International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4115

(04/2017)

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 – Requirements and use cases

Reference architecture for IoT device capability exposure

Recommendation ITU-T Y.4115

International Telecommunication Union

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.4115

Reference architecture for IoT device capability exposure

Summary

Recommendation ITU-T Y.4115 specifies the reference architecture of IoT device capability exposure (IoT DCE) which supports IoT applications in DCE devices (e.g., smart phones, tablets and home gateways) to access device capabilities exposed by IoT devices connected to the DCE device.

This Recommendation clarifies the concept of the IoT DCE, identifies its general characteristics and common requirements and provides the reference architecture for the IoT DCE and relevant high-level common procedures.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4115	2017-04-29	20	11.1002/1000/13266

Keywords

Device capability, device capability exposure, Internet of things.

* 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 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
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Introduction	2
7	General characteristics of IoT DCE	3
	7.1 Provision of standardized uniform interfaces	3
	7.2 Discovery and exposure of IoT devices	4
	7.3 Collection and exposure of data to IoT applications	4
	7.4 Collection and exposure capabilities of the connected IoT devices	4
	7.5 Access to the capabilities of the connected IoT devices	4
	7.6 Security and privacy protection	4
8	Common requirements of IoT DCE	4
	8.1 Communication with the IoT devices	4
	8.2 Publication of the IoT device capabilities	4
	8.3 Subscription to the exposed IoT device capabilities	5
	8.4 Access to the exposed IoT device capabilities	5
	8.5 Security protection and privacy preservation	5
9	Reference architecture of IoT DCE	5
	9.1 Profile management functional component (PM-FC)	6
	9.2 Auth agent management functional component (AAM-FC)	8
	9.3 Application management functional component (AM-FC)	8
	9.4 Device proxy management functional component (DPM-FC)	8
	9.5 Device proxy	9
	9.6 Auth agent	9
	9.7 Interface DCE-1	9
	9.8 DCE device and external entities	10
10	Common reference procedures of IoT DCE	10
	10.1 Registration of the IoT devices	10
	10.2 Publication of the exposed IoT device capabilities	10
	10.3 Subscription to the exposed IoT device capabilities	11
	10.4 Access to the exposed IoT device capabilities	13
11	Security considerations	13

Page

Appendix I – Use cases of IoT DCE 14
I.1 Leveraging personal data integration for wearable devices 14
I.2 Leveraging centralized controlling for home devices 15
Appendix II – Implementation example of IoT DCE 17
Bibliography 18

Recommendation ITU-T Y.4115

Reference architecture for IoT device capability exposure

1 Scope

This Recommendation specifies the reference architecture for IoT device capability exposure.

The scope of this Recommendation includes:

– the concept, general characteristics and requirements of IoT device capability exposure,

– the reference architecture for IoT device capability exposure including common procedures.

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

[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 [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 device [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, date capture, data storage and data processing.

3.1.4 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 device capability exposure (DCE): A functional entity to manage the connected Internet of things (IoT) devices in an IoT area network, to expose the capabilities of the connected IoT devices to IoT applications and to support the IoT applications to access the exposed device capabilities.

NOTE – Through device capability exposure, IoT applications can dynamically discover the connected IoT devices.

3.2.2 DCE device: A device (e.g., smart phone, tablet, home gateway) that hosts the device capability exposure (DCE) and connects to external IoT devices, and provides underlying hardware/software support for implementing the functionalities of DCE.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAM-FC	Auth Agent Management Functional Component of the IoT DCE
AM-FC	Application Management Functional Component of the IoT DCE
API	Application Programming Interface
DCE	Device Capability Exposure
DPM-FC	Device Proxy Management Functional Component of the IoT DCE
FC	Functional Component
IoT	Internet of Things
NFC	Near Field Communication
OS	Operating System
PC	Personal Computer
PM-FC	Profile Management Functional Component of the IoT DCE
UPnP	Universal Plug and Play
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity

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

IoT devices for individual consumers, especially wearable devices (e.g., watches, glasses, headbands and belts), are accepted in the market and are becoming more and more popular. Usually, consumers use their device capability exposure (DCE) devices (e.g., smart phones, tablets and home gateways) to manage IoT devices. There are two kinds of solutions for using DCE devices to manage IoT devices, vertical solutions and horizontal solutions.

In vertical solutions, a device manufacturer is usually also an application vendor. When a device manufacturer launches a new IoT device (e.g., a smart watch) onto the market, it has to provide its own applications (for each of the target operating system (OS) platforms) that will allow consumers to access and manage devices through their DCE devices. In addition, in vertical solutions there are many obstacles to one IoT application integrating the capabilities of different types of IoT devices at the same time.

In horizontal solutions, IoT devices and relevant applications are separated. Device manufacturers launch IoT devices and provide relevant software proxies supporting open uniform interfaces for the DCE devices. Based on the open standard interfaces, other application vendors can develop applications to access those of the IoT devices via the proxies. Therefore, horizontal solutions can overcome the disadvantages of the vertical solutions mentioned above.

The IoT device capability exposure (IoT DCE), a common integration middleware in DCE devices, uses one type of horizontal solution. The IoT DCE dynamically discovers, connects and accesses the IoT devices in an IoT area network, and exposes capabilities of the connected external IoT devices to upper IoT applications with standardized uniform interfaces. Using the uniform interfaces provided by the IoT DCE, the upper IoT applications in a DCE device can dynamically discover, subscribe and access the exposed capabilities of the IoT devices as published on the IoT DCE.

