International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4459

(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

Digital entity architecture framework for Internet of things interoperability

Recommendation ITU-T Y.4459

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.4459

Digital entity architecture framework for Internet of things interoperability

Summary

Recommendation ITU-T Y.4459 introduces a digital entity architecture and its prospective in addressing interoperability and security among Internet of things (IoT) applications.

This Recommendation defines an architecture framework for information-oriented services that makes use of existing infrastructures, including the Internet infrastructure, to enhance secure and managed information sharing over a distributed networking environment. It defines an architecture framework for information management based on the use of digital entities, and a common set of secure services that will help the registration, discovery, resolution and dissemination of such digital entities. The set of services is designed to facilitate sharing across any storage boundaries, any heterogeneous application boundaries and any organization boundaries.

A digital entity architecture defines a minimum set of needed architectural components and services to provide a generic information and service interoperability. It will facilitate the interoperability of identification, description, representation, access, storage and security of IoT devices. This architecture framework encourages a common security and management interface across different IoT applications.

Under a digital entity architecture, information represented in digital form is structured as digital entities, each of which has an associated unique persistent identifier. However, metadata contained in the digital entities (e.g., location of the object) could be updated without changing its identifier.

The identifier allows the digital entities to be identified and discovered, regardless of where they are located or stored. Digital entities are not confined within any particular application boundary and may be moved from host to host, accessed from application to application, shared from organization to organization, without losing its ownership or management control, in order to enhance interoperability. A digital entity's data model allows ownership and access control information to be defined by data owners independently of any specific applications.

This Recommendation can be used with different identification and addressing protocols (e.g., Internet protocol (IP) and/or non-IP based networks).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4459	2020-01-12	20	11.1002/1000/13861

Keywords

Digital entity architecture, Internet of things, interoperability, security.

---

* 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.4459

Digital entity architecture framework for Internet of things interoperability

1 Scope

The intent of this Recommendation is to describe digital entity architecture features and their capabilities to meet relevant requirements of the Internet of things (IoT) [ITU-T Y.2066], especially the security and interoperability issues in IoT applications. This digital entity architecture is consistent with [ITU-T X.1255] [1]. Other functional architectures may also be applicable for the IoT (e.g., [b-ITU-T Y.4500.1]).

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.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 address [b-ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.2 attribute [b-ITU-T X.1252]: Information bound to an entity that specifies a characteristic of the entity.

3.1.3 device [b-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.

3.1.4 digital entity [ITU-T X.1255]: An entity represented as, or converted to, a machine independent data structure consisting of one or more elements in digital form that can be parsed by different information systems; the structure helps to enable interoperability among diverse information systems in the Internet.

3.1.5 element [ITU-T X.1255]: Part of a digital entity consisting of a type-value pair, where the type is represented by a resolvable persistent identifier and the value is the relevant digital information for that type.

---

[1] [ITU-T X.1255], which is based on a digital object architecture, provides a framework for discovery of identity management information.

3.1.6 entity [b-ITU-T Y.2720]: Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.

3.1.7 federated registries [ITU-T X.1255]: A collection of interoperable registries that register metadata and participate in a common set of methods to share information reliably and in a commonly understood format.

3.1.8 identifier [ITU-T X.1255]: A sequence of bits used to obtain state information about the digital entity being identified; typically, this is done via an appropriate resolution system.

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

3.1.10 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.

3.1.11 metadata [ITU-T X.1255]: Structured information that pertains to the identity of users, systems, services, processes, resources, information or other entities.

3.1.12 persistent identifier [ITU-T X.1255]: A unique identifier that resolves to state information about a digital entity and that is resolvable for at least as long as the digital entity exists.

3.1.13 registry [ITU-T X.1255]: A mechanism for registering metadata about digital entities and storing metadata schemas, and which provides an ability to search the registry for persistent identifiers based on the use of the metadata schemas.

3.1.14 repository [ITU-T X.1255]: An interface that accepts deposits of digital entities, enables their retention, and provides secure access to the digital entities via their identifiers.

3.1.15 resolution system [ITU-T X.1255]: A system that accepts identifiers known to the system as input, and provides relevant state information about the entity being identified.

3.1.16 thing [b-ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.1.17 trust [b-ITU-T Y.2720]: A measure of reliance on the character, ability, strength or truth of someone or something.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

IdM Identity Management

IoT Internet of things

6LoWPAN IPv6 over Low -Power Wireless Personal Area Network

PKI Public Key Infrastructure

5 Conventions

None.

6 Digital entity architecture overview

This clause provides an overview of digital entity architecture, its purpose and motivation. Details of service components will also be described here, including how these components work together, and how they may be used to support interoperability of IoT applications.

6.1 General description

This open architecture framework allows secure and managed information sharing across heterogeneous information systems. This Recommendation defines the minimum set of needed architectural components and services that together, provide a generic information and service interoperability framework. Other functional architectures may also be applicable for the IoT (e.g., [b-ITU-T Y.4500.1]).

At the core of this architecture framework is the concept that any information represented in digital form may be structured as a digital entity and be assigned a globally unique identifier.

This identifier will resolve into state information about the digital entity that will persist in a resolution system independently of any changes made to the digital entity it resolves to. This state information may include location information, metadata, checksums, signatures, certificates, public keys, etc. These pieces of information associated with the digital entity are considered as the digital entity's attributes. A digital entity is used to represent IoT entities, e.g., over the transmission control protocol (TCP)/Internet protocol (IP) network, regardless of its underlying implementation.

