International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4455

(10/2017)

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

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Reference architecture for Internet of things network capability exposure

Recommendation ITU-T Y.4455

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.4455

Reference architecture for Internet of things network capability exposure

Summary

Recommendation ITU-T Y.4455 introduces Internet of things (IoT) network capability exposure (NCE). The IoT NCE is a functional entity in network domain, and facilitates IoT applications and services to make full use of capabilities of their underlying networks. The IoT NCE can optimize user experience, improve network efficiency and expose network capability in order to optimize IoT applications and services.

Recommendation ITU-T Y.4455 clarifies the concept of the IoT NCE, identifies its general characteristics and common requirements, and provides the reference architecture and relevant capabilities for the IoT NCE. Additionally, it provides several use cases and common procedures to illustrate the concept and the architecture of the IoT NCE.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.4455	2017-10-29	20	11.1002/1000/13389

Keywords

Capability, Internet of things, network capability exposure.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4455

Reference architecture for Internet of things network capability exposure

1 Scope

This Recommendation specifies reference architecture for Internet of things (IoT) network capability exposure (NCE). The scope of this Recommendation includes:

– the concept, general characteristics and requirements of IoT NCE;

– reference architecture for IoT NCE.

2 References

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 capability [b-ITU-R M.1224-1]: The ability of an item to meet a service demand of given quantitative characteristics under given internal conditions.

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

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

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

3.1.4 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CCM	Car Communication Manager
CDMA	Code Division Multiple Access
EC-FC	Exposure Coordination Functional Component
ES-FC	Exposure Supporting Functional Component
GSM	Global System for Mobile communications
ICT	Information and Communication Technology
IoT	Internet of things
LTE	Long Term Evolution
NA-FC	Network Agent Functional Component
NAM-FC	Network Agent Management Functional Component
NB-IoT	Narrowband IoT
NCE	Network Capability Exposure
QoS	Quality of Service
REST	Representational State Transfer
SCEF	Service Capability Exposure Framework
SDO	Standards Development Organization
SSAS	Service Support and Application Support
TLS	Transport Layer Security
WCDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide interoperability for Microwave Access

5 Conventions

The following conventions are used 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 Recommendation is to be claimed.

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

6 Introduction to the Internet of things network capability exposure

IoT NCE is a flexible approach developed for IoT network providers, which uses open or proprietary network application programming interfaces (APIs), such as RESTful APIs, to expose the capabilities of IoT networks.

Currently, from the perspective of network providers, due to a lack of uniform standards, various proprietary platforms have to be deployed and maintained in order to expose their various network capabilities (such as IoT device management or dynamic communication management). From the perspective of developers who integrate those network capabilities, they have to pay more costs to develop and maintain their applications and services in order to integrate the various platforms and their related APIs.

The IoT NCE is a functional entity (see Figure 6-1) that facilitates IoT applications, services and IoT devices to make full use of capabilities of their underlying networks. Those networks with different information communication technologies (e.g., 3GPP-based networks, 3GPP2-based networks and WiMAX-based networks) publish open or proprietary APIs for their network capabilities on the IoT NCE. IoT NCE publishes network capabilities according to access policies and network requests. IoT applications and services can subscribe and access the exposed network capabilities using the reference points provided by the IoT NCE. Through the IoT NCE, IoT applications and services, and relevant IoT devices can interact with underlying networks to access the network capabilities exposed by the underlying networks.

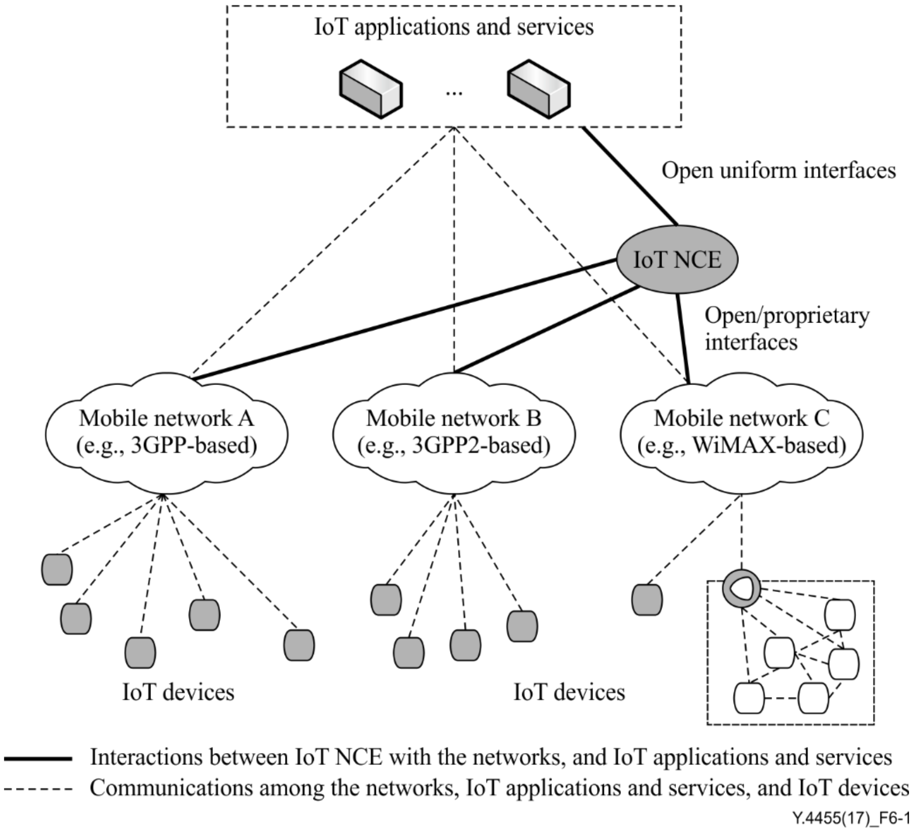
IoT applications and services
...
Open uniform interfaces
IoT NCE
Open/proprietary interfaces
Mobile network A (e.g., 3GPP-based)
Mobile network B (e.g., 3GPP2-based)
Mobile network C (e.g., WiMAX-based)
IoT devices
IoT devices
Interactions between IoT NCE with the networks, and IoT applications and services
Communications among the networks, IoT applications and services, and IoT devices
Y.4455(17)_F6-1

Figure 6-1 – Overview of the Internet of things network capability exposure

NOTE 1 – 3GPP-based network refers to a network mainly based on the communication standards specified by the Third Generation Partnership Project, e.g., global system for mobile communications (GSM), wideband code division multiple access (WCDMA), long term evolution (LTE) and narrowband IoT (NB-IoT).

NOTE 2 – 3GPP2-based network refers to a network mainly based on the communication standards specified by the Third Generation Partnership Project 2 (3GPP2), e.g., code division multiple access (CDMA) one and CDMA 2000.

NOTE 3 – WiMAX-based network refers to a network mainly based on the series of communication standards, e.g., [b-IEEE 802.16], specified by the worldwide interoperability for microwave access (WiMAX) forum.

7 General characteristics of the Internet of things network capability exposure

This clause provides general characteristics of the IoT NCE.