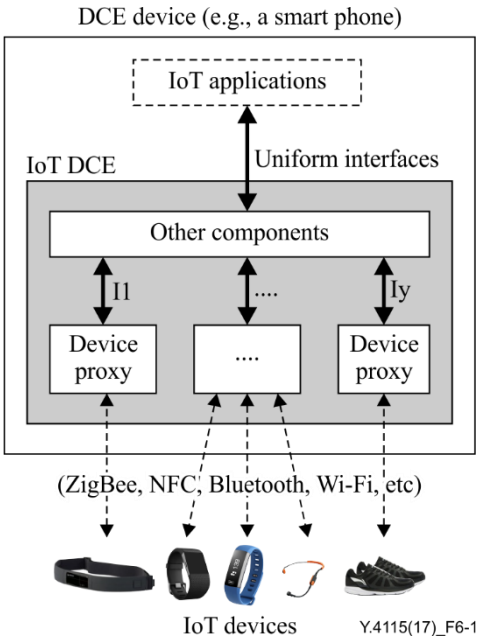

Figure 6-1 – Overview for IoT DCE

The IoT DCE in a DCE device (e.g., a smart phone) as shown in Figure 6-1, integrates the underlying device proxies through interfaces (e.g., *I1* to *Iy*) provided by the manufacturers to interact with relevant IoT devices (e.g., the hairpin, belt, watches, glasses and shoes) respectively and provides uniform interfaces to upper IoT applications, with which the upper IoT applications can access the device capabilities of those IoT devices.

7 General characteristics of IoT DCE

This clause describes the general characteristics of the IoT DCE.

7.1 Provision of standardized uniform interfaces

The IoT DCE provides standardized uniform interfaces. When using these standardized uniform interfaces, IoT applications can discover and access the data and capabilities of the IoT devices.

7.2 Discovery and exposure of IoT devices

The IoT DCE discovers the IoT devices automatically and exposes the information of the IoT devices to upper IoT applications. Through the standardized uniform interfaces exposed by the IoT DCE, the upper IoT applications have the capabilities to discover the connected IoT devices.

NOTE – The IoT DCE supports various kinds of device communication technologies, such as universal serial bus (USB), wireless fidelity (Wi-Fi), Bluetooth and near field communication (NFC).

7.3 Collection and exposure of data to IoT applications

The IoT DCE collects data from the connected IoT devices and exposes the data to upper IoT applications as needed. The upper IoT applications enable access to the data exposed by the IoT DCE.

7.4 Collection and exposure capabilities of the connected IoT devices

The IoT DCE collects the capabilities of the connected IoT devices automatically and exposes the capabilities to upper IoT applications. The upper IoT applications are enabled to discover the capabilities of the connected IoT devices.

7.5 Access to the capabilities of the connected IoT devices

The IoT DCE supports the upper IoT applications access to the capabilities of the IoT devices exposed by the IoT DCE. The IoT DCE receives and verifies the requests of the upper IoT applications and then forwards the requests to the connected IoT devices and delivers the results from the connected IoT devices to the upper IoT applications.

7.6 Security and privacy protection

The IoT DCE provides multi-level security and privacy protection support to IoT data and capabilities. The IoT DCE exposes the IoT data and device capabilities according to the security and privacy protection policies of the connected IoT devices.

8 Common requirements of IoT DCE

This clause provides common requirements of the IoT DCE.

8.1 Communication with the IoT devices

The communication-related requirement of the IoT DCE is as follows:

– The IoT DCE is required to be able to communicate with the IoT devices connected to the DCE device.

8.2 Publication of the IoT device capabilities

The IoT devices can register and publish their capabilities on the IoT DCE. The published information describes the device and relevant exposed device capabilities. In addition, the IoT devices can provide proxies to leverage the IoT DCE and the IoT applications to access the exposed device capabilities.

The publication-related requirements of the IoT DCE are as follows:

– The IoT DCE is required to support the IoT devices to publish their device capabilities.

– The IoT DCE is required to support the IoT devices to manage (e.g., add, update delete, etc.) published device capabilities.

– The IoT DCE is recommended to adhere to exposed IoT device policies.

8.3 Subscription to the exposed IoT device capabilities

The IoT applications can discover and subscribe one or more exposed device capabilities on the IoT DCE. After the discovery and subscription, the IoT applications can get the descriptions of the exposed device capabilities and notifications of the states of IoT devices. The descriptions of the exposed device capabilities include information of the devices and relevant exposed capabilities, and information to access the subscribed device capabilities as well as information on relevant access policies.

The subscription related requirements of the IoT DCE are as follows:

– The IoT DCE is required to support the IoT applications to discover and subscribe the exposed device capabilities.

– The IoT DCE is required to support the IoT applications to get the descriptions of accessing the subscribed exposed device capabilities.

– The IoT DCE is required to notify the IoT applications on the state of IoT devices and/or the exposed device capabilities as needed.

8.4 Access to the exposed IoT device capabilities

The IoT DCE can support the IoT applications to access the exposed device capabilities.

The access related requirement of the IoT DCE is as follows:

– The IoT DCE is required to permit the authorized IoT applications to access subscribed exposed device capabilities.

8.5 Security protection and privacy preservation

The security related requirements of the IoT DCE are as follows:

– The IoT DCE is required to provide the necessary security mechanisms when exposing device capabilities.

– The IoT DCE is required to provide privacy preservation when exposing device capabilities.

