International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4416

(06/2018)

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

Architecture of the Internet of things based on next generation network evolution

Recommendation ITU-T Y.4416

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.4416

Architecture of the Internet of things based on next generation network evolution

Summary

Recommendation ITU-T Y.4416 provides a description of the architecture of the Internet of things (IoT) based on next generation network evolution (NGNe), taking account of the IoT reference model specified in Recommendation ITU-T Y.4000/Y.2060, the IoT common requirements specified in Recommendation ITU-T Y.4100/Y.2066, and the IoT functional framework and capabilities specified in Recommendation ITU-T Y.4401/Y.2068. It describes extensions to NGNe functional entities, reference points and NGNe functional components, and enhancement to NGNe capabilities as described in Recommendation ITU-T Y.2012, and other related Recommendations in order to support the IoT.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4416	2018-06-29	20	11.1002/1000/13638

Keywords

Architecture, capability enhancement, functional entity, functional component, Internet of things (IoT), next generation network evolution (NGNe), reference point.

* 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

Page

Recommendation ITU-T Y.4416

Architecture of the Internet of things based on next generation network evolution

1 Scope

This Recommendation describes an architecture of the Internet of things (IoT) based on extensions and enhancement to next generation network evolution (NGNe) functional entities, reference points and components as described in [ITU-T Y.2012], and other related Recommendations. The Recommendation takes into account the IoT reference model specified in [ITU-T Y.4000], the IoT common requirements specified in [ITU-T Y.4100], and the IoT functional framework and capabilities specified in [ITU-T Y.4401].

The scope of this Recommendation includes:

– the extension to NGNe functional entities to support the IoT;

– the extension of NGNe reference points to support the IoT;

– the extension of NGNe components to support the IoT;

– the enhancement to NGNe capabilities to support the IoT.

Security of the extensions and enhancement specified in this Recommendation is also considered.

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.2012]	Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.
[ITU-T Y.2701]	Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
[ITU-T Y.2704]	Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.
[ITU-T Y.4000]	Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.
[ITU-T Y.4100]	Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.
[ITU-T Y.4401]	Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application network interface [ITU-T Y.2012]: Interface which provides a channel for interactions and exchanges between applications and NGN elements. The ANI offers capabilities and resources needed for realization of applications.

NOTE – ANI stands for application network interface.

3.1.2 application provider [ITU-T Y.2012]: A general reference to a provider that offers applications to the customers making use of the services capabilities provided by the NGN.

3.1.3 functional architecture [ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains..

3.1.4 functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

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

3.1.6 reference point [ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AM-FE	Access Management Functional Entity
AN-FE	Access Node Functional Entity
ANI	Application Network Interface
AS-FE	Application Support Functional Entity
CD&LC-FE	Content Distribution and Location Control Functional Entity
CDC-FE	Content Delivery Control Functional Entity
CDP-FE	Content Delivery Processing Functional Entity
CN	Component Number
EC	Enhanced Capability
GSC-FE	General Services Control Functional Entity

IdM	Identity Management
IoT	Internet of Things
IoT-DEC-FE	IoT Data Exchange Control Functional Entity
IoT-DEM-FE	IoT Data Event Management Functional Entity
IoT-DKM-FE	IoT Data Knowledge Management Functional Entity
IoT-DMF	IoT Data Management Function
IoT-DPC-FE	IoT Data Processing Control Functional Entity
IoT-DPE-FE	IoT Data Policy Enforcement Functional Entity
IoT-DQC-FE	IoT Data Querying Control Functional Entity
IoT-DSA-FE	IoT Data Service Adaptation Functional Entity
IoT-DSC-FE	IoT Data Storage Control Functional Entity
IoT-DV-FE	IoT Device Functional Entity
IoT-EAC-FE	IoT End-point Access Control Functional Entity
IoT-EEM-FE	IoT End-point Event Management Functional Entity
IoT-EKM-FE	IoT End-point Knowledge Management Functional Entity
IoT-EPE-FE	IoT End-point Policy Enforcement Functional Entity
IoT-EPF	IoT End-Point Function
IoT-EUD-FE	IoT End-User Device Functional Entity
IoT-GW-FE	IoT Gateway Functional Entity
IoT-LSC-FE	IoT Location Service Control Functional Entity
IoT-LTC-FE	IoT Location Transport Control Functional Entity
IoT-SCF	IoT Service Control Function
IoT-SEM-FE	IoT Service Event Management Functional Entity
IoT-SKM-FE	IoT Service Knowledge Management Functional Entity
IoT-SPA-FE	IoT Service Provision Adaptation Functional Entity
IoT-SPE-FE	IoT Service Policy Enforcement Functional Entity
IoT-SRC-FE	IoT Service Resource Control Functional Entity
IoT-SSC-FE	IoT Service Session Control Functional Entity
IoT-TAM-FE	IoT Transport Awareness Management Functional Entity
IoT-TCA-FE	IoT Transport Configuration Adaptation Functional Entity
IoT-TCF	IoT Transport Control Function
IoT-TEM-FE	IoT Transport Event Management Functional Entity
IoT-TKM-FE	IoT Transport Knowledge Management Functional Entity
IoT-TPE-FE	IoT Transport Policy Enforcement Functional Entity
IoT-TRC-FE	IoT Transport Resource Control Functional Entity
IP	Internet Protocol
NACF	Network Attachment Control Function

NGN	Next Generation Network
NGNe	Next Generation Network evolution
NICE	Network Intelligence Capability Enhancement
P-CSC-FE	Proxy Call Session Control Functional Entity
PD-FE	Policy Decision Functional Entity
RACF	Resource and Admission Control Function
RFID	Radio Frequency Identification
S-CSC-FE	Serving Call Session Control Functional Entity
SL-FE	Subscription Locator Functional Entity
SNI	Service Network Interface
TLM-FE	Transport Location Management Functional Entity
TRC-FE	Transport Resource Control Functional Entity

5 Conventions

In this Recommendation:

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

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

The keywords "can optionally" 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 Overview of NGNe functional extension to support the IoT

6.1 IoT requirements motivating extensions and enhancement of NGNe

The high-level characteristic requirements of the IoT are specified in [ITU-T Y.4000]; these unique characteristic requirements that cannot be fulfilled in next generation network (NGN) functional architecture as specified in [ITU-T Y.2012] and in functional architecture of network intelligence capability enhancement (NICE) as specified in [b-ITU-T Y.2302] are as follows: autonomic access to the IoT from IoT devices; autonomic networking with the IoT from IoT gateways and end-user devices; autonomic service provisioning to IoT users; and management of the data of things.

6.1.1 The requirement for autonomic access

The characteristic requirement for autonomic access to the IoT can be fulfilled by identification-based connectivity, device mobility and adaptable connectivity capabilities, as specified in [ITU-T Y.4401]. In order to support these capabilities, IoT end-point functions (IoT-EPFs) should be added to the NGN functional architecture [ITU-T Y.2012].

6.1.2 The requirement for autonomic networking

The characteristic requirement of autonomic networking of the IoT gateway and the end-user devices can be fulfilled by self-configuring for networking, self-healing for networking, self-optimizing for networking, self-protecting for networking, content-aware communication, location-based communication, transport acknowledgement and adaptable networking capabilities, as specified in [ITU-T Y.4401]. In order to support these capabilities, the IoT-EPFs, IoT transport control functions (IoT-TCFs) and related reference points should be added to the NGN functional architecture specified in [ITU-T Y.2012]. The access node functional entity (AN-FE), transport location management functional entity (TLM-FE) and access management functional entity (AM-FE) specified in [ITU-T Y.2012] should also be enhanced in order to support these IoT capabilities.

6.1.3 The requirement for autonomic service provision

The characteristic requirement for autonomic service provision by the IoT can be fulfilled by semantic based service, service composition, autonomic service, location-based and context aware service, service discovery, adaptable service provision and service provision acknowledgement capabilities as specified in [ITU-T Y.4401]. In order to support these capabilities, the IoT service control functions (IoT-SCFs) and related reference points should be added to the NGN functional architecture specified in [ITU-T Y.2012]. The serving call session control functional entity (S-CSC-FE), proxy call session control functional entity (P-CSC-FE), subscription locator functional entity (SL-FE) and general services control functional entity (GSC-FE) specified in [ITU-T Y.2012] should also be enhanced in order to support these IoT capabilities.

6.1.4 The requirement for managing the data of things

The characteristic requirement for thing data management by the IoT can be fulfilled by data storage, data processing, data querying, data access control, open information exchange, semantic data operation and autonomic data operation capabilities as specified in [ITU-T Y.4401]. In order to support these capabilities, the IoT data management functions (IoT-DMFs) and related reference points should be added to the NGN functional architecture specified in [ITU-T Y.2012]. The content distribution and location control functional entity (CD&LC-FE), content delivery control functional entity (CDC-FE), and content delivery processing functional entity (CDP-FE) specified in [ITU-T Y.2012] should also be enhanced in order to support these IoT capabilities.

6.2 The extension of functional entities

In order to support the IoT, the following functional entities should be extended in the NGN functional architecture. The extension is illustrated in Figure 6-1. The extended functional entities in Figure 6-1 are coloured in green.

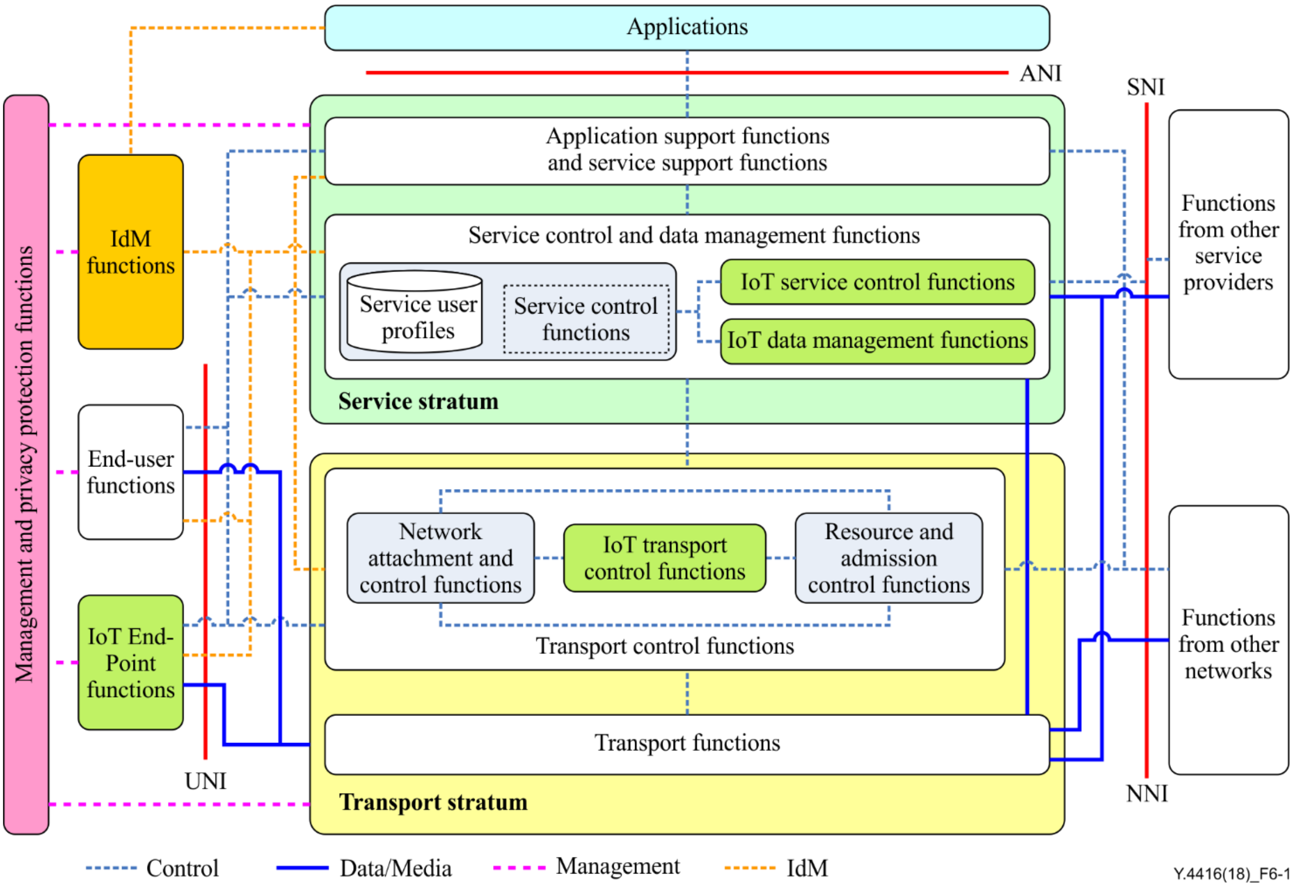
Applications
ANI
SNI
Management and privacy protection functions
IdM functions
Application support functions and service support functions
Service control and data management functions
Service user profiles
Service control functions
IoT service control functions
IoT data management functions
Service stratum
Functions from other service providers
End-user functions
IoT End-Point functions
Network attachment and control functions
IoT transport control functions
Resource and admission control functions
Transport control functions
Transport functions
Transport stratum
Functions from other networks
UNI
NNI
Control
Data/Media
Management
IdM
Y.4416(18)_F6-1

Figure 6-1 – NGNe functional entity extensions to support the IoT

6.2.1 IoT end-point functions

The IoT-EPFs provide capabilities for access to IoT devices from NGNe networks, access to NGNe networks from IoT devices and control of these accesses.

The IoT-EPFs provide the connectivity capabilities, such as identification-based connectivity, thing status notification, device mobility and adaptable connectivity, specified in [ITU-T Y.4401], which can be used to connect radio frequency identification (RFID) readers, sensors and other IoT devices without direct human intervention. The reference points between the IoT-EPFs and transport functions can be specified to support direct attachment with IoT devices.

6.2.2 IoT transport control functions

The IoT-TCFs interact with the network attachment control functions (NACFs) and the resource and admission control functions (RACFs) to provide event-based communication, periodic communication, unicast communication, multicast communication, broadcast communication, anycast communication, error control for communications, quality of service enabling communication, self-configuring for networking, self-healing for networking, self-optimizing for networking, self-protecting for networking, content-aware communication, location-based communication, transport acknowledgement and adaptable networking capabilities as specified in [ITU-T Y.4401], which can fulfil the communication requirements of the IoT specified in [ITU-T Y.4100].

6.2.3 IoT data management functions

The IoT-DMFs contain data storage, data processing, data querying, data access control, open information exchange, semantic data operation, and autonomic data operation capabilities as specified in [ITU-T Y.4401], which can fulfil the IoT data management requirements specified in [ITU-T Y.4100].

6.2.4 IoT service control functions

The IoT-SCFs contain service prioritization, semantic based service, service composition, mobility service, autonomic service, location-based and context aware service, service discovery, service subscription, adaptable service provision and service provision acknowledgement capabilities as specified in [ITU-T Y.4401], which can fulfil some IoT service requirements specified in [ITU-T Y.4100].

NOTE – "Autonomic service", as specified in [ITU-T Y.4401], involves automatic capture, transfer and thing data analysis capabilities, as well as automatic service provisioning based on predefined rules or policies.

6.3 The extension of reference points

The reference points extended to support the IoT can be classified into two categories: the extended reference points between the different extended functional entities to support the IoT; and the extended reference points between the extended functional entities to support the IoT and the existing functional entities specified in [ITU-T Y.2012].

The extended reference points between the different extended functional entities include those within the same extended functions to support the IoT, such as the IoT-EPFs, IoT-TCFs, IoT-DMFs and IoT-SCFs, and extended reference points between the extended functional entities that belong to different extended functions, such as the IoT-EPFs, IoT-TCFs, IoT-DMFs and IoT-SCFs, to support the IoT.

The extended reference points between the extended functional entities to support the IoT and the existing functional entities specified in [ITU-T Y.2012] include: extended reference points between IoT-EPFs and transport processing functional entities specified in [ITU-T Y.2012]; extended reference points between IoT-EPFs and service control functional entities specified in [ITU-T Y.2012]; extended reference points between IoT-TCFs and transport processing functional entities specified in [ITU-T Y.2012]; extended reference points between IoT-DMFs and content delivery functional entities specified in [ITU-T Y.2012]; extended reference points between IoT-DMFs and application support functions and service support functions specified in [ITU-T Y.2012]; extended reference points between IoT-SCFs and service control functional entities specified in [ITU-T Y.2012]; and extended reference points between IoT-SCFs and application support functions and service support functions specified in [ITU-T Y.2012].

6.4 The extension of IoT components

The extended components to support the IoT are related to the extension of NGN evolution in the deployment view as specified in [ITU-T Y.4401] in order to support IoT capabilities. The IoT end-point components, IoT transport control components, IoT data management components, and IoT service control components are four categories of the extended components. The component specified in this Recommendation refers to any functional component that can be deployed and executed independently in the context of NGN evolution.

In the IoT end-point component category, the following basic extended components are identified: IoT end-point support component; IoT device component; IoT gateway component; and IoT end-user device component.

