International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3071

(03/2017)

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

Future networks

Data aware networking (information centric networking) – Requirements and capabilities

Recommendation ITU-T Y.3071

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.3071

Data aware networking (information centric networking) – Requirements and capabilities

Summary

Recommendation ITU-T Y.3071 specifies the requirements and capabilities of data aware networking (DAN) to realize the use cases and scenarios described in Supplement 35 to the ITU-T Y-series Recommendations, which are expected to be major applications/services provided on DAN. One of the objectives reflecting emerging requirements for future networks is data awareness as specified in Recommendation ITU-T Y.3001. DAN is expected to have capabilities optimized to handle enormous amounts of data and to enable users to access desired data safely, easily, quickly and accurately, regardless of their location. DAN can be described as networking whose central aim is retrieving information, i.e., information centric networking (ICN).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3071	2017-03-29	13	11.1002/1000/13253

Keywords

DAN, data awareness, data aware networking, future networks, ICN, information centric networking.

---

* 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.3071

Data aware networking (information centric networking) – Requirements and capabilities

1 Scope

This Recommendation specifies the requirements of data aware networking (information centric networking) derived from the use cases and scenarios described in [b-ITU-T Y.Sup. 35]. One of the objectives reflecting emerging requirements for future networks is data awareness as specified in [ITU-T Y.3001]. This Recommendation identifies the capabilities to fulfil the requirements and describes the components including their corresponding capabilities.

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.3001] Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*.

[ITU-T Y.3031] Recommendation ITU-T Y.3031 (2012), *Identification framework in future networks*.

[ITU-T Y.3033] Recommendation ITU-T Y.3033 (2014), *Framework of data aware networking for future networks*.

[ITU-T Y.3034] Recommendation ITU-T Y.3034 (2015), *Architecture for interworking of heterogeneous component networks in ID/locator split-based future networks*.

[ITU-T M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.3 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.4 data ID [ITU-T Y.3033]: An identifier used to identify a data object. It has a form of a series of digits, characters and symbols or any of these combinations, which generally do not have any meaning.

NOTE – In this Recommendation, the terms "data ID" and "ID" are used interchangeably.

3.1.5 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.6 data name [ITU-T Y.3033]: A string of alpha-numeric characters that is used to identify the data object. A data name, which may have variable length, is usually configured in such a way that it would be easier to be read and remembered by humans.

NOTE – In this Recommendation, the terms "data name", "NDO name", and simply "name" are used interchangeably.

3.1.7 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.8 named data object (NDO) [b-ITU-T Y.Sup. 35]: A data object that is identifiable by a name.

3.1.9 peer-entity authentication [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 DAN element: A network component that forwards messages to producers, consumers, and other data aware networking (DAN) elements.

3.2.2 DAN realm: A set of data aware networking (DAN) elements operated under one DAN realization and managed by an organization. Different DAN realms may adopt different DAN realizations such as naming convention, communication models including push and pull models and name resolution mechanisms.

3.2.3 NDO consumer: A component that makes requests on named data objects (NDOs).

3.2.4 NDO producer: A component holding named data objects (NDOs) and make them reachable by corresponding requests. An NDO producer may be an actual owner of the NDO or a delegate of the actual owner.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APL Application

DAN Data Aware Networking

ICN Information Centric Networking

ID Identifier

NDO Named Data Object

5 Conventions

None.

6 Justification

It is essential to define the capabilities of DAN to bring its concept into reality.

Several use case scenarios for DAN have been introduced in [b-ITU-T Y.Sup. 35], which can be realized in different ways, e.g., with different combinations of capabilities. This aspect encourages the identification of the capabilities of DAN to realize various use case scenarios.

For this reason, this Recommendation intends to specify the requirements of DAN that are derived from the use case scenarios, and then defines its capabilities considering previously performed studies, such as those on communication based on name or identifier (ID) in [ITU-T Y.3031] [ITU-T Y.3033] [ITU-T Y.3034]. Understanding the requirements and components of DAN enables the enrichment of the process of developing additional use case scenarios.

7 Requirements for DAN

7.1 Forwarding

- NDO name based forwarding function:
  It is required that a request be forwarded by attaching the name or ID of the NDO to the request.
- Request aggregation function:
  It is recommended that DAN elements be equipped with the function to aggregate requests to the same NDO to reduce network traffic and server load.
- Subscription:
  DAN is required to provide a mechanism for an NDO consumer to register description(s) to identify one or more NDOs that the consumer is interested in receiving when they are published.
- Publication:
  DAN is required to provide a mechanism for an NDO producer to publish NDOs to the network. The published NDOs may be distributed to consumers whose subscription matches the published NDOs.
- Packet forwarding loop avoidance function:
  DAN is required to have functions to avoid or resolve packet forwarding loops.

7.2 Routing

- NDO registration function:
  It is required that the unique name or ID of an NDO be registered to DAN so that NDO consumers can access the NDO with the name or ID.
- NDO location resolution function:
  DAN optionally provides the facility for a DAN element to ask for a forwarding direction when the DAN element cannot judge the forwarding direction of a request for an NDO.
- Advertisement function for the availability of NDOs:
  It is required that availability information of NDOs be disseminated to help in the choice of the correct direction of request forwarding.
- Network selection function for requests to reach an NDO:
  It is required that appropriate network interfaces be selected to forward requests in order to reach a specified NDO.

7.3 Mobility

- Consumer mobility:
  DAN is required to provide a mechanism for a consumer to maintain undisrupted message flows while the consumer is in motion.
- NDO mobility:
  DAN is required to provide a mechanism for NDOs to re-locate without disrupting NDO availability when the NDOs change their locations.

- Network mobility:
  DAN optionally provides an efficient mechanism for a network to maintain seamless network connection for its mobility.

7.4 Security

- Access control:
  It is required that DAN be equipped with a mechanism to examine and confirm the authenticity of consumers and that NDO be accessible only by the authorized consumers.
- Network security function from malicious attacks:
  DAN is required to have a mechanism to protect its functions from malicious network attacks.
- NDO availability:
  DAN is required to provide a mechanism to ensure that the NDOs published in networks are available for authorized consumers.
- NDO origin authentication:
  DAN is required to be equipped with a mechanism to examine and confirm the authenticity of the owners of NDOs.
- NDO name verification:
  DAN is required to be equipped with a mechanism to examine and confirm the mapping between an NDO and its name or ID.
- NDO integrity:
  DAN is required to be equipped with a mechanism to examine and confirm the data integrity of NDOs.

7.5 Management

[ITU-T M.3400] defines the standard network management functions and DAN is also required to provide similar management functions, which include:

- Performance management
- Fault management
- Configuration management
- Accounting management
- Security management

DAN specific management functions are expected to be required. One of the potential DAN specific management functions is the function to manage NDOs. The NDO management function may include monitoring and regulation of NDO accesses and the number of NDOs, as well as withdrawal of NDOs. Further development of DAN technologies is required before the requirements on DAN specific management functions are defined.

7.6 Miscellaneous

- NDO cache function:
  It is required that DAN elements be equipped with a cache that temporally holds NDOs to reduce unnecessary duplicated transmission of the same NDO. The cache may be populated by NDOs either passing by or allocated proactively.
- NDO fragmentation function:
  It is required that DAN elements fragment large NDOs into a series of smaller units for network transmission.
- Function of updating and versioning NDOs:
  DAN optionally provides versioning capability to update content while keeping its name.

7.7 Use case specific

- Processing function:
  DAN optionally provides the capability to process NDOs before transmitting them in order to adapt the NDOs to the capability of the receiving consumer or to aggregate information.
- Process registration function:
  When a processing function is available in DAN, a mechanism to register the description of the process is required.
- Process scheduling and coordination function:
  DAN optionally has a capability to recognize data processing requests, coordinate the requested processing placed at appropriate DAN elements, and schedule the processing.
- NDO and processing description retrieval function:
  DAN elements optionally have a capability to retrieve data processing descriptions and the NDOs to be processed by the requested processing.
- Explicit processing allocation function:
  DAN elements optionally have a capability to allocate data processing function to a specified location.
- Data collection function:
  DAN elements optionally have a capability to collect sensor data and store the data in their storage.
- Long live period of cached data:
  Cached data can optionally have a long live period before the cached data are deleted. This function is indispensable to the dissemination of information that is accessed by a large number of users, e.g., disaster-related information, using DAN.
- Consumer and cache location function:
  DAN optionally has a mechanism to identify networks and geographical locations of consumers and caches.
- NDO distribution scheduling function:
  DAN optionally has a function to estimate the arrival time of mobile consumer requests to DAN elements and the duration that the consumers are connected to the DAN elements. DAN also optionally has a capability to schedule delivery of appropriate NDOs to the DAN elements before the consumer request arrives.
- Multiple NDO request function:
  DAN optionally provides a mechanism to request multiple NDOs in one request.
- Vehicle-to-vehicle communication function:
  lDAN optionally provides the capability for a vehicle-onboard DAN element to directly communicate with other vehicle-onboard DAN elements.
- Vehicle-to-roadside-infrastructure communication function:
  DAN optionally provides the capability for a vehicle-onboard DAN element to communicate with roadside producers that give location specific information.
- Distribution of information among fragmented networks:
  DAN optionally provides a mechanism to distribute NDOs while a DAN network is fragmented into multiple DAN networks with intermittent connections among them.
- Function to specify service classes in NDO names:
  DAN can optionally specify service classes in NDO names in order to provide appropriate service quality for communication services.
- Service class provisioning function:
  DAN is optionally equipped with a mechanism to provide the appropriate communication quality for different communication services specified in NDO names.

8 Capabilities of DAN

8.1 Configuration of DAN components

Figure 1 shows the configuration of a DAN network consisting of the following components (see clause 3.2 for definitions of the terms):

- NDO producers
- NDO consumers
- DAN elements
- DAN realms

When there are multiple DAN realms, the DAN elements connecting heterogeneous DAN realms act as gateways to make appropriate conversions of names, IDs, protocols, etc. so that the DAN realms can communicate with each other.

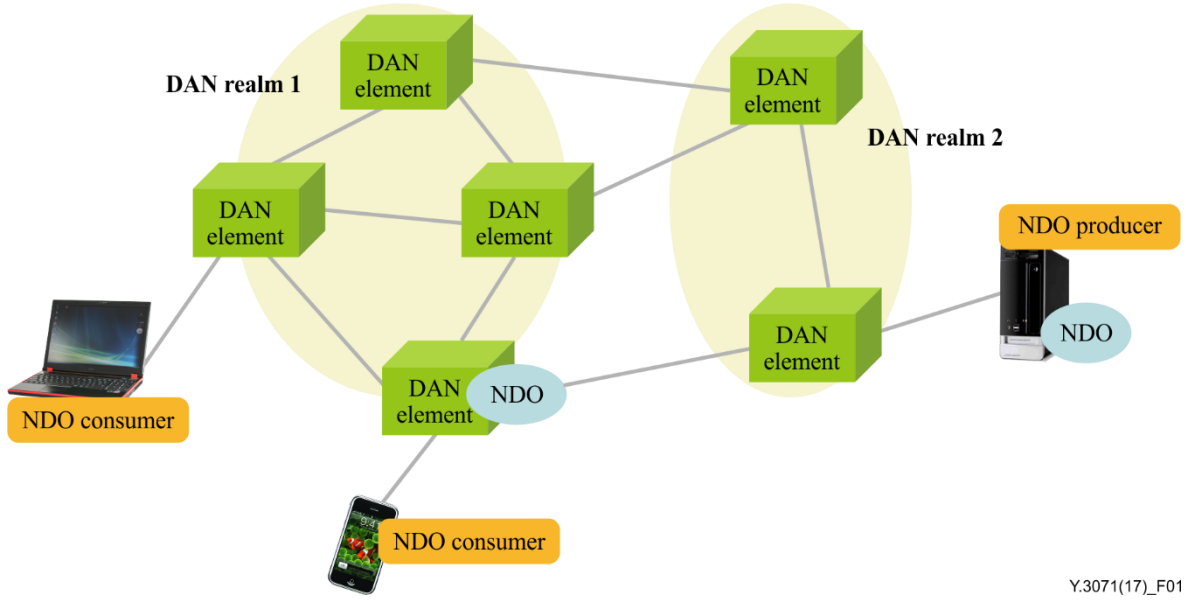

Figure 1 – Overall network structure of DAN

8.2 Capabilities

DAN is composed of the capabilities shown in Figure 2. There are five major capabilities: data capability, control capability, security capability, management capability and application capability. The capabilities can be further subdivided into functional blocks as shown in Figure 2.

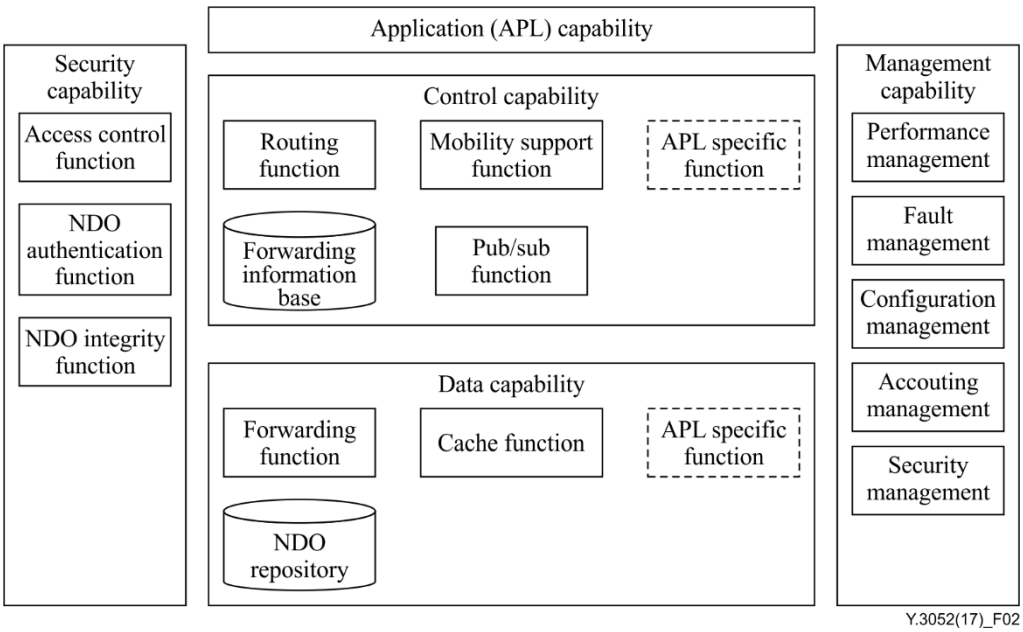

Figure 2 – Functional view of DAN capabilities

8.2.1 Data capability

The data capability has functional blocks as follows:

- Forwarding function:
  This functional block contains an NDO name-based forwarding function, request aggregation function and packet forwarding loop avoidance function.
- Cache function:
  This functional block includes storage to cache NDOs and their accompanying control functions.
- NDO repository:
  The repository is the storage to hold original content.

Additionally, application specific functional blocks may be placed in the data capability.

8.2.2 Control capability

The control capability has functional blocks as follows:

- Routing function:
  The routing functional block is composed of an NDO registration function, NDO location resolution function, advertisement function for the availability of NDOs and network selection function for messages to reach an NDO.
- Mobility support function:
  The mobility support function includes a consumer mobility function, NDO mobility function and network mobility function.
- Forwarding information base:
  The forwarding information base is the storage to hold information to determine the direction of forwarding and is to be used by the forwarding function.
- Publish/subscribe function:
  This functional block includes publication and subscription functions.

Additionally, application specific functional blocks may be placed in the control capability.

8.2.3 Security capability

The security capability has functional blocks as follows:

- Access control function:
  The access control function is a mechanism to secure data confidentiality so that an NDO is only accessible by authorized consumers.
- NDO authentication function:
  The NDO authentication function is a mechanism to secure data authenticity so that an NDO is claimed to be true by an authorized entity.
- NDO integrity function:
  The NDO integrity function is a mechanism to examine and confirm the integrity of an NDO so that an NDO is ensured to be the same as the source.

8.2.4 Management capability

The management capability is the function block to provide network management functions. [ITU-T M.3400] defines the standard network management function groups and DAN is also required to facilitate the management functions defined in [ITU-T M.3400], which are:

- performance management;
- fault management;
- configuration management;
- accounting management;
- security management.

8.2.5 Application capability

The application capability contains network service functions. The network service functions in the application capability do not include user applications that only send and receive messages among communicating network users. Instead, the network service functions are functions to implement and control application specific network behaviour.

9 Security considerations

DAN provides mechanisms to guarantee secrecy, integrity and availability of NDOs, as well as verifying the owners of NDOs by means of the capabilities described in clause 8.2.3. To operate the mechanisms properly, an additional mechanism to distribute cryptographic keys may be required.

Revealing the NDO access history by NDO consumers is an intrinsic problem in DAN where NDO names are expected to be long-lived. Even if the name itself does not reveal the content of the NDO, the name can be used to retrieve the NDO and the content may be known.

The new network function, caching, potentially poses a new security threat to network users. For example, placing improper NDOs in a cache prevents access to the correct NDOs and forcing the cache to store improper NDOs reduces cache efficiency.

10 Environmental considerations

The environmental considerations in this Recommendation are mainly subject to those provided by DAN as specified in [ITU-T Y.3033]. Additional energy reduction by DAN may come from the processing capability provided by DAN elements. The processing capability can be used to reduce the amount of data and the number of messages to be transferred over DAN. Although the processing increases energy consumption at one DAN element, reduction in the number of messages being exchanged lowers energy consumption in the other DAN elements, which results in energy reduction in the entire network.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT Applications*.

[b-ITU-T Y.Sup. 35] ITU-T Y-series Recommendations – Supplement 35 (2016), *ITU-T Y.3033 – Data-aware networking – Scenarios and use cases*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017