all data types to be associated with the identifier. It should also define common mechanisms that allow trust and/or credentials to be established over the information associated with the identifier, so that users can validate the information as needed.

6.3 Operation model

The operation model of the identifier service refers to the essential operations that should be provided by the identifier service to support smart city applications, as well as how these operations should be carried out by the identifier service. The operation model should also define crucial features that will allow cohesive operations among different identifier service components.

More importantly, the identifier service for smart city applications should provide well-defined, built-in security services in each of its service operations. The security services should include options to protect service integrity and data confidentiality, as well as service non-repudiation whenever needed.

7 Requirements for identifier services in smart city applications

7.1 General identifier service requirements

7.1.1 Compatibility with existing smart city practice

An identifier service for smart cities shall consider existing practices in smart city applications. It is required to allow for existing smart city applications to continue to operate, and provide mechanisms to establish an interface with other smart city applications. The identifier service shall be flexible enough to support any naming convention in existing smart city applications.

7.1.2 Extendibility

Different smart city applications may require different data associated to its identifiers. The identifier service for smart cities is required to support application-defined data and meta-data structure, and allow applications to register their data and meta-data structure. The identifier resolution and administration system shall be able to handle all data types associated with the identifiers.

7.1.3 Efficiency in resolution

The identifier service for smart cities is required to be efficient from a time perspective, especially for identifier resolution. If the identifier service also supports identifier administration, it is recommended to allow for a separate service interface to be defined for the administration.

The resolution service can optionally use a number of techniques to improve efficiency. These may include, but are not limited to, measurement of the response times to other identifier services, caching, reducing or optimizing the number of queries and handling defective or non-responding identifier servers.

To gain better performance, the identifier service may also define caching mechanisms in order to reduce the amount of network traffic due to resolution requests.

7.1.4 Scalability

The identifier service is required to be scalable in terms of supporting an ever-increasing number of identifiers for smart cities, and also for its ever-growing applications. A distributed service model is required to support such scalability. In the distributed service model, the service may be managed such that individual organizations may manage and operate their own identifier service independently. It is optional that each identifier service operation can establish multiple service replications (mirroring) to provide service redundancy and load balancing. It is also optional to define mechanisms to support the concept of service clusters, identifiers and/or service requests.

7.1.5 International support

The smart city identifier service is required to support Unicode, which includes most of the characters currently used around the world. There are multiple ways to encode Unicode characters in network transmission. For maximum efficiency and compatibility, an 8-bit Unicode transformation format (UTF-8) is the recommended encoding method for smart city identifier services.

7.2 General security requirements

7.2.1 Secure resolution

The identifier service is required to have an appropriate level of security in terms of identifier resolution. It shall provide service integrity so that clients may validate any data received from the identifier service. It shall also provide an option with an appropriate level of data confidentiality in the resolution process during network transmission.

7.2.2 Discretionary access control

Many smart city applications require discretionary access control to its identified information. An identifier service for smart city is required to allow access control to be defined for information associated to its identifier. Such access control shall be defined independent from the server administrator to allow for maximum flexibility. To realize this, the identifier service is required to implement an interface for client authentication and authorization.

7.2.3 Distributed management and administration interface

Smart city applications involved in real-time control and management of IoT devices may also require change or update of status data associated to its identifier. The identifier service for smart city is required to provide secure administrative interface so that applications can manage and update identifier attributes in a timely manner.

7.3 Requirements related to the service model

7.3.1 Interoperability: Distributed service model

The identifier service for smart city applications is required to support a distributed service model. The identifier service shall consist of distributed service components that will support both peer level and hierarchical level of service distribution.

The peer-level distributed service model is required for the distributed management of identifier services across different smart city applications, either within or outside of any city boundaries. It allows each smart city application to provide its own identifier service independently, yet operates cooperatively among its peers (see Figure 1).

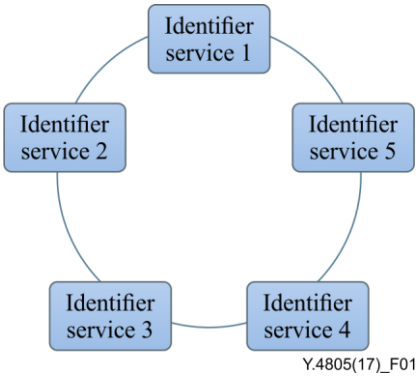

Figure 1 – Peer-level distributed service model

The hierarchical-level distributed service model fits smart city applications reflecting a hierarchical organization management structure. It enables any organization to provide a commonly shared identifier service across multiple domains of subsidiaries, yet also leaving each subsidiary the option to operate its own identifier service whenever needed (see Figure 2).

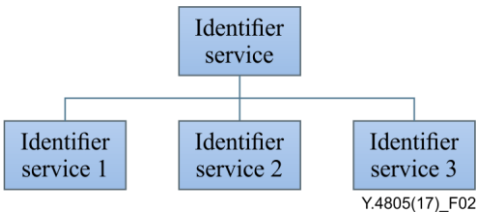

Figure 2 – Hierarchical-level distributed service model

7.3.2 Interoperability: Distributed root service

All hierarchical services require a root service to anchor the service hierarchy. The DNS root service is an example of such service. The identifier service for smart city applications is required to provide a root service to be used as the starting point for registering any of the service components under the service hierarchy. It shall also be used to provide trusted service referrals to any of the service components whenever needed. Such root service is required for any hierarchical identifier service for smart city applications as well. The root service shall be distributed so that it is not subject to any single point of failure. It shall also allow peer level management from multi-stakeholders so that this root is not under control of any single entity. Where different states or organizations operate their own instances of a root server for an identifier service, they shall take appropriate measures to prevent single points of failure.