In the IoT transport control component category, the following extended basic components are identified: IoT transport control support component; IoT transport awareness control component; IoT transport resource control component; and IoT location transport control component.

In the IoT data management component category, the following extended basic components are identified: IoT data management support component; IoT data storage control component; IoT data querying control component; IoT data processing control component; and IoT data exchange control component.

In the IoT service control component category, the following extended basic components are identified: IoT service control support component; IoT service session control component; IoT service resource control component; and IoT location service control component.

NOTE – The extended functional components specified in this Recommendation to support of IoT are only based on the principle of specifying functional components as described in [ITU-T Y.2012], in order to adopt the implementation-independent approach of specifying the IoT architecture based on NGN evolution.

6.5 Enhancement to NGNe capabilities

Enhanced capabilities to support the IoT are related to the functional entities or functional components that are specified in the NGN architecture [ITU-T Y.2012] that interact with extended functional entities or extended functional components to support the IoT.

According to the classification of these involved functional entities or functional components as specified in [ITU-T Y.2012], the enhanced capabilities to support the IoT can be classified into those for: transport functional entities; service functional entities; content delivery functional entities; application support functional entities; and the management functional component. These categories of enhanced capabilities to support the IoT are described in clause 10.

7 Functional entities extended to support the IoT

In order to support the capabilities of the IoT specified in [ITU-T Y.4401], functional entities require extension in the following categories: the IoT-EPFs, IoT-TCFs, IoT-DMFs and IoT-SCFs, which are described separately in clauses 7.1 to 7.4.

NOTE 1 – The term "knowledge" used in the following text refers to rules, policies, or other available forms that reflect the awareness or understanding of information and can be used to control network access, data transport, data management and service provision operations effectively and efficiently in the IoT.

NOTE 2 – The term "knowledge" generally refers to a familiarity, awareness or understanding of someone or something by human beings. In this Recommendation, knowledge refers to the familiarity, awareness or understanding of users, managers, contexts or applications that are related to the IoT by some extended functional entities to support the IoT.

7.1 IoT end-point functions

In order to support identification-based connectivity, thing status notification device mobility and adaptable connectivity capabilities as specified in [ITU-T Y.4401], the IoT-EPFs include following functional entities: the IoT end-point event management functional entity (IoT-EEM-FE); IoT end-point policy enforcement functional entity (IoT-EPE-FE); IoT end-point knowledge management functional entity (IoT-EKM-FE); IoT end-point access control functional entity (IoT-EAC-FE); IoT device functional entity (IoT-DV-FE); IoT gateway functional entity (IoT-GW-FE); and IoT end-user device functional entity (IoT-EUD-FE).

The functional entities specified within the IoT-EPFs, and the functional entities that interact with the IoT-EPFs are illustrated in Figure 7-1. The functional entities encased by dashed lines are specified in [ITU-T Y.2012] and are not specified again in this Recommendation.

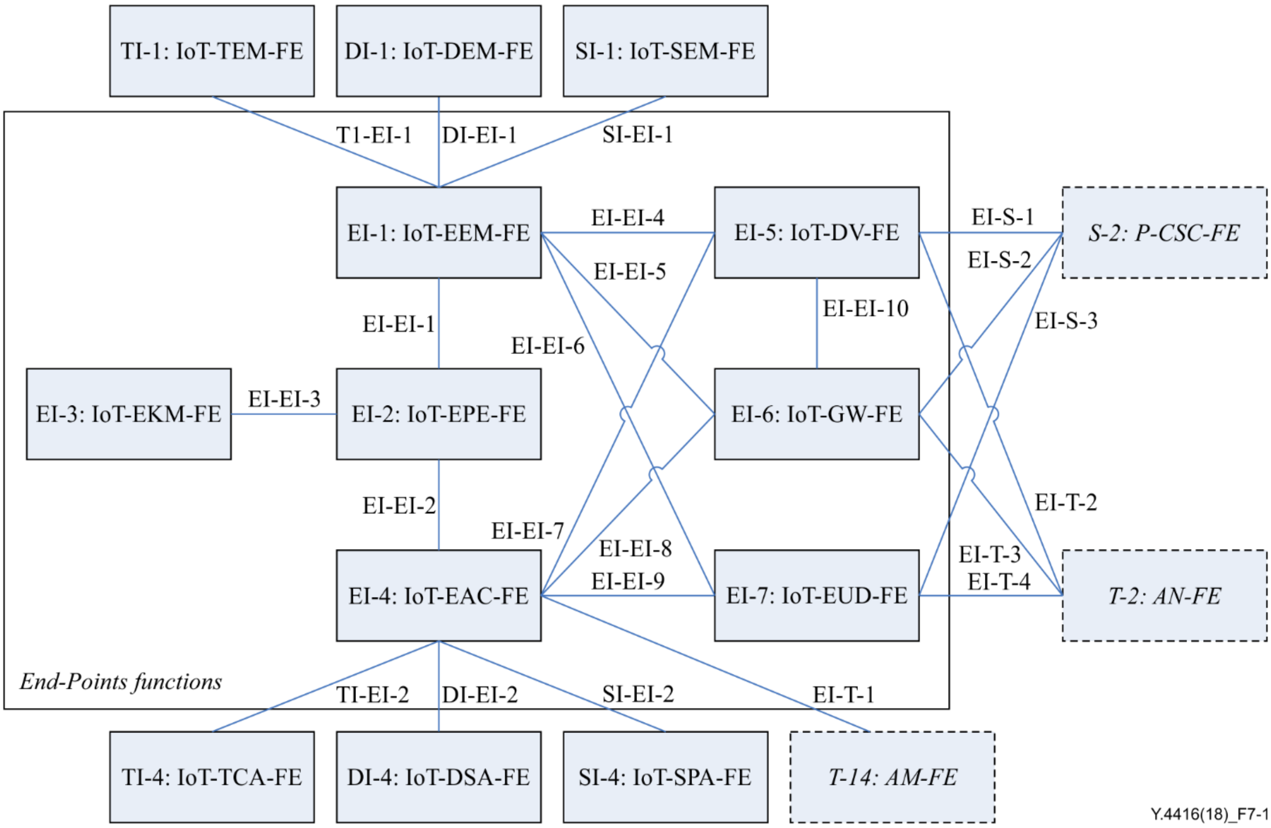

Figure 7-1 – IoT end-point related functional entities

7.1.1 EI-1: IoT end-point event management functional entity (IoT-EEM-FE)

The IoT-EEM-FE gathers information about: the events that occur in the IoT-DV-FE, IoT-GW-FE or IoT-EUD-FE of the IoT-EPFs; the events from the IoT transport event management functional entity (IoT-TEM-FE) of the IoT-TCFs; the events from the IoT service event management functional entity (IoT-SEM-FE) of the IoT-SCFs; and the events from the IoT data event management functional entity (IoT-DEM-FE) of the IoT-DMFs; determines actions based on predefined policies and derived rules in the IoT-EPFs from the IoT-EPE-FE, and may initiate other related tasks in the IoT-DV-FE, IoT-GW-FE or IoT-EUD-FE.

NOTE 1 – The derived rules in the IoT-EPFs originate from the knowledge related to the IoT-EPFs.

NOTE 2 – The IoT-EEM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by capturing events occurring in the IoT-EPFs, IoT-TCFs, IoT-SCFs, and IoT-DMFs.

7.1.2 EI-2: IoT end-point policy enforcement functional entity

The IoT-EPE-FE makes decisions based on predefined policies and knowledge related to the IoT-EPFs from the IoT-EKM-FE, considering IoT end-point access control results from the IoT-EAC-FE and the related event information from the IoT-EEM-FE.

NOTE 1 – The IoT-EPE-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by enforcing predefined policies and derived rules related to the IoT-EPFs from the IoT-EKM-FE.

NOTE 2 – The IoT-EPE-FE needs to interact with IoT management entities to introduce and update the relevant policies. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.1.3 EI-3: IoT end-point knowledge management functional entity (IoT-EKM-FE)

The IoT-EKM-FE gathers, provides and updates knowledge related to the IoT-EPFs, and provides rules derived from the end-point knowledge to the IoT-EPE-FE in order to support adaptable capabilities and autonomic capabilities in the IoT-EPFs.

NOTE 1 – It is assumed that knowledge related to the IoT-EPFs is represented in the rules, and may be regarded as derived rules and used in the IoT-EPE-FE.

NOTE 2 – The IoT-EKM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by derivation from the knowledge that is predefined and updated in the IoT-EPFs.

NOTE 3 – The IoT-EKM-FE needs to interact with IoT management entities to introduce and update the knowledge base, knowledge learning mechanisms (such as machine learning techniques) and relevant rules. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.1.4 EI-4: IoT end-point access control functional entity (IoT-EAC-FE)

The IoT-EAC-FE is the control entity in the IoT-EPFs. It accepts access requests from the IoT-DV-FE, IoT-GW-FE or IoT-EUD-FE, provides flexible access configurations to different networks based on the predefined policies and derived policies from the IoT-EPF-FE, provides authentication to different networks, and checks security and privacy protection policies and rules on access to different networks from the IoT-EPE-FE.

The IoT-EAC-FE interacts with the IoT transport configuration adaptation functional entity (IoT-TCA-FE), IoT data service adaptation functional entity (IoT-DSA-FE) and IoT service provision adaptation functional entity (IoT-SPA-FE) to coordinate operations related to the IoT, and interacts with the T-14: AM-FE specified in [ITU-T Y.2012] to coordinate operations related to the NGNe.

NOTE – It is assumed that security and privacy protection policies and rules are managed and implemented in the IoT-EPE-FE.

7.1.5 EI-5: IoT device functional entity (IoT-DV-FE)

The IoT-DV-FE gets configurations of the device-related connectivity to networks or to gateway from the IoT-EAC-FE, provides connectivity to networks or to gateways based on the identification of devices by interacting with the IoT-GW-FE, the T-2: AN-FE or the S-2: P-CSC-FE specified in [ITU-T Y.2012], collects and transfers data of things sensed by device, and supports device mobility.

7.1.6 EI-6: IoT gateway functional entity (IoT-GW-FE)

The IoT-GW-FE gets configurations of the gateway connectivity to networks from the IoT-EAC-FE, provides connectivity to networks based on the identification of gateways by interacting with the T-2: AN-FE or the S-2: P-CSC-FE specified in [ITU-T Y.2012], provides connectivity to devices based on the identification of devices, collects, buffers and transfers data of things sensed by connected devices, and executes IoT applications.

7.1.7 EI-7: IoT end-user device functional entity (IoT-EUD-FE)

The IoT-EUD-FE gets configurations of the end-user device connectivity to networks from the IoT-EAC-FE, provides connectivity to networks based on the identification of users by interacting with the T-2: AN-FE or the S-2: P-CSC-FE specified in [ITU-T Y.2012], provides capabilities, such as identification-based connectivity, provides connectivity to devices based on the identification of devices, provides user authentication, collects, buffers and transfers data of things sensed by connected devices, provides user operation interfaces, and executes IoT applications.

7.2 IoT transport control functions

In order to support event-based communication, periodic communication, quality of service enabling communication, autonomic networking (i.e., self-configuring, self-healing, self-optimizing and self-protecting networking), content-aware communication, location-based communication, transport acknowledgement, and adaptable networking capabilities as specified in [ITU-T Y.4401], the IoT-TCFs include the following functional entities: the IoT-TEM-FE; IoT transport policy enforcement functional entity (IoT-TPE-FE); IoT transport knowledge management functional entity (IoT-TKM-FE); IoT-TCA-FE; IoT transport awareness management functional entity (IoT-TAM-FE); IoT transport resource control functional entity (IoT-TRC-FE); and IoT location transport control functional entity (IoT-LTC-FE).

The functional entities specified within the IoT-TCFs and the functional entities that interact with the IoT-TCFs are illustrated in Figure 7-2. The functional entities encased by dashed lines are specified in [ITU-T Y.2012].

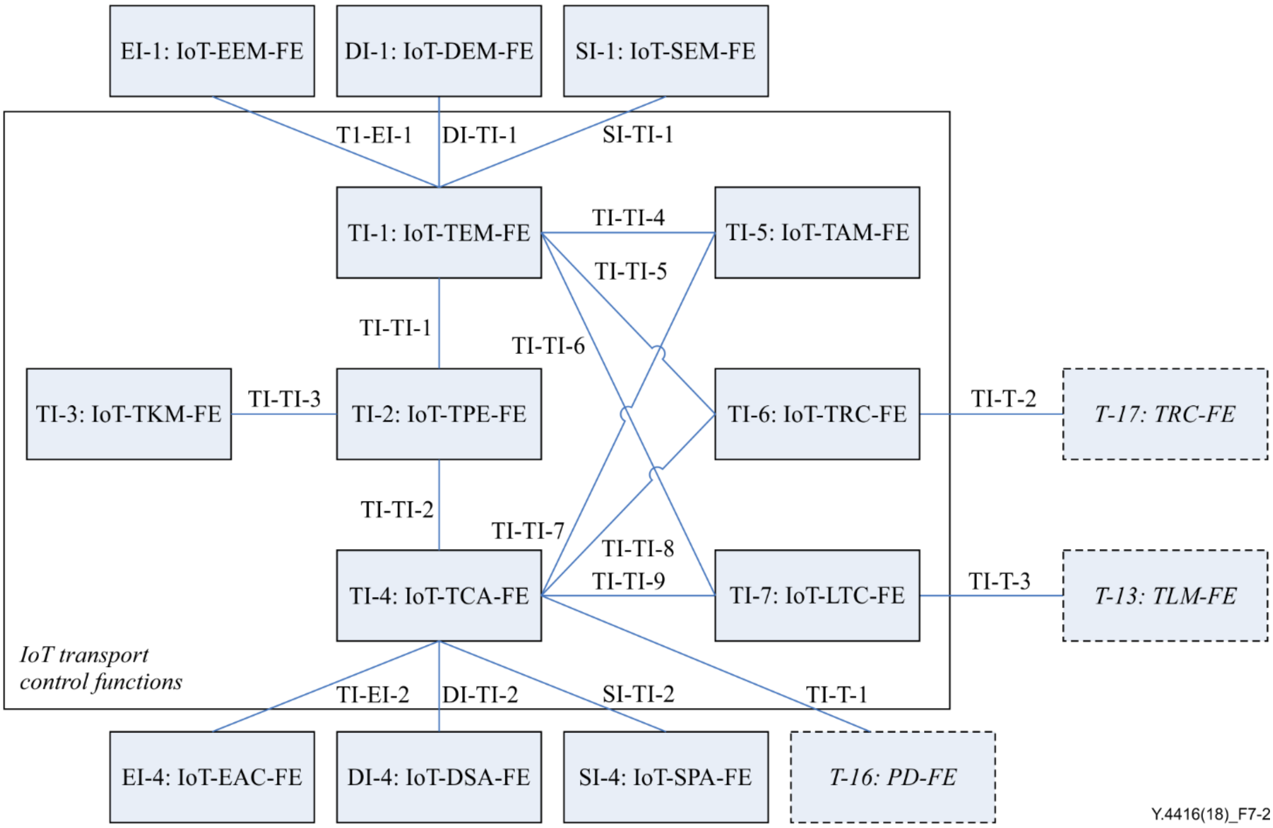

Figure 7-2 – IoT transport control functional entities

7.2.1 TI-1: IoT transport event management functional entity (IoT-TEM-FE)

The IoT-TEM-FE gathers information about the events that occur in the IoT-TAM-FE, IoT-TRC-FE or IoT-LTC-FE of the IoT-TCFs, the events from the IoT-EEM-FE of the IoT-EPFs, the events from the IoT-SEM-FE of the IoT-SCFs, and the events from the IoT-DEM-FE of the IoT-DMFs, determines actions based on predefined policies and derived rules in the IoT-TCFs from the IoT-TPE-FE, and may initiate other related tasks in the IoT-TAM-FE, IoT-TRC-FE or IoT-LTC-FE.

NOTE 1 – The derived rules in the IoT-TCFs originate from the knowledge related to the IoT-TCFs.

NOTE 2 – The IoT-TEM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by capturing events occurring in the end-point functions, the IoT-TCFs, the IoT-SCFs, and the IoT-DMFs.

7.2.2 TI-2: IoT transport policy enforcement functional entity (IoT-TPE-FE)

The IoT-TPE-FE makes decisions based on predefined policy rules and knowledge related to the IoT-TCFs, considering IoT transport configuration adaptation results, transport knowledge and the input from transport event management.

NOTE 1 – The IoT-TPE-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by enforcing predefined policies and derived rules related to the IoT-TCFs from the IoT-TKM-FE.

NOTE 2 – The IoT-TPE-FE needs to interact with IoT management entities to introduce and update the relevant policies. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.2.3 TI-3: IoT transport knowledge management functional entity (IoT-TKM-FE)

The IoT-TKM-FE gathers, provides and updates knowledge related to transport functionalities, and provides rules derived from the transport knowledge to the IoT-TPE-FE in order to support adaptable capabilities and autonomic capabilities in the IoT-TCFs.