9 Reference architecture of IoT DCE

As described in clause 6, the IoT DCE is a functional entity in a DCE device and leverages IoT applications in the DCE device to discover and access the exposed capabilities of the IoT devices that are connected to the DCE device. The IoT DCE consists of four functional components, profile management (PM-FC), Auth agent management (AAM-FC), application management (AM-FC) and device proxy management (DPM-FC). In addition, the IoT DCE includes a group of extensible functional components, device proxies and Auth agents. The AM-FC of the IoT DCE exposes an interface, DCE-1, to support IoT applications to access the exposed IoT devices and relevant device capabilities. Figure 9-1 shows the reference architecture of IoT DCE.

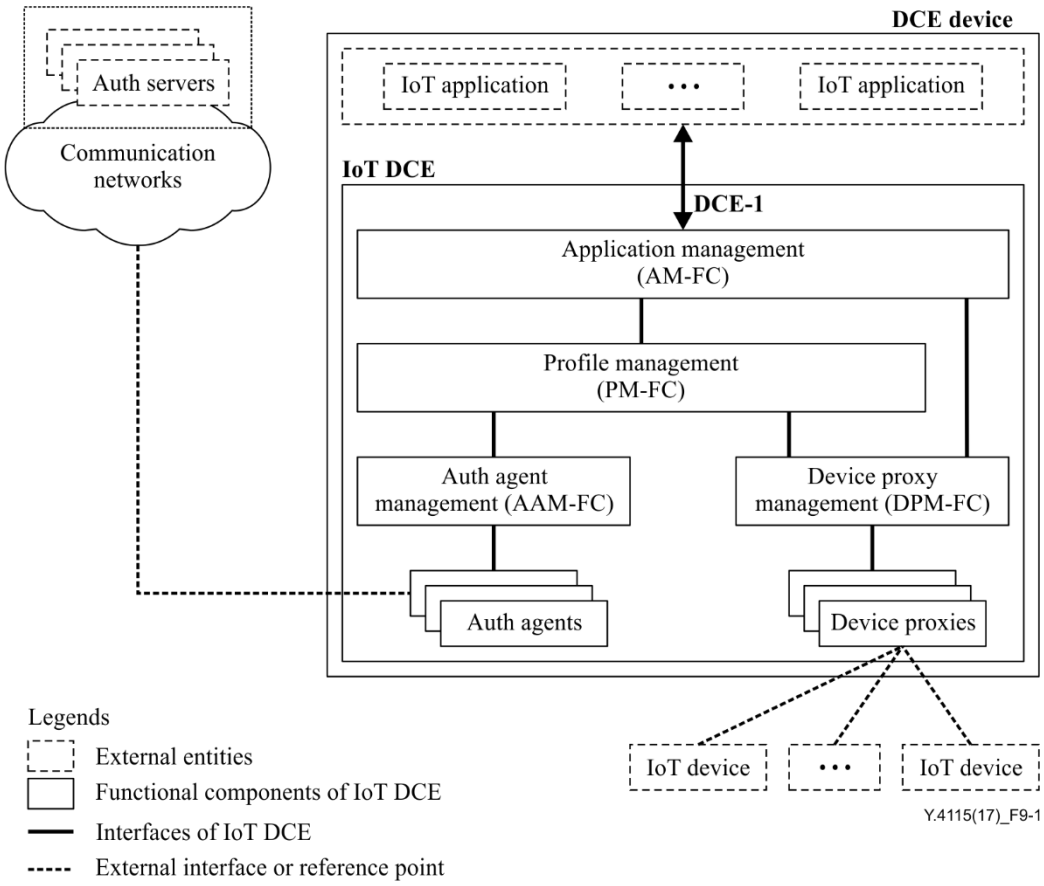

Figure 9-1 – Reference architecture of IoT DCE

NOTE 1 – The IoT DCE is working at the device layer in IoT reference model [ITU-T Y.4000].

NOTE 2 – The device proxies are responsible for communication directly with IoT devices connected with the DCE device. Each device proxy should support at least one type of communication technology (e.g., WI-FI, Bluetooth and Zigbee) for the IoT area network. This Recommendation does not specify the external interfaces for communications between the device proxies and the IoT devices.

NOTE 3 – Auth agents are responsible for communication with external Auth servers to provide remote access control functions for the IoT applications to subscribe and access the device capabilities published on the IoT DCE. This Recommendation does not specify the reference points for the communications between the Auth servers and the Auth agents.

9.1 Profile management functional component (PM-FC)

The PM-FC performs access control for the IoT applications to discover, subscribe and access the device capabilities exposed by the IoT devices.

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

– Management for device capabilities exposed by IoT devices,
  – Registering or unregistering exposed device capabilities of IoT devices.
  – Managing the information (see clause 10.2) of registered device capabilities.
  – Setting access profiles of the exposed device capabilities.
  – Tracking states (e.g., available or unavailable) of the registered device capabilities.
– Publishing the exposed device capabilities of IoT devices according to their access profiles and the policies of IoT DCE.

- Supporting IoT applications in order to discover the capabilities of the published device.
  - Providing information (see clause 10.2) of device capabilities to IoT applications.
- Supports IoT applications to subscribe the published device capabilities,
  - Validating the access permissions related to subscription.
  - Supporting IoT applications to subscribe or unsubscribe to the published device capabilities.
  - Maintaining the subscription state.
  - Notifying the IoT applications of the change states of the subscribed device capabilities.
- Supporting IoT applications to access subscribed device capabilities
  - Validating the access permissions for the access requests.
  - Processing the access requests from IoT applications, coordinating with other functional components of IoT DCE.