7.3.3 Security: Root of trust

The root service is required to serve to anchor the trust for the hierarchical identifier service. Under the hierarchical identifier service, an identifier service shall issue credentials to its derived identifier services. The credential of any identifier service is recommended to be a public key signed by the higher-level identifier service, and shall be used to provide a mean of service integrity upon client request. Any client using an identifier service is required to be able to trace its credential up to the root service, to validate the authenticity of the identifier service.

7.3.4 Security: Replication and mirroring

Any identifier service in the distributed identifier service can optionally establish multiple replication services to prevent any single point of failure. Multiple peer-level identifier services among the replication sites are required to permit concurrent identifier administrations. In this case, it is required that mechanisms are established for the prevention of race conditions, where multiple replication sites attempt to update the same identifier record at the same time.

7.3.5 Interoperability: Caching service

The identifier service is required to support caching to help reduce unnecessary network traffic. The identifier resolution result is recommended to contain a standard Time-To-Live (TTL) field to indicate how long the data are valid for. A dedicated caching service can optionally be deployed to support a specific user community.

7.3.6 Interoperability: Support for iterative and recursive resolution service

An identifier service is recommended to send queries iteratively or recursively to another identifier service instance on behalf of an end client. The identifier service making those queries may cache the answers that are returned.

7.4 Requirements of data model

7.4.1 Security: Common scheme for access-control over identifier attributes

Many smart city applications require access-control of identifier attributes. For any certain identifier, it is possible that only a subset of its attributes is openly accessible to the general public, while all other attributes are accessible only to certain authorized parties upon identifier resolution.

The data model of the identifier service for smart city applications is required to include a common scheme for the access-control over identifier attributes. In particular, it shall allow role-based or group-based access-control to be defined on any subset of identifier attributes.

7.4.2 Security: Support for credential validation

In distributed computing, service integrity only provides a mean to prove that the data is coming from an authorized service. It does not necessarily give any credential that the data is trustworthy. The identifier service for smart city applications is required to provide service integrity as discussed earlier in this Recommendation, and also provide options for credential validation. The credential validation is recommended to be defined in terms of options of third-party digital signature associated with the identifier attributes, or references to third-party validation service that can be used to validate the authenticity or credibility of identifier attributes.

7.4.3 Security: Support for discretionary administration and identifier ownership

The data model of the identifier service is required to provide options for the individual identifier administrator, independent from the hosting service, and allow for discretionary administration of the identifier and its attributes. Implementations of the identifier service shall provide means to protect the identifier and its attributes so that only authorized changes can be made to the identifier or its attributes.

Allowing discretionary administration is important in smart city applications where each identified subject may interact directly with the identifier service to perform real-time update on its attributes, without reliance on any centralized server administrator. It also minimizes potential security risks from unauthorized changes to identifiers hosted at the identifier service.

7.4.4 Interoperability: Extendable data model

Identifiers for smart city applications are used to associate different kinds of information for its identified subject. The data model for the identifier service is required to be flexible enough to support new data types to be defined for identifier attributes in smart city applications. A smart city application shall have the option to define its own data type and register it with the identifier service.

7.4.5 Interoperability: Adaptable naming scheme

There are many smart city applications that have their own identification schemes. It is practically difficult to change the naming schemes of these applications. The identifier service for smart city applications is required to define a flexible naming scheme to support adapting the names used by existing smart city applications.

7.5 Requirements of operation model

7.5.1 Security: Secure operations

The identifier service for smart cities is required to support a full set of secured identifier operations, including:

1) creating or registering a new identifier and associating a set of attributes to the identifier;
2) resolving or querying for the attributes associated to any registered identifier;
3) updating or modifying securely identifier attributes associated to an existing identifier;
4) deleting an identifier or removing any attributes associated to the identifier.

The identifier service should provide standard protocol interfaces to support any of these operations. Appropriate authentication and authorization mechanisms shall also be provided by the identifier service to promote the security of these operations.

7.5.2 Interoperability: Cohesive operation of identifier service under distributed environment

Each identifier service in the service hierarchy is required to work cohesively under a distributed environment. Upon receiving a service request, the identifier service receiving the request shall resolve it recursively or iteratively. In the recursive mode, the identifier service shall forward the service request to the responsible identifier service, obtain the response from the responsible identifier service, and return the result back to the client. Under the iterative mode, the identifier service shall return a reference to the responsible identifier service to the client, and direct the client to re-send its request to the responsible identifier service.

7.5.3 Security: Trust among identifier service hierarchy

Each identifier service under the distributed hierarchy is required to receive its service credentials from the higher-level identifier service in the hierarchy. The credential is recommended to be issued in terms of a signed public key, or some kind of public-key certificate. Such credential is necessary in providing service integrity under a distributed environment. It shall also be used as a means of service non-repudiation under certain conditions. A client interacting with any of the identifier services shall have the option to trace its service credential all the way to the root identifier service, in order to validate its authenticity. Caching of such validation is recommended to avoid unnecessary repeated operations provided that the cached validation will expire or somehow time out.

Bibliography

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

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

[b-ITU-T Y.2261] Recommendation ITU-T Y.2261 (2006), *PSTN/ISDN evolution to NGN*.

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

[b-ITU-T Y.4108] Recommendation ITU-T Y.4108/Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*.

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, 2017