NOTE 1 – It is assumed that knowledge related to the IoT-TCFs is represented in rules, and may be regarded as derived rules and used in the IoT-TPE-FE.

NOTE 2 – The IoT-TKM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by derivation from the knowledge that is predefined and updated in the IoT-TCFs.

NOTE 3 – The IoT-TKM-FE needs to interact with IoT management entities to introduce and update the knowledge base, knowledge learning mechanisms (such as machine learning techniques), and relevant rules. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.2.4 TI-4: IoT transport configuration adaptation functional entity (IoT-TCA-FE)

The IoT-TCA-FE is the control entity in the IoT-TCFs. It coordinates the transport requirements from the IoT-EAC-FE, IoT-DSA-FE and IoT-SPA-FE, interacts with the IoT-TAM-FE, IoT-TRC-FE and IoT-LTC-FE to gather information related to transport resources, content awareness and locations, interacts with the policy decision functional entity (T-16: PD-FE) specified in [ITU-T Y.2012] and gets the adaptable configurations.

7.2.5 TI-5: IoT transport awareness management functional entity (IoT-TAM-FE)

The IoT-TAM-FE is responsible for storing and processing content awareness events and related data, and initiating content awareness transport operations.

7.2.6 TI-6: IoT transport resource control functional entity (IoT-TRC-FE)

The IoT-TRC-FE interacts with the transport resource control functional entity (T-17: TRC-FE) specified in [ITU-T Y.2012] in order to monitor and schedule the transport resources related to IoT operations.

7.2.7 TI-7: IoT location transport control functional entity (IoT-LTC-FE)

The IoT-LTC-FE interacts with the T-13: TLM-FE specified in [ITU-T Y.2012] in order to monitor the locations of transport participants and provide location-related transport capabilities in the IoT.

7.3 IoT data management functions

In order to support data storage, data processing, data querying, data access control, open information exchange and autonomic data operation capabilities as specified in [ITU-T Y.4401], the IoT-DMFs include the following functional entities: the IoT-DEM-FE, IoT data policy enforcement functional entity (IoT-DPE-FE), IoT data knowledge management functional entity (IoT-DKM-FE), IoT-DSA-FE, IoT data storage control functional entity (IoT-DSC-FE), IoT data querying control functional entity (IoT-DQC-FE), IoT data processing control functional entity (IoT-DPC-FE) and IoT data exchange control functional entity (IoT-DEC-FE).

The functional entities specified within the IoT-DMFs and the functional entities that interact with the IoT-DMFs are illustrated in Figure 7-3. The functional entities encased by dashed lines are specified in [ITU-T Y.2012].

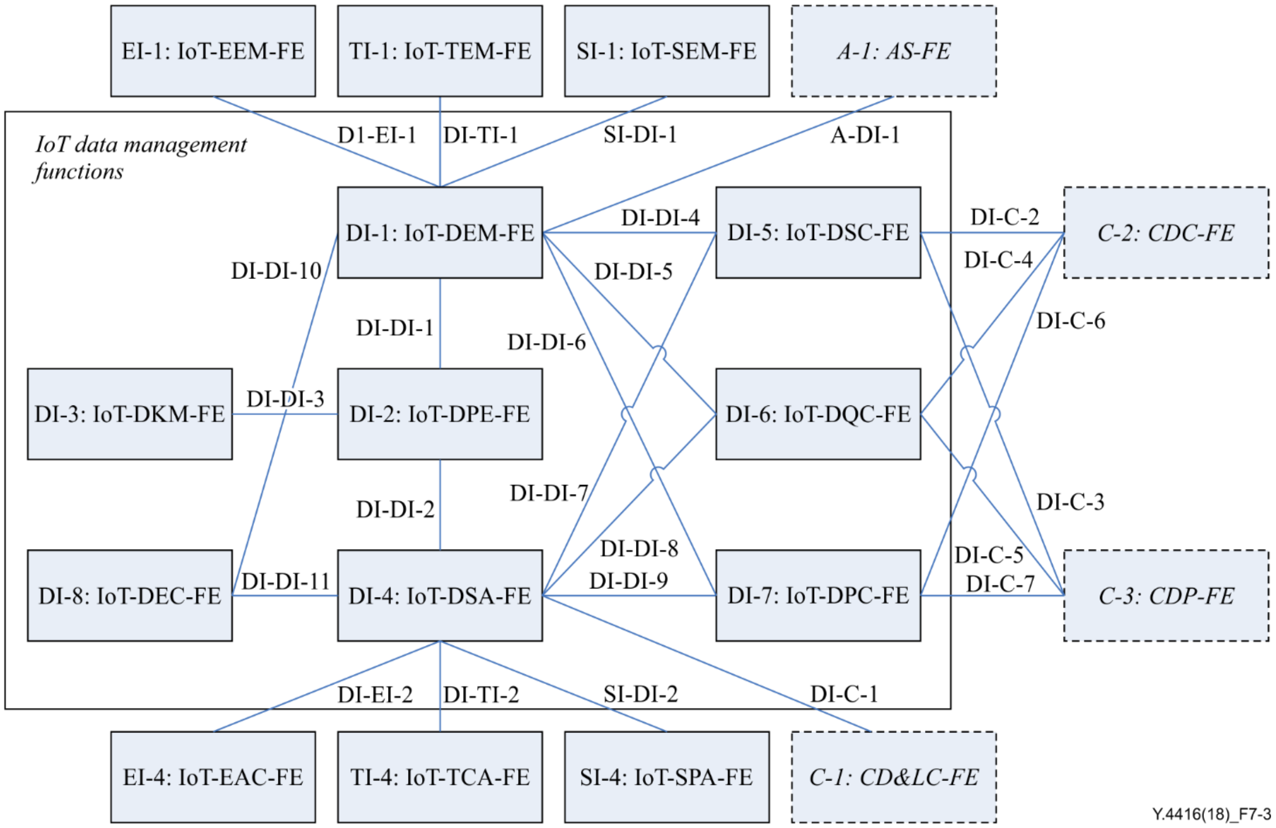

Figure 7-3 – IoT data management functional entities

7.3.1 DI-1: IoT data event management functional entity (IoT-DEM-FE)

The IoT-DEM-FE gathers information about the events that occur in the IoT-DSC-FE, IoT-DQC-FE, IoT-DPC-FE or IoT-DEC-FE of the IoT-DMFs, the events from the IoT-TEM-FE of the IoT-TCFs, the events from the IoT-SEM-FE of the IoT-SCFs, and the events from the IoT-EEM-FE of the end-points functions, determines actions based on predefined policies and derived rules in the IoT-DMFs, and may initiate other related tasks in the IoT-DSC-FE, IoT-DQC-FE, IoT-DPC-FE or IoT-DEC-FE.

The IoT-DEM-FE interacts with application support functional entity (A-1: AS-FE) specified in [ITU-T Y.2012], in order to provide IoT data services in an adaptable way required by different applications.

NOTE 1 – The derived rules in the IoT-DMFs originate from the knowledge related to the IoT-DMFs.

NOTE 2 – The IoT-DEM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by capturing events occurring in the end-points functions, the IoT-TCFs, the IoT-SCFs, and the IoT-DMFs.

7.3.2 DI-2: IoT data policy enforcement functional entity (IoT-DPE-FE)

The IoT-DPE-FE makes decisions based on predefined policies and knowledge related to the IoT-DMFs from the IoT-DKM-FE, and considering IoT data service adaptation results from the IoT-DSA-FE, and the related event information from the IoT-DEM-FE.

NOTE 1 – The IoT-DPE-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by enforcing predefined policies related to the IoT-DMFs and derived rules from the IoT-DKM-FE.

NOTE 2 – The IoT-DPE-FE needs to interact with IoT management entities to introduce and update the relevant policies. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.3.3 DI-3: IoT data knowledge management functional entity (IoT-DKM-FE)

The IoT-DKM-FE gathers, provides and updates knowledge related to the IoT-DMFs, and provides rules derived from the data knowledge to the IoT-DPE-FE in order to support adaptable capabilities and autonomic capabilities in the IoT-DMFs.

NOTE 1 – It is assumed that knowledge related to the IoT-DMFs is represented in rules, and may be regarded as derived rules and used in the IoT-DPE-FE.

NOTE 2 – The IoT-DKM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by derivation from the knowledge that is predefined and updated in the IoT-DMFs.

NOTE 3 – The IoT-DKM-FE needs to interact with IoT management entities to introduce and update the knowledge base, knowledge learning mechanisms (such as machine learning techniques), and relevant rules. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.3.4 DI-4: IoT data service adaptation functional entity (IoT-DSA-FE)

The IoT-DSA-FE is the control entity in the IoT-DMFs. It controls the IoT data operations that occur in the IoT-DSC-FE, the IoT-DQC-FE, the IoT-DPC-FE and the IoT-DEC-FE. It coordinates the IoT data operations with the IoT-EAC-FE, the IoT-TCA-FE and the IoT-SPA-FE in order to provide IoT data-related services. It interacts with the C-1: CD&LC-FE specified in [ITU-T Y.2012] in order to cope with the IoT multimedia data, especially the IoT video or audio data.

7.3.5 DI-5: IoT data storage control functional entity (IoT-DSC-FE)

The IoT-DSC-FE is responsible for storing and transferring IoT data based on the internal resource requirements and the external application requirements. It interacts with the C-2: CDC-FE and the C-3: CDP-FE specified in [ITU-T Y.2012] in order to cope with IoT multimedia data storage, especially IoT video or audio data storage.

7.3.6 DI-6: IoT data querying control functional entity (IoT-DQC-FE)

The IoT-DQC-FE is responsible for monitoring, performing and controlling IoT data querying. It interacts with the C-2: CDC-FE and the C-3: CDP-FEspecified in [ITU-T Y.2012] in order to cope with IoT multimedia data querying, especially IoT video or audio data querying.

7.3.7 DI-7: IoT data processing control functional entity (IoT-DPC-FE)

The IoT-DPC-FE is responsible for monitoring, performing and controlling IoT data processing. It interacts with the C-2: CDC-FE and the C-3: CDP-FE specified in [ITU-T Y.2012] in order to cope with IoT multimedia data processing, especially IoT video or audio data processing.

7.3.8 DI-8: IoT data exchange control functional entity (IoT-DEC-FE)

The IoT-DEC-FE is responsible for monitoring, performing and controlling data exchange with the functional entities that are outside the IoT, such as the functional entities implemented in data centres in specific application domains.

NOTE – Description of the functional entities to interact with the IoT-DEC-FE, such as the data exchange control functional entities specified and implemented in data centres, lies outside the scope of this Recommendation.

7.4 IoT service control functions

In order to support service prioritization, service composition, autonomic service, location-based and context aware service, mobility service and adaptable service provision capabilities as specified in [ITU-T Y.4401], the IoT-SCFs include the following functional entities: the IoT-SEM-FE, IoT service policy enforcement functional entity (IoT-SPE-FE), IoT service knowledge management functional entity (IoT-SKM-FE), IoT-SPA-FE, IoT service session control functional entity (IoT-SSC-FE), IoT service resource control functional entity (IoT-SRC-FE) and IoT location service control functional entity (IoT-LSC-FE).

The functional entities specified within the IoT-SCFs and the functional entities that interact with the IoT-SCFs are illustrated in Figure 7-4. The functional entities encased by dashed lines are specified in [ITU-T Y.2012].

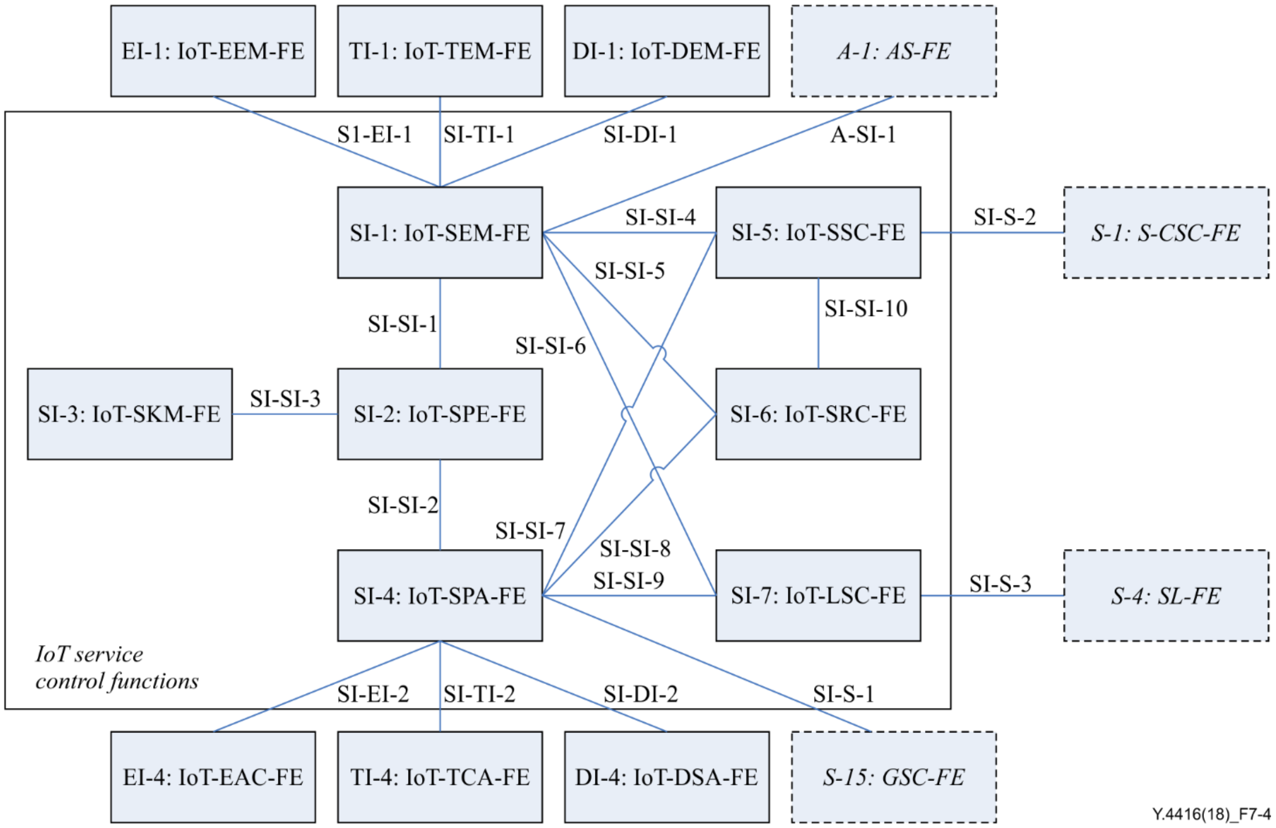

Figure 7-4 – IoT service control functional entities

7.4.1 SI-1: IoT service event management functional entity (IoT-SEM-FE)

The IoT-SEM-FE gathers information about the events that occur in the IoT-SSC-FE, IoT-SRC-FE or IoT-LSC-FE of the IoT-SCFs, the events from the IoT-TEM-FE of the IoT-TCFs, the events from the IoT-SEM-FE of the IoT-SCFs and the events from the IoT-EEM-FE of the end-points functions, determines actions based on predefined policies and derived rules in the IoT-SCFs from the IoT-SPE-FE, and may initiate other related tasks in the IoT-SSC-FE, IoT-SRC-FE or IoT-LSC-FE.

The IoT-SEM-FE interacts with the A-1: AS-FE specified in [ITU-T Y.2012], in order to provide IoT services in an adaptable way required by different applications.

NOTE 1 – The derived rules in the IoT-SCFs originate from the knowledge related to the IoT-SCFs.

NOTE 2 – The IoT-SEM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by capturing events occurring in the end-point functions, the IoT-TCFs, the IoT-SCFs and the IoT-DMFs.

7.4.2 SI-2: IoT service policy enforcement functional entity (IoT-SPE-FE)

The IoT-SPE-FE makes decisions based on predefined policies and rules derived from knowledge related to the IoT-SCFs from the IoT-SKM-FE, and considers IoT service provision adaptation results from the IoT-SPA-FE and the related event information from the IoT-SEM-FE.

NOTE 1 – The IoT-SPE-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by enforcing predefined policies related to the IoT-SCFs and derived rules from the IoT-SKM-FE.

NOTE 2 – The IoT-SPE-FE needs to interact with IoT management entities to introduce and update the relevant policies. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.4.3 SI-3: IoT service knowledge management functional entity (IoT-SKM-FE)

The IoT-SKM-FE gathers, provides and updates knowledge related to the IoT-SCFs, and provides rules derived from the service knowledge to the IoT-SPE-FE in order to support adaptable capabilities and autonomic capabilities in the IoT-SCFs.

NOTE 1 – It is assumed that knowledge related to the IoT-SCFs is represented in rules, and may be regarded as derived rules and used in the IoT-SPE-FE.

NOTE 2 – The IoT-SKM-FE can be used to support autonomic operations specified in [ITU-T Y.4401] by derivation from the knowledge that is predefined and updated in the IoT-SCFs.