7.1 Supporting multiple networks

The IoT NCE supports a wide variety of networks to expose their network capabilities. Different networks (e.g., 3GPP based, 3GPP2 based and WiMAX based) can be connected with the IoT NCE in order to publish part or all of their network capabilities on the IoT NCE.

The IoT NCE supports exposure of various types of network capabilities, including, but not limited to the following.

– Subscriber network information tracking capability: IoT applications and services can use this capability to dynamically track their subscriber network information (e.g., location, identifier, device capability, service type, access type, cell congestion).

– Quality of service (QoS) customization capability: IoT applications and services can use this capability to request networks to provide specific end-to-end QoS for their subscribers.

– Location capability: IoT applications and services can use this capability to get their subscribers' dynamic locations and historical location information.

– Charging capability: IoT application and services can use this capability to get charging information.

– Broadcasting capability: IoT applications and services can use this capability to initiate service requests from the network side and send data to their service subscribers.

– Network edge computing capability: Reasonable deployment of computation capability at network boundary can significantly reduce service latency and improve network efficiency.

7.2 Exposing network capabilities

On exposure of its reference points, networks can register and expose part or whole of their network capabilities on the IoT NCE. Additionally, the IoT NCE supports networks to manage access policies for their exposed capabilities as published on the IoT NCE.

The IoT NCE can expose reference points for IoT applications and services, with which the IoT applications or services can discover, subscribe and access network capabilities as exposed by the same or different network(s), even if the networks use different communication technologies.

7.3 Security

The IoT NCE allows the networks to control, through setting access policies, what or which types of IoT applications and services can subscribe and access their exposed network capabilities.

7.4 Compatibility

The IoT NCE supports networks to expose selected capabilities to IoT applications and services, via APIs defined by the Open Mobile Alliance (OMA), the Global System for Mobile Communications Alliance (GSMA), other standards development organizations (SDOs), or network providers' proprietary APIs.

The IoT NCE can support interworking with other platforms exposing network or service capabilities for special networks, e.g., a service capability exposure framework (SCEF) within 3GPP systems [b-3GPP TR 23.708] (see Appendix III).

8 Working models of the Internet of things network capability exposure

The IoT NCE supports two types of working model: the single network working model and the multiple networks working model. In these two working models, the IoT application and services interact with IoT devices through the networks; however, IoT applications and services access subscribed network capabilities via the IoT NCE, not directly to the networks.

8.1 Single network working model of the Internet of things network capability exposure

In the single network working model (see Figure 8-1), one network provider deploys a network (e.g., mobile network A) and also provides an IoT NCE to expose network capabilities.

In this single network working model, the network can register on the IoT NCE and can request the IoT NCE to expose network capabilities on the IoT NCE; the IoT NCE publishes network capabilities according to requests from the network. Whenever the states of the exposed network capabilities are changed, the network can notify updated states to the IoT NCE.

In addition, in this single network working model, IoT applications and services can register on the IoT NCE and can discover, subscribe and access one or more of the exposed network capabilities as published on the IoT NCE. When successfully subscribed to exposed network capabilities, IoT applications and services can get relevant notifications and can access subscribed network capabilities. According to the access requests from IoT applications and services, the IoT NCE can invoke target network capabilities to get services from the network and can forward the network responses to IoT applications and services.

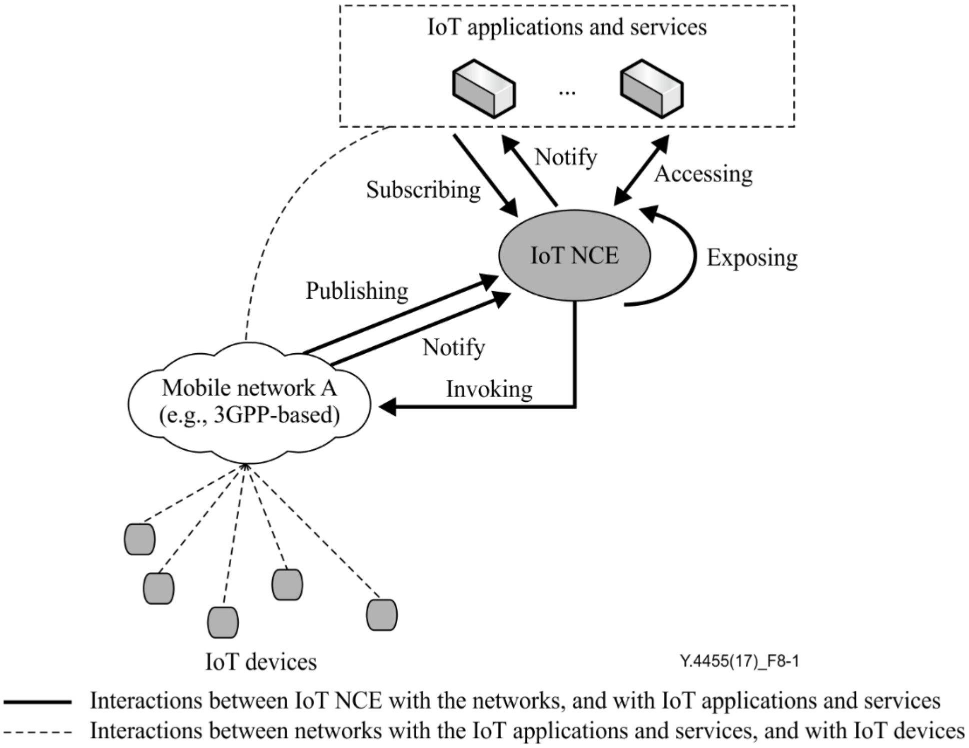
IoT applications and services
...
Notify
Accessing
Subscribing
IoT NCE
Exposing
Publishing
Notify
Invoking
Mobile network A
(e.g., 3GPP-based)
IoT devices
Y.4455(17)_F8-1
Interactions between IoT NCE with the networks, and with IoT applications and services
Interactions between networks with the IoT applications and services, and with IoT devices

Figure 8-1 – Single network working model of the IoT NCE

8.2 Multiple network working model of the Internet of things network capability exposure

In the multiple network working model (see Figure 8-2), networks (e.g., mobile network A and mobile network B) can be deployed by a single or by different network providers and the IoT NCE is independent of the networks.

As in the single network working model, exposed network capabilities need to be registered and published on the IoT NCE; and the networks should update the states of their exposed network capabilities.

Similarly, IoT applications and services can register on the IoT NCE and can discover, subscribe to and access one or more exposed network capabilities as published on the IoT NCE and can get relevant notifications.

The key differences from the single network working model are as follows.

- IoT applications and services can subscribe to network capabilities exposed by different networks.
- IoT applications and services can receive notifications as provided by different networks.
- When IoT applications and services access subscribed network capabilities for themselves or for indicated IoT devices, they should provide network information so that the IoT NCE can connect to the networks to invoke the network capabilities.