NOTE – A digital entity is sometimes referred to as a digital object. The essential fixed attribute of a digital entity is its associated unique persistent identifier, which can be resolved to current state information about the digital entity, including its location(s), access controls, and validation, by submitting a resolution request to the resolution system. Examples of other intrinsic digital entity element attributes are date last modified, date created and size.

IoT devices communicating with different protocols can be made accessible over private and public networks or the Internet using protocols including TCP/IP.

The architecture framework can be used with different identification and addressing protocols (e.g., IP and/or non-IP based network protocols). The architecture allows any digital information, structured as a digital entity, to be securely identified, discovered and disseminated independently from any specific systems, services, or applications where the information may be created or stored.

The architecture framework consists of three basic and fundamental components that when implemented, yield the following services: a global identifier service, a repository service and a registry service.

The global identifier service allows a globally unique identifier to be assigned to any digital entity. The identifier service provides a resolution and administration protocol that is used to resolve an identifier into the state information associated with the digital entity, such as storage location and provenance information, may be retrieved and managed in a secure fashion. The identifier service shall be a distributed service with built-in security such as service integrity, service non-repudiation, data integrity, data authentication, data confidentiality and discretionary access control on any identifier's associated state information.

The set of distributed repository services facilitates the secure storage, access and dissemination of digital entities based on the use of their identifiers. A repository is in itself a digital entity which may or may not contain other digital entities.

A digital entity can perform a list of operations including accessing other digital entities, creating new digital entities, etc. The repository could represent a set of IoT devices, which are digital entities.

A digital entity may have many attributes associated with the object. It may have attributes that describe the nature of the IoT device. It may also have actionable attributes that refer to computer programs that can interact with the IoT device, such as turning on and off the device, or get the temperature reading of the device. In addition to these, the digital entity may also have attributes that define who may have access to its attributes and who may make interactions to the IoT devices via the device interface described in these attributes.

A digital entity can be constructed and used as a digital representation of a physical IoT device. The system components, specifically the registry, have the capability to make such entities discoverable and accessible. IoT interoperability requires application programming interfaces (APIs) so that digital entities may interact with their devices. Digital entity registries allow devices and applications using different protocols to query the metadata contained in the digital entities and to get relevant information that would enable them to achieve interoperability through appropriate APIs.

This approach could be used to leverage specific access controls of convenience for each repository. On the other hand, a repository could be a digital entity that provides access to the data generated by a single IoT device. This architecture framework does not limit the number of repositories.

A set of federated registry services allows discovery of any digital entity. The digital entity registry can provide search operations. This information could be any metadata or data within the digital entity. The federated registry service can be used to discover a digital entity across: 1) different types of digital entity metadata entries across different registry services; 2) different levels of network connectivity across different registry services; 3) different sorts of data and information management services; and 4) different types of security and access control. Policies for trust management, including authentication and authorization of client requests, shall be clearly defined and managed among the set of federated registry services.

Under the architecture framework, each service component, the identifier service, the registry service and the repository service shall have the security service built-in to protect service integrity, data confidentiality as well as service non-repudiation. Trust and trust management among different service components be established prior to any service exchange.

By making use of structuring digital entities, the set of architecture services allows to maintain information about the current location of digital entities such that digital information can be identified, discovered and disseminated in a way that is transparent to the users and be independent of specific storage or other technologies that assemble or generate the digital information. In other words, the architecture framework defines a set of services that facilitates the secure management of information by eliminating many of the technological variability that makes information inaccessible over time.

Figure 1 and Figure 2 are provided to clarify the process for digital entity creation and attributes assignment representing the architecture components. They also show how the architecture could be used to support interoperability.

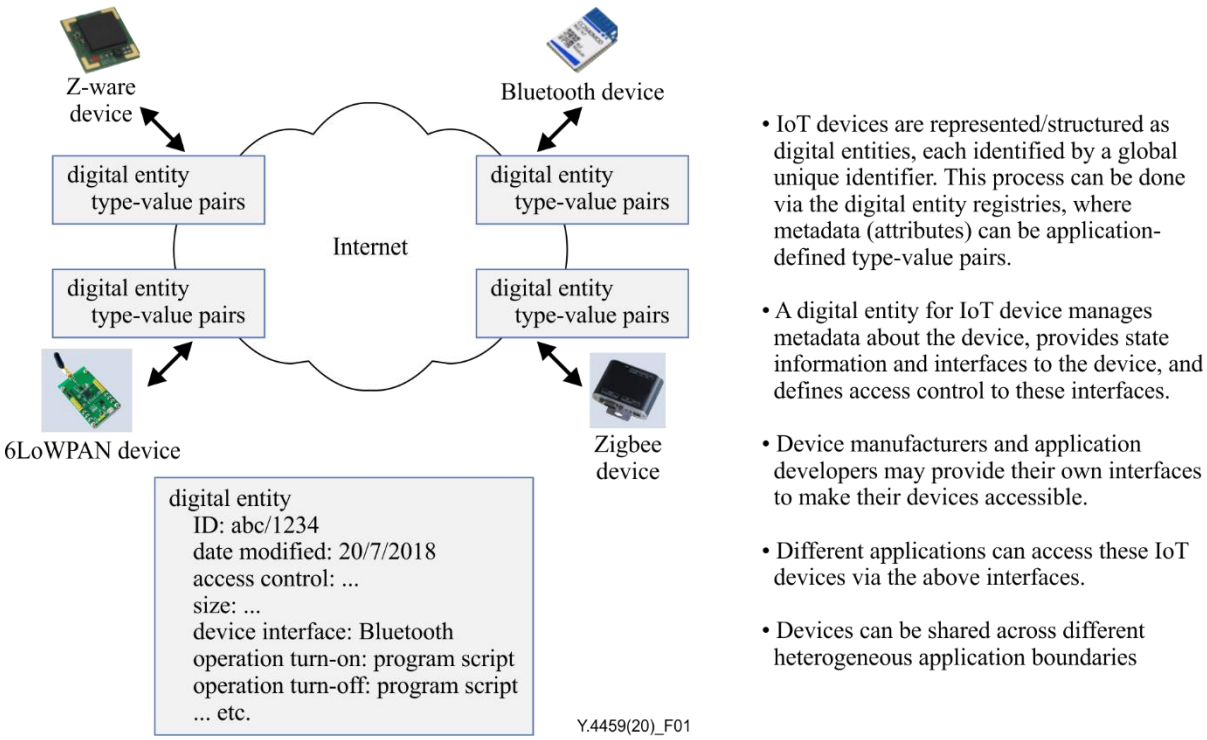

Figure 1 – Process for digital entity creation and attributes assignment

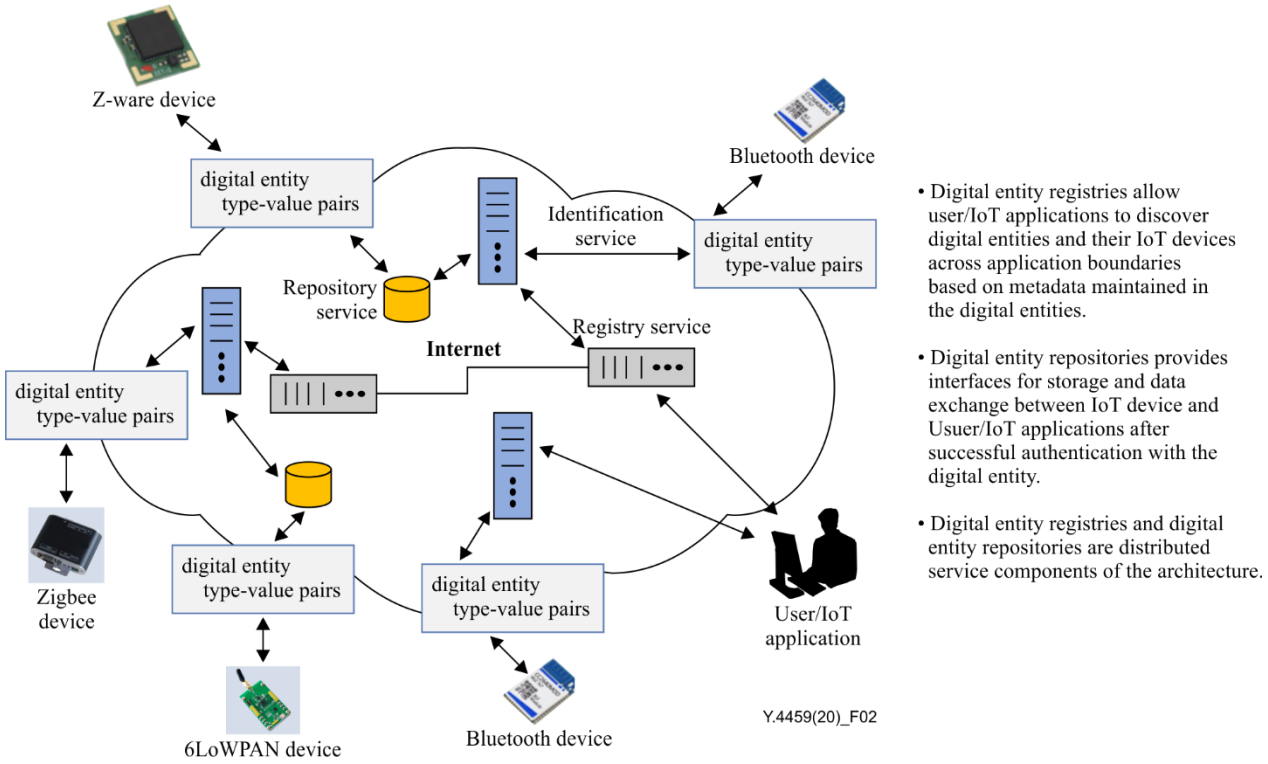

Figure 2 – Architecture representation and components

6.2 Interoperability aspects for IoT applications

A range of IoT interoperability products, approaches, and initiatives exist or are under development. Examples include those that rely on common service layer and common service entity implementations, service-oriented architectures or the domain name system. Other work on IoT interoperability is also ongoing in other standardization developing organizations and consortia.

There are different types of interoperability, including:

1) technical interoperability, which is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate;

2) syntactical interoperability, which is usually associated with data formats. The messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables;

3) semantic interoperability, which is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding of the meaning of the content (information) being exchanged.

Most of these approaches concentrate on defining a set of common interface among different applications. The architecture defines a common set of services that allows information to be encapsulated, registered and discovered regardless of the application boundaries, thus allow the information sharing across different application boundaries. The architecture framework may be integrated with any of the above approaches (e.g., common service layer, service-oriented architecture) and to promote information sharing across different applications.

A digital entity may have many attributes. It may have attributes that describe the nature of the IoT device. It may also have actionable attributes that refers to computer programs that can interact with the IoT device, such as turn on and off the device, or get the temperature reading of the device. Besides all these, the digital entity may also have attributes that define who may have access to its attributes, and who may make interactions to the IoT devices via the device interface described in these attributes.

A digital entity may be considered as the surrogate of an IoT device, regardless of its underlying implementation. Information about primitive IoT devices can be made accessible over the Internet. The physical IoT devices themselves can also be accessed.

This Recommendation defines a minimum set of needed architectural components, and services to provide a generic information and service interoperability. This architecture framework is technology neutral, light-weight in its requirements, and can easily be grafted onto existing technologies to maximize its adoption. It will facilitate the interoperability of identification, description, representation, access, storage and security of IoT devices.

This section presents core aspects of the architecture and its components to facilitate IoT interoperability in the following core aspects:

6.2.1 IoT device identification and resolution

Identification service including resolution is core requirement of IoT systems and a core principle of the architecture. The architecture however has a more specific requirement for its identifiers and that is every identifier needs to be resolvable into state information value about the digital entity it identifies, or in this case the IoT device it identifies. Access controls can be used to restrict resolution access to some of those values.

The results from the resolution should be in the form of type-value pairs for simplicity of adoption. Each type by itself has a unique identifier that can globally be resolvable identifier into a description of its uses, formats, encodings, etc., to promote their global reusability and value processing.

The system identification service described in general terms in this Recommendation can support implementation of certain security capabilities such as public key infrastructure (PKI) to allow data encryption and non-repudiation of all servers within the resolution service that were used for each resolution, integrity validation of all state information values and capability to enforce access restrictions to some of the values within the state information. The architecture can intrinsically

accommodate and implement PKI so it can generate its own keys and certificates. The architecture also has the capability to support third-party certificates.

In the data structure, a digital entity can represent a file, a service, a database or a device or any combination thereof.

It is possible to create relationships between different digital entities or define a digital entity with complex typed operations. These two approaches provide a flexible yet powerful way to manage complex information.

The following list describes some of the characteristics of the identification system that can be of use to the IoT.

– the ability to be integrated with any other existing identification systems currently used by IoT manufacturers to provide an overarching interoperability of identifier resolution;

– the verification of existence and uniqueness. A registry and a resolution system are required to verify that a particular identifier exists and is in effect unique. This is a critical function that enables any new IoT device identifiers to be proven globally unique;

– tan identification service structured to provide intrinsic non-repudiation functionality that can verify the source of the specific resolution service. It is of a critical importance that there is a mechanism that enables accessor services or clients to authenticate the IoT device with which they are interacting;

– non-repudiation, typically consisting of values signed by object, via the key of the object, on behalf of the IoT device;

– the ability to accommodate encryption. An IoT device may need to provide some level of encryption to mitigate associated risks such as man in the middle attack;

– access control. IoT devices may need to provide an access control capability to control what entities that can access information about the device or the device itself;

– a means to associate state information with each digital entity/IoT device identifier. This state information would be returned following a resolution request as a set of type-value pairs. The type would be itself an identifier that would resolve into a set of descriptions of the type. This flexibility would enable IoT industries to use their own type system for describing their IoT devices and enable the rest of the IoT community to acquire the information needed to process the specific type-value.

  Examples of types and/or attributes include:

  • an IoT device type;

  • a description of the IoT device. This could be at human level but could also provide machine description;

  • state information. State information includes information about the state of the IoT device (e.g., where it is, what its status is);

  • interface specifications. Each IoT device provides an identifier that uniquely specifies the interface used to interact with other IoT devices and systems. For example, such interface specification provides the underlying physical interface used for communication;

  • access to service interface(s). Each network accessible IoT device may provide a reference to their service interface(s). For some, this could be a uniform resource identifier (URI), while for others, a simple IP address; there could be others as well. A given IoT device could have different service interfaces.

  • linking to IoT device archive storage. Many IoT devices will be generating data throughout their operational life. The architecture could link to the data storage location.

6.2.2 Access to IoT devices

To be accessible, IoT devices need to provide a standard interface for reading and writing data, setting their parameters and issuing device specific operations that will vary from one IoT device to another.

Through the fundamental components of a global identifier service, a repository service and a registry service, the architecture could provide access to an IoT device. This could be done through any standard light-weight protocol that makes use of the notion of globally resolvable types to specify its operations. As a result, any data or service can be directly accessed using its specific type of operation or access request. More importantly, this type of access request can be discovered and its functionality understood by any client interacting with the architecture.

A set of simple yet typed based operations are intended to enable support all types of devices. Some of the advantages of such approach are that:

– the architecture allows a flexible digital entity data model that can provide a basic but customizable and extensible approach to providing access to any IoT device's data;

– the architecture supports access to IoT devices using any protocol that enables any IoT device specific operations to be performed. For example, an IoT device may enable a specific operation for specifying calibration settings, configuring the device or populating its own internal database(s). The manufacturer can specify such operation by creating a new digital entity to represent information about the device with its own unique identifier and with the associated operation description in the state information. When the client queries the IoT device using the generic protocol for the list of operations it can perform, the IoT device will return that manufacturers specific operation type. Using the typing system, which is an intrinsic part of the architecture, the client would be able to determine what the operations are and whether they are useful operations for it to request. This intrinsic extensibility of the protocol can be used by any and all IoT device manufacturers to develop new operations while still remaining interoperable. Such protocol can be defined to intrinsically support many different types of access control practices.

6.2.3 Architecture data structures for IoT data archiving

Some IoT devices will generate data but will not necessarily have local storage capabilities. In such cases, the architecture could be used to create an archiving service to provide persistent access to these digital entities' data for as long as desired. The architecture provides many solutions for addressing this sort of requirement. It can use a combination of identifier linking, where an IoT identifier could resolve to state information about the IoT device such as providing the identifier for its archive digital entity for instance, or could specify a standard archive operation within digital entity's types/attributes to provide simple client access.

In general, the architecture could be used to provide the following solutions to IoT data archiving:

– enabling a simple type-based repository model to support interoperable deposit of and access to data generated by any IoT devices represented as digital entities;

– specification of metadata about when, where and how the IoT data can be acquired;

– specification of metadata about the type(s) of data acquired;

– specification of specific access controls over the archival data.

6.2.4 Search and discovery of digital entities representing IoT devices

Searching and discovery of digital entities is a key functionality of the architecture. Likewise, the ability to search and discover digital entities representing IoT devices and/or their data archiving is important in increasing their value of usefulness. This is the role of registries that contain metadata about digital entities and have the ability to collaborate with other registries to facilitate searches among them.

The architecture access control and security mechanism at their digital entity level and reflected at the level of the registry should be configured to provide the needed security to make sure that each digital entity, and therefore the IoT device, can control access to their data.

The specific modality of search and discovery of IoT devices will be very specific to the manufacturer, sellers and clients that will be using these IoT devices with the goal of maximizing their usefulness and value but the architecture will enable many different sorts of searches and discoveries. Some search possibilities include:

– discovery of IoT devices types. The search in this case could be for instance a temperature sensor type IoT device;
– IoT devices interface and operations;
– IoT device by location;
– IoT device by type of data generated. For example, a client could want to interact with IoT devices that possess a certain type of data;
– IoT device by owner;
– by the value of a specific type of data that IoT devices generate. For example, the client may want to find out about all IoT devices that are reporting a specific value range for a particular type of data.

7 Security services for IoT applications

This clause describes how the architecture could assist in overcoming challenges related to IoT security.

7.1 Observations on IoT security

In IoT applications, most smart devices concentrate on providing communication capabilities without much thought about security protections. Interfaces to smart devices generally allows status monitoring and basic device-control operations. Because of factor limitations or power consumption concerns, the majority of such devices do not provide any advanced security capacities beyond simple pairing and/or simple user login. Such devices do not provide management interfaces for role-based or group-based access control. Once connected or paired, smart devices generally grant total control to the connected party.

Lack of security protections at the device level poses risks related to data sharing between different IoT applications. Console-based hubs can overcome such limitations by acting as a control centre for connected smart devices within a local domain. However, interfaces to hub devices differ from vendor to vendor, with each vendor providing different levels of security protections that may be in some cases primitive or limited in nature.

IoT applications working with such devices require security protections to be developed in each application. Most IoT applications apply access boundaries with their own sets of user authentication/authorization mechanisms. IoT devices and service operations are strictly confined within the application boundary accessible only to users registered with the IoT application.

The choice of security protections in IoT applications vary from vendor to vendor unless standardized security mechanisms are used. Many IoT applications concentrate on providing user-friendly functionality and place limited emphasis on security protections. For example, many IoT applications use authentication schemes that may be subjected to man-in-the middle attacks or replay-attacks, making information associated with the user account vulnerable to cyber-attack.

Security attacks upon one IoT applications can also spread across different IoT applications. Users of different IoT applications likely share their authentication credentials (e.g., password) across these applications. A security breach in one IoT application may make other IoT applications vulnerable.

Application based security protection in IoT can enable many Internet intrusion attacks. Any time an IoT application is compromised, the attacker may gain unauthorized control to all devices connected with that IoT application and obtain access to its registered user information.

Figure 3 provides typical IoT application-level security, where security protection is implemented per application. Any time an application is intruded, all devices under the application protection become vulnerable.

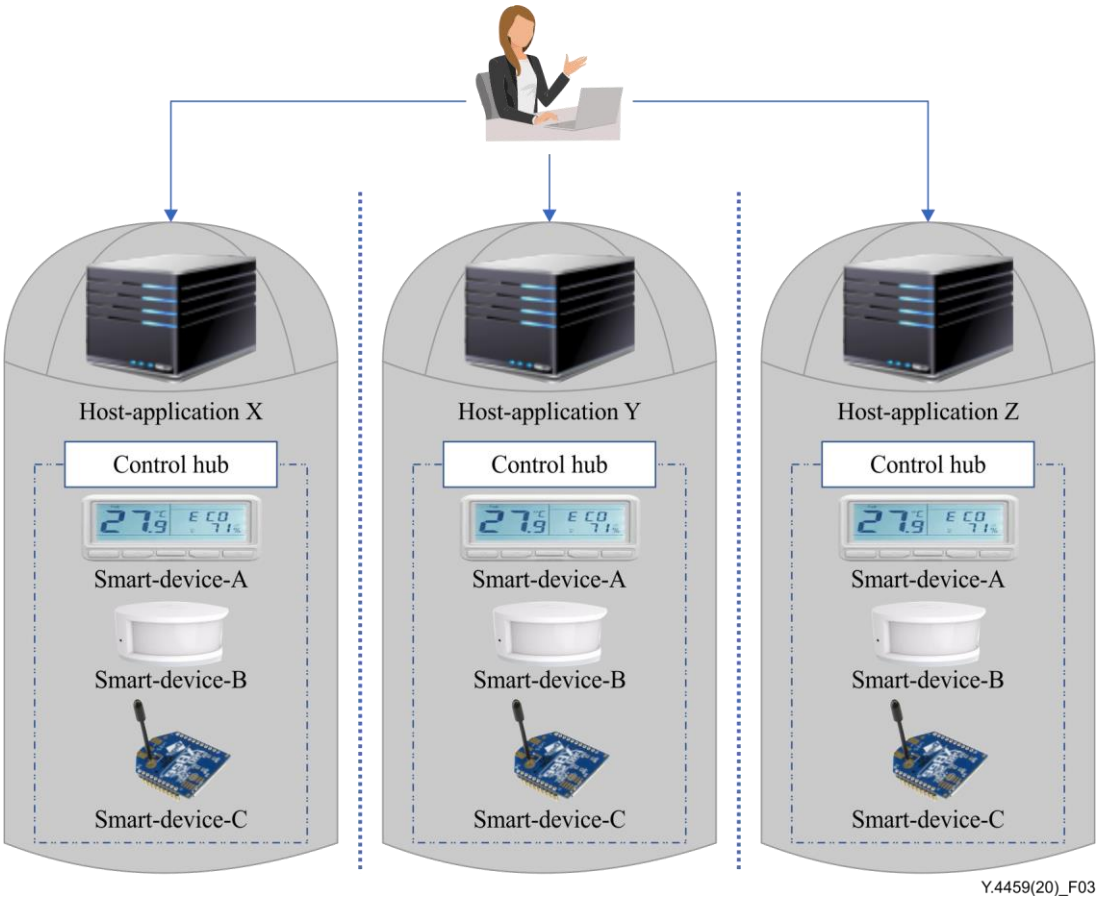

Figure 3 – Typical IoT application-level security implemented per application

An intrusion into one IoT application will not only defeat the protection on IoT devices that are accessible by that application but may also expose privacy information for its entire user community. Such information may further facilitate the attacker to intrude into other IoT applications that have overlaps in their user communities.

7.2 Architecture for IoT security

The set of services in the architecture framework is not limited to any specific security implementation or algorithms. Rather, security service implementations and algorithms may be integrated into a service, if appropriate, as they become available. For example, the exact type of security implementation and/or algorithm can be given a global unique identifier. Such an identifier is exchanged during the client-server service initiation protocol. This allows better security implementation and/or algorithms to be deployed dynamically as they become available. It also allows customized security implementation per individual application security requirement without sacrificing the possibility for future interoperability.

[ITU-T X.1255] defines a common framework that allows information in digital form to be structured as digital entity along with a global persistent identifier that can be used as the unique reference to the digital entity. The architecture is consistent with [ITU-T X.1255], which states that:

1) "The resolution system should be a distributed, secure, high-performance resolution system designed to enable persistent reference to digital entities over long periods of time and over changes in location, access methods, ownership and other mutable attributes."

2) "Enabling the discovery of identity management information is a primary objective of the open architecture set forth in this Recommendation; however, the determination of trust is left to the user to determine. Additional functionality or services can be supported within the architecture in the form of optional components/modules (software and/or hardware). In this sense, the architecture could include a trust framework as an optional capability, as well as enhance/enrich a discovery response with trust information or even support a trust determination. External entities would have the ability to determine whether they want to receive this trust information directly. They could choose to deactivate the feature and seek to collect trust information on their own or even from their own sources to make a trust determination."

3) "A given repository can contribute metadata for the same entities to multiple registries, and a given registry can accept metadata from multiple repositories. Collecting metadata from multiple repositories into a single registry enables the federation of these repositories. Allowing these repositories to contribute metadata about the same entities to multiple registries enables a single repository to be part of multiple federations, distinguished perhaps by serving different communities, using different metadata schemas, different approaches to indexing and searching, and other capabilities."

Because it is consistent with the [ITU-T X.1255], the architecture can be implemented in a way that supports secure and trusted information discovery, resolution and dissemination over the Internet. Security and trust management are an integral part of such services. This will help address the security issues in IoT applications in the following aspects.

The architecture features which support security include the following:

– access control. Each digital entity can have its own type-based access control. That can be used to restrict read, write access as well as the ability to perform any of the other operations that the digital entity may have;

– non-repudiation. With the implementation of an encryption mechanism consistent with this recommendation, each digital entity repository and registry has the capability to sign their service response with their respective private key to enable the client to verify the source of the information. PKI services using the architecture could be configured to generate certificates within the system with no third-party involvement. It also has the capability to support third-party certificates. This would allow a device or group of devices would be able to sign their information enabling clients to have a higher level of trust in the authenticity of the information originating from the IoT device;

– confidentiality. The repository service should support encryption over all of its service exchanges. Although not all IoT devices may want to have encrypted sessions, the ability to support encryption would be one of the benefits of using the architecture services.

7.2.1 Discretionary ownership and security management

The architecture allows structuring of any smart-device into a digital entity. Each digital entity would have a global and unique identifier that makes it discoverable and accessible to any IoT applications. It can also include data specifying the ownership and access control of the device. The architecture framework can be implemented and configured in a way that uses the ownership definition to control management and administration of the device. The access control information allows IoT applications to safeguard the device from unauthorized access and/or unwanted exposure. Ownership and management of IoT devices should be defined and administrated separately from IoT applications. Intrusion into any IoT application would then not be equivalent to losing control of the IoT devices, making IoT applications a much less vulnerable target.

Each user of any IoT applications may also be structured as a digital entity. Authentication and user privacy information would no longer be managed by the IoT application, but by the individual who have ownership of the user account. IoT applications could thus delegate security protection to their user community. The IoT application itself would not need and would not have access to authentication or privacy information of each individual user. Intrusion into any individual user account, due to improper security practice of the individual user, would not spread the harm to the entire user community.

Figure 4 shows the architecture-based IoT application security, where individual devices are structured as digital entities, with discretionary ownership and security protection defined, independent from the hosting application.

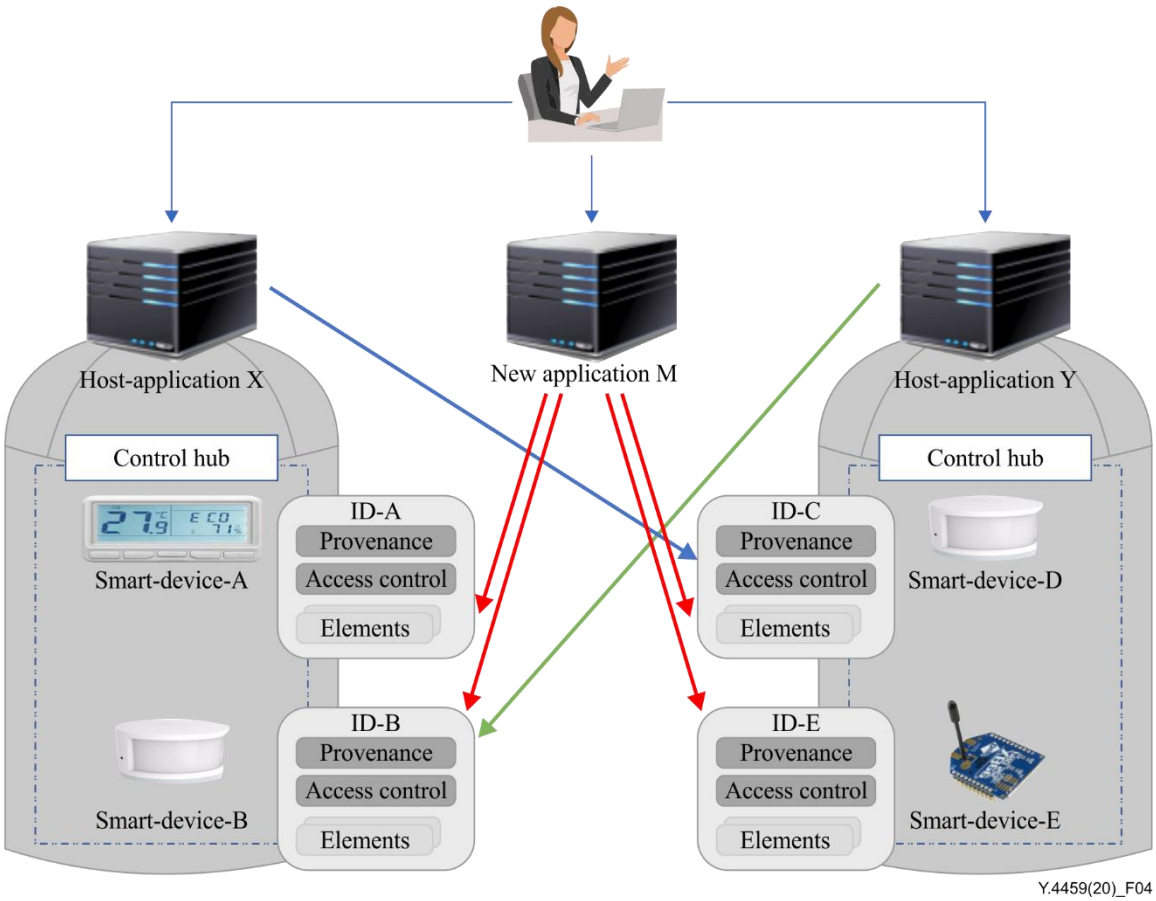

Figure 4 – Architecture-based IoT application security at device level independent from hosting application

Structuring of individual smart devices and individual user information into Digital entities with discretionary ownership and access control would not require IoT applications to protect the device and any of its user information, but concentrate on providing better application service.

7.2.2 Separation of authentication from authorization

The architecture provides an identifier service that can be used not only to identify information structured as a digital entity, but also to designate a principal or service requestor interacting with the service (e.g., a repository service). The identifier service describes how trust and trust management may be incorporated between any principal or other service components, consistent with [ITU-T X.1255]. Additionally, the architecture identifier service should be configured to provide secure and trusted resolution and management of identifier and identifier attributes over the various interfaces and network protocols including public Internet. The architecture secure identifier service would allow IoT applications to separate their authentication service from authorization service. User

authentication, which is a process typically achieved by validating the binding between an identifier (e.g., user-id) to an attribute (e.g., an authentication key), should be implemented so that it is delegated to a trusted third-party identifier service provider whose business is to protect the authentication keys for its registered users.

The separation of authentication from authorization will relieve individual IoT applications from the task of maintaining the user account information and the concern about the consequences in user account information being compromised. It also allows the application to concentrate more on its authorization policies, and application features that will better serve the information for its clients.

7.2.3 Common baseline security infrastructure

All implementations of the architecture for IoT management should implement a baseline of security protections for IoT applications as outlined in this recommendation. This can allow for better security practices across different IoT applications by mitigating the impact of any security compromise in one application from affecting any others. This should not interfere with IoT application-specific security mechanisms.

8 Architecture overarching model for a general IoT interoperability framework

This clause describes how the architecture could assist in overcoming challenges related to IoT interoperability.

8.1 Observations on IoT interoperability

Current IoT systems integrate a variety of elements including but not limited to: devices incorporating embedded network computers, data and application gateways and cloud-based information management and processing systems. Many IoT applications are developed within distinct vertical domains with different requirements and priorities such as home entertainment, building automation, and industrial systems, each incorporating a variety of alternative protocols and APIs. As a consequence, the vast majority of the current generation of IoT systems are developed using proprietary and vertically integrated approaches for all aspects of system architecture from the end device, to cloud based services which are tightly integrated. This design model may not anticipate direct interoperability between different categories of IoT devices. For example, IoT devices installed as part of a building automation system would not typically interoperate with home monitoring devices obtained from the secondary market and installed by the end occupier.

As a result, distinct IoT applications, as illustrated in Figure 3 for example, are frequently structured as information silos and thus are either unable to share resources at all levels of the systems architecture or reliant on existing interoperability platforms to do so.

Devices deployed as part of different IoT applications may be unable to identify each other and thus not able to interact directly. Such devices are designed to operate only within a specific application domain using closed or proprietary software, identifier systems and communication protocols and would be typically associated with a specific data processing back-end. For example, kitchen appliances procured from different manufacturers may be unable to recognise and communicate with environmental monitoring devices coexisting in the same property and serving the same end user.

Similarly, users can be affected by a lack of interoperability between different IoT platforms which requires a specific and often proprietary service discovery, service management and monitoring interfaces. Users are thus required to maintain multiple authentication accounts to access each individual platform despite the fact that they serve the same purpose. For example, the same person would be required to operate multiple remote controls to operate access to buildings such as garage gates in different properties rather than be able to employ a common way to identify their authority to access these locations.

IoT systems can create isolated data silos. For example, wearable devices may store information in repositories that other relevant IoT devices could access perhaps using different APIs. Yet, environmental monitoring devices may be combined to create integrated systems based on the use of digital entities in order to reveal useful patterns that can improve the well-being of those in that environment.

8.2 Architecture for IoT interoperability

The architecture can help to act as a base architecture in addressing interoperability aspects in IoT implementations discussed in previous section. Entities in each IoT applications, including smart devices, applications services and application users registered with the IoT application can be structured into digital entities. Each digital entity would have a globally unique identifier, which can be associated with the set of attributes describing the underlying entity.

For example, a smart device used in an IoT application could be given a global identifier with attributes that define its ownership, access control and various service interfaces to communicate with the device.

The global identifier would allow the device to be discovered and accessed not only by its original IoT application, but by other applications that wish to interact with the device. Ownership and access control defined within the digital entity could allow secure access to the device across different IoT applications without losing necessary security protection. That interface to interact with the device could be discovered on-the-fly without being confined within the original application.

Similarly, information about a user-entity registered with any IoT application could be structured as a digital entity as well and assigned a global unique identifier. User information could thus be applied across different IoT applications in user authentication and service authorization. Shared user identity reference across different IoT applications would not only make it easier for the user to exchange information from one IoT application to another, but also would also allow better sharing of information across IoT application boundaries.

Additionally, an application service implemented by an individual IoT application could also be structured as a digital entity and would make itself available to other IoT applications. For the application service, the digital entity would have a global unique identifier that could be used to make reference to the service. It would also have a set of attributes that fully describe the application service, including its administration and service interface, as well as security protections (e.g., access control) over its operation.

Application services represented as digital entities could facilitate service exchange and integration among different IoT applications. New IoT applications could thus be developed by integrating different application services from different existing applications. Such integration would encourage better information sharing across different IoT applications. When implemented consistently with this recommendation, each IoT application could retain its existing practice while making its service data and resources available under a public yet secure service interface, defined and managed by individual application itself.

The set of services, which the architecture can support, allows smart devices, user entities and application services to be represented as digital entities so that they can be discovered, shared or accessed securely across different IoT applications. This helps in freeing information entities from their hosting boundaries, application boundaries and organization boundaries, and could be a step in enabling interoperability among IoT applications.

The open architecture and framework described in [ITU-T X.1255], regardless of any specific implementation, would allow interoperability among heterogeneous applications without the need for each individual application to relinquish its control of its information domain.

Individual repository service providers may deploy configuration and policies to determine what entities can exercise control of the repository in order to provide added security protection.

The architecture identifier service can be used to define what information can be shared, with whom the information may be shared, and how the information will be shared. Interoperable applications can be developed by interacting with each individual application, and provide interoperability integrated service based on real-time data feed from individual applications.

Appendix I

Other bibliographic documents

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

Reading the following document is not necessary to understand or implement this Recommendation.

Managing Access to Digital Information, Cross-Industry Working Team, May 1997, http://www.xiwt.org/documents/ManagAccess-1.pdf

Bibliography

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

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

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

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

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