NOTE 3 – The IoT-SKM-FE needs to interact with IoT management entities to introduce and update the knowledge base, knowledge learning mechanisms (such as machine learning techniques) and relevant rules. These capabilities and relevant reference points lie outside the scope of this Recommendation.

7.4.4 SI-4: IoT service provision adaptation functional entity (IoT-SPA-FE)

The IoT-SPA-FE is a control entity in the IoT-SCFs. It coordinates the IoT service-related operations with the IoT-EAC-FE, the IoT-TCA-FE and the IoT-DSA-FE in order to provide IoT adaptable services. It interacts with the S-15: GSC-FE specified in [ITU-T Y.2012], in order to use existing NGN service capabilities to support IoT services.

7.4.5 SI-5: IoT service session control functional entity (IoT-SSC-FE)

The IoT-SSC-FE is responsible for monitoring, performing and controlling session-related IoT services. It interacts with the S-1: S-CSC-FE specified in [ITU-T Y.2012], in order to use existing NGN service capabilities.

NOTE 1 – The IoT-SSC-FE provides the capability related to IoT session control, e.g., session setup, modification and teardown related to IoT services.

NOTE 2 – The IoT-SSC-FE may interact with the IoT-SRC-FE in order to guarantee that the resources required by the service can be fulfilled by the other parties in the session. The occurrence of this interaction between the IoT-SSC-FE and IoT-SRC-FE depends on the quality of service required by IoT customers.

7.4.6 SI-6: IoT service resource control functional entity (IoT-SRC-FE)

The IoT-SRC-FE is responsible for monitoring and scheduling resources related to IoT service provisioning.

NOTE – The resources monitored and distributed by the IoT-SRC-FE are specific to the IoT capabilities and are related to the IoT service provisioning, such as IoT data identification, IoT data storage and IoT data processing.

7.4.7 SI-7: IoT location service control functional entity (IoT-LSC-FE)

The IoT-LSC-FE interacts with the S-4: SL-FE specified in [ITU-T Y.2012] in order to monitor the locations of service subscribers.

The location traced or positioned by the IoT-LSC-FE is not only limited within that subscriber location as that located by the S-4: SL-FE specified in [ITU-T Y.2012], but also includes the location of things and service providers related to the IoT service provisioning in order to support location-based and context aware services in the IoT specified in [ITU-T Y.4401].

8 Reference points extended to support the IoT

The reference points extended to support the IoT include those internal to the IoT-EPFs, internal to the IoT-TCFs, internal to the IoT-DMFs, internal to the IoT-SCFs, and among the IoT-EPFs, IoT-TCFs, IoT-DMFs and IoT-SCFs that are the extended functions to support the IoT.

NOTE 1 – The extended reference points internal to the IoT-EPFs refer to the extended reference points between the different extended functional entities that are internal to the IoT-EPFs. Similar explanations can be used for extended reference points internal to the IoT-TCFs, internal to the IoT-DMFs, and internal to the IoT-SCFs.

The reference points extended to support the IoT also include those between the IoT-EPFs and transport processing functional entities specified in [ITU-T Y.2012], between the IoT-EPFs and service control functional entities specified in [ITU-T Y.2012], between the IoT-TCFs and transport processing functional entities specified in [ITU-T Y.2012], between the IoT-DMFs and content delivery functional entities specified in [ITU-T Y.2012], between the IoT-DMFs and application support functions and service support functions specified in [ITU-T Y.2012], between the IoT-SCFs and service control functional entities specified in [ITU-T Y.2012], and extended reference points between the IoT-SCFs and application support functions and service support functions specified in [ITU-T Y.2012].

NOTE 2 – From the implementation perspective, the extended reference points defined in this Recommendation can be simplified, but this lies outside the scope of this Recommendation.

8.1 Extended reference points internal to IoT-end-point functions

The extended reference points between the functional entities in the IoT-EPFs are as follows.

- Reference point EI-EI-1 between EI-1: IoT-EEM-FE and EI-2: IoT-EPE-FE, it can be used by the IoT-EEM-FE to make decisions based on predefined policies enforced by the IoT-EPE-FE when an event occurs.
- Reference point EI-EI-2 between EI-4: IoT-EAC-FE and EI-2: IoT-EPE-FE, it can be used by the IoT-EAC-FE to request or perform end-point access control based on predefined policies enforced by the IoT-EPE-FE.
- Reference point EI-EI-3 between EI-3: IoT-EKM-FE and EI-2: IoT-EPE-FE, it can be used by the IoT-EKM-FE to derive and update the knowledge based on predefined policies enforced by the IoT-EPE-FE.
- Reference point EI-EI-4 between EI-1: IoT-EEM-FE and EI-5: IoT-DV-FE, it can be used by the IoT-EEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-DV-FE.
- Reference point EI-EI-5 between EI-1: IoT-EEM-FE and EI-6: IoT-GW-FE, it can be used by the IoT-EEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-GW-FE.
- Reference point EI-EI-6 between EI-1: IoT-EEM-FE and EI-7: IoT-EUD-FE, it can be used by the IoT-EEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-EDU-FE.
- Reference point EI-EI-7 between EI-4: IoT-EAC-FE and EI-5: IoT-DV-FE, it can be used by the IoT-EAC-FE to request or perform access control on the IoT-DV-FE.
- Reference point EI-EI-8 between EI-4: IoT-EAC-FE and EI-6: IoT-GW-FE, it can be used by the IoT-EAC-FE to request or perform access control on the IoT-GW-FE.
- Reference point EI-EI-9 between EI-4: IoT-EAC-FE and EI-7: IoT-EUD-FE, it can be used by the IoT-EAC-FE to request or perform access control on the IoT-EUD-FE
- Reference point EI-EI-10 between EI-5: IoT-DV-FE and EI-6: IoT-GW-FE, it can be used by the IoT-DV-FE to connect with the IoT-GW-FE to transfer data to the IoT.

8.2 Extended reference points internal to IoT transport control functions

The extended reference points between the functional entities in the IoT-TCFs are as follows.

- Reference point TI-TI-1 between TI-1: IoT-TEM-FE and TI-2: IoT-TPE-FE, it can be used by the IoT-TEM-FE to make decisions based on predefined policies enforced by the IoT-TPE-FE when an event occurs.

- Reference point TI-TI-2 between TI-4: IoT-TCA-FE and TI-2: IoT-TPE-FE, it can be used by the IoT-TCA-FE to request or perform transport configuration adaptation based on predefined policies enforced by the IoT-TPE-FE.
- Reference point TI-TI-3 between TI-3: IoT-TKM-FE and TI-2: IoT-TPE-FE, it can be used by the IoT-TKM-FE to derive and update the knowledge based on predefined policies enforced by the IoT-TPE-FE.
- Reference point TI-TI-4 between TI-1: IoT-TEM-FE and TI-5: IoT-TAM-FE, it can be used by the IoT-TEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-TAM-FE.
- Reference point TI-TI-5 between TI-1: IoT-TEM-FE and TI-6: IoT-TRC-FE, it can be used by the IoT-TEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-TRC-FE.
- Reference point TI-TI-6 between TI-1: IoT-TEM-FE and TI-7: IoT-LTC-FE, it can be used by the IoT-TEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-LTC-FE.
- Reference point TI-TI-7 between TI-4: IoT-TCA-FE and TI-5: IoT-TAM-FE, it can be used by the IoT-TCA-FE to request or perform transport configuration adaptation based on events occurring in the IoT-TAM-FE.
- Reference point TI-TI-8 between TI-4: IoT-TCA-FE and TI-6: IoT-TRC-FE, it can be used by the IoT-TCA-FE to request or perform transport configuration adaptation based on events occurring in the IoT-TRC-FE.
- Reference point TI-TI-9 between TI-4: IoT-TCA-FE and TI-7: IoT-LTC-FE, it can be used by the IoT-TCA-FE to request or perform transport configuration adaptation based on events occurring in the IoT-LTC-FE.

8.3 Extended reference points internal to IoT-data management functions

The extended reference points between the functional entities in IoT-DMFs are as follows.

- Reference point DI-DI-1 between DI-1: IoT-DEM-FE and DI-2: IoT-DPE-FE, it can be used by the IoT-DEM-FE to make decisions based on predefined policies enforced by the IoT-DPE-FE when an event occurs.
- Reference point DI-DI-2 between DI-4: IoT-DSA-FE and DI-2: IoT-DPE-FE, it can be used by the IoT-DSA-FE to request or perform data service adaptation based on predefined policies enforced by the IoT-DPE-FE.
- Reference point DI-DI-3 between DI-3: IoT-DKM-FE and DI-2: IoT-DPE-FE, it can be used by the IoT-DKM-FE to derive and update the knowledge based on predefined policies enforced by the IoT-DPE-FE.
- Reference point DI-DI-4 between DI-1: IoT-DEM-FE and DI-5: IoT-DSC-FE can be used by the IoT-DEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-DSC-FE.
- Reference point DI-DI-5 between DI-1: IoT-DEM-FE and DI-6: IoT-DQC-FE, it can be used by the IoT-DEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-DQC-FE.
- Reference point DI-DI-6 between DI-1: IoT-DEM-FE and DI-7: IoT-DPC-FE, it can be used by the IoT-DEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-DPC-FE.
- Reference point DI-DI-7 between DI-4: IoT-DSA-FE and DI-5: IoT-DSC-FE, it can be used by the IoT-DSA-FE to request or perform data service adaptation based on events occurring in the IoT-DSC-FE.

- Reference point DI-DI-8 between DI-4: IoT-DSA-FE and DI-6: IoT-DQC-FE, it can be used by the IoT-DSA-FE to request or perform data service adaptation based on events occurring in the IoT-DQC-FE.
- Reference point DI-DI-9 between DI-4: IoT-DSA-FE and DI-7: IoT-DPC-FE, it can be used by the IoT-DSA-FE to request or perform data service adaptation based on events occurring in the IoT-DPC-FE.
- Reference point DI-DI-10 between DI-8: IoT-DEC-FE and DI-1: IoT-DEM-FE, it can be used by the IoT-DEM-FE in a timely fashion to request or respond to the service request or other events occurring in the IoT-DEC-FE.
- Reference point DI-DI-11 between DI-8: IoT-DEC-FE and DI-4: IoT-DSA-FE, it can be used by the IoT-DSA-FE to request or perform data service adaptation based on events occurring in the IoT-DEC-FE.

8.4 Extended reference points internal to IoT-service control functions

The extended reference points between the functional entities in the IoT-SCFs are as follows:

- Reference point SI-SI-1 between SI-1: IoT-SEM-FE and SI-2: IoT-SPE-FE, it can be used by the IoT-SEM-FE to make decisions based on predefined policies enforced by the IoT-SPE-FE when an event occurs.
- Reference point SI-SI-2 between SI-2: IoT-SPE-FE and SI-4: IoT-SPA-FE, it can be used by the IoT-SPA-FE to request or perform service provision adaptation based on predefined policies enforced by the IoT-SPE-FE.
- Reference point SI-SI-3 between SI-2: IoT-SPE-FE and SI-3: IoT-SKM-FE, it can be used by the IoT-SKM-FE to derive and update the knowledge based on predefined policies enforced by the IoT-SPE-FE.
- Reference point SI-SI-4 between SI-1: IoT-SEM-FE and SI-5: IoT-SSC-FE, it can be used by the IoT-SEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-SSC-FE.
- Reference point SI-SI-5 between SI-1: IoT-SEM-FE and SI-6: IoT-SRC-FE, it can be used by the IoT-SEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-SRC-FE.
- Reference point SI-SI-6 between SI-1: IoT-SEM-FE and SI-7: IoT-LSC-FE, it can be used by the IoT-SEM-FE in a timely fashion to indicate or respond to the service request or other events occurring in the IoT-LSC-FE.
- Reference point SI-SI-7 between SI-5: IoT-SSC-FE and SI-4: IoT-SPA-FE, it can be used by the IoT-SPA-FE to request or perform service provision adaptation based on the events occurring in the IoT-SSC-FE.
- Reference point SI-SI-8 between SI-6: IoT-SRC-FE and SI-4: IoT-SPA-FE, it can be used by the IoT-SPA-FE to request or perform service provision adaptation based on the events occurring in the IoT-SRC-FE.
- Reference point SI-SI-9 between SI-7: IoT-LSC-FE and SI-4: IoT-SPA-FE, it can be used by the IoT-SPA-FE to request or perform service provision adaptation based on the events occurring in the IoT-LSC-FE.
- Reference point SI-SI-10 between SI-5: IoT-SSC-FE and SI-6: IoT-SRC-FE, it can be used by the IoT-SSC-FE to provide quality-constrained service through the relevant resource allocation from the IoT-SRC-FE.

8.5 Extended reference points external to IoT-end-point functions

The extended reference points between a functional entity of the IoT-EPFs and a functional entity outside the IoT-EPFs are as follows.

- Reference point EI-T-1 between EI-4: IoT-EAC-FE and T-14: AM-FE, it can be used to set or get the information about the access networks for implementing specific access control.
- Reference point EI-T-2 between EI-5: IoT-DV-FE and T-2: AN-FE, it can be used to connect IoT devices with existing networks, such as the Internet if the AN-FE is Internet protocol (IP) capable.
- Reference point EI-T-3 between EI-6: IoT-GW-FE and T-2: AN-FE, it can be used to connect IoT gateways with existing networks, such as the Internet if the AN-FE is IP capable.
- Reference point EI-T-4 between EI-7: IoT-EUD-FE and T-2: AN-FE, it can be used to connect end-user devices with existing networks, such as the Internet if the AN-FE is IP capable.
- Reference point EI-S-1 between EI-5: IoT-DV-FE and S-2: P-CSC-FE, it can be used to initiate, teardown and maintain an IoT device session required by IoT applications or forward an IoT device session request from IoT devices.
- Reference point EI-S-2 between EI-6: IoT-GW-FE and S-2: P-CSC-FE, it can be used to initiate, teardown and maintain an IoT gateway session required by IoT applications or forward an IoT gateway session request from IoT devices.
- Reference point EI-S-3 between EI-7: IoT-EUD-FE and S-2: P-CSC-FE, it can be used to initiate, teardown and maintain an end-user device session required by IoT applications or forward an end-user device session request from IoT devices.

NOTE – The extended reference points external to IoT-EPFs that are not specified in this clause are specified in clauses 8.6 to 8.8.

8.6 Extended reference points external to IoT transport control functions

The extended reference points between a functional entity of the IoT-TCFs and a functional entity outside of the IoT-TCFs are as follows.

- Reference point TI-EI-1 between TI-1: IoT-TEM-FE and EI-1: IoT-EEM-FE, it can be used to exchange event occurring notifications between the IoT-TEM-FE and IoT-EEM-FE.
- Reference point TI-EI-2 between TI-4: IoT-TCA-FE and EI-4: IoT-EAC-FE, it can be used to coordinate the configuration and adaptation activities between the IoT-TCA-FE and IoT-EAC-FE.
- Reference point TI-T-1 between TI-4: IoT-TCA-FE and T-16: PD-FE, it can be used to adjust the configuration of the IoT transport in order to adapt to the rules of existing networks.
- Reference point TI-T-2 between TI-6: IoT-TRC-FE and T-17: TRC-FE, it can be used to detect and determine the requested quality of services along the specific path in existing networks.
- Reference point TI-T-3 between TI-7: IoT-LTC-FE and T-13: TLM-FE, it can be used to set or get the specific location information from the existing networks to provide its location awareness transport control capacities.

NOTE – The extended reference points external to the IoT-TCFs that are not specified in this clause are specified in clauses 8.7 and 8.8.

8.7 Extended reference points external to IoT-DMF

The extended reference points between a functional entity of the IoT-DMFs and a functional entity outside of the IoT-DMF are as follows.

- Reference point DI-EI-1 between DI-1: IoT-DEM-FE and EI-1: IoT-EEM-FE, it can be used to exchange event occurring notifications between the IoT-DEM-FE and IoT-EEM-FE.
- Reference point DI-EI-2 between DI-4: IoT-DSA-FE and EI-4: IoT-EAC-FE, it can be used to coordinate configuration and adaptation activities between the IoT-DSA-FE and IoT-EAC-FE.
- Reference point DI-TI-1 between DI-1: IoT-DEM-FE and TI-1: IoT-TEM-FE, it can be used to exchange event occurring notifications between the IoT-DEM-FE and IoT-TEM-FE.
- Reference point DI-TI-2 between DI-4: IoT-DSA-FE and EI-4: IoT-TCA-FE, it can be used to coordinate configuration and adaptation activities between the IoT-DSA-FE and IoT-TCA-FE.
- Reference point DI-C-1 between DI-4: IoT-DSA-FE and C-1: CD&LC-FE, it can be used to control the distribution of the IoT data, gather information related to processing of IoT data and adapt to the data management requirements of IoT applications.
- Reference point DI-C-2 between DI-5: IoT-DSC-FE and C-2: CDC-FE, it can be used by the IoT-DSC-FE to control the transfer of IoT data into existing networks and report the controlling status.
- Reference point DI-C-3 between DI-5: IoT-DSC-FE and C-3: CDP-FE, it can be used by the IoT-DSC-FE to cache, store and deliver IoT data to end-point devices based on the requirements of IoT applications through using existing networks.
- Reference point DI-C-4 between DI-6: IoT-DQC-FE and C-2: CDC-FE, it can be used by the IoT-DQC-FE to control the transfer of IoT data into existing networks and report the controlling status.
- Reference point DI-C-5 between DI-6: IoT-DQC-FE and C-3: CDP-FE, it can be used by the IoT-DQC-FE to cache, store and deliver IoT data to end-point devices based on the requirements of IoT applications through using existing networks.
- Reference point DI-C-6 between DI-7: IoT-DPC-FE and C-2: CDC-FE, it can be used by the IoT-DPC-FE to control the transfer of IoT data into existing networks and report the controlling status.
- Reference point DI-C-7 between DI-7: IoT-DPC-FE and C-3: CDP-FE, it can be used by the IoT-DPC-FE to cache, store and deliver IoT data to end-point devices based on the requirements of IoT applications through using the existing networks.
- Reference point A-DI-1 between A-1: AS-FE and C-3: IoT-DEM-FE, it can be used by the IoT-DEM-FE to indicate or accept data management requests from IoT applications.