In Figure 8-2, an IoT service has subscribed to a network capability (such as the QoS customization capability referred to in clause 7.1) for the IoT device X (that remains in mobile network A) and the IoT device Y (that remains in mobile network B). The subscribed network capabilities are exposed by mobile networks A and B. When the IoT service requests this network capability for IoT devices X and Y, it needs to provide network-related information to allow the IoT NCE to recognize and interact with the target mobile networks A and B.

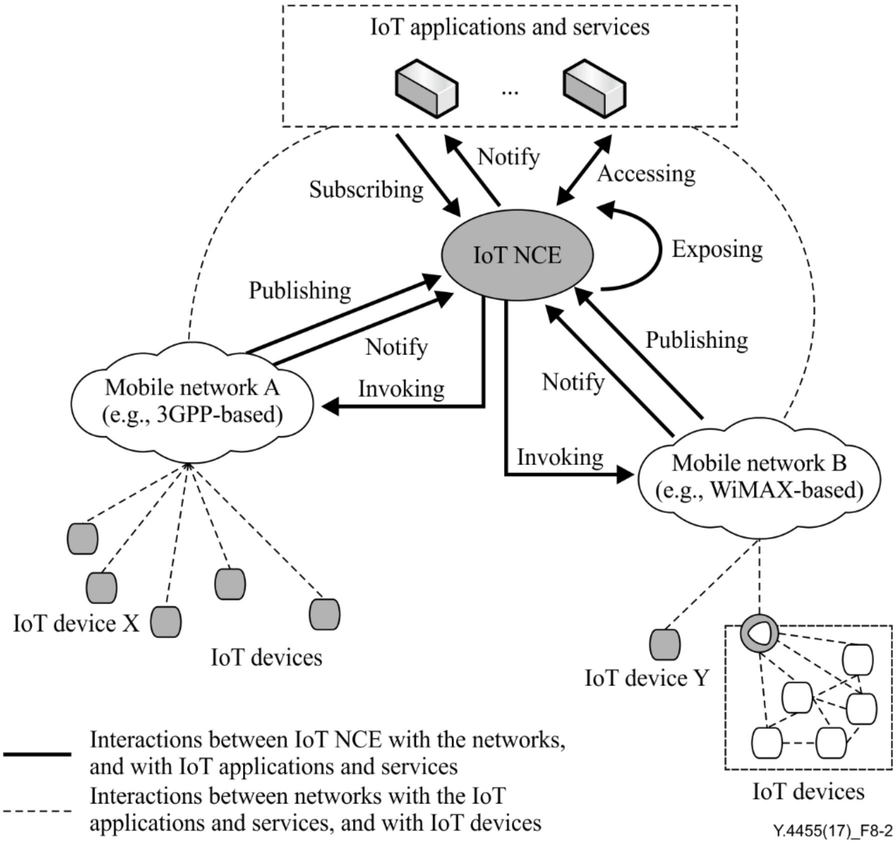

Figure 8-2 – Multiple networks working model of IoT NCE

9 Common requirements of the IoT NCE

This clause provides common requirements of the IoT NCE.

9.1 Requirements for publication of exposed network capabilities

Requirements and recommendations for publication of the exposed network capabilities follow.

- The IoT NCE is required to support authorized networks to register and publish their network capabilities.
- The IoT NCE is required to support authorized networks to manage (e.g., add, update, delete and search) their published network capabilities.
- The IoT NCE is recommended to allow authorized networks to set access policies for IoT applications and services accessing exposed network capabilities.

– The IoT NCE is recommended to support authorized networks to track the subscriptions of their exposed network capabilities.

9.2 Requirements for subscription of the exposed network capabilities

Requirements and recommendations for subscription to exposed network capabilities follow.

– The IoT NCE is required to support IoT applications and services to discover and subscribe the exposed network capabilities.

– The IoT NCE is required to support IoT applications and services to subscribe multiple exposed network capabilities provided by the same or different network(s).

– The IoT NCE is recommended to notify IoT applications and services, when the information of the subscribed exposed network capabilities are changed.

– The IoT NCE is recommended to notify authorized networks as needed, when their exposed network capabilities are subscribed.

9.3 Requirements for accessing exposed network capabilities

Requirements and recommendations for accessing exposed network capabilities follow.

– The IoT NCE is required to support authorized IoT applications and services to access one or more subscribed network capability(ies) provided by the same or different network(s).

– The IoT NCE is recommended to define access policies for exposed network capabilities based on configuration parameters (e.g., time/days, location).

9.4 Requirements for reference points

Requirements and recommendations for reference points follow.

– The IoT NCE is required to expose reference points for IoT applications and services to discover, subscribe to and access the network capabilities as published on the IoT NCE.

– The IoT NCE is recommended to expose reference points for networks to publish and manage network capabilities.

9.5 Security requirement

The following is the common security requirement for IoT NCE.

– The IoT NCE is required to authorize and authenticate IoT applications and services.

9.6 Other requirement

In addition to items listed in clauses 9.1 to 9.5, the following is also required.

– The IoT NCE is required to support statistics functions.

10 Reference architecture of the IoT NCE

The IoT NCE works at the service support and application support (SSAS) layer in the IoT reference model [ITU-T Y.4000] and provides a reference point (NCE-1) to IoT applications and services in the application layer. The IoT NCE cooperates with other external functional entities in the network layer and SSAS layer. In addition, the IoT NCE utilizes the management capabilities and security capabilities provided by other external functional entities. Figure 10-1 shows the reference architecture of the IoT NCE.