  NOTE 1 – The access profiles and the policies of IoT DCE include, but are not limited to:
  - Rules for IoT devices to register to and unregister from the IoT DCE.
  - Rules for IoT devices to expose their device capabilities.
  - Rules for IoT applications to subscribe and unsubscribe the exposed device capabilities of the IoT devices.
  - Rules for IoT DCE to notify subscribed information of the exposed device capabilities to the IoT applications.
  - Rules for IoT applications to access the exposed device capabilities of the IoT devices.

  NOTE 2 – For each IoT device, the PM-FC can indicate access profiles.

The PM-FC performs three types of access control modes, local access control, remote access control and hybrid access control:

- In the local access control mode, the PM-FC generates local access permissions for the IoT applications to subscribe or access the IoT devices and exposed device capabilities, based on the access requests and local access profiles. In this case, the local access permissions are the final access permissions.
- The remote access control mode is only applicable when an IoT device is associated with an available Auth agent. When an IoT application requests to subscribe or access those types of IoT devices and device capabilities, the PM-FC retrieves remote access permissions from external Auth servers through the associated Auth agent. In this case, the remote access permissions are the final access permissions.
- In the hybrid access mode, the PM-FC combines the local access permissions (see the local access control mode) and remote access permissions (see the remote access control mode) to generate final access permissions. The hybrid access mode is only applicable to the IoT devices which are associated with an available Auth agent.

  NOTE 3 – In the hybrid access mode, the IoT DCE can perform dual authorizations: local access permissions decide which IoT applications can subscribe and access the IoT devices and remote access permissions decide what device capabilities can be subscribed and accessed by the IoT application as having local access permissions. For example (see clause 9.8.3), the IoT DCE can use local access profiles to decide which IoT applications can subscribe and access the cardiac pacemaker and can use remote access permissions provided by a related Auth server to decide what device capabilities of the cardiac pacemaker can be subscribed and accessed by the indicated IoT applications.

9.2 Auth agent management functional component (AAM-FC)

The AAM-FC manages Auth agents and supports PM-FC to perform access control for the IoT applications to subscribe and access the device capabilities published on the IoT DCE.

The AAM-FC, coordinating with PM-FC, provides the following functionalities:

– Registration management of the Auth agents, e.g., registering or unregistering;

– Maintaining association state between the registered Auth agents and the connected IoT devices;

– Tracking states of the registered Auth agents, e.g., available or unavailable;

– Coordinating with Auth agents to retrieve remote access permissions for IoT applications to subscribe and access the device capabilities published on the IoT DCE.

NOTE – The AAM-FC interacts with the Auth agents using internal interfaces of the IoT DCE which are not specified in this Recommendation.

9.3 Application management functional component (AM-FC)

The AM-FC exposes the uniform interface, DCE-1 (see clause 9.7) and supports the IoT applications to discover, subscribe and access the device capabilities published on the IoT DCE.

The AM-FC, coordinating with the PM-FC and DPM-FC and device proxies, provides the following functionalities:

– Supporting the IoT applications to discover and subscribe the published device capabilities of the registered IoT devices,

– Sending the notifications when the state(s) of the subscribed device capabilities are changed,

– Supporting the IoT applications to access the subscribed device capabilities and performing data format transformation between the IoT DCE and the IoT applications if needed

NOTE – The AM-FC, coordinating with DPM-FC and associated device proxies, can create and maintain communication sessions (see clause 10.4) between an IoT application and an IoT device when they need to exchange real-time data streams within a continuous period of time.

9.4 Device proxy management functional component (DPM-FC)

The DPM-FC manages device proxies and IoT devices and supports the IoT applications to access the subscribed device capabilities. The DPM-FC manages and accesses IoT devices through device proxies.

The DPM-FC, coordinating with the PM-FC and AM-FC, provides the following functionalities:

– Registration management for device proxies, e.g., registered to or unregistered from the IoT DCE.

– Association state management for device proxies, e.g., associated with or disassociated from IoT devices.

– Supporting registration and publication functions as needed,

  – When an IoT device actively registers and publishes its device capabilities on the IoT DCE, the DPM-FC coordinates with PM-FC to manage relevant information (see clause 9.1).

– Tracking the state(s) (e.g., connected or disconnected) of the registered IoT devices through associated device proxies

– Tracking the state(s) (e.g., available or unavailable) of the exposed device capabilities of the registered IoT devices through associated device proxies

– Supporting the AM-FC to notify the IoT applications of the updated state(s) of the registered IoT devices and exposed device capabilities.

– Supporting IoT applications to access subscribed device capabilities of the IoT device(s), through associated device proxies.

The DPM-FC can provide data transformation between the IoT DCE and the IoT devices if needed.

9.5 Device proxy

The device proxy is a functional component of the IoT DCE, which interacts directly with its associated IoT device(s). The DPM-FC can manage multiple device proxies and each device proxy can be associated with one or more IoT devices.

The IoT DCE can generate new device proxies according to the request of IoT devices. In this case, the IoT devices need to provide relevant information to the IoT DCE.

The device proxy provides the following functionalities:

– Supporting the DPM-FC to track the state(s) of its associated IoT device(s), e.g., connected or disconnected.

– Supporting the DPM-FC to track the state(s) of the exposed device capabilities of its associated IoT device(s), e.g., available or unavailable.

– Coordinating with other functional components of IoT DCE to support the IoT applications to access the exposed device capabilities of its associated IoT devices

NOTE – The DPM-FC and the device proxies can perform data format transformation between the IoT DCE and the IoT device(s). This Recommendation does not provide mechanisms on the data format transformation.