NOTE – The extended reference points external to IoT-DMF that are not specified in this clause are specified in clause 8.8.

8.8 Extended reference points external to IoT-service control functions

The extended reference points between a functional entity of the IoT-SCFs and a functional entity outside the IoT-SCFs are as follows.

- Reference point SI-EI-1 between SI-1: IoT-SEM-FE and EI-1: IoT-EEM-FE, it can be used to exchange event occurring notifications between the IoT-SEM-FE and IoT-EEM-FE.
- Reference point SI-EI-2 between SI-4: IoT-SPA-FE and EI-4: IoT-EAC-FE, it can be used to coordinate configuration and adaptation activities between the IoT-SPA-FE and IoT-EAC-FE.
- Reference point SI-TI-1 between SI-1: IoT-SEM-FE and TI-1: IoT-TEM-FE, it can be used to exchange event occurring notifications between the IoT-SEM-FE and IoT-TEM-FE.
- Reference point SI-TI-2 between SI-4: IoT-SPA-FE and EI-4: IoT-TCA-FE, it can be used to coordinate configuration and adaptation activities between IoT-SPA-FE and IoT-TCA-FE.

- Reference point SI-DI-1 between SI-1: IoT-SEM-FE and DI-1: IoT-DEM-FE, it can be used to exchange event occurring notifications between the IoT-SEM-FE and IoT-DEM-FE.
- Reference point SI-DI-2 between SI-4: IoT-SPA-FE and DI-4: IoT-DSA-FE, it can be used to coordinate the configuration and adaptation activities between the IoT-SPA-FE and IoT-DSA-FE.
- Reference point SI-S-1 between SI-4: IoT-SPA-FE and S-15: GSC-FE, it can be used to request or confirm provisioning of the existing network services that do not require initiating and maintaining network-mediated session functionalities.
- Reference point SI-S-2 between SI-5: IoT-SSC-FE and S-1: S-CSC-FE, it can be used to initiate, teardown and maintain a device-to-device session required by IoT applications.
- Reference point SI-S-3 between SI-7: IoT-LSC-FE and S-4: SL-FE, it can be used to set or get the location for holding the service subscriber data.
- Reference point A-SI-1 between A-1: AS-FE and SI-1: IoT-SEM-FE, it can be used by the IoT-SEM-FE to indicate or accept service requests from IoT applications.

9 Components extended to support the IoT

In this Recommendation, a component refers to a functional component that can be deployed and executed independently in the context of NGN evolution. The extended components to support the IoT are related to the extension of NGN evolution in the deployment view [ITU-T Y.4401] in order to support IoT capabilities. The classification of extended components to support the IoT in the context of NGN evolution is illustrated in Figure 9-1. The IoT end-point components, IoT transport control components, IoT data management components and IoT service control components are four categories of extended components, indicated by green boxes.

In Figure 9-1, the blue lines indicate possible interactions related to NGNe service components, the green lines possible interactions related to transport networks, the red lines the possible interactions related to the IoT service control components, the brown lines the possible interaction related to the IoT data management components, the purple lines the possible interactions related to NGNe transport control components, the black line the possible interactions among different service platforms, and the pink lines the possible interaction related to the management and privacy protection components.

In Figure 9-1, the dashed lines illustrate interactions that lie outside the scope of this Recommendation, as are the components encased by dashed lines.

NOTE 1 – The IoT data management components and IoT service control components may be deployed in one or several service platforms [ITU-T Y.4401] that can be interconnected with other service platforms.

NOTE 2 – The categories of the extended components can also be regarded as different classes of the extended components, that is, the IoT end-point component class, the IoT transport control component class, the IoT data management component class and the IoT service control component class. These four classes of extended components can be instantiated into deployable extended components based on current technologies. For example, the class of the IoT end-point component can be now instantiated into the IoT end-point support component, the IoT device component, the IoT gateway component and the IoT end-user device component that can be implemented and deployed by applying current technologies.

NOTE 3 – The number for each extended component given in this clause consists of three parts: The first is "CN", i.e., the abbreviation for "component number". The second is a letter of the alphabet that represents the category to which the extended component belongs, i.e.: "E" represents the IoT end-point component category; "T" represents the IoT transport control component category; "D" represents the IoT data management component category; and "S" represents the IoT service control component category. The third is the digit that represents the sequential number of the component in the same category of extended components.

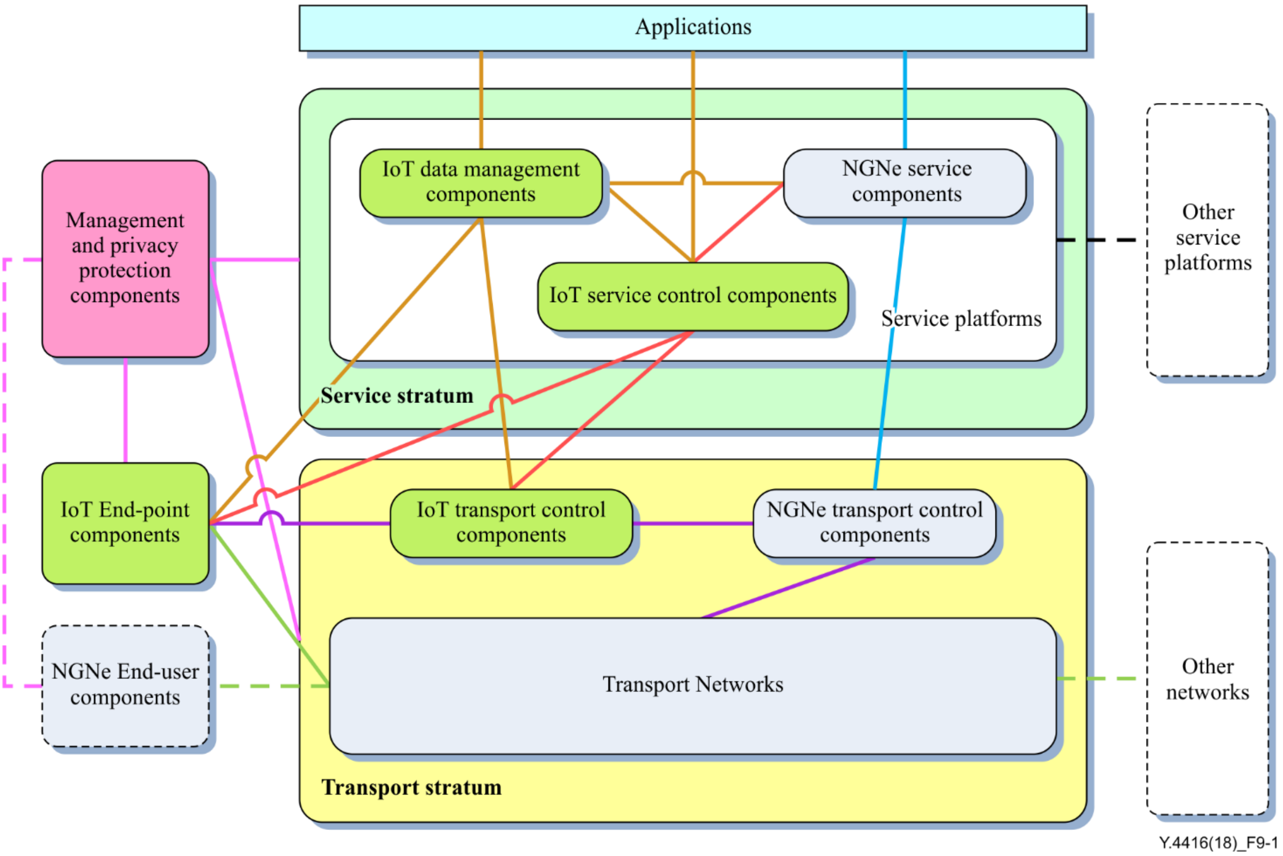

Figure 9-1 – The extended components in the context of NGNe

9.1 IoT end-point components

In the IoT end-point component category, the following basic extended components are identified: IoT end-point support component; IoT device component; IoT gateway component; and IoT end-user device component.

The number, name, functionalities and included functional entities, described in clause 7, of these extended components are listed in Table 1.

Table 1 – List of IoT end-point components

Component number	Component name	Component functionalities	Included functional entities
CN-E-1	IoT end-point support component	– Manages events related to IoT end-point components – Makes decisions on access control and configurable control of the IoT end-point components	EI-1: IoT-EEM-FE EI-2: IoT-EPE-FE EI-3: IoT-EKM-FE EI-4: IoT-EAC-FE
CN-E-2	IoT device component	– Configures devices for connecting with networks or gateways – Provides connectivity with networks or gateways based on the identification of devices – Collects and transfers data of things – Executes IoT applications if it is required	EI-1: IoT-EEM-FE EI-2: IoT-EPE-FE EI-3: IoT-EKM-FE EI-4: IoT-EAC-FE EI-5: IoT-DV-FE

Table 1 – List of IoT end-point components

Component number	Component name	Component functionalities	Included functional entities
CN-E-3	IoT gateway component	– Configures gateways for connecting with networks – Provides connectivity with networks based on the identification of devices – Collects, buffers, and transfers data of things – Provides application support services, and executes IoT applications	EI-1: IoT-EEM-FE EI-2: IoT-EPE-FE EI-3: IoT-EKM-FE EI-4: IoT-EAC-FE EI-6: IoT-GW-FE
CN-E-4	IoT end-user device component	– Configures devices for connecting with networks – Provides connectivity with networks based on the identification of devices – Collects, buffers, and transfers data of things – Provides user authentication, and executes IoT applications if it is required	EI-1: IoT-EEM-FE EI-2: IoT-EPE-FE EI-3: IoT-EKM-FE EI-4: IoT-EAC-FE EI-7: IoT-EUD-FE

NOTE 1 – The IoT end-point support component can be used independently and opened to provide an IoT end-point platform for third party development of IoT end-point value-added capabilities.

NOTE 2 – The IoT device component, IoT gateway component and IoT end-user device component can be combined to form extended compound components to support the IoT. When these components are combined, duplicate functionalities can be removed.

9.1.1 CN-E-1: IoT end-point support component

The IoT end-point support component manages events related to IoT end-point components, and makes decisions on access control and configurable control of the IoT end-point components based on predefined policies and derived rules from related knowledge.

The IoT end-point support component consists of the IoT-EEM-FE, IoT-EPE-FE, IoT-EKM-FE and IoT-EAC-FE specified in clause 7.1.

9.1.2 CN-E-2: IoT device component

The IoT device component configures devices for connection with networks or gateways, provides connectivity with networks or gateways based on the identification of devices, collects and transfers data of things, and executes IoT applications, if required.

The IoT device component consists of an IoT end-point support component and the IoT-DV-FE specified in clause 7.1.

9.1.3 CN-E-3: IoT gateway component

The IoT gateway component configures gateways for connection with networks, provides connectivity with networks based on the identification of devices, collects, buffers and transfers data of things, provides application support services, and executes IoT applications.

The IoT gateway component consists of an IoT end-point support component and the IoT-GW-FE specified in clause 7.1.

9.1.4 CN-E-4: IoT end-user device component

The IoT end-user device component configures devices for connection with networks, provides connectivity with networks based on the identification of devices, collects, buffers and transfers data of things, provides user authentication, and executes IoT applications, if required.

The IoT end-user device component consists of an IoT end-point support component and the IoT-EUD-FE specified in clause 7.1.

9.2 IoT transport control components

In the IoT transport control component category, the following extended basic components are identified: the IoT transport control support component; IoT transport awareness control component; IoT transport resource control component; and IoT location transport control component.

The component number, name, functionalities and included functional entities, described in clause 7, of these extended components are listed in Table 2.

Table 2 – List of the IoT transport control components

Component number	Component name	Component functionalities	Included functional entities
CN-T-1	IoT transport control support component	– Manages events related to IoT transport control components – Makes decisions on transport control and other internal operations of the IoT transport control components	TI-1: IoT-TEM-FE TI-2: IoT-TPE-FE TI-3: IoT-TKM-FE TI-4: IoT-TCA-FE
CN-T-2	IoT transport awareness control component	– Gathers, stores and processes the content awareness events and related data – Initiates content awareness transport control operations	TI-1: IoT-TEM-FE TI-2: IoT-TPE-FE TI-3: IoT-TKM-FE TI-4: IoT-TCA-FE TI-5: IoT-TAM-FE
CN-T-3	IoT transport resource control component	– Monitors the usage of the transport resources – Schedules the transport resources	TI-1: IoT-TEM-FE TI-2: IoT-TPE-FE TI-3: IoT-TKM-FE TI-4: IoT-TCA-FE TI-6: IoT-TRC-FE
CN-T-4	IoT location transport control component	– Locates, traces and processes the positions of IoT end-point components – Initiates location-related IoT transport operations	TI-1: IoT-TEM-FE TI-2: IoT-TPE-FE TI-3: IoT-TKM-FE TI-4: IoT-TCA-FE TI-7: IoT-LTC-FE

NOTE 1 – The IoT transport control support component can be used independently and opened to provide an IoT transport control platform for third party development of IoT transport value-added capabilities.

NOTE 2 – The IoT transport awareness control component, IoT transport resource control component and IoT location transport control component can be combined to form extended compound components to support the IoT. When these components are combined, duplicate functionalities can be removed.

9.2.1 CN-T-1: IoT transport control support component

The IoT transport control support component manages events related to the IoT transport control components, and makes decision on transport control and other internal operations of the IoT transport control components based on predefined policies and derived rules from related knowledge.

The IoT transport control support component consists of the IoT-TEM-FE, IoT-TPE-FE, IoT-TKM-FE and IoT-TCA-FE specified in clause 7.2.

9.2.2 CN-T-2: IoT transport awareness control component

The IoT transport awareness control component gathers, stores and processes the content awareness events and related data, and initiates content awareness transport control operations.

The IoT transport awareness control component consists of an IoT transport control support component and the IoT-TAM-FE specified in clause 7.2.

9.2.3 CN-T-3: IoT transport resource control component

The IoT transport resource control component monitors the usage of transport resources, and schedules the transport resources based on predefined policies and derived rules from related knowledge in order to support the quality of the IoT transport operations.

The IoT transport resource control component consists of an IoT transport control support component and the IoT-TRC-FE specified in clause 7.2.

9.2.4 CN-T-4: IoT location transport control component

The IoT location transport control component locates, traces and processes the positions of IoT end-point components, and initiates location-related IoT transport operations based on predefined policies and derived rules from related knowledge.

The IoT location transport control component consists of an IoT transport control support component and the IoT-LTC-FE specified in clause 7.2.

9.3 IoT data management components

In the IoT data management component category, the following extended basic components are identified: IoT data management support component; IoT data storage control component; IoT data querying control component; IoT data processing control component; and IoT data exchange control component.

The number, name, functionalities and included functional entities, described in clause 7, of these extended components are listed in Table 3.

Table 3 – List of the IoT data management components

Component number	Component name	Component functionalities	Included functional entities
CN-D-1	IoT data management support component	– Manages events related to the IoT data management components – Makes decisions and adaptably controls IoT data management and other internal operations of the IoT data management components	DI-1: IoT-DEM-FE DI-2: IoT-DPE-FE DI-3: IoT-DKM-FE DI-4: IoT-DSA-FE
CN-D-2	IoT data storage control component	– Monitors and controls the operations of storing and transferring IoT data – Initiates IoT data storage-related operations	DI-1: IoT-DEM-FE DI-2: IoT-DPE-FE DI-3: IoT-DKM-FE DI-4: IoT-DSA-FE DI-5: IoT-DSC-FE

Table 3 – List of the IoT data management components

Component number	Component name	Component functionalities	Included functional entities
CN-D-3	IoT data querying control component	– Monitors and controls execution of IoT data querying – Initiates necessary IoT data querying-related operations	DI-1: IoT-DEM-FE DI-2: IoT-DPE-FE DI-3: IoT-DKM-FE DI-4: IoT-DSA-FE DI-6: IoT-DQC-FE
CN-D-4	IoT data processing control component	– Monitors and controls the execution of IoT data processing – Initiates necessary IoT data processing-related operations	DI-1: IoT-DEM-FE DI-2: IoT-DPE-FE DI-3: IoT-DKM-FE DI-4: IoT-DSA-FE DI-7: IoT-DPC-FE
CN-D-5	IoT data exchange control component	– Monitors and controls the requirements and execution of data exchange with components that are outside the IoT – Initiates necessary IoT data exchange-related operations	DI-1: IoT-DEM-FE DI-2: IoT-DPE-FE DI-3: IoT-DKM-FE DI-4: IoT-DSA-FE DI-8: IoT-DEC-FE

NOTE 1 – The IoT data management support component can be used independently and opened to provide an IoT data management platform for third party development of IoT data management value-added capabilities.