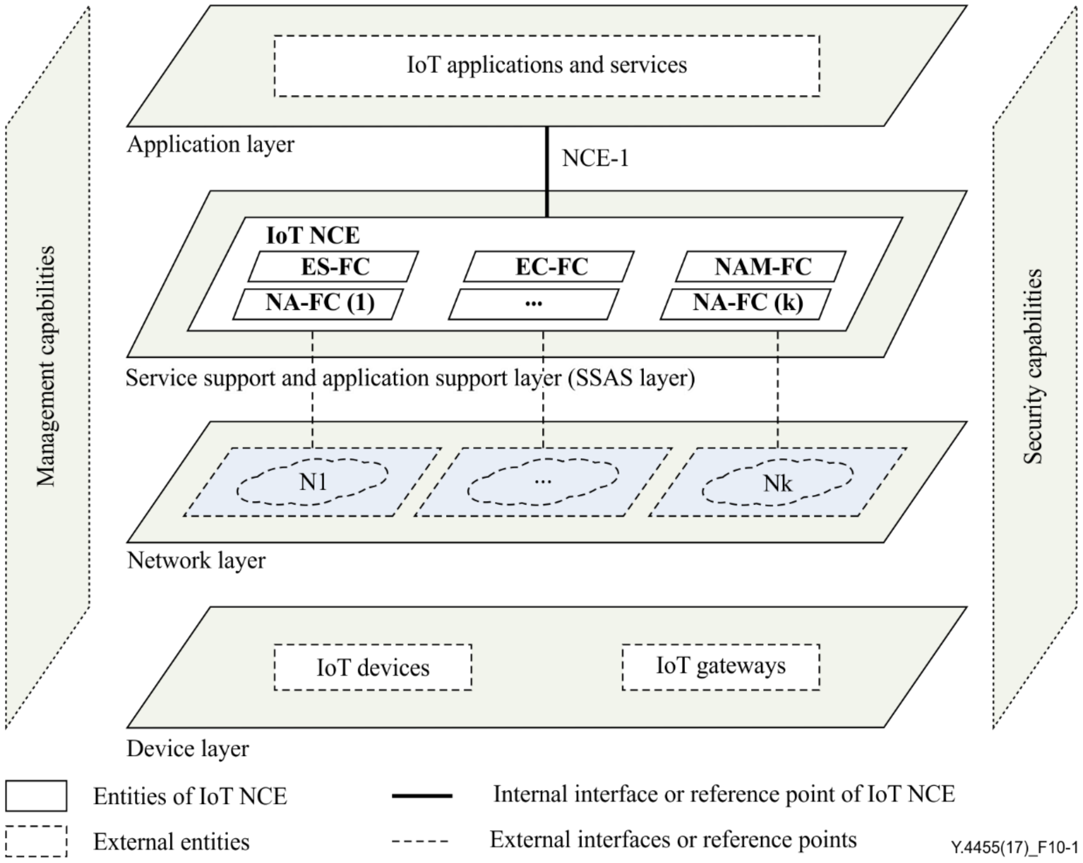

Figure 10-1 – Reference architecture of IoT NCE

The IoT NCE includes three functional components, namely the exposure supporting functional component (ES-FC), the exposure coordination functional component (EC-FC) and the network agent management functional component (NAM-FC), which operate at the SSAS layer. In addition, the IoT NCE contains a series of network agent functional components (NA-FCs) that interact with the external entities of the networks in the network layer.

As shown in Figure 10-1, the IoT NCE can cooperate with multiple networks (e.g., network N_1 to network N_k) and those networks can support different communication technologies.

Figure 10-2 shows the internal relationships between the functional components of the IoT NCE. The EC-FC exposes reference point NCE-1 to IoT applications and services. The NAM-FC manages the NA-FCs, the NA-FCs interact with networks. The ES-FC provides coordination functions and provides support to the EC-FC and NAM-FC.

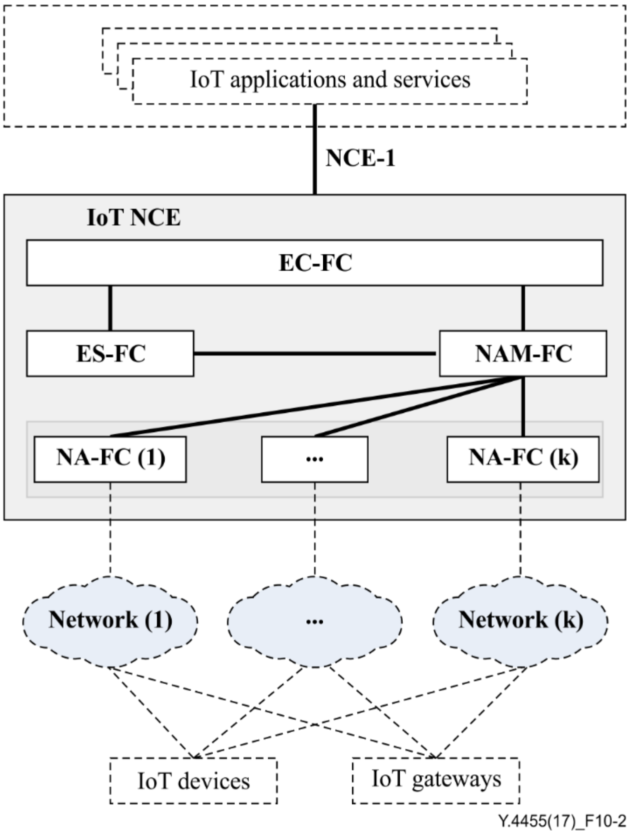

Figure 10-2 – Functional components of the IoT NCE

NOTE – The functional components of the IoT NCE coordinate with each other by internal interfaces. This Recommendation does not specify the internal interfaces.

10.1 Exposure supporting functional component

The ES-FC provides access control for networks to expose their network capabilities and provides access control for IoT applications and services to discover, subscribe to and access network capabilities exposed by networks.

The ES-FC, coordinating with other functional components of the IoT NCE, provides the following functionalities.

– Management for network capabilities exposed by networks:
  - registering or unregistering exposed network capabilities of networks;
  - managing the information (see clause 11.1) of registered network capabilities;
  - setting access profiles of exposed network capabilities;
  - maintaining states (e.g., available or unavailable) of exposed network capabilities.

– Publishing the exposed network capabilities of networks according to their access profiles and the policies of the IoT NCE.

– When IoT applications and services discover the published network capabilities:
  - providing information (see clause 11.1) on network capabilities to IoT applications and services.

– When IoT applications and services subscribe to published network capabilities:
  - validating access permissions related to the subscription;
  - maintaining the subscription state.

– When IoT applications and services access subscribed network capabilities:

- validating access permissions for access requests;
- processing access requests from IoT applications and services.

NOTE – The ES-FC can indicate access profiles for each network. The access profiles and the policies of IoT NCE include, but are not limited to:

– Rules for networks to expose their network capabilities.

– Rules for IoT applications and services to subscribe to and unsubscribe from exposed network capabilities.

– Rules for IoT NCE to notify subscribed information of the exposed network capabilities to the IoT applications and services.

– Rules for IoT applications and services to access the exposed network capabilities.

10.2 Exposure coordination functional component

The EC-FC exposes a reference point, NCE-1 (see clause 10.5), to allow IoT applications and services to discover, subscribe to and access exposed network capabilities.

The EC-FC, coordinating with other functional components of the IoT NCE, through reference point NCE-1, provides the followed functionalities:

– supporting IoT applications and services to discover and subscribe to published network capabilities,

– sending notifications when the state(s) of subscribed network capabilities are changed,

– supporting IoT applications and services to access subscribed network capabilities and providing data format transformation between the IoT NCE, and IoT applications and services, if needed.

10.3 Network agent management functional component

The NAM-FC manages NA-FCs and performs accesses to exposed network capabilities through NA-FCs subject to the requests of IoT applications and services.

The NAM-FC, coordinating with other functional components of IoT NCE, provides the following functionalities:

– supporting the ES-FC to manage the registration and exposure of network capabilities;

– calling the NA-FC to track the state(s) (e.g., available or unavailable) of exposed network capabilities;

– supporting the EC-FC to notify IoT applications and services of the updated state(s) of exposed network capabilities;

– supporting IoT applications and services to access subscribed network capabilities through NA-FCs.

10.4 Network agent functional component

The NA-FCs interact directly with networks subject to the requests of IoT applications and services and provide data transformation between the IoT NCE and relevant networks.

The NA-FC can interact with one or more networks.

The NA-FC, coordinating with other functional components of IoT NCE, provides the following functionalities:

– tracking the state(s) of exposed network capabilities, e.g., available or unavailable;

– interacting with networks to support IoT applications and services to access exposed network capabilities.

NOTE 1 – When an IoT application or service subscribes to one network capability published on the IoT NCE, if needed, the corresponding NA-FC can interact with the network that exposes the network capability to check the remote access permission (see clause 11.2).

NOTE 2 – The NA-FC can provide data format transformation between the IoT NCE and the networks. This Recommendation does not provide mechanisms on the data/protocol format transformation between the NA-FCs and the networks.

10.5 Reference point NCE-1

The reference point NCE-1 is exposed by the EC-FC to allow IoT applications and services to discover, subscribe to and access network capabilities published on the IoT NCE and to receive notifications about the updated states of the subscribed network capabilities.

The following interactions can be performed via the reference point NCE-1:

– IoT applications and services discover the network capabilities published on the IoT NCE;

– IoT applications and services subscribe to the network capabilities published on the IoT NCE;

– IoT applications and services access subscribed network capabilities;

– EC-FC notifies IoT applications and services of the updated state(s) of the subscribed network capabilities.

11 Common capabilities of the IoT NCE

This clause provides common capabilities that correspond to the requirements listed in clause 9.

11.1 Publishing

The IoT NCE is able to collect information on network capabilities to be exposed to IoT applications and services. The information about exposed network capabilities includes, but is not limited to:

– name of the network capabilities;

– description of the network capabilities;

– access approaches and relevant parameters;

– access profiles.

The IoT NCE is able to publish the collected information of network capabilities, in order to allow IoT applications and services to discover and subscribe.

Clause II.1 provides a reference procedure for exposing and publishing network capabilities.

11.2 Subscribing

The IoT NCE is able to allow IoT applications and services to discover and subscribe to published network capabilities on the IoT NCE, through the reference point NCE-1 exposed by the EC-FC.

The IoT NCE is able to support an IoT application or service to subscribe to one or more network capability(ies) and the subscribed network capabilities may be exposed by one or more networks.

In the subscription process, the IoT NCE is able to validate the access permission according to the policies of the IoT NCE and the access profiles related to the network capability.

Alternatively, the IoT NCE is also able to connect to the network that exposes the network capability to negotiate access permission.

Clause II.2 provides a reference procedure for subscribing to the published network capabilities.

NOTE – This Recommendation does not specify interactions between the IoT NCE and networks.

11.3 Accessing

When an IoT application or service requests to access subscribed network capabilities, the IoT NCE is able to support the IoT application or service to access the network capabilities. The IoT NCE is also able to verify the access permission as needed.

Clause II.3 provides reference procedures for accessing subscribed network capabilities.

11.4 Delivering

When an IoT application or service requests the IoT NCE to deliver information (e.g., information about IoT devices to be served) in order to invoke network capabilities, the IoT NCE is able to deliver the relevant request.

Clause II.4 provides related reference procedures.

12 Security considerations

The IoT NCE, IoT applications and services, IoT devices, and networks are usually deployed in different domains and may be in untrusted environments. The IoT NCE is required to provide a security mechanism to authorize and authenticate IoT applications and services to discover, subscribe to and access network capabilities.

Additionally, the security mechanism should support security transportation technologies such as transport layer security (TLS) when the IoT data are transported between the IoT NCE and IoT applications and services, and between the IoT NCE and the networks.

Appendix I

Use cases of the Internet of things network capability exposure

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

This appendix provides some use cases to illustrate the concept of the IoT NCE.

I.1 Use case for exposing mobility management capabilities

This case shows an IoT service called the car communication manager (CCM) service that facilitates its service subscribers (cars) to negotiate network resources with mobile networks to get expected communication resources.

It is assumed that there are three mobile networks (A, B and C) that each support different information and communication technologies (ICTs) individually (shown in Figure I.1) and the mobile networks have exposed their relevant network capabilities on the IoT NCE. It is also assumed that the mobile networks each provide mobile communication supports in turn when the car is moving from Area 1 to Area 4.

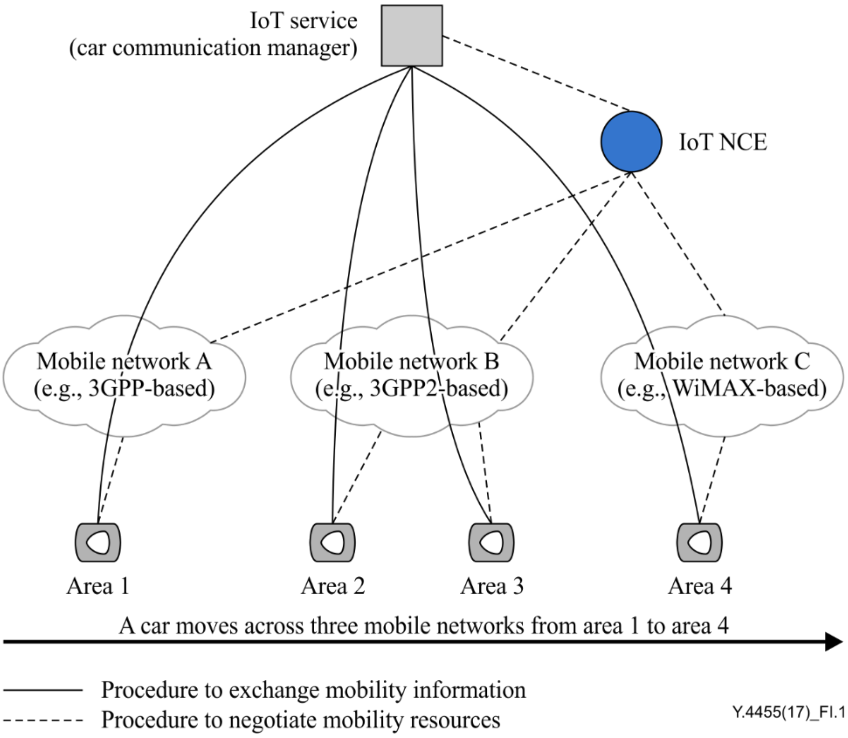
IoT service
(car communication manager)
IoT NCE
Mobile network A
(e.g., 3GPP-based)
Mobile network B
(e.g., 3GPP2-based)
Mobile network C
(e.g., WiMAX-based)
Area 1
Area 2
Area 3
Area 4
A car moves across three mobile networks from area 1 to area 4
Procedure to exchange mobility information
Procedure to negotiate mobility resources
Y.4455(17)_FI.1

Figure I.1 – Use case for exposing mobility management capabilities

If the car contains mobility sensors, the CCM service can get its dynamic mobility-related information (e.g., static or mobile, moving speed, location) uploaded by the car automatically. If the driver of the car wants to get consistent communication resources from the three mobile networks, he or she can subscribe to the relevant service from the CCM service. The CCM service can facilitate the car to get the expected communication resources with the following steps.

1 The CCM service subscribes to the exposed service capabilities for an enhanced mobile communication service exposed by the three mobile networks individually.

2 According to the real-time location of the car, the CCM service searches for a mobile network to serve the car through the subscribed service capabilities.

3 The CCM service calls the subscribed service capabilities to deliver the information about the car and its mobility information (including expected network resources) to the mobile network that is to provide the communication service to the car.

4 The mobile network then configures its mobility parameters to allocate network resources to the car to provide the expected optimized mobile communication, subject to the subscriptions of the CCM service and the mobility information of the car.

5 When the car moves to the next mobile network, the CCM service makes contact with it and repeats steps 2 to 4.

In this case, through publishing and exposing their capabilities about meticulous communication management to the CCM service and its subscribers via the IoT NCE, the CCM service and its subscribers can get the expected communication resources when crossing different mobile networks.

Appendix II

Common procedures of the Internet of things network capability exposure

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

This appendix provides some common procedures to illustrate the reference architectures (see clause 10) and common capabilities (see clause 11) of the IoT NCE.

II.1 Publication of the network capabilities to be exposed

Figure II.1 shows the common procedures of a network to expose and publish its network capabilities on the IoT NCE. The major procedures are outlined as follows.

Step 1: The network registers its network capabilities on the IoT NCE through the reference point NCE-1. The registration data provided by the network includes the information on the network and the information on the network capabilities to be exposed (see clause 11.1).

Steps 2 and 3: The NA-FC, collaborating with other functional components of the IoT NCE, processes the registration request, including validating the information and checking permission.

If the registration request is validated and accepted, the IoT NCE publishes the network capabilities.

Steps 4 and 5: The IoT NCE sends a response to the network. The response information includes whether the registration request is accepted, whether the network capabilities are published and the publishing information if published.

Step 6: If the registration request is accepted and the exposed network capabilities are published, the network should update the state of the network capabilities to the IoT NCE when the state is changed.

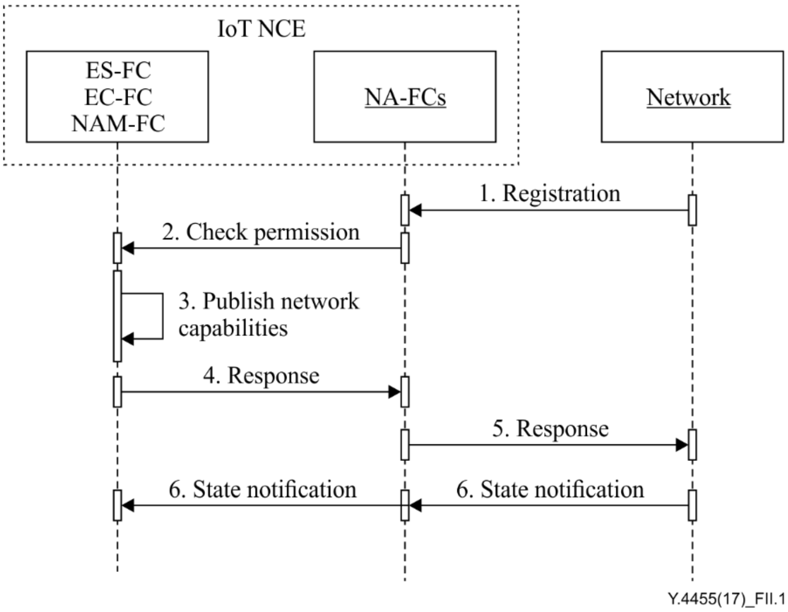

Figure II.1 – Flow for exposing and publishing network capabilities

II.2 Subscription to published network capabilities

Figure II.2 shows the common procedures of an IoT service to subscribe to published network capabilities on the IoT NCE. The major procedures are outlined as follows.

Step 1: An IoT service sends a subscription request to the IoT NCE to subscribe to one or a group of network capabilities. The target network capabilities can be exposed by one or more networks.

Step 2: The IoT NCE validates the subscription request and checks access permission of the IoT service to subscribe to the target network capabilities.

The IoT NCE checks access permission according to the access policies of the target network capabilities and the policies of IoT NCE.

The IoT NCE, if needed, can get remote access permission from the networks that expose the target network capabilities. In this case, if the target network capabilities are provided by different networks, the IoT NCE connects the networks one by one.

Steps 3, 4, 5 and 6: After checking the access permission, the IoT NCE sends a subscription response to the IoT service and sends a subscription notification to the networks that expose the target network capabilities.

If the subscription request is validated and accepted, the subscription response to the IoT service includes the information about the subscribed network capabilities (see clause 11.1). In this case, the subscription notification sent to networks includes subscription information (e.g., who is subscribing to the network capabilities and which network capabilities are subscribed).

If the subscription request is not validated or not accepted, the subscription response to the IoT service includes the rejection information and the IoT NCE may not send subscription information to the networks.

Step 7: If the subscription request is successful, the IoT NCE sends the IoT service the state notification that is received from the networks continuously; otherwise, the IoT NCE will not send anything to the IoT service.

NOTE – From the perspective of the IoT service, it is transparent that the NA-FCs interact with the networks exposing the network capabilities. The IoT service subscribes to the published network capabilities from the IoT NCE and does not interact directly with the networks.

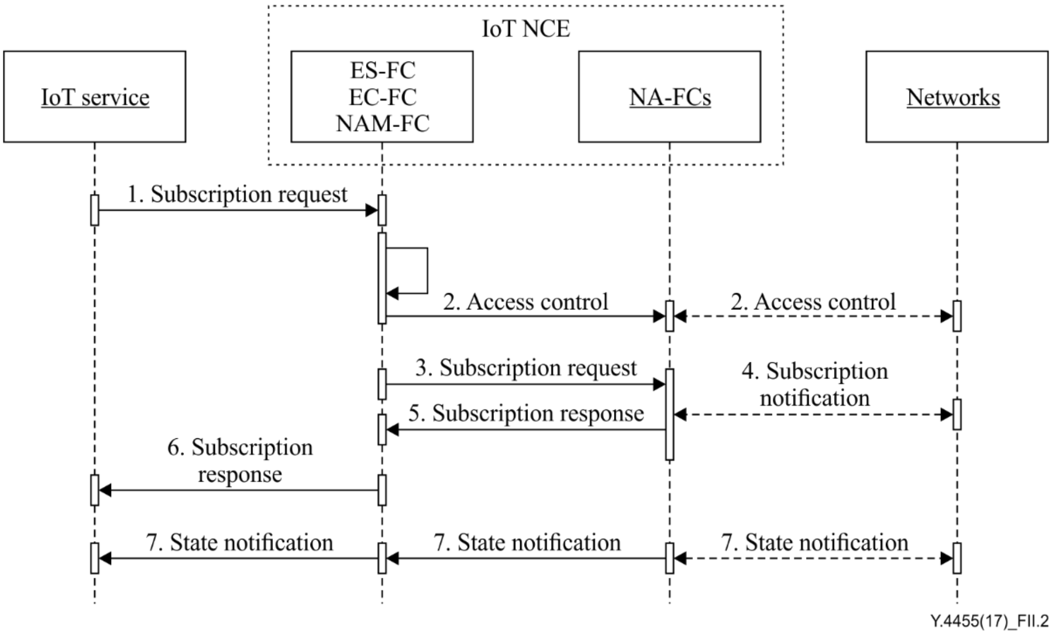

Figure II.2 – Flow for subscribing to published network capabilities

II.3 Accessing subscribed network capabilities from IoT service

Figure II.3 shows the common procedures of an IoT service to access subscribed network capabilities through the IoT NCE. The major procedures are outlined as follows.