9.6 Auth agent

The Auth agents, coordinating with external Auth servers, support the AAM-FC and the PM-FC to perform remote access controls (see clause 9.1) for IoT applications to subscribe and access device capabilities published on the IoT DCE. Each Auth agent can be associated with one external Auth server.

An Auth agent can optionally be associated with one or more IoT devices as connected to the IoT DCE. If an IoT device is not associated with any Auth agent, remote access control for this IoT device will not be performed.

The IoT DCE can generate new Auth agents according to the request of IoT devices. In this case, the IoT devices need to provide relevant information to the IoT DCE

The Auth agents provide the following functionalities:

– Interacts with external Auth servers to get remote access permissions for IoT applications to subscribe and access the device capabilities published on the IoT DCE.

NOTE – The AAM-FC interacts with the Auth agents using internal interfaces of the IoT DCE which are not specified in this Recommendation.

9.7 Interface DCE-1

The interface DCE-1 is exposed by the AM-FC to allow IoT applications to discover, subscribe and access the device capabilities published on the IoT DCE and to receive notifications about the updated states of the subscribed device capabilities.

The following interactions can be performed via the interface DCE-1:

– IoT applications discover the IoT devices connected to IoT DCE

– IoT applications discover the device capabilities published on the IoT DCE

– IoT applications subscribe to the device capabilities published on the IoT DCE

– IoT applications access the subscribed device capabilities

– AM-FC notifies IoT applications of the updated state(s) of the subscribed device capabilities

9.8 DCE device and external entities

9.8.1 DCE device

DCE devices host the IoT DCE and IoT applications. DCE devices connect to external IoT devices and provide underlying hardware/software supports for the IoT DCE and IoT applications.

9.8.2 IoT device

The IoT devices [ITU-T Y.4000] are external entities of the IoT DCE. The IoT devices connect to the DCE devices and communicate with IoT DCEs and IoT applications. The device capabilities of an IoT device can be registered and published on the IoT DCE. Through the IoT DCE, the IoT applications on the DCE device can interact with the IoT devices connected to the DCE device.

9.8.3 Auth server

Auth servers in the network domain are external entities and optional for the IoT DCE. The Auth servers, cooperating with relevant Auth agents of IoT DCEs, perform remote access control for the IoT applications to subscribe and access the published device capabilities of the IoT devices through the IoT DCE.

One Auth server can serve multiple Auth agents.

NOTE – Auth Servers can be deployed by third parties to control exposing and accessing policies for specific IoT devices. For example, a cardiac pacemaker vendor can deploy an Auth server and provide specific Auth agents, with which to implement access controls to only allow the IoT applications to access data from relevant cardiac pacemakers and not to access other critical device capabilities (e.g., start, stop and adjust the cardiac pacemakers).

10 Common reference procedures of IoT DCE

10.1 Registration of the IoT devices

There are two kinds of approaches to register IoT devices to the IoT DCE; one is initiated by IoT devices and the other is initiated by the IoT DCE.

If an IoT device supports registration functions, it can register itself to the IoT DCE. In this case, the IoT device can provide needed information (see clauses 9.5 and 9.6) and request the IoT DCE to generate a new device proxy and/or a new Auth agent and then associate with them; alternatively, the IoT device can associate itself with an existing device proxy and/or an existing Auth agent in the IoT DCE.

The IoT DCE can discover the connected IoT devices. When an unregistered IoT device is found, the IoT DCE can register the IoT device and associate the IoT device with an existing device proxy and/or Auth agent.

10.2 Publication of the exposed IoT device capabilities

When an IoT device is registered to the IoT DCE, the information about its device capabilities to be exposed to IoT applications can be published on the IoT DCE. The information on the exposed device capabilities includes, but is not limited to:

– Name of the device capabilities
– Description of the device capabilities
– Access approaches and relevant parameters
– Access profiles

The above information can be delivered by IoT devices and can also be collected by the IoT DCE.

The PM-FC manages and publishes the information of the exposed device capabilities of the registered IoT devices, according to the policies of the IoT DCE and the access profiles related to the device capabilities.

When the device capabilities of an IoT device are published on the IoT DCE, the IoT applications can discover, subscribe and access those device capabilities through the DCE-1 interface.

10.3 Subscription to the exposed IoT device capabilities

10.3.1 Subscription with local access permissions

This procedure shows how an IoT application subscribes the published device capabilities of an IoT device on the IoT DCE (see Figure 10-1).

In this procedure, the IoT application requests to subscribe to the exposed device capabilities; then the IoT DCE sends relevant notifications to the IoT application if the subscription requests are accepted. The main steps are outlined below:

Step 1 An IoT application sends a request to the IoT DCE through the interface DCE-1 for subscribing exposed IoT device capabilities of an IoT device. The AM-FC processes the request.

Step 2 The AM-FC requests the PM-FC to verify the relevant access permission. The PM-FC then verifies and generates the access permission according to the relevant access profiles and forwards the results to the AM-FC.

Step 3 The AM-FC responds to the subscription request according to the access permission. If the IoT application cannot get permission to access the IoT device and the relevant exposed capabilities, the subscription request is rejected; then the procedure is stopped.

Step 4 If the subscription request is accepted, the IoT DCE continuously tracks the states of the subscribed IoT device and the relevant exposed capabilities. The PM-FC cooperates with the DPM-FC to monitor the relevant state.

Step 5 If the relevant states are changed, the AM-FC generates and sends the relevant notifications (see clause 9.7) to the IoT application through the interface DCE-1.

Figure 10-1 shows the flow when subscribing IoT device capabilities with local access permissions.

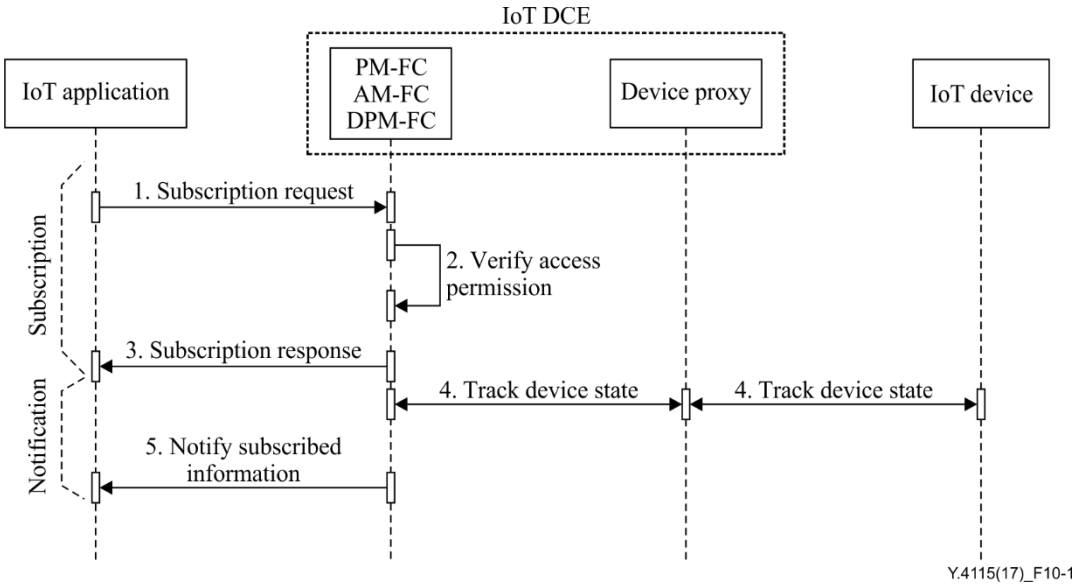

Figure 10-1 – Flow for subscribing IoT device capabilities with local access permissions

10.3.2 Subscription with remote access permissions

This procedure shows how an IoT application subscribes to the published device capabilities on the IoT DCE. The IoT device is associated with an Auth agent (see Figure 10-2).

In this procedure, the IoT application requests to subscribe the exposed IoT device capabilities; then the IoT DCE sends the relevant notifications to the IoT application if the subscription requests are accepted. The main steps are outlined below:

Step 1 An IoT application sends a request to the IoT DCE through the interface DCE-1 for subscribing exposed device capabilities of an IoT device. The AM-FC processes the requests.

Step 2 The AM-FC requests the PM-FC to verify access permission. The PM-FC verifies and generates a local access permission according to relevant local access profiles and then requests the AAM-FC to perform a remote access permission validation. The AAM-FC calls the associated Auth agent to request the remote access permission.

Step 3 The associated Auth agent forwards the request to the relevant external Auth server (if one exists). The Auth server checks the request and generates a remote access permission and sends the remote access permission to the associated Auth agent.

Step 4 The associated Auth agent sends the remote access permission to the PM-FC through the AAM-FC.

Step 5 The PM-FC combines the local access permission and remote access permission (if the remote access permission has been successfully obtained) to generate a final access permission. The PM-FC then forwards the final access permission to IoT application via the AM-FC and interface DCE-1.

NOTE 1 – If the relevant external Auth server does not exist and/or does not respond to the request, the IoT DCE can send a rejection information to IoT application and terminate the procedure; optionally, the IoT DCE can only perform local access permission control.

NOTE 2 – If the IoT application cannot get permission to access the exposed device capabilities, the subscription request is rejected; then the procedure is stopped.

Step 6 Same as *step 4* in Figure 10-1.

Step 7 Same as *step 5* in Figure 10-1.

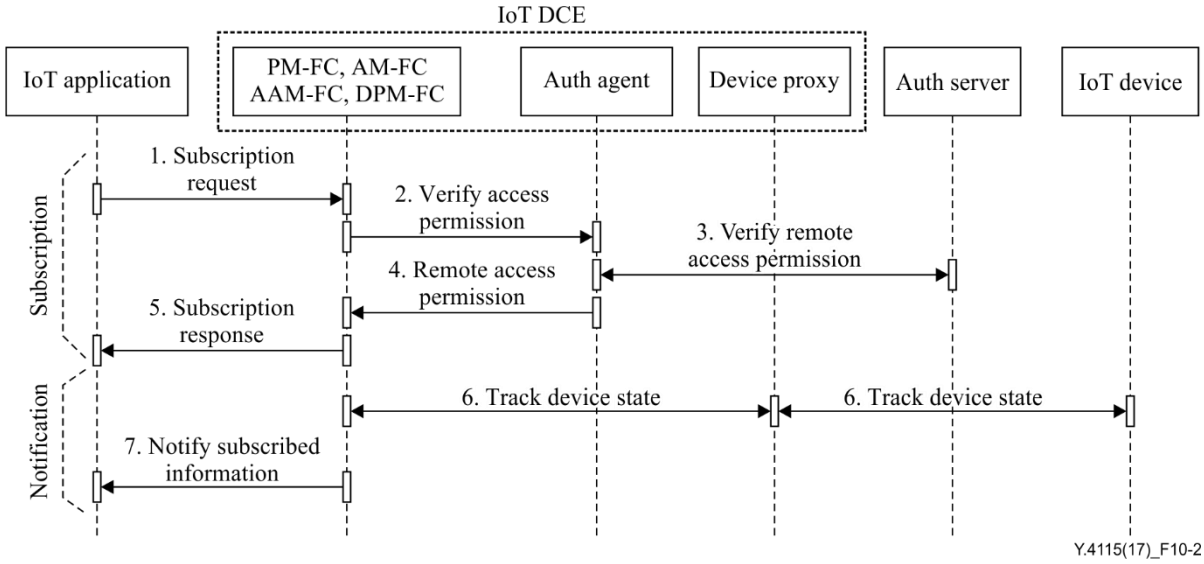

Figure 10-2 – Flow for subscribing IoT device capabilities with remote access permissions

10.4 Access to the exposed IoT device capabilities

When an IoT application is successful in subscribing to an IoT device and the relevant exposed device capabilities, it can request to interact with the IoT device through interface DCE-1 when the IoT device is connected to the DCE device. The IoT DCE verifies the access permission and provides support to establish communication sessions between the IoT application and IoT device.

Figure 10-3 shows high level procedures for an IoT application to access an IoT device and its exposed capabilities, the main steps are outlined below:

Step 1 An IoT application requests to access an exposed device capability of an IoT device. This request is sent to the AM-FC through the interface DCE-1. The AM-FC requests the PM-FC to verify the relevant access permission.

Step 2 The PM-FC verifies the relevant access permission for the access request. If the IoT application does not subscribe to the device capabilities, the PM-FC rejects the request, then generates objection information and proceeds to *step 4*; otherwise it goes to *step 3*.

Step 3 The AM-FC forwards the access request from the IoT application to the DPM-FC. The DPM-FC calls the associated device proxy to check the device state of the IoT device. The device state may include: whether the IoT device is connected and active, whether the IoT device supports the needed device capability, etc.

Step 4 The AM-FC sends the access response to the IoT application via interface DCE-1. If the request is rejected, or the device is unavailable, or the device capabilities are not supported, the IoT application should stop to access the IoT device; otherwise it proceeds to *step 5*.

Step 5 The IoT application continues to access the device capabilities. A communication session is established between the IoT application and the IoT device. The IoT application uses this session to interact with the IoT device.

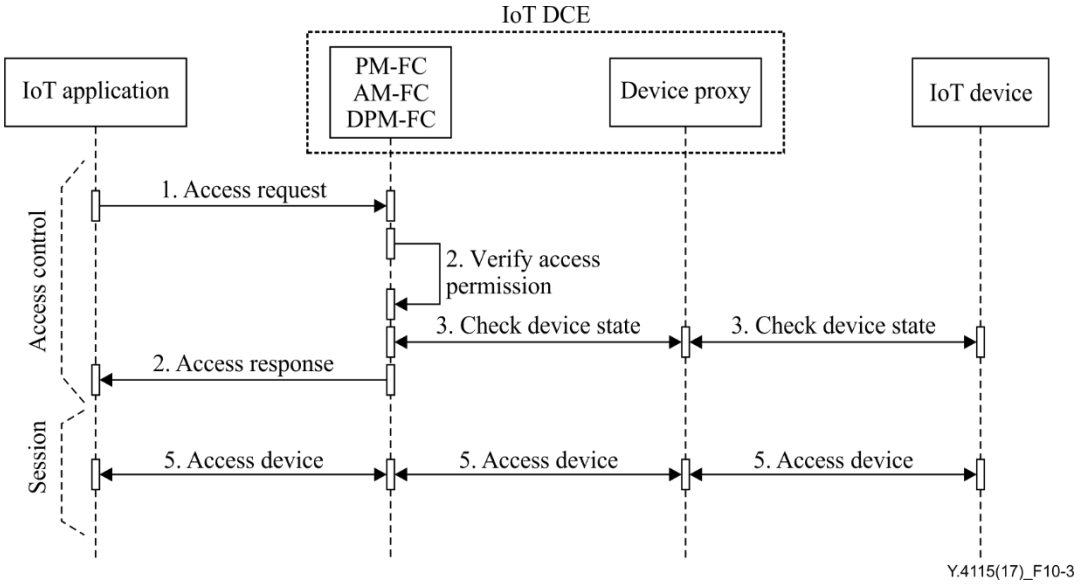

Figure 10-3 – Flow for accessing to exposed IoT device capabilities

11 Security considerations

The IoT DCE can provide privacy preservation via profile management functions performed by the PM-FC when exposing device capabilities.

Appendix I

Use cases of IoT DCE

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

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

I.1 Leveraging personal data integration for wearable devices

Wearable devices are becoming more popular and one person may have more than one wearable device. In typical vertical solutions (see Figure I.1), one application in a user's smart phone is usually related to one brand of wearable devices. For instance, as shown in Figure I.1, glasses proxy and relevant Apps can only interact with one type of glass.

If a personal info app (PInfo App) in a smart phone wants to integrate personal data from the user's glasses, belts and shoes, it needs to use the proprietary interfaces (e.g., *Iga*, *Iba* and *Isa*) provided by the relevant proxies individually. If the user buys other wearable devices, the PInfo App should be updated to support new IoT devices. However this is not very convenient and creates a bad user experience.

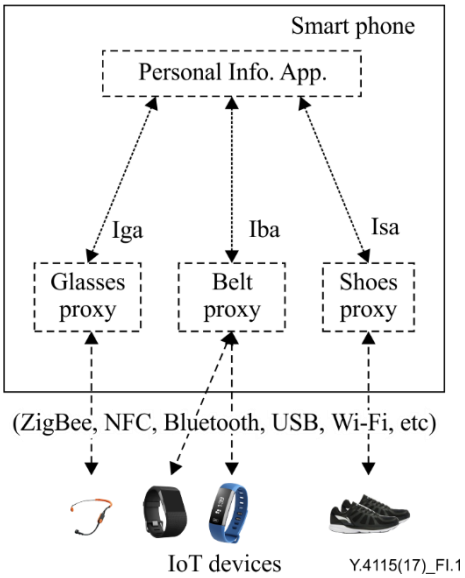

Figure I.1 – Use case of personal data integration – Typical case

If an IoT DCE is deployed in the smart phone, as shown in Figure I.2, the PInfo App only interacts with the IoT DCE and not directly with the wearable devices individually. Used with the interface DCE-1 provided by the IoT DCE, the Pinfo App can dynamically discover and access the wearable devices. The IoT DCE can dynamically monitor and integrate devices' proxies and relevant wearable devices and exposes the devices' capabilities to the upper IoT applications (e.g., the Pinfo App). In this scenario, it is unnecessary for the Pinfo App to know and integrate the proprietary interfaces (e.g., *Iga*, *Iba* and *Isa*). The IoT DCE enhances personal data integration efficiencies and improves the relevant user experiences.

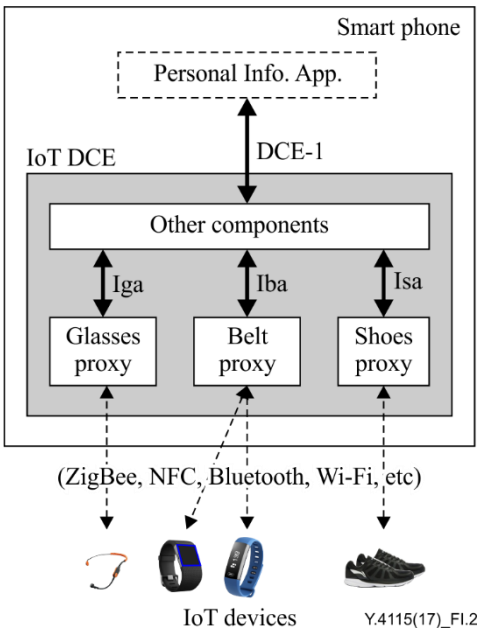

Figure I.2 – Use case of personal data integration – Case using IoT DCE

I.2 Leveraging centralized controlling for home devices

Smart home devices (e.g., as shown in Figure I.3, sensing devices, smart appliances, health devices and smart furniture) usually come from different vendors which may support various types of communication technologies defined by other standard development organizations (SDOs), such as open interconnect consortium (OIC) or the UPnP forum, etc.

Assuming that a user's smart phone hosts the IoT DCE and a relevant IoT application such as the home device centre (HDC App). The user can use the HDC App to manage his home devices even though the devices support different communication technologies. When the user is back at home, the IoT DCE dynamically discovers the user's home devices and exposes the devices' capabilities to the HDC App according to the user's policy, the user then selects and accesses his/her home devices. In this case, the user only uses one application, the HDC App, to manage all of his/her home devices.

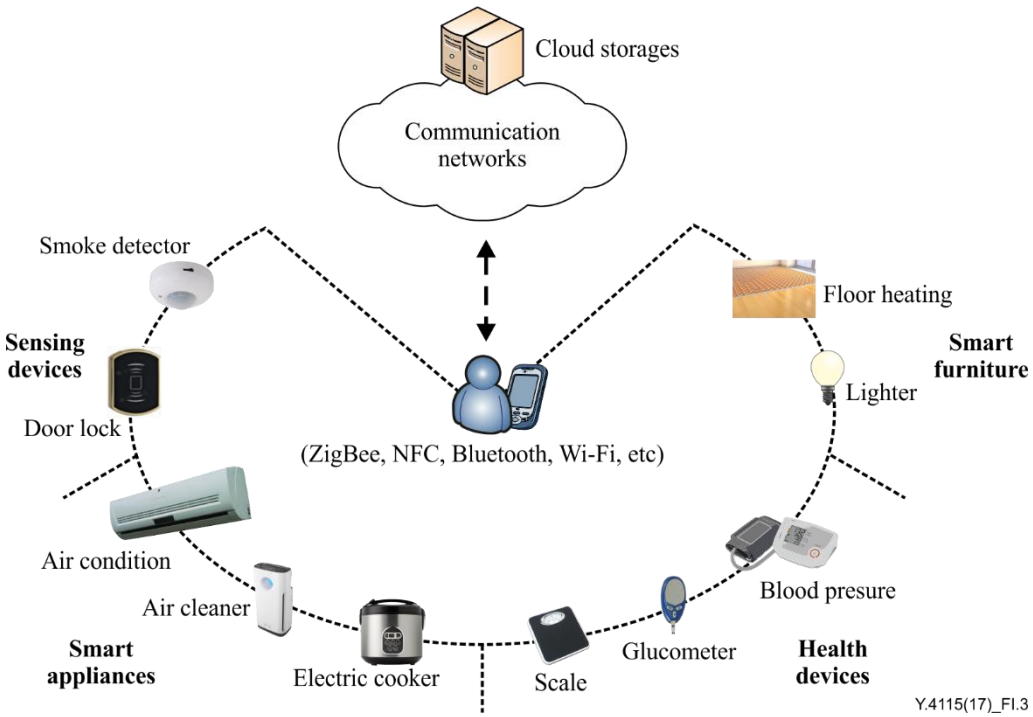

Figure I.3 – Use case of centralized controlling for home devices

Appendix II

Implementation example of IoT DCE

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

NOