International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4111/Y.2076

(02/2016)

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

Next Generation Networks – Frameworks and functional architecture models

Semantics based requirements and framework of the Internet of things

Recommendation ITU-T Y.4111/Y.2076

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND 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

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4111/Y.2076

Semantics based requirements and framework of the Internet of things

Summary

Recommendation ITU-T Y.4111/Y.2076 specifies the semantics based requirements and framework of the Internet of things (IoT) as a basis for further IoT semantics based standardization work, including semantic aspects for IoT services in different business domains, semantically enhanced IoT capabilities and others.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4111/Y.2076	2016-02-13	13	11.1002/1000/12705

Keywords

Internet of things, semantics based capability framework, semantics based requirements.

* 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/.

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Y.4111/Y.2076

Semantics based requirements and framework of the Internet of things

1 Scope

This Recommendation specifies the semantics based requirements and framework of the Internet of things (IoT).

Taking into consideration the IoT reference model [ITU-T Y.4000] and building on the common requirements of IoT [ITU-T Y.4100], semantics based requirements are specified, including those related to the four layers (application, service support and application support (SSAS), network, and device layer) and the management and security capabilities of the IoT reference model, as well as semantics based requirements across layers.

Based on the identified IoT semantics based requirements and existing semantic technologies, the semantics based capability framework of the IoT is specified.

The scope of this Recommendation includes:

– introduction to semantic technologies for the IoT;

– semantics based use cases for IoT actors;

– semantics based requirements of the IoT;

– semantics based capability framework of the IoT.

Appendix I provides IoT applications scenarios highlighting the value of semantic technologies in the IoT.

2 References

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

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

[ITU-T Y.4100] Recommendation ITU-T Y.4100/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 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

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

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

3.1.2 ontology [b-ITU-T X.1570]: An explicit specification of a conceptualization.

3.1.3 thing [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), that is capable of being identified and integrated into communication networks.

3.1.4 semantics [b-ITU-T Z.341]: The rules and conventions governing the interpretation and assignment of meaning to constructions in a language.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 data model: A representation structure for data that can organize data as elements in the structure and standardize the meaning of data elements and their relationships.

NOTE – Data models usually use vocabularies to describe their data elements and data elements' relationships. A semantic data model uses vocabularies complying with ontologies. For more information, refer to http://www.w3.org/standards/semanticweb/.

3.2.2 data set: A collection of data that conforms to a particular data model.

NOTE – A semantic data set conforms to a semantic data model (it can be a collection of native semantic data or a collection of semantically annotated data). For more information, refer to http://www.w3.org/standards/semanticweb/.

3.2.3 IoT ontology: An ontology for the IoT that includes the union of ontologies for the different components of the IoT, including the relationships between these ontologies.

NOTE 1 – An important part of the IoT ontology concerns the ontologies for IoT devices and things.

NOTE 2 – The development of the IoT ontology is an evolving process that is expected to take into account new concepts as far as needed along its development.

3.2.4 query: Technology that can programmatically retrieve information from data sets.

NOTE – A semantic query uses semantic technologies to retrieve information from semantic data sets. For more information, refer to http://www.w3.org/standards/semanticweb/ .

3.2.5 semantic description language: Language used to formally model and describe ontologies. For more information, refer to http://www.w3.org/standards/semanticweb/.

3.2.6 vocabulary: The set of terms defined, classified and used to describe concepts and relationships of a particular area of concern.

NOTE – The word "ontology" is used for a more complex and quite formal collection of terms, whereas "vocabulary" is used when such strict formalism is not necessary. For more information, refer to http://www.w3.org/standards/semanticweb/.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AL Application Layer

DL Device Layer

DM Device Management

IoT Internet of Things

NL Network Layer

OWL Web Ontology Language

RDF Resource Description Framework

RIF Rule Interchange Format

SMS Semantic Management Support

SMSC Semantic Management Support Capabilities

SPARQL SPARQL Protocol and RDF Query Language

SSAS Service Support and Application Support

SSASL Service Support and Application Support Layer

SSSC Semantic Security Support Capabilities

UML Unified Modelling Language

XACML Extensible Access Control Markup Language

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 needs not be present to claim conformance.

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

6 Introduction to semantic technologies for the IoT

Due to the growing number of interconnected things and related communication connections, as well as the variety of IoT devices and related connectivity, the volume and types of data generated by the things as well as the number and type of services provided by the IoT infrastructure are increasing more and more quickly. As a result of these phenomena, requirements for automatic operations, consistency, interoperability and reusability of the IoT infrastructure are becoming more and more urgent.

Semantic technologies (i.e., technologies based on semantics) are promising candidates to meet the foresaid requirements for the IoT infrastructure. Semantic technologies for IoT enable the efficient description of data (e.g., collected data and virtual representation of physical things) and services, so that machines and humans can have a common understanding of the exchanged data and processed services in the IoT infrastructure in order to benefit automatic operations, analysis and processing activities. In addition, semantic technologies can enhance representation, annotation, discovery, analytics, interoperability, reusability and composability of data and services.

The semantic technologies are applicable to the different layers of the IoT reference model [ITU-T Y.4000]. For example: in the application layer (AL), semantic technologies can help to provide users with a smart human-machine interface; in the service support and application support layer (SSASL), semantic technologies can help capabilities and resources deployed in distributed nodes (e.g., devices, gateways, servers) to be discovered and interoperated in an automatic way; in the network layer (NL), semantic technologies can simplify and help to automate network configuration; in the device layer (DL), semantic technologies can help the IoT infrastructure to understand different device properties such as computation and storage capacity and sensor types, etc.