Step 1: The IoT service sends the request to access the subscribed network capabilities to the IoT NCE through the reference point NCE-1. In the access request, it may include one or more network capabilities and the target network capabilities may be exposed by one or more networks.

Step 2: The IoT NCE validates the access request and checks access permission. If part or all of the target network capabilities in the access request are not subscribed, the IoT NCE may reject the access request.

NOTE – There are many methods for controlling access permission. The method in Step 2 is a simple example. This Recommendation does not limit the methods for controlling access permission.

Steps 3, 4, 5 and 6: If the access request is rejected, the IoT NCE sends the access response to the IoT service and includes the reasons for the rejection. The IoT NCE then ends the access request.

If the access request is accepted, the NA-FCs of the IoT NCE send access requests to the networks exposing the target network capabilities. In this case, if the target network capabilities are exposed by different networks, the IoT NCE calls the corresponding NA-FC to connect the networks one by one.

The IoT NCE receives the access response from the networks and forwards it to the IoT service.

When the access response is received for its access request, the IoT service may end this access request.

Step 7: After the access response, the networks may send access reports to the IoT NCE and the IoT NCE may forward part or all of the access reports to the IoT service.

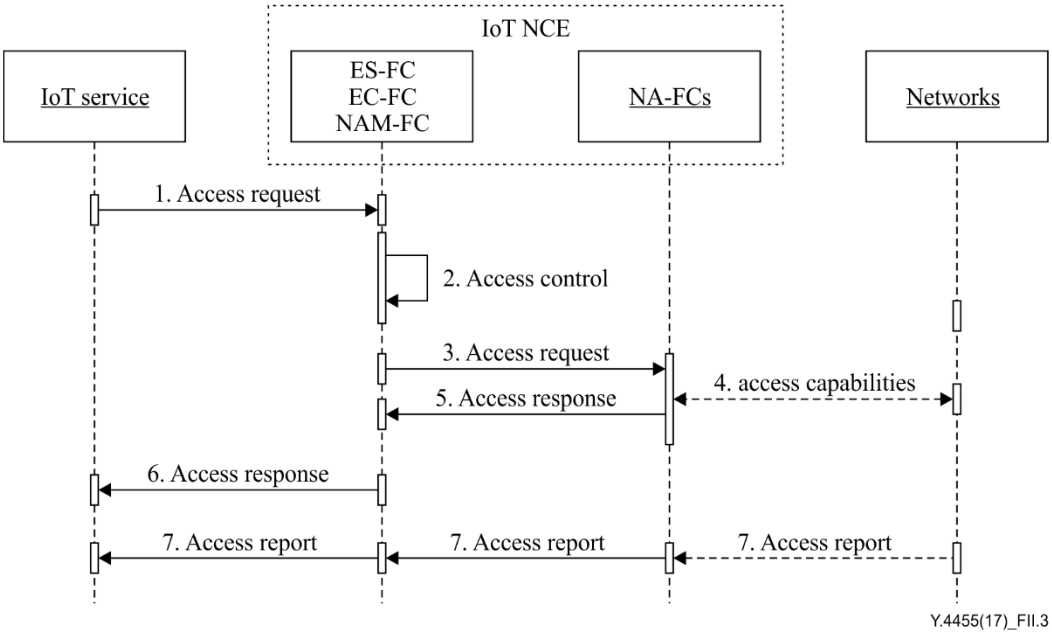

Figure II.3 – Flow for accessing subscribed network capabilities from the IoT service

NOTE – The corresponding NA-FC translates the access request according to the approaches with which the NA-FC interacts with the networks exposing the subscribed network capabilities. The NA-FC also translates the responses from the networks and forwards the translated responses to the IoT service through the reference point NCE-1.

II.4 Invoking the subscribed network capabilities to serve IoT devices

NOTE – This common procedure differs from that in clause II.3. An IoT application or service may request the networks providing the subscribed network capabilities to serve the indicated IoT devices. In this case, the IoT application or service can deliver information (e.g., a list of IoT devices to be served) to the network to invoke the network capabilities (e.g., to serve the IoT devices to be delivered through the request).

Figure II.4 shows the common procedures of an IoT service to invoke subscribed network capabilities through the IoT NCE in order to request the networks to serve indicated IoT devices. The major procedures are outlined as follows.

Step 1: The IoT service sends the IoT NCE the request to invoke the subscribed network capabilities to serve IoT devices. The invoking request can include one or more network capabilities and the target network capabilities can be exposed by one or more networks.

The invoking request also indicates the IoT devices to be served.

Step 2: The IoT NCE validates the invoking request and checks the access permission. If part or all of the target network capabilities in the invoking request are not subscribed, the IoT NCE may reject the invoking request.

NOTE – There are many methods for controlling access permission. The method in Step 2 is a simple example. This Recommendation does not limit the methods for controlling access permission.

Steps 3, 4, 5 and 6: If the invoking request is rejected, the IoT NCE sends the invoking response to the IoT service and includes the reasons for the rejection. The IoT NCE then ends the invoking request.

If the access request is accepted, the NA-FCs of the IoT NCE send invoking requests to the networks exposing the target network capabilities. In this case, if the target network capabilities are exposed by different networks, the IoT NCE calls the corresponding NA-FC to connect the networks one by one.

The IoT NCE receives the invoking response from networks and forwards to the IoT service.

When the invoking response is received for its invoking request, the IoT service may acknowledge the results and end this invoking request.

Step 7: If the networks accept the invoking request, they serve the indicated IoT devices to access the network capabilities that the IoT service subscribed and requested.

NOTE – The invoking request from the IoT service may include the identifiers of the IoT devices that will access the target network capabilities. This Recommendation does not limit the methods that networks use to identify IoT devices.

Step 8: When IoT devices access network capabilities according to the invoking request of the IoT service, the networks may send access reports to the IoT NCE and the IoT NCE may forward part or all of the access reports to the IoT service.