NOTE 2 – The IoT data storage control component, IoT data querying control component, IoT data processing control component and IoT data exchange control component can be combined to form extended compound components to support the IoT. When these components are combined, duplicate functionalities can be removed.

9.3.1 CN-D-1: IoT data management support component

The IoT data management support component manages events related to IoT data management components, and makes decisions and adaptably controls on IoT data management and other internal operations of the IoT data management components, based on predefined policies and derived rules from related knowledge.

The IoT data management support component consists of the IoT-DEM-FE, IoT-DPE-FE, IoT-DKM-FE and IoT-DSA-FE specified in clause 7.3.

9.3.2 CN-D-2: IoT data storage control component

The IoT data storage control component monitors and controls the operations of storage and transfer of IoT data based on the available storage resources and the application requirements, and initiates IoT data storage-related operations based on predefined policies and derived rules from related knowledge in order to implement IoT data operations.

The IoT data storage control component consists of an IoT data management support component and the IoT-DSC-FE specified in clause 7.3.

9.3.3 CN-D-3: IoT data querying control component

The IoT data querying control component monitors and controls the execution of IoT data querying, and initiates necessary IoT data querying-related operations, such as IoT data collection and transfer operations, based on predefined policies and derived rules from related knowledge in order to implement the required IoT data querying operations.

The IoT data querying control component consists of an IoT data management support component and the IoT-DQC-FE specified in clause 7.3.

9.3.4 CN-D-4: IoT data processing control component

The IoT data processing control component monitors and controls the execution of IoT data processing, and initiates necessary IoT data processing-related operations, such as IoT data cleaning, collection, transfer, and cloud computing operations, based on predefined policies and derived rules from related knowledge in order to implement the required IoT data processing operations.

The IoT data processing control component consists of an IoT data management support component and the IoT-DPC-FE specified in clause 7.3.

9.3.5 CN-D-5: IoT data exchange control component

The IoT data exchange control component monitors and controls the requests and execution of data exchange with functional components outside the IoT, and initiates necessary IoT data exchange-related operations, such as IoT data collection and transfer operations, based on predefined policies and derived rules from related knowledge in order to implement the required IoT data exchange operations.

The IoT data exchange control component consists of an IoT data management support component and the IoT-DEC-FE specified in clause 7.3.

9.4 IoT service control components

In the IoT service control component category, the following extended basic components are identified: IoT service control support component; IoT service session control component; IoT service resource control component; and IoT location service control component.

The number, name, functionalities and included functional entities, described in clause 7, of these extended components are listed in Table 4.

Table 4 – List of the IoT service control components

Component number	Component name	Component functionalities	Included functional entities
CN-S-1	IoT service control support component	– Manages events related to the IoT service control components – Makes decisions and adaptably controls IoT service control and other internal operations of the IoT service control components	SI-1: IoT-SEM-FE SI-2: IoT-SPE-FE SI-3: IoT-SKM-FE SI-4: IoT-SPA-FE
CN-S-2	IoT service session control component	– Monitors and controls a session related to IoT services – Initiates IoT session-related control operations	SI-1: IoT-SEM-FE SI-2: IoT-SPE-FE SI-3: IoT-SKM-FE SI-4: IoT-SPA-FE SI-5: IoT-SSC-FE
CN-S-3	IoT service resource control component	– Monitors the usage of service resources – Schedules the service resources	SI-1: IoT-SEM-FE SI-2: IoT-SPE-FE SI-3: IoT-SKM-FE SI-4: IoT-SPA-FE SI-6: IoT-SRC-FE

Table 4 – List of the IoT service control components

Component number	Component name	Component functionalities	Included functional entities
CN-S-4	IoT location service control component	– Locates, traces and processes the positions of IoT service components – Initiates location-related IoT service provisioning	SI-1: IoT-SEM-FE SI-2: IoT-SPE-FE SI-3: IoT-SKM-FE SI-4: IoT-SPA-FE SI-7: IoT-LSC-FE

NOTE 1 – The IoT service control support component can be used independently and opened to provide IoT service control platform for third party development of IoT service control value-added capabilities.

NOTE 2 – The IoT service session control component, IoT service resource control component, and IoT location service control component can be combined to form extended compound components to support the IoT. When these components are combined, the duplicated functionalities can be removed.

9.4.1 CN-S-1: IoT service control support component

The IoT service control support component manages events related to the IoT service control components, and makes decisions and adaptably controls IoT service control and other internal operations of the IoT service control components based on predefined policies and derived rules from related knowledge.

The IoT service control support component consists of the IoT-SEM-FE, IoT-SPE-FE, IoT-SKM-FE, IoT-SPA-FE specified in clause 7.4.

9.4.2 CN-S-2: IoT service session control component

The IoT service session control component monitors and controls a session related to IoT services based on the available resources and application requirements, and initiates IoT session-related control operations based on predefined policies and derived rules from related knowledge in order to implement IoT session-related operations.

The IoT service session control component consists of an IoT service control support component and the IoT-SSC-FE specified in clause 7.4.

9.4.3 CN-S-3: IoT service resource control component

The IoT service resource control component monitors the usage of the service resources, and schedules the service resources based on predefined policies and derived rules from related knowledge in order to support the quality of the IoT service provisioning.

The IoT service resource control component consists of an IoT service control support component and the IoT-SRC-FE specified in clause 7.4.

9.4.4 CN-S-4: IoT location service control component

The IoT location service control component locates, traces and processes the positions of IoT service components, and initiates location-related IoT service provisioning based on predefined policies and derived rules from related knowledge.

The IoT location service control component consists of an IoT service control support component and the IoT-LSC-FE specified in clause 7.4.

10 Capability enhancement to support the IoT

Enhanced capabilities to support the IoT involve the functional entities or functional components that are specified in the NGN architecture [ITU-T Y.2012] that interact with extended functional entities or extended functional components to support the IoT.

According to the classification of these involved functional entities or functional components as specified in [ITU-T Y.2012], the enhanced capabilities to support the IoT can be classified into those for: transport functional entities; service functional entities; content delivery functional entities; application support functional entities; and the management functional component.

Clauses 10.1 to 10.5 and Tables 5 to 9 describe and list the enhanced capabilities to support the IoT.

NOTE 1 – Tables 5 to 9 include the following columns: enhancement number that represents the number of enhanced capabilities in this Recommendation, enhanced entity that represents the entities specified in [ITU-T Y.2012] in which enhanced capabilities are deployed, enhanced capability that represents the capabilities to be enhanced to support of the IoT, and relevant extensions that represents the extended components with that the enhanced capabilities are related.

NOTE 2 – The number for each enhanced capability given in this clause consists of three parts: The first is "EC", i.e., the abbreviation for "enhanced capability". The second is a letter of the alphabet that represents the category to which the enhanced capability belongs, i.e.; "T" represents the enhanced capabilities of transport functional entities category; "S" represents the enhanced capabilities of service functional entities category; "C" represents the enhanced capabilities of content delivery functional entities category; "A" represents the enhanced capabilities of application support functional entities category; and "M" represents the enhanced capabilities of management functional component category. The third is a digit that represents the sequential number of the enhanced capability in the same category of enhanced capabilities.

10.1 Enhanced capabilities of transport functional entities

The enhanced capabilities of transport functional entities involve both transport processing functional entities and transport control functional entities specified in [ITU-T Y.2012]. The enhanced capabilities of transport functional entities are as follows.

- EC-T-1: The capability to adopt access interfaces from the IoT-DV-FE, IoT-GW-FE and IoT-EUD-FE requires enhancement in the T-2: AN-FE specified in [ITU-T Y.2012], in order to support functionalities specified in IoT end-point components.
- EC-T-2: The capability to exchange location information with the IoT-LTC-FE requires enhancement in the T-13: TLM-FE specified in [ITU-T Y.2012], in order to support functionalities specified in the IoT transport control components.
- EC-T-3: The capability to identify configured parameters from the IoT-DV-FE, IoT-GW-FE and IoT-EUD-FE requires enhancement in the T-14: AM-FE specified in [ITU-T Y.2012], in order to support functionalities specified in IoT end-point components.
- EC-T-4: The capability to exchange transport control policies with the IoT-TCA-FE requires enhancement in the T-16: PD-FE specified in [ITU-T Y.2012], in order to support functionalities specified in IoT transport control components.
- EC-T-5: The capability to exchange transport resource information with the IoT-TRC-FE requires enhancement in the T-17: TRC-FE specified in [ITU-T Y.2012], in order to support functionalities specified in IoT transport control components.

These enhanced capabilities of transport functional entities are listed in Table 5.

Table 5 – List of enhanced capabilities of transport functional entities

Enhancement number	Enhanced entity	Enhanced capability	Relevant extensions
EC-T-1	T-2: AN-FE, access node functional entity	The capability to adopt access interfaces from the IoT device functional entity (IoT-DV-FE), IoT gateway functional entity (IoT-GW-FE) and IoT end-user device functional entity (IoT-EUD-FE)	IoT end-point components
EC-T-2	T-13: TLM-FE, transport location management functional entity	The capability to exchane location information with the IoT location transport control functional entity (IoT-LTC-FE)	IoT transport control components
EC-T-3	T-14: AM-FE, access management functional entity	The capability to identify configured parameters from the IoT device functional entity (IoT-DV-FE), IoT gateway functional entity (IoT-GW-FE) and IoT end-user device functional entity (IoT-EUD-FE)	IoT end-point components
EC-T-4	T-16: PD-FE, policy decision functional entity	The capability to exchange transport control policies with the IoT transport configuration adaptation functional entity (IoT-TCA-FE)	IoT transport control components
EC-T-5	T-17: TRC-FE, transport resource control functional entity	The capability to exchange transport resource information with the IoT transport resource control functional entity (IoT-TRC-FE)	IoT transport control components

10.2 Enhanced capabilities of service control functional entities

The enhanced capabilities of service control functional entities specified in [ITU-T Y.2012] are as follows:

- EC-S-1: The capability to exchange session control information with the IoT-SSC-FE is required to be enhanced in the S-1: S-CSC-FE specified in [ITU-T Y.2012], in order to support IoT session control functionalities specified in IoT service control components.
- EC-S-2: The capability to adopt the interfaces from the IoT-DV-FE, IoT-GW-FE and IoT-EUD-FE is required to be enhanced in the S-2: P-CSC-FE specified in [ITU-T Y.2012], in order to support session-related functionalities specified in IoT end-point components.
- EC-S-3: The capability to adopt the interfaces from the IoT-LSC-FE is required to be enhanced in the S-4: SL-FE specified in [ITU-T Y.2012], in order to support IoT location-based service control functionalities specified in IoT service control components.
- EC-S-4: The capability to exchange service control information except for session control information with the IoT-SPA-FE is required to be enhanced in the S-15: GSC-FE specified in [ITU-T Y.2012], in order to support IoT non-session service control functionalities specified in IoT service control components.

These enhanced capabilities of service control functional entities are listed in Table 6.

Table 6 – List of enhanced capabilities of service control functional entities

Enhancement number	Enhanced entity	Enhanced capability	Relevant extensions
EC-S-1	S-1: S-CSC-FE, serving call session control functional entity	The capability to exchange session control information with the IoT service session control functional entity (IoT-SSC-FE)	IoT service control components
EC-S-2	S-2: P-CSC-FE, proxy call session control functional entity	The capability to adopt the interfaces from the IoT device functional entity (IoT-DV-FE), IoT gateway functional entity (IoT-GW-FE) and IoT end-user device functional entity (IoT-EUD-FE)	IoT end-point components
EC-S-3	S-4: SL-FE, subscription locator functional entity	The capability to adopt the interfaces from the IoT location service control functional entity (IoT-LSC-FE)	IoT service control components
EC-S-4	S-15: GSC-FE, general services control functional entity	The capability to exchange service control information except for session control information with the IoT service provision adaptation functional entity (IoT-SPA-FE)	IoT service control components

10.3 Enhanced capabilities of content delivery functional entities

The enhanced capabilities of content delivery functional entities specified in [ITU-T Y.2012] are as follows:

- EC-C-1: The capability to exchange content control information with the IoT-DSA-FE is required to be enhanced in the C-1: CD&LC-FE specified in [ITU-T Y.2012], in order to support IoT adaptable data control functionalities specified in IoT data management components.
- EC-C-2: The capability to adopt the interfaces from the IoT-DSC-FE, the IoT-DQC-FE, and the IoT-DPC-FE is required to be enhanced in the C-2: CDC-FE specified in [ITU-T Y.2012], in order to support IoT content delivery control functionalities specified in IoT data management components.
- EC-C-3: The capability to adopt the interfaces from the IoT-DSC-FE, the IoT-DQC-FE, and the IoT-DPC-FE is required to be enhanced in the C-3: CDP-FE specified in [ITU-T Y.2012], in order to support IoT content processing control functionalities specified in IoT data management components.

These enhanced capabilities of content delivery functional entities are listed in Table 7.

Table 7 – List of enhanced capabilities of content delivery functional entities

Enhancement number	Enhanced entity	Enhanced capability	Relevant extensions
EC-C-1	C-1: CD&LC-FE, content distribution and location control functional entity	The capability to exchange content control information with the IoT data service adaptation functional entity (IoT-DSA-FE)	IoT data management components
EC-C-2	C-2: CDC-FE, content delivery control functional entity	The capability to adopt the interfaces from the IoT data storage control functional entity (IoT-DSC-FE), the IoT data querying control functional entity (IoT-DQC-FE), and the IoT data processing control functional entity (IoT-DPC-FE)	IoT data management components
EC-C-3	C-3: CDP-FE, content delivery processing functional entity	The capability to adopt the interfaces from the IoT data storage control functional entity (IoT-DSC-FE), the IoT data querying control functional entity (IoT-DQC-FE), and the IoT data processing control functional entity (IoT-DPC-FE)	IoT data management components

10.4 Enhanced capability for application support functional entities

The enhanced capability for application support functional entities specified in [ITU-T Y.2012] is as follows.

- EC-A-1: The capability to adopt the interfaces from the IoT-DEM-FE and the IoT-SEM-FE is required to be enhanced in the A-1: AS-FE specified in [ITU-T Y.2012], in order to support IoT adaptable data control functionalities specified in IoT data management components, and to support IoT adaptable service provisioning specified in IoT service control components.

The enhanced capability for application support functional entities is listed in Table 8.

Table 8 –Enhanced capability for application support functional entities

Enhancement number	Enhanced entity	Enhanced capability	Relevant extensions
EC-A-1	A-1: AS-FE, application support functional entity	The capability to adopt the interfaces from the IoT data event management functional entity (IoT-DEM-FE) and IoT service event management functional entity (IoT-SEM-FE)	IoT data management components, and IoT service control components

10.5 Enhanced capability for the management functional component

There is only one management component described in the NGN architecture [ITU-T Y.2012], which is the management functions component, so that the enhancement to NGN management capabilities relates only to the management functions component.

According to [ITU-T Y.2012], there are five different types of function included in the management functions component, i.e., functions related to fault management, configuration management, accounting management, security management and performance management. There is no privacy-related management explicitly specified in the NGN architecture [ITU-T Y.2012].

Based on the required IoT capabilities specified in [ITU-T Y.4401], the privacy protection capability is mandatory for support of the IoT, and should be added to the management functions component of the NGN specified in [ITU-T Y.2012]. So the management functions component needs to be enhanced in the management and privacy protection component.

NOTE 1 – The description of NGN management architecture is not specified in [ITU-T Y.2012]; the high-level NGN management architecture is specified in [b-ITU-T M.3060]. The enhancement to the functional entities of NGN management specified in [b-ITU-T M.3060] to support the IoT lies outside the scope of this Recommendation.

NOTE 2 – NGN privacy protection is specified in clause 7.3.8 of [ITU-T Y.2701]. It only focuses on the protection of the subscriber's private information, such as location of data, identities, phone numbers and network addresses. It does not cover most privacy capabilities required by the IoT, as specified in [ITU-T Y.4401].

The enhanced capabilities of management functional component are as follows, and are also listed in Table 9.

- EC-M-1: The capability for privacy protected communication is required to be enhanced in the management functions component specified in [ITU-T Y.2012], in order to support privacy protection communication-related applications of the IoT, such as the applications of locating or tracing IoT devices. This enhanced capability may be implemented and deployed in the IoT service control components, IoT transport control components and IoT end-point components, as required by specific privacy protection mechanisms.
- EC-M-2: The capability for privacy protected data management is required to be enhanced in the management functions component specified in [ITU-T Y.2012], in order to support data-related applications in the IoT, such as personal healthcare applications. This enhanced capability may be implemented and deployed in the IoT data management components and IoT end-point components as required by specific privacy protection mechanisms.
- EC-M-3: The capability for privacy protected service provision is required to be enhanced in management functions component specified in [ITU-T Y.2012], in order to support IoT service provisioning, such as location-aware services. This enhanced capability may be implemented and deployed in the IoT service control components and IoT end-point components.

Table 9 – List of enhanced capabilities of management functional component

Enhancement number	Enhanced components	Enhanced capability	Relevant extensions
EC-M-1	Management functions component	The capability of privacy protected communication is required to be enhanced in order to support the IoT communication related applications.	IoT service control components, IoT transport control components, and IoT end-point components.
EC-M-2	Management functions component	The capability of privacy protected data management is required to be enhanced in order to support the data related applications in the IoT.	IoT data management components and IoT end-point components.
EC-M-3	Management functions component	The capability of privacy protected service provision is required to be enhanced in order to support the IoT services provisioning.	IoT service control components and IoT end-point components.

11 Security considerations

The security requirements within the functional requirements and architecture of the NGN that are specified in [ITU-T Y.2701] are still valid in the extension of functional entities, reference points and functional components and the enhancement to NGNe capabilities to support the IoT as specified in this Recommendation.

The security mechanisms that can be used to fulfil security requirements of the NGN are specified in [ITU-T Y.2704], and these security mechanisms can also be applied to the extension of functional entities, reference points and functional components, as well as the enhancement to NGN capabilities to support the IoT as specified in this Recommendation.

The other security capabilities required by the extension of functional entities, reference points and functional components, as well as the enhancement to NGN capabilities for support of the IoT, are specified in clause 8.7 of [ITU-T Y.4401].

Appendix I

Use-cases of the IoT architecture based on NGNe

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

NGN applications can be classified into those that are communication oriented and data oriented. The evolution of NGN can support cloud computing services and related applications. Cloud computing services have capabilities to store and process data. These evolved applications can be classified as data-oriented applications.

IoT applications can also be classified into those that are communication oriented and data oriented. However, IoT applications differ from NGN applications in the autonomic applications that are described by requirements for autonomic networking and autonomic service provisioning in [ITU-T Y.4000].

The use cases in clauses I.1 to I.3 show extended functional entity uses, reference points and functional components specified in this Recommendation to support the IoT.

I.1 Autonomic communications between IoT devices

When an IoT device identifies the occurrence of a critical event, it initiates a communication to its master IoT device, such as an IoT gateway, to report the event. It is a typical use case of autonomic communication between IoT devices. This use case is shown in Figure I.1.

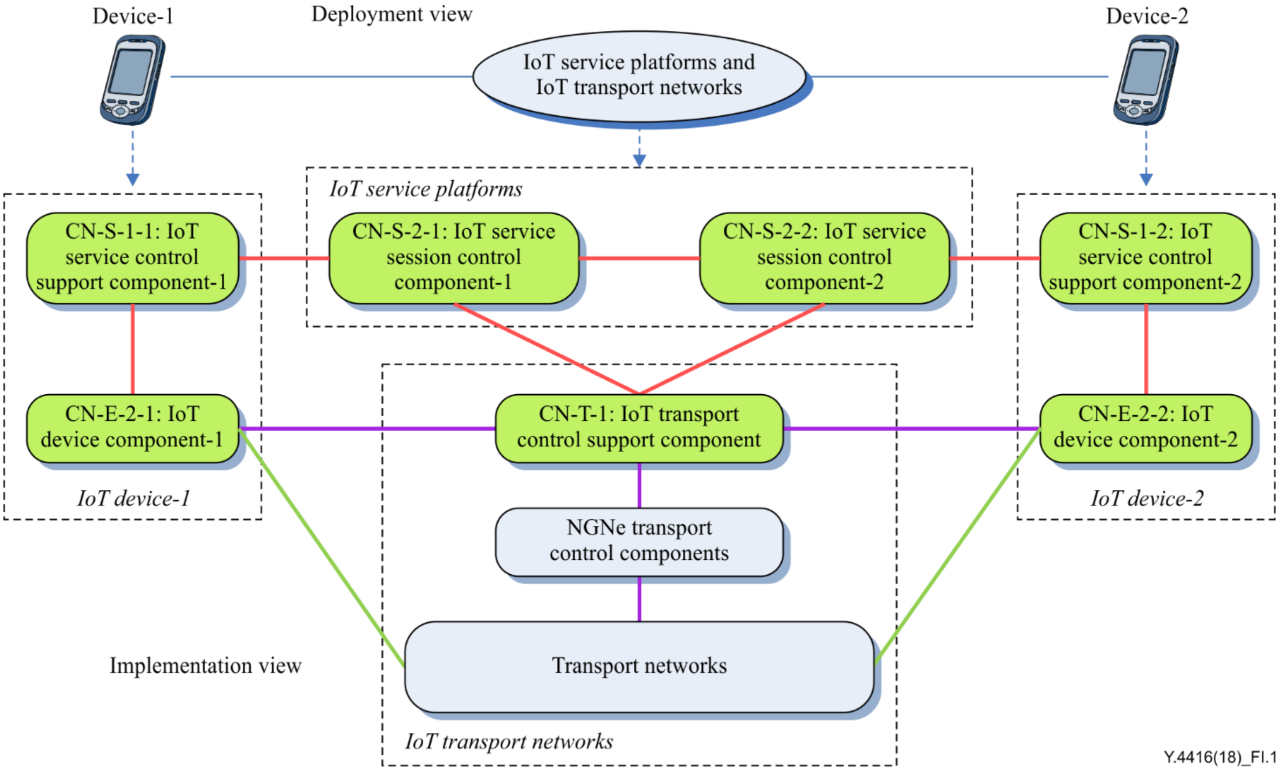
Device-1
Deployment view
Device-2
IoT service platforms and IoT transport networks
IoT service platforms
CN-S-1-1: IoT service control support component-1
CN-S-2-1: IoT service session control component-1
CN-S-2-2: IoT service session control component-2
CN-S-1-2: IoT service control support component-2
CN-E-2-1: IoT device component-1
CN-T-1: IoT transport control support component
CN-E-2-2: IoT device component-2
IoT device-1
IoT device-2
NGNe transport control components
Implementation view
Transport networks
IoT transport networks
Y.4416(18)_FI.1

Figure I.1 – A use case of autonomic communication between IoT devices

The functional framework in the deployment view for the autonomic communications in this use case consists of two IoT devices, and IoT service platforms and IoT transport networks as illustrated in Figure I.1.

The functional framework in the implementation view for the autonomic communications in this use case consists of the IoT device components and the IoT service control support components implemented in the IoT devices, the IoT service session control components implemented in the IoT service platforms, and the IoT transport control support component, NGNe transport control components, and transport networks implemented in the IoT transport networks, which are illustrated in Figure I.1. All these IoT functional components are defined in clause 9.

One possible message interaction of these IoT functional components to provide autonomic communication capability in this use case is shown in Figure I.2. This message interaction is described as follows.

(1) The CN-E-2-1 captures an event that makes a decision based on some related policies or knowledge to send a session initiation request to CN-S-1-1 deployed in IoT device-1 through the reference point SI-EI-1 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(2) The CN-S-1-1 forwards this request to the CN-S-2-1 deployed in the IoT service platforms through the reference point SI-SI-1 described in clause 8.4, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(3) This session request is validated by the SI-2: IoT-SPE-FE, forwarded to the SI-4: IoT-SPA-FE, and both SI-2 and SI-4 are the functional entities implemented in CN-S-2-1. The SI-4 in CN-S-2-1 sends a transport configuring request to the TI-4: IoT-TCA-FE implemented in CN-T-1 through the reference point SI-TI-2 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(4) The TI-4 in CN-T-1 replies with the transport configuring response through the reference point SI-TI-2 that the CN-S-2-1 cannot initiate session directly with IoT device-2.

(5) The SI-4 in CN-S-2-1 forwards the session request to the CN-S-2-2 through SI-SI-2 described in clause 8.4, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(6) This session request is validated by the SI-2: IoT-SPE-FE implemented in CN-S-2-2, forwarded to the SI-4: IoT-SPA-FE) implemented in CN-S-2-2. The SI-4 in CN-S-2-2 sends a transport configuring request to the TI-4: IoT-TCA-FE implemented in CN-T-1 through the reference point SI-TI-2 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(7) The TI-4 in CN-T-1 replies with the transport configuring response through the reference point SI-TI-2 that the CN-S-2-2 can initiate session directly with IoT device-2.

(8) The SI-4 in CN-S-2-2 forwards this request to the SI-5: IoT-SSC-FE implemented in CN-S-2-2 through reference point SI-SI-7. The SI-5 in CN-S-2-2 sets this session configuration and forwards this session request to the SI-1: IoT-SEM-FE implemented in CN-S-2-2 through the reference point SI-SI-5. The SI-1 in CN-S-2-2 forwards the session request to the SI-2: IoT-SPE-FE implemented in CN-S-1-2 that is deployed in IoT device-2, through the reference point SI-SI-1. All the reference points in this step are described in clause 8.4.

(9) This session request is validated by the SI-2: IoT-SPE-FE implemented in CN-S-1-2, forwarded to the SI-4: IoT-SPA-FE implemented in CN-S-1-2 through the reference point SI-SI-2 described in clause 8.4. The SI-4 in CN-S-1-2 delivers the request to the EI-4: IoT-EAC-FE implemented in the CN-E-2-2 deployed in IoT device-2, through the reference point SI-EI-2 described in clause 8.8.

(10) The EI-4 in the CN-E-2-2 validates the request for initiating a session from IoT device-1 to IoT device-2, and returns the session confirmation to the SI-4 in CN-S-1-2 through the reference point SI-EI-2 described in clause 8.8.

(11) This session initiation confirmation is forwarded through CN-S-1-2, CN-S-2-2, CN-S-2-1 and CN-S-1-1, and sent to the EI-4: IoT-EAC-FE implemented in CN-E-2-1 deployed in IoT device-1.

(12) The IoT device-1 starts to communicate automatically with IoT device-2.

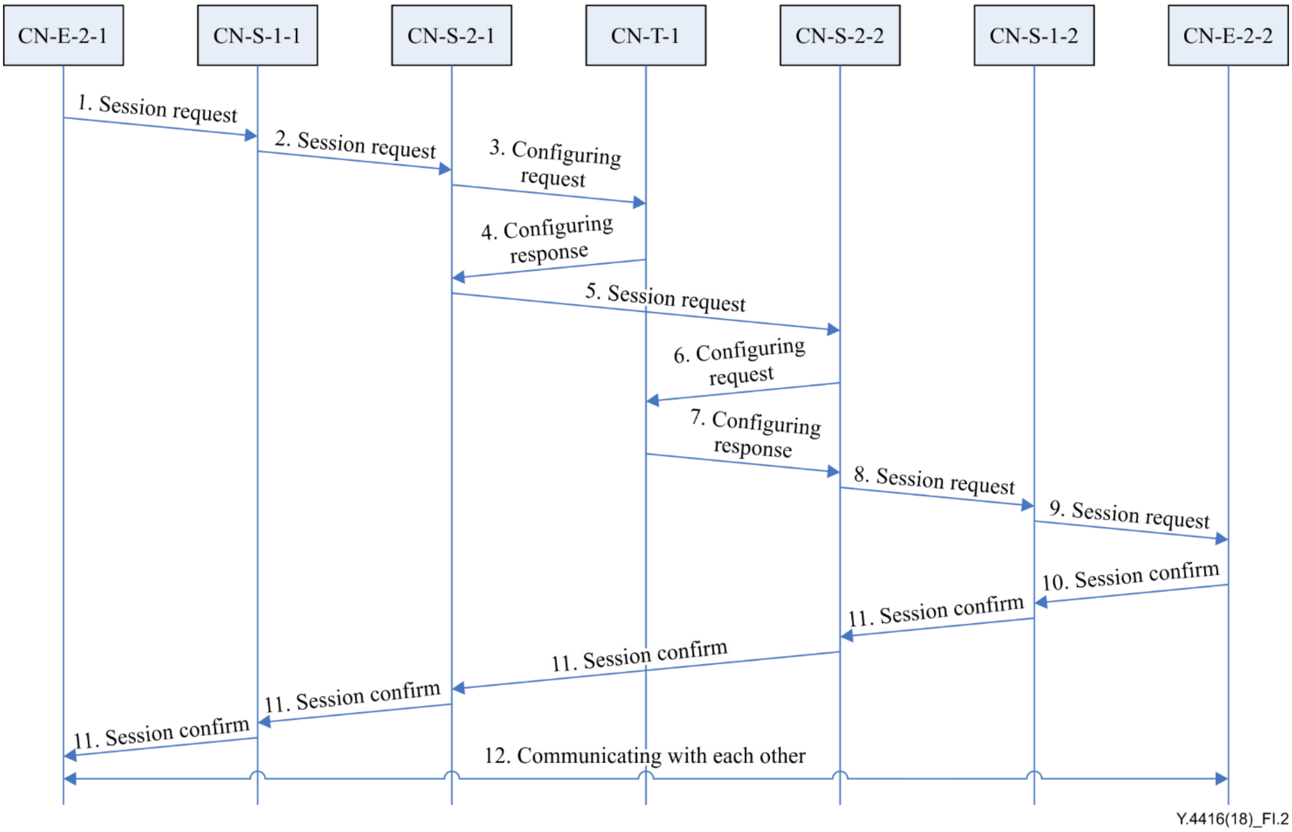

Figure I.2 – One scenario for autonomic communication

The foregoing description of the autonomic communication use case illustrates that the extended functional entities described in clause 7, extended reference points described in clause 8 and extended functional components described in clause 9 of this Recommendation can work cooperatively to support the capability for autonomic communication.

I.2 Autonomic data collection from IoT devices

IoT devices are required automatically to aggregate data to the IoT gateway or to the data server based on predefined policies. Figure I.3 shows a typical use case of autonomic data collection from IoT devices.

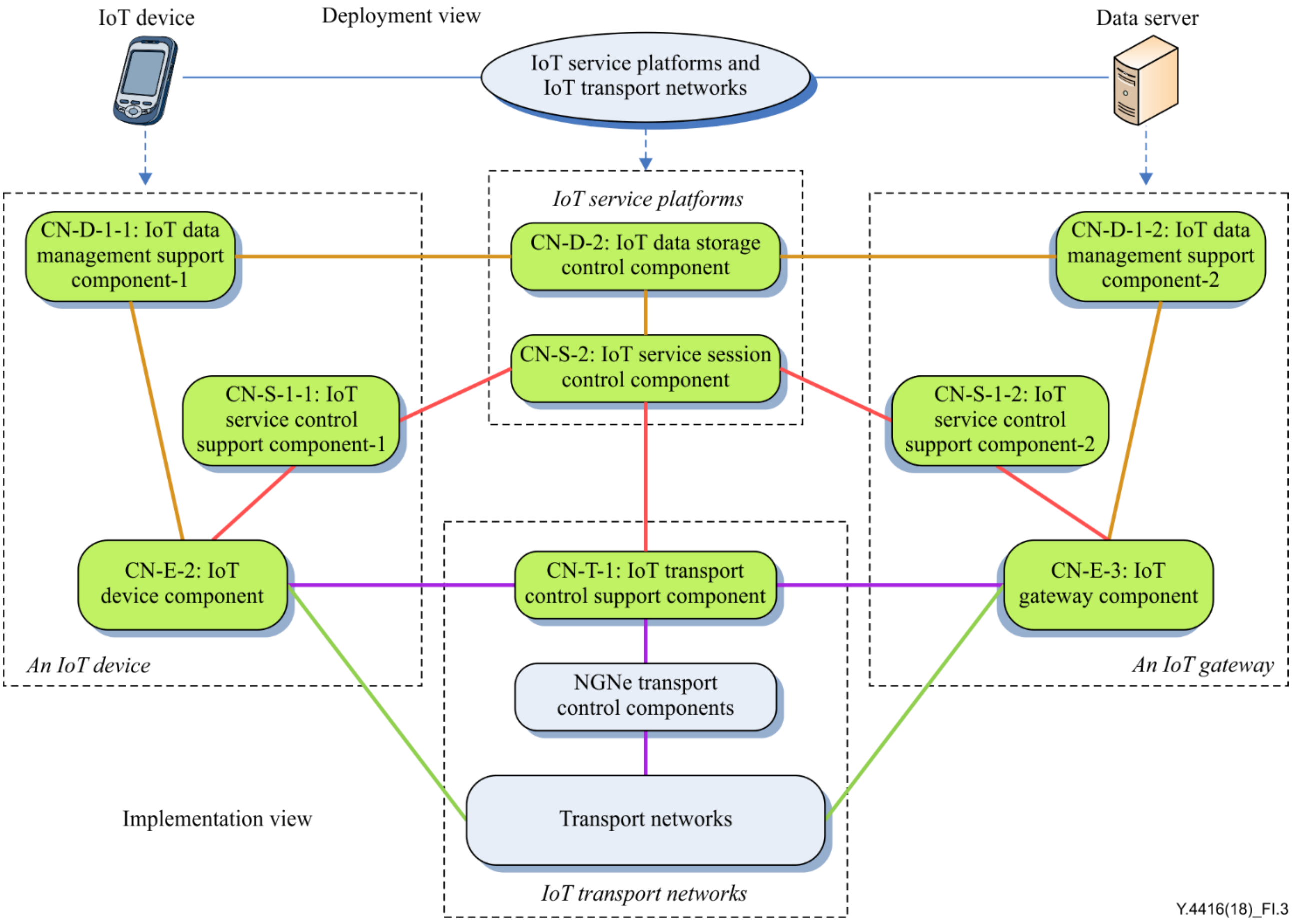
IoT device
Deployment view
Data server
IoT service platforms and IoT transport networks
IoT service platforms
CN-D-1-1: IoT data management support component-1
CN-D-2: IoT data storage control component
CN-D-1-2: IoT data management support component-2
CN-S-2: IoT service session control component
CN-S-1-1: IoT service control support component-1
CN-S-1-2: IoT service control support component-2
CN-E-2: IoT device component
CN-T-1: IoT transport control support component
CN-E-3: IoT gateway component
An IoT device
An IoT gateway
NGNe transport control components
Implementation view
Transport networks
IoT transport networks
Y.4416(18)_FI.3

Figure I.3 – A use case of autonomic data collection from IoT devices

The functional framework in the deployment view for the autonomic data collection in this use case consists of an IoT device, a data server or gateway, and IoT service platforms and IoT transport networks as illustrated in Figure I.3.

The functional framework in the implementation view for autonomic data collection in this use case consists of the IoT device component, the IoT service control support component, and the IoT data management support component implemented in the IoT devices, and the IoT gateway component, the IoT service control support component, and the IoT data management support component implemented in the IoT gateway; the IoT service session control component, IoT data storage control component implemented in the IoT service platforms; and the IoT transport control support component, NGNe transport control components, and transport networks implemented in the IoT transport networks, which are illustrated in Figure I.3. All these functional components to support the IoT are described in clause 9.

One possible message interaction of these extended IoT functional components for providing autonomic data collection capability in this use case is shown in Figure I.4. This message interaction is described as follows.

(1) The CN-E-2 captures an event that makes a decision based on some related policies or knowledge to initiate a data transfer session, so it sends a session initiation request to CN-S-1-1 deployed in the IoT device through the reference point SI-EI-1 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(2) The CN-S-1-1 forwards this request to the CN-S-2 deployed in the IoT service platforms through the reference point SI-SI-1 described in clause 8.4, by means of message exchange

mechanisms that are to be specified in other Recommendations for implementing this reference point.

(3) After validating this session request, CN-S-2 sends a transport configuring request to CN-T-1 deployed in the IoT transport networks. CN-T-1 validates this configuring request and returns a positive configuring response to CN-S-2. Both of them are through the reference point SI-TI-2 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(4) The CN-S-2 forwards the session request to CN-S-1-2 that is deployed in the IoT gateway through the reference point SI-SI-2 described in clause 8.4, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(5) After validating this session request, CN-S-1-2 delivers the session request to the CN-E-3 deployed in the IoT gateway, through the reference point SI-EI-2 described in clause 8.8.

(6) The CN-E-3 validates and confirms the session initiation request from the IoT device to the IoT gateway, through CN-S-1-2, CN-S-2, and CN-S-1-1, and sends a session initiation confirmation message back to CN-E-2.

(7) The CN-E-2 send a data storage request to CN-D-1-1 deployed in the IoT device through the reference point DI-EI-1 described in clause 8.7, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(8) The CN-D-1-1 forwards this storage request to CN-D-2 deployed in the IoT service platforms through the reference point DI-DI-1 described in clause 8.3, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(9) After validating this storage request, CN-D-2 forwards this request to CN-D-1-2 deployed in the IoT gateway through the reference point DI-DI-2 described in clause 8.3, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(10) After validating this storage request, CN-D-1-2 delivers it to CN-E-3 deployed in the IoT gateway through the reference point DI-EI-2 described in clause 8.7.

(11) The CN-E-3 validates and confirms this storage request from the IoT device to the IoT gateway, through CN-D-1-2, CN-D-2 and CN-D-1-1, and sends a storage confirmation message to CN-E-2.

(12) The data is starts to be collected from the IoT device by the IoT gateway.

NOTE – The related functional entities in this use case can be derived from the related reference points based on both the functional entity specifications in clause 7 and the reference point specifications in clause 8.

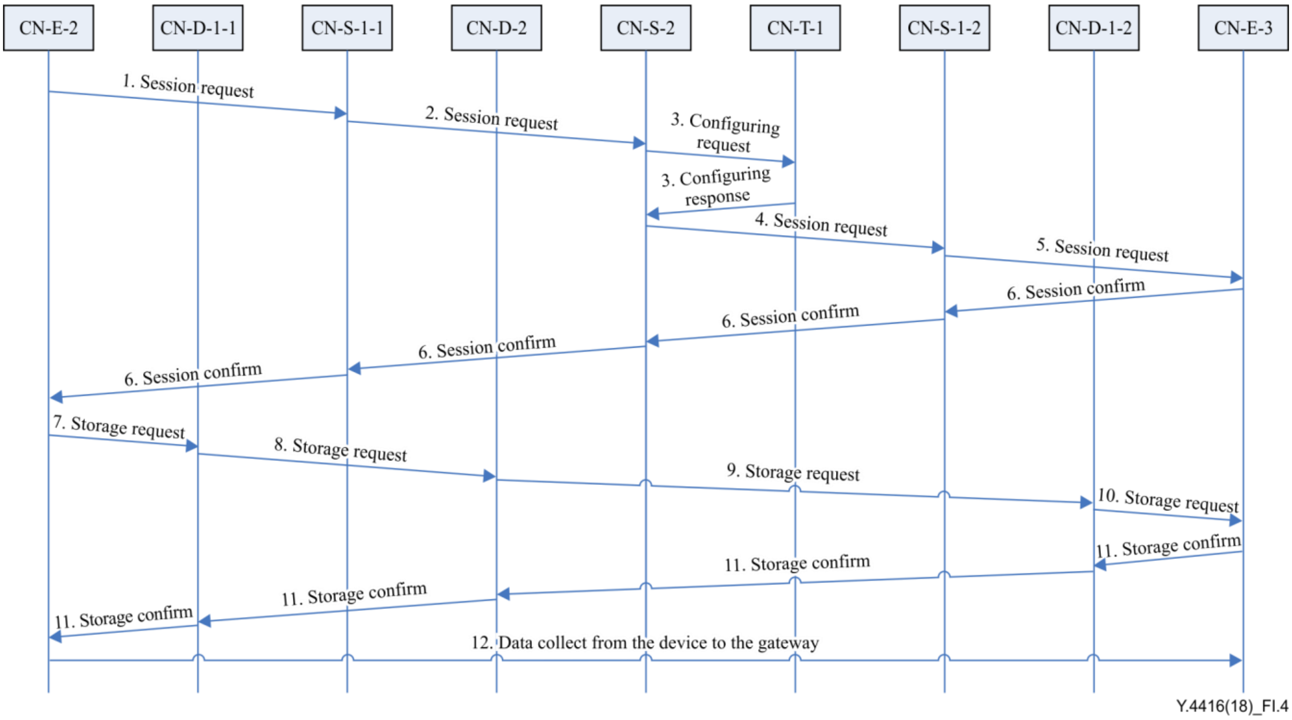

Figure I.4 – One possible message interaction in the autonomic data collection use case

I.3 Autonomic service provisioning to the IoT user

IoT devices are required to automatically provide service to the IoT user based on predefined policies. Figure I.5 shows a typical use case of autonomic service provisioning.

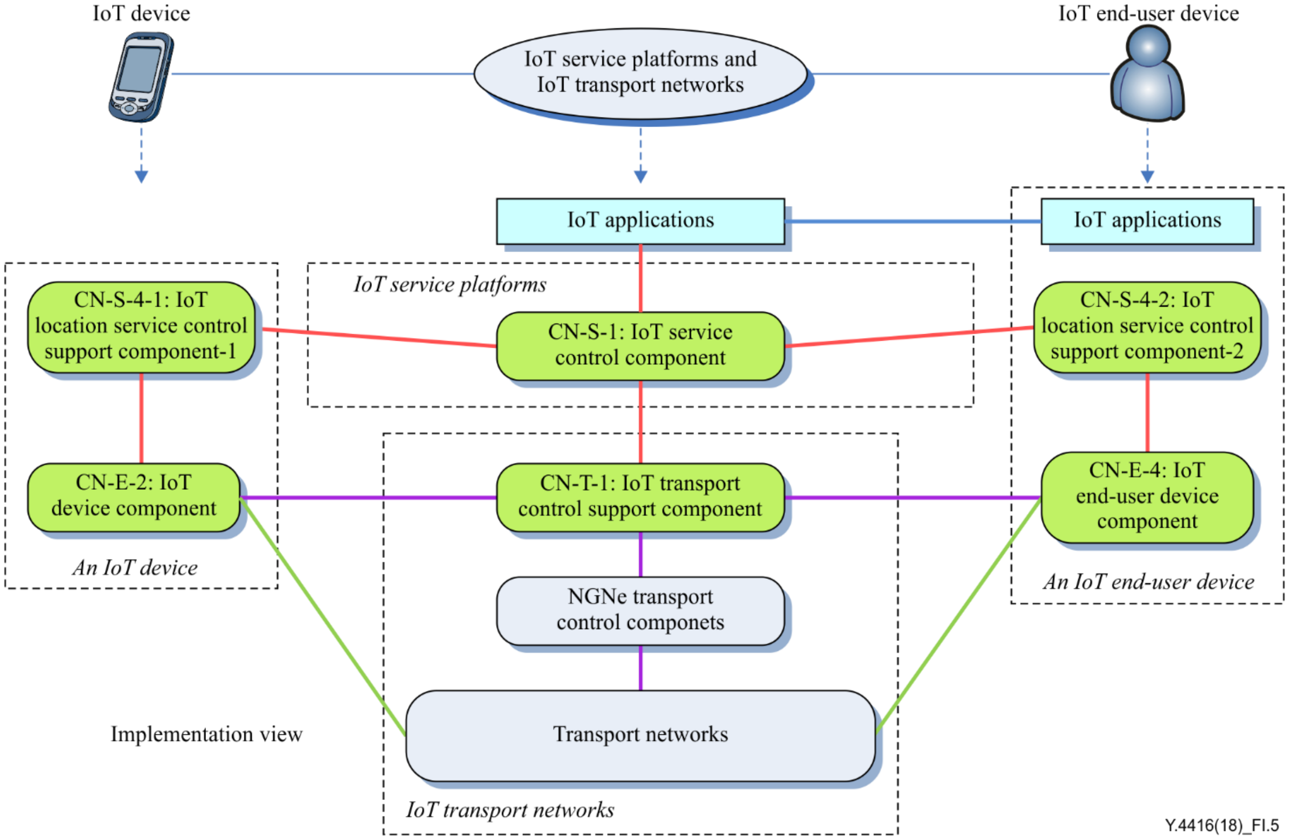
IoT device
IoT end-user device
IoT service platforms and IoT transport networks
IoT applications
IoT applications
IoT service platforms
CN-S-4-1: IoT location service control support component-1
CN-S-1: IoT service control component
CN-S-4-2: IoT location service control support component-2
CN-E-2: IoT device component
CN-T-1: IoT transport control support component
CN-E-4: IoT end-user device component
An IoT device
An IoT end-user device
NGNe transport control componets
Implementation view
Transport networks
IoT transport networks
Y.4416(18)_FI.5

Figure I.5 – A use case of autonomic service provisioning to the IoT applications

The functional framework in the deployment view for autonomic service provisioning in this use case consists of an IoT device, an IoT end-user device, and IoT service platforms and IoT transport networks as illustrated in Figure I.5.

The functional framework in the implementation view for autonomic service provisioning in this use case consists of an IoT device component and an IoT location service control component implemented in the IoT device; an IoT end-user device component, a IoT location service control component and the IoT applications implemented in the IoT end-user device; the IoT service control support component implemented in the IoT service platforms; and the IoT transport control support component, NGNe transport control components, and transport networks implemented in the IoT transport networks, which are illustrated in Figure I.5.

One possible message interaction of these extended IoT functional components for providing autonomic service provisioning capability in this use case is shown in Figure I.6. This message interaction is described as follows.

(1) The CN-E-2 captures an event that makes a decision based on some related policies or knowledge to send a location-based service request to CN-S-4-1 deployed in the IoT device through the reference point SI-EI-1 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(2) The CN-S-4-1 forwards this service request to the CN-S-1 deployed in the IoT service platforms through the reference point SI-SI-1 described in clause 8.4, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(3) After validating this location-based service request, CN-S-1 sends transport configuring request to CN-T-1 deployed in the IoT transport networks. CN-T-1 validates this configuring request and returns a positive configuring response to CN-S-1. Both of them are through the reference point SI-TI-2 described in clause 8.8, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(4) The CN-S-1 forwards this location-based service request to CN-S-4-2 that is deployed in the IoT end-user device through the reference point SI-SI-2 described in clause 8.4, by means of message exchange mechanisms that are to be specified in other Recommendations for implementing this reference point.

(5) After validating this service request, CN-S-4-2 delivers this location-based service request to CN-E-4 deployed in the IoT end-user device through the reference point SI-EI-2 described in clause 8.8.

(6) The CN-E-4 validates and confirms this location-based service request from the IoT device to the IoT end-user device, through CN-S-4-2, CN-S-1 and CN-S-4-1, and sends a service confirmation message to CN-E-2.

(7) The location-based service starts to be provided from the IoT device to the IoT end-used device.

NOTE – The related functional entities in this use case can be derived from the related reference points based on both the functional entity specifications in clause 7 and the reference point specifications in clause 8.

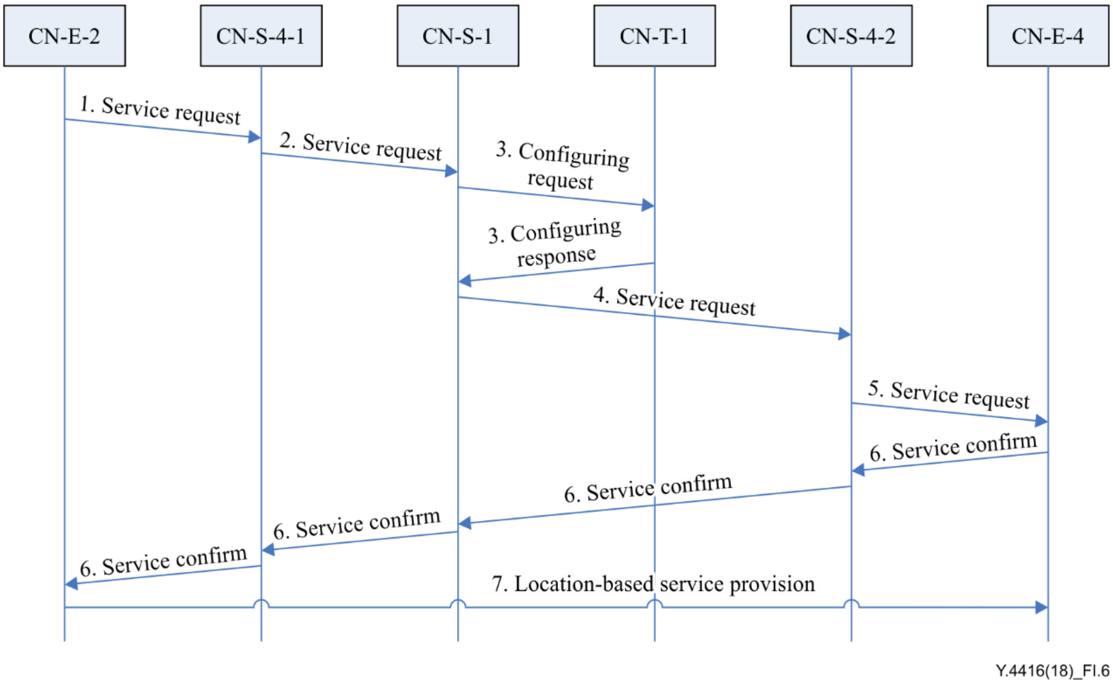

Figure I.6 – One possible message interaction in the use case of autonomic service provisioning

Bibliography

[b-ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the Management of Next Generation Networks*.

[b-ITU-T Y.2302] Recommendation ITU-T Y.2302 (2014), *Network intelligence capability enhancement – 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, 2018