Concerning security capabilities of the IoT reference model, semantic technologies can benefit the security related decision making (e.g., based on semantic technologies, resources access rights can be deduced). Furthermore, semantic technologies can enhance the conventional description of security policies, thus helping the security negotiation process between different IoT components (e.g., device, IoT application server, platform and network).

Concerning management capabilities of the IoT reference model, semantic technologies can facilitate the understanding of service logging reports by both machines and humans and also facilitate automatic configuration of IoT components.

In summary, semantic technologies reveal outstanding features for applicability to the IoT, including, but not limited to, the following:

- consistency: Through semantic technologies, data and services can refer to the same meaning across time, location and IoT components;
- scalability: Through semantic technologies, data and services can be managed locally to IoT components (e.g., semantic annotation can help local interpretation of data reducing the need to involve other IoT components). This increases the IoT technical component independence (components become loosely coupled) and decentralizes the management, leading to enhanced scalability. Moreover, the service reachability can be more easily expanded to reach more users and the functional evolution of services can be rationalized;
- re-usability: Through semantic technologies, data and services can be reused and composed to construct new data and services;
- analytics and actionable knowledge: Through semantic technologies, merging, correlation and analysis of diverse data generated by the IoT, together with data from external sources such as social media, events and news, can be facilitated in order to produce actionable knowledge;
- interoperability: Based on semantic technologies, the interoperability level [b-SI] of data and services of the IoT within one application domain and/or among different application domains can be improved;
- human-machine interaction: On one hand, since semantic technologies are based on natural human concepts, data and services become easier for humans to understand. On the other hand, since semantic technologies are formal ways to express concepts, data and services can also be understood by machines. This can improve the interaction between humans and the IoT.

7 Semantics based use cases for IoT actors

The IoT actors considered in these use cases are from those defined in [ITU-T Y.4100].

Actors and use case diagrams are modelled in unified modelling language (UML) [b-UML].

In Figure 7-1, some semantics based use cases for IoT actors are identified.

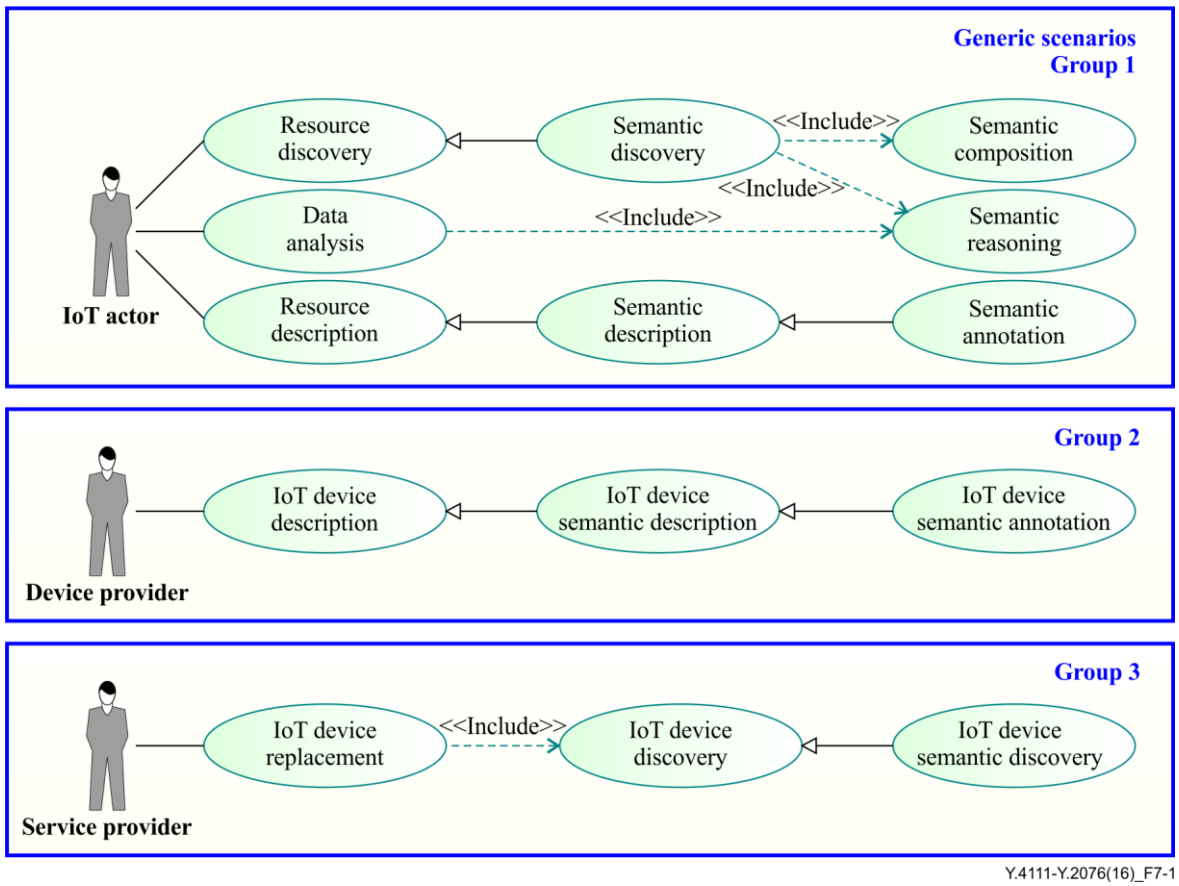


Figure 7-1 – Semantics based use cases for IoT actors

These groups of use cases shown in Figure 7-1 describe a non-exhaustive set of scenarios from which corresponding requirements can be derived.

The first group of use cases (Group 1) deals with generic scenarios where semantics is used by IoT actors, including for resource description, resource discovery and data analysis.

The second group of use cases (Group 2) deals with the description of IoT devices by the "device provider" actor that uses the semantic description of IoT devices.

The third group of use cases (Group 3) deals with the replacement of an IoT device. A "service provider" actor semantically discovers new IoT devices that have replaced original IoT devices.

8 Semantics based requirements of the IoT

8.1 General semantics based requirements for IoT

NOTE – Appendix I describes some IoT application scenarios using semantic technologies which address requirements identified in this clause.

8.1.1 IoT ontology

As defined in clause 3, the IoT ontology is an ontology for the IoT that includes the union of ontologies for the different components of the IoT, including the relationships between these ontologies.

IoT ontology is required to be the foundation of the IoT for semantic annotation, semantic interoperability, semantic discovery, semantic reasoning and semantic composition so that consistent meanings and relationships can be setup across different IoT components.

Existing ontologies related to the IoT such as for example semantic sensor network ontology [b-SSNO], are recommended to be integrated into a complete IoT ontology ecosystem, which covers all the components of the IoT.

NOTE – How to expand and reuse existing ontologies related to the IoT in the IoT ecosystem is outside of the scope of this Recommendation.

8.1.2 Semantic annotation

To realize the added value of semantics, the data exchanged in the IoT need to be described via semantic descriptions.

Semantic annotation, as a non-intrusive technique, is generally used for the semantic description of IoT data in order to describe characteristics of IoT resources (e.g., collected data, IoT devices and IoT applications) and to indicate relationships between IoT resources in a consistent and maintainable way.

It is required to use semantic annotation to implement semantic description.

The semantic annotation is required to be based on IoT ontology and appropriate data models, as well as predefined description languages.

It is required to support interoperability between different semantic description languages used for semantic annotation.

NOTE – One possible way to achieve interoperability is via language translation.

8.1.3 Semantic interoperability

Semantic interoperability addresses interoperability at the semantic level [b-SI], based on the meaning of exchanged data between IoT components rather than only on the representation of exchanged data. The meaning of exchanged data can be described via semantic annotation.

In practice, semantic technologies can provide support for an increased level of interoperability among different IoT components. These technologies may be implemented in different ways in the different IoT components, according to the different parties and the different application domains.

Semantic interoperability depends on the semantic annotation of the exchanged data and the interfaces of the interacting IoT components.

Semantic interoperability is recommended in the IoT so that the data transferred across different IoT components can be easily understood by each IoT technical component.

8.1.4 Semantic discovery

Semantic discovery enables the discovery of IoT resources via the meaning of query requests (semantic query) rather than the query requests' data sets.

Semantic discovery depends on IoT ontology, semantic annotation of IoT resources and semantic query.

Semantic discovery is recommended in the IoT so that IoT resources can be discovered according to the meaning of query requests.

8.1.5 Semantic reasoning

Semantic reasoning enables reasoning based on semantic annotation of IoT resources, IoT ontology and semantic rules.

Based on IoT ontology and semantic rules, semantic reasoning analyses semantic annotation to obtain implicit meanings and relationships concerning IoT resources. For example, in the case of semantic annotation describing a device as "daylight lamp", semantic reasoning can infer "daylight lamp" is also a kind of "lamp".

Semantic reasoning is recommended in the IoT so that implicit meanings and relationships concerning IoT resources can be deduced from semantically annotated information.

Semantic rules are required to be based on IoT ontology so that the meaning of semantic rules can be consistent across IoT components.

8.1.6 Semantic composition

Based on IoT ontology and semantic annotation of IoT resources, semantic composition can compose appropriate IoT resources to create new (semantically annotated) IoT resources. As a concrete example, via semantic composition, the data for "average temperature" of a room can be created by composing the "temperature" data from several individual sensors in the room.

The rules of semantic composition are based on IoT ontology.

Semantic composition can be used when straightforward semantic discovery fails to satisfy a particular semantic query. In such a case, the semantic composition process can start with an adequate query decomposition process, followed by the semantic discovery processes launched by those partial queries. The returned results for partial queries can then be adequately composed in order to satisfy the original semantic query.

Semantic composition is recommended in the IoT so that new (semantically annotated) IoT resources can be created based on existing ones.

NOTE – The newly created resources are then automatically annotated.

8.2 Semantics based requirements for IoT with respect to the IoT reference model

The following clauses describe semantics based requirements for IoT with respect to the different layers and cross-layer capabilities of the IoT reference model [ITU-T Y.4000].

8.2.1 Semantics based requirements for the device layer

1) Semantic annotation

The device layer (DL) is required to be empowered by semantic annotation for the description of IoT devices and their collected data:

− semantic annotation for IoT devices

Semantic annotation is required to be supported for the description of IoT devices.

Semantic annotation is required to be based on ontology and the semantic data model of the IoT as well as predefined semantic description languages. In this way, the data sets related to IoT devices, e.g., the type and functions of an IoT device, the operations supported by the IoT device and other information, can be correctly understood by other IoT components.

− semantic annotation for the collected data

Semantic annotation is required to be supported for the description of the data collected by IoT devices.

Semantic annotation is required to be based on ontology and the semantic data model of the IoT as well as predefined semantic description languages. In this way, the information related to the collected data, e.g., the meaning, origin, standard value and reliability of the collected data as well as other information can be correctly understood by other IoT components.

The data collected by IoT devices are recommended to be transformed into a semantic format, e.g., resource description framework (RDF) triples [b-RDF11].

The data collected by IoT devices are required to be linked to predefined semantic data models complying with the IoT ontology.

The data collected by IoT devices are recommended to be associated with provenance information.

NOTE – Provenance information is useful to provide correct contextualisation and traceability of the collected data.

8.2.2 Semantics based requirements for the SSAS layer

1) Semantic annotation

The SSAS layer is required to support semantic annotation for the description of IoT resources.

NOTE – The IoT resources semantically annotated in the SSAS layer can belong to different layers.

All semantically annotated information is required to be organized according to predefined data models.

2) Semantic discovery

The SSAS layer is recommended to support semantic discovery of IoT resources.

3) Semantic interoperability

The SSAS layer is required to support semantic interoperability, based on the semantically annotated information of IoT resources. In this way, IoT resources can be accessed, understood and exchanged by different IoT components.

4) Semantic reasoning

The SSAS layer is recommended to support semantic reasoning for IoT resources. With semantic reasoning, the semantically annotated information of IoT resources can be further enriched.

5) Semantic composition

The SSAS layer is recommended to support semantic composition of IoT resources. With semantic composition, the SSAS layer can compose IoT resources to create new resources based on the semantically annotated information of IoT resources.

8.2.3 Semantics based requirements for the network layer

1) Semantic annotation

The network layer (NL) is required to be empowered by semantic annotation for the description of IoT resources of the network layer.

Semantic annotation is recommended to be supported to facilitate the network configuration based on ontology and the semantic data model of the IoT. In this way, the information related to the network operations, e.g., the status of the network, the type of the network (e.g., fixed network, mobile network, etc.), the capabilities which can be exposed by the network and other information, can be correctly understood by other IoT components.

2) Semantic discovery

The network layer is recommended to be empowered by semantic discovery for the discovery of IoT resources of the network layer.

Semantic discovery is recommended to be supported in order to find relevant IoT resources, e.g., network interfaces or network connections, based on semantic query and ontology.

8.2.4 Semantics based requirements for the application layer

1) Semantic annotation

The application layer (AL) is required to be empowered by semantic annotation for describing IoT resources of the application layer and in support to semantic discovery of IoT resources.

2) Semantic discovery

The application layer is recommended to be empowered by semantic discovery for discovering the desired IoT resources.

3) Semantic reasoning and semantic composition

The application layer is recommended to be empowered by semantic reasoning.

The application layer is recommended to be empowered by semantic composition.

8.2.5 Semantics based requirements for the management capabilities

The requirements for the management capabilities are as follows:

1) Semantic annotation

The management capabilities are required to be empowered by semantic annotation for the description of management functions and related parameters. The management functions of IoT are generally distributed across different IoT components. With the help of semantic annotation, the information related to the management functions, e.g., device remote triggers and software/firmware updates, etc., can be correctly understood by all IoT components.

2) Semantic interoperability

The management capabilities are required to be empowered by semantic interoperability to support interworking among different types of management operations (e.g., among management operations based on TR069 protocols [b-TR069] and management operations based on Open Mobile Alliance (OMA) device management (DM) protocols [b-OMADM]). In such a way, the management functions, whose implementation can be based on various technologies or standards, can be triggered across different IoT components.

8.2.6 Semantics based requirements for the security capabilities

The requirements for the security capabilities are as follows:

1) Semantic annotation

The IoT uses a plethora of heterogeneous protocols and technologies for security, which may originate interoperability issues.

Security capabilities are recommended to be empowered by semantic annotation for security policies and mechanisms.

2) Security policy management

The IoT is required to support security policy management capabilities in order to provide control rules pertaining to access control, privacy protection, trust and authentication, etc.

Security policies are recommended to be specified using semantic description languages, such as RDF [b-RDF] and web ontology language (OWL) [b-OWL], or using a dedicated ontology.

3) Access control

The IoT is required to support access control capabilities in order to provide protection of information by restricting access to and/or modification of IoT resources only to those entities authorized to do so.

In order to efficiently do so, access control rules are required to be provided (e.g., by policy information points [b-RFC 2904]) and be comprehensible.

NOTE – Access control rules can be specified declaratively using specific access policy description languages, such as extensible access control markup language (XACML) [b-XACML], or using semantic description languages, such as RDF and OWL, or using a dedicated ontology.

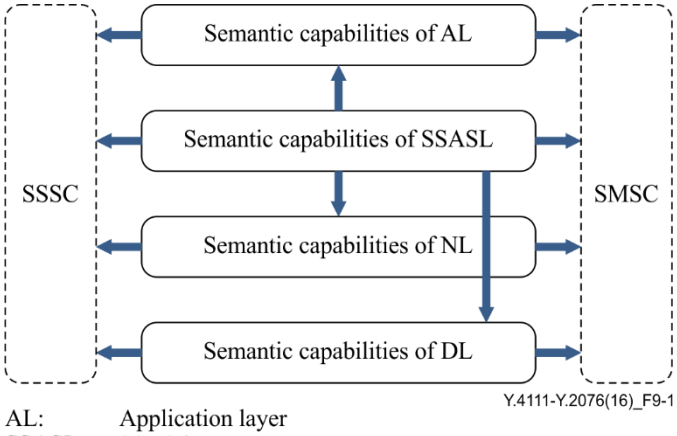
9 Semantics based capability framework of the IoT

9.1 Overview

In this clause, the IoT semantic capabilities are derived based on the requirements in clause 8.

9.1.1 The distribution of semantic capabilities in the IoT reference model

Figure 9-1 positions the semantic capabilities at the various layers as well as the cross-layer of the IoT reference model [ITU-T Y.4000]: application layer, SSAS layer, network layer, device layer, management capabilities and security capabilities. It also shows the high-level relationships among the semantic capabilities positioned at these various layers and the cross-layer.



AL: Application layer
SSASL: SSAS layer
NL: Network layer
DL: Device layer
SSSC: Semantic security support capabilities
SMSC: Semantic management support capabilities

Figure 9-1 – Semantic capabilities in the IoT reference model and their relationships

Concerning the four horizontal layers, the starting points of the directional arrows shown in Figure 9-1 are the semantic capabilities of the SSAS layer and the end points of these directional arrows are the semantic capabilities of the application layer, network layer and device layer. The intention is to indicate that the semantic capabilities of the SSAS layer can be invoked by the semantic capabilities of the application layer, network layer and device layer.

Concerning the cross-layer capabilities, the directional arrows start from the application layer, SSAS layer, network layer and device layer and end at semantic security support capabilities (SSSC) or semantic management support capabilities (SMSC). The intention is to indicate that the SMSC and SSSC of the IoT can invoke the semantic capabilities in the application layer, the SSAS layer, the network layer and the device layer.

Semantic capabilities of the IoT can operate on exposed IoT resources.

9.1.2 Global view of the IoT semantics based capability framework

Figure 9-2 provides a global view of the IoT semantics based capability framework based on the IoT reference model [ITU-T Y.4000].

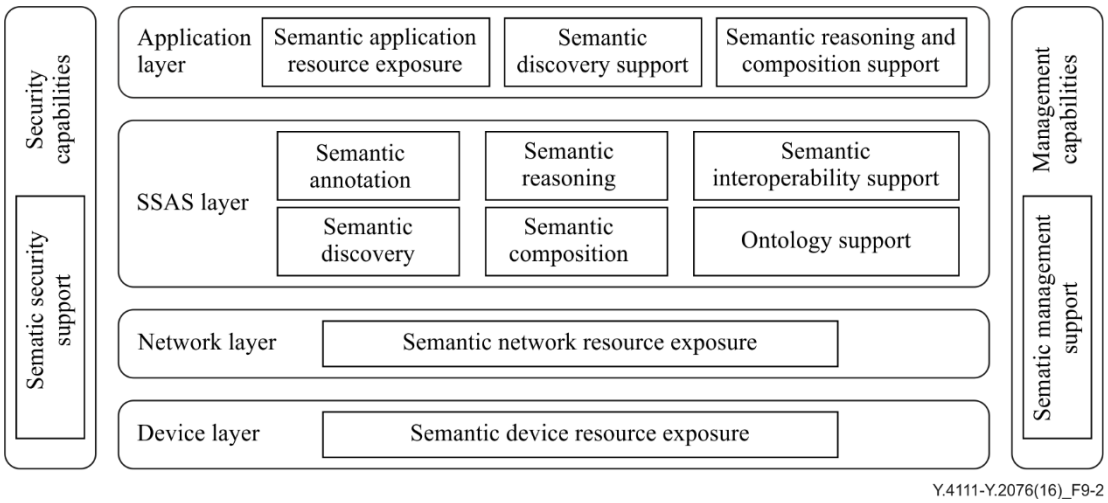


Figure 9-2 – Global view of the IoT semantics based capability framework

The SSAS layer supports semantic capabilities, including semantic annotation, semantic discovery, semantic reasoning, semantic composition and semantic interoperability support capabilities, in order to meet the requirements described in clause 8.2.2. The SSAS layer also provides the ontology support capability for semantic enablement at all layers.

The network layer supports the network resource semantic exposure capability in order to expose the resources in the network layer to the SSAS layer for semantic annotation and semantic discovery. The exposure capability conforms to the requirements in clause 8.2.3 which state that the network layer is recommended to expose its resources to the SSAS layer for semantic annotation and discovery.

The device layer supports the device resource semantic exposure capability in order to expose the resources in the device layer to the SSAS layer for semantic annotation and semantic discovery. The exposure capability conforms to the requirements in clause 8.2.1 which state that the device layer is required to expose its resources to the SSAS layer for semantic annotation and discovery.

The application layer supports the application resource semantic exposure capability in order to expose the resources in the application layer to the SSAS layer for semantic annotation and semantic discovery. The exposure capability conforms to the requirements in clause 8.2.4 which state that the application layer is required to expose its resources to the SSAS layer for semantic annotation and discovery. The application layer also supports the semantic discovery support capability and the semantic reasoning and composition support capability in order to enable the usage by IoT applications of semantic discovery, semantic reasoning and semantic composition capabilities in the SSAS layer according to the requirements in clause 8.2.4.

Security capabilities and management capabilities support, respectively, the semantic security support capability (SSSC) and the SMSC, in order to semantically enhance the security capabilities and the management capabilities.