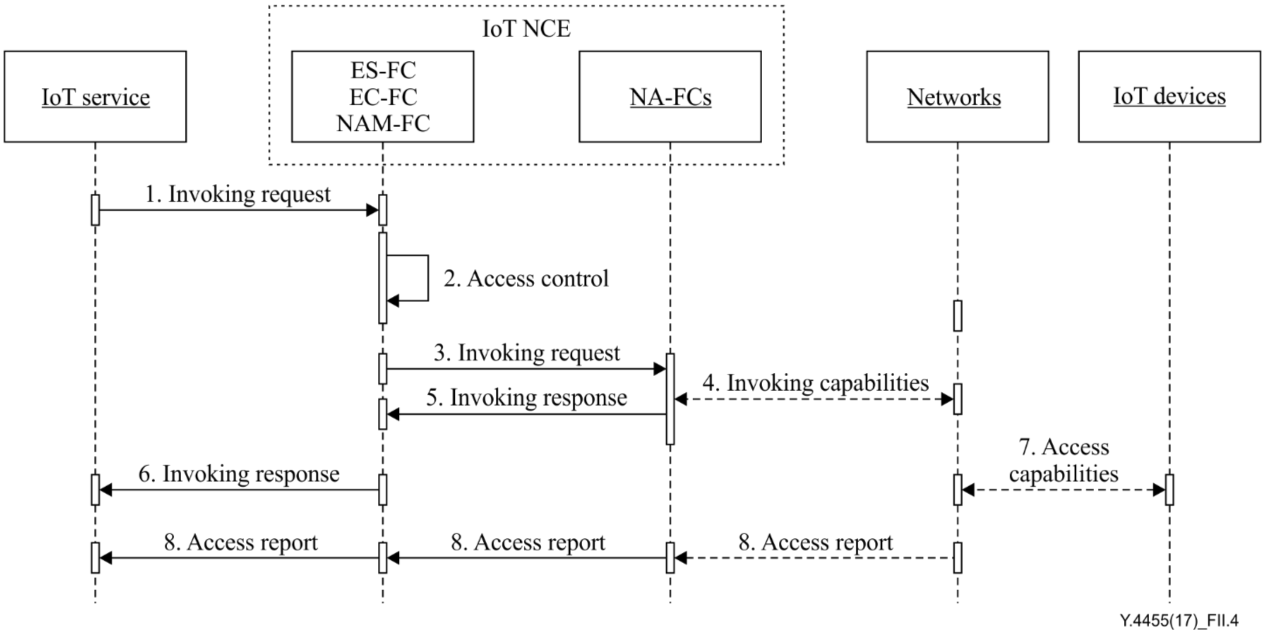

Figure II.4 – Flow for invoking to subscribed network capabilities to serve IoT devices

NOTE – The corresponding NA-FC translates the invoking request according to the approaches with which the NA-FC interacts with the networks exposing the subscribed network capabilities. The NA-FC also translates the responses from the networks and forwards the translated responses to the IoT service through the reference point NCE-1.

Appendix III

Interworking with service capability exposure framework within 3GPP systems

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

A SCEF can be deployed in a 3GPP system. Traditionally, the networks in the 3GPP system may publish network capabilities on the SCEF and the applications may access the published network capabilities through the SCEF.

The IoT NCE can interwork with the SCEF, based on a special NA-FC. The SCEF may expose the network capabilities on the IoT NCE.

In this case, when an IoT service accesses a network capability exposed by the SCEF, the special NA-FC transforms and forwards the access request to the SCEF and the SCEF then accesses the target network capabilities and forwards the access response to the NA-FC. The IoT NCE then transforms and forwards the access response to the IoT service.

Figure III.1 (a) and (b) shows the methods of interworking with SCEF within the 3GPP system.

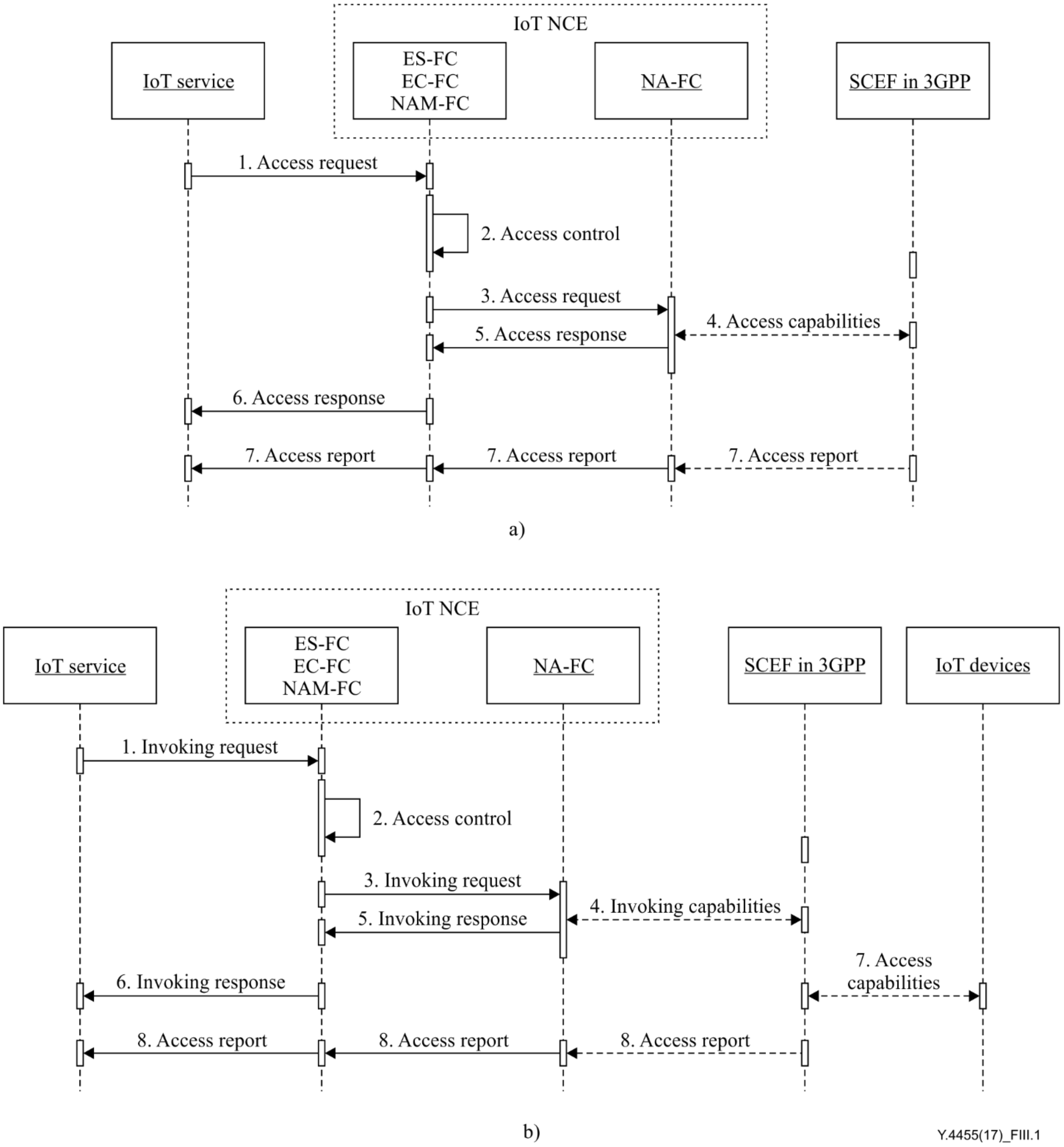

Figure III.1 – Flow for interworking with SCEF within 3GPP systems

Bibliography

[b-ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for International Mobile Telecommunications (IMT).*

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

[b-IEEE 802.16] ANSI/IEEE Std 802.16-2009, *IEEE Standard for local and metropolitan area networks – Part 16: Air interface for broadband wireless access systems*.

[b-3GPP TR 23.708] 3GPP TR 23.708 (2015), *Architecture enhancements for service capability exposure (Release 13).*
http://www.tech-invite.com/3m23/tinv-3gpp-23-708.html

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2017