9.1.3 The exposure of IoT resources

There are IoT resources at the different layers of the IoT reference model.

NOTE 1 – The IoT resources associated with the security and management capabilities of the IoT reference model can be seen as resources distributed in the four layers of the IoT reference model.

Figure 9-3 describes the relationship among IoT resources and the various semantic resource exposure capabilities.

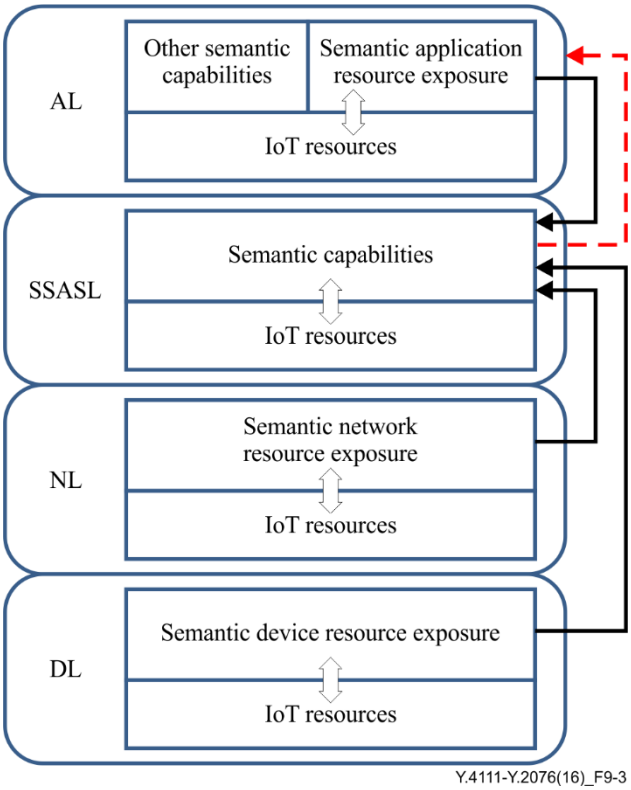


Figure 9-3 – Relationship among IoT resources and the various semantic resource exposure capabilities

As shown in Figure 9-3, the IoT resources in the device layer, the network layer and the application layer can be exposed to the SSAS layer via, respectively, the semantic device resource exposure capability, the semantic network resource exposure capability and the semantic application resource exposure capability. The SSAS layer can expose IoT resources of each layer to the application layer.

NOTE 2 – In Figure 9-3, the semantic capabilities in the SSAS layer include: semantic annotation, semantic discovery, semantic reasoning, semantic composition and semantic interoperability support capabilities.

NOTE 3 – The other semantic capabilities in the application layer indicated in Figure 9-3 include: semantic discovery support capability and the semantic reasoning and composition support capability.

The details about these resource exposure capabilities, as well as other semantic capabilities at each layer, are specified in the following clauses.

9.2 Application layer

9.2.1 Semantic application resource exposure

The semantic application resource exposure capability is used to expose the IoT resources of the application layer to the SSAS layer for semantic annotation.

The semantic application resource exposure capability is required in the application layer in order to expose the IoT resources in the application layer based on a predefined data model. The exposed IoT resources can be described in a predefined format via possible support of a standard semantic description language.

9.2.2 Semantic discovery support

The semantic discovery support capability is used to support applications in the application layer for the invocation of the semantic discovery capability in the SSAS layer.

The semantic discovery support capability is required to use a predefined format and standard semantic query language (e.g., SPARQL [b-SPARQL]) in order to invoke the semantic discovery capability in the SSAS layer according to the applications' requests.

9.2.3 Semantic reasoning and composition support

The semantic reasoning and composition support capability is used to support the transfer of the semantic rules defined by applications from the application layer to the SSAS layer so that semantic reasoning and composition can be executed according to the applications' needs.

The semantic reasoning and composition support capability is recommended in the application layer.

If the semantic reasoning and composition support capability is enabled, it is required to use a predefined format and standard semantic languages such as rule interchange format (RIF) [b-RIF], to transfer the semantic rules according to the applications' needs.

9.3 SSAS layer

9.3.1 Semantic annotation

The semantic annotation capability is used to semantically annotate IoT resources exposed to the SSAS layer.

The semantic annotation capability is required in the SSAS layer to semantically annotate IoT resources based on IoT ontology in a standard semantic language. When the exposed IoT resource is not described in a semantic way, the semantic annotation capability needs to translate it into a standard semantic description, e.g., based on the data model used by the exposed IoT resource.

9.3.2 Semantic discovery

The semantic discovery capability enables the discovery of IoT resources via semantic queries.

The semantic discovery capability is required to support discovery filters described via standard semantic query languages (e.g., SPARQL).

The semantic discovery capability is required to be able to trigger semantic composition capabilities in case it fails to satisfy a particular semantic query.

9.3.3 Semantic reasoning

The semantic reasoning capability is used to analyse the explicit semantically annotated IoT resources in order to obtain some implicit information.

The semantic reasoning capability is recommended in the SSAS layer.

If the semantic reasoning capability is enabled, it is required to run semantic reasoning based on IoT ontology.

NOTE – The information derived via semantic reasoning can be added to the semantic description of the related IoT resources via semantic annotation, for example with the goal to benefit further semantic discovery operations.

9.3.4 Semantic composition capability

The semantic composition capability composes IoT resources in order to create new (semantically annotated) resources.

The semantic composition capability is required to be based on IoT ontology for the configuration of its composition rules (for composition and de-composition processes).

The semantic composition capability is required to support requests by the semantic discovery capability in the case where the semantic discovery capability fails to satisfy a particular semantic query.

9.3.5 Semantic interoperability support

The semantic interoperability support capability is used to support the exchange of semantic information among different IoT components for the purpose of semantic level interoperability.

The semantic interoperability support capability is required to use a predefined format to exchange semantic information.

NOTE – Examples of exchanged semantic information include semantically annotated data sets related to exchanged data as well as to interfaces of the interacting IoT components.

9.3.6 Ontology support capability

The ontology support capability provides IoT ontology for semantic capabilities.

The ontology support capability is required to provide IoT ontology for the following semantic capabilities:

- the semantic annotation capability in order to annotate IoT resources;
- the semantic discovery capability in order to resolve the meaning of queries;
- the semantic composition capability in order to configure composition rules;
- the semantic reasoning capability in order to analyse the semantically annotated information of IoT resources for obtaining implicit information;
- the semantic interoperability support capability in order to semantically annotate exchanged data and interfaces of the interacting IoT components.

The ontology support capability is required to be able to integrate within the IoT ontology existing ontologies as well as newly created ontologies.

9.4 Network layer

9.4.1 Semantic network resource exposure

The semantic network resource exposure capability is used to expose the IoT resources in the network layer to the SSAS layer for semantic annotation.

The semantic network resource exposure capability is recommended in the network layer to expose the IoT resources in the network layer based on a predefined format via possible support of a standard semantic description language.

9.5 Device layer

9.5.1 Semantic device resource exposure

The semantic application resource exposure capability is used to expose the IoT resources in the device layer to the SSAS layer for semantic annotation.

The semantic network resource exposure capability is required in the device layer to expose IoT resources in the device layer based on a predefined format via possible support of a standard semantic description language.

9.6 Management capabilities

9.6.1 Semantic management support capability

The SMSC enhances the management capabilities of the IoT via the support of semantically annotated data sets.

The semantic management support capability is recommended to support semantic annotation of management functions and semantic level interoperability of management functions using semantic annotation capability and semantic interoperability capability in the SSAS layer.

9.7 Security capabilities

9.7.1 Semantic security support capability

The semantic security support capability (SSSC) enhances the security capabilities of the IoT via the support of semantically annotated data sets.

The semantic security support capability is recommended to support semantic annotation of security policies (e.g., access control rules) and semantic level interoperability of security mechanisms using semantic annotation capability and semantic interoperability capability in the SSAS layer.

Appendix I

IoT application scenarios using semantic technologies

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

I.1 Semantics-enabled home automation

In this IoT application scenario, as shown in Figure I.1, a home gateway is deployed for the support of home automation applications.

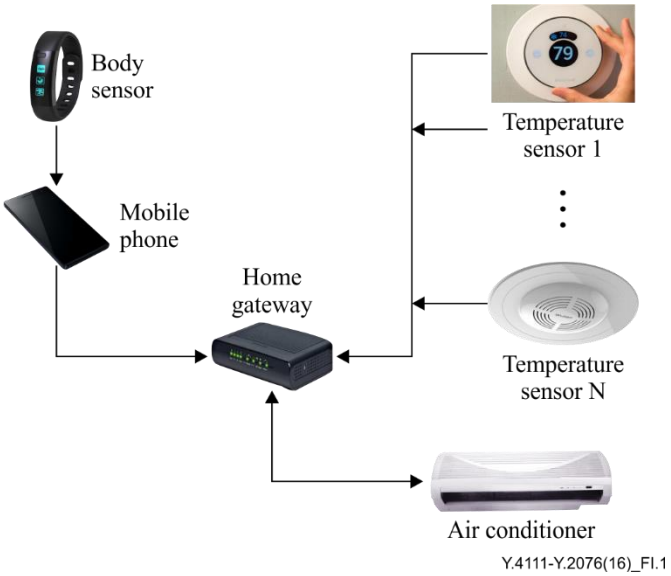


Figure I.1 – Semantics-enabled home automation

The body sensors of the home owner (e.g., embedded in the watch, sports band) collect the body monitoring data (e.g., skin temperature, heart rate, skin humidity) and send them to the mobile phone of the home owner.

When the home owner enters the house, the mobile phone automatically connects to the home gateway and sends the body monitoring data to the home gateway. The body monitoring data sent by the mobile phone are semantically annotated. Based on the semantic annotation, the home gateway can understand the meaning of the received body monitoring data and get the body status of the home owner.

In the case where the home gateway finds that the home owner's skin temperature is high, with the help of semantic reasoning, the home gateway can infer that the home owner may need a cooler environment. The home automation application in the home gateway can then initiate the following process:

1) The home automation application queries the average temperature of the room. With the help of semantic discovery and semantic composition, the home gateway automatically composes all the temperature sensors in the room to form a virtual object that combines all the measurements in order to generate an approximate average temperature. The formed virtual object directly provides the approximate average temperature of the room and exposes it to the home automation application in the home gateway.
2) The home automation application in the home gateway checks whether the approximate average temperature of the room is higher than a comfortably cool level or not. If the

approximate average temperature of the room is higher, the home automation application will reduce the temperature.

3) The home automation application queries the device in the room that can reduce the temperature. With the help of semantic discovery, the air conditioner and its operations are exposed to the home automation application. The home automation application controls the air conditioner in order to reduce the room temperature to a cooler level until the relevant body monitoring data sent from the mobile phone become normal.

I.2 Semantics enabled location-based service

A semantics-enabled location-based service can provide users with a spatial inquiring service. IoT semantic technologies are used for the implementation of a semantics enabled location-based service.

As an example of this service, this clause describes the process related to a specific spatial inquiry: finding all gas stations within 10 miles offering a gas price lower than a given amount.

One possible way to offer a semantics-enabled location-based service is shown in Figure I.2.

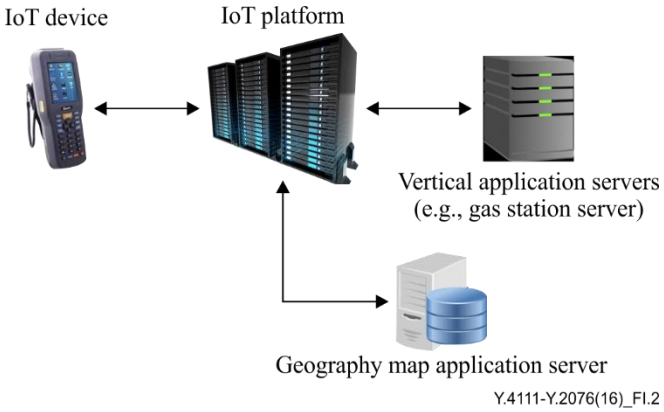


Figure I.2 – Semantics enabled location-based service

The application layer of the IoT device provides semantic discovery support functionality, which can send out query requests in a semantic way. For the specific inquiry above, i.e., finding all the gas stations within 10 miles with a gas price lower than a given amount, a query request is sent out to the IoT platform according to the specific IoT ontology used by the IoT device and in corresponding semantic description language. At the same time, the current location information of the IoT device (e.g., latitude and longitude) is sent out to the IoT platform.

The IoT platform retrieves the query request and triggers the semantic discovery functionality. The semantic discovery functionality fails because it cannot find an IoT resource that meets the query request directly. Then a semantic composition functionality is triggered which composes feedback from a geographical map application server and feedback from multiple gas station application servers. The geographical map application server returns the list of gas stations that are within 10 miles of the IoT device. Gas station application servers feedback corresponding gas stations' location information. The semantic composition functionality of the IoT platform composes these feedbacks and produces the answer for the query request of the IoT device.

Bibliography

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

[b-ITU-T Z.341] Recommendation ITU-T Z.341 (1988), *Glossary of terms*.

[b-ETSI-TR 101 584] ETSI TR 101 584 V2.1.1 (2013), *Machine-to-Machine Communications (M2M); Study on Semantic support for M2M Data*. <http://www.etsi.org/deliver/etsi_tr/101500_101599/101584/02.01.01_60/tr_101584v020101p.pdf>

[b-RFC 2904] IETF RFC 2904 (2000), *AAA Authorization Framework*. <https://tools.ietf.org/html/rfc2904>

[b-XACML] OASIS Standard (2013), *eXtensible Access Control Markup Language (XACML) Version 3.0*. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf>

[b-OMADM] Open Mobile Alliance (2012), *OMA Device Management V2.0*. <http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/dm-v2-0>

[b-OWL] OWL (2012), *Web Ontology Language (OWL)*. <http://www.w3.org/OWL/>

[b-RDF] W3C Specification (2004), *Resource Description Framework (RDF)*. <http://www.w3.org/RDF/>

[b-RDF11] W3C Recommendation (2014), *Resource Description Framework (RDF). Concepts and Abstract Syntax*. <http://www.w3.org/TR/rdf11-concepts/>

[b-RIF] W3C specification, *RIF Overview (Second Edition)*. <http://www.w3.org/TR/rif-overview/>

[b-SemanticWeb] W3C Semantic Web, *Semantic Web overview*. <http://www.w3.org/standards/semanticweb>

[b-SSNO] W3C Semantic Sensor Network Incubator Group (2005), *Semantic Sensor Network Ontology*. <http://purl.oclc.org/NET/ssnx/ssn>

[b-SI] European Research Cluster on the Internet of Things, *IoT Semantic Interoperability: Research Challenges, Best Practices, Solutions and Next Steps, IERC AC4 Manifesto "Present and Future"*. <http://www.probe-it.eu/wp-content/uploads/2013/10/IERC-AC4-SemanticInteroperabilityManifesto-V1_130830-Final1.pdf>

[b-SPARQL] K. Kyzirakos, M. Karpathiotakis, and M. Koubarakis (2010), *Developing Registries for the Semantic Sensor Web Using stRDF and stSPARQL*, Int'l Workshop Semantic Sensor Networks. <http://people.csail.mit.edu/pcm/tempISWC/workshops/SSN2010/paper8.pdf>

[b-TR069] Broadband Forum TR-069 Amendment 5 (2013), *CPE WAN Management Protocol*. <http://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf>

[b-UML] Object Management Group (OMG), (2014), *Unified Modeling Language (UML®) Resource Page*. <http://www.uml.org/>

[b-AIOTI-WG3] AIOTI WG03 IoT Standardization (2015), *Semantic Interoperability*, Release 2.0. <https://docbox.etsi.org/SmartM2M/Open/AIOTI/!!20151014Deliverables/AIOTI_WG3_SemanticInterop_Release_2_0a.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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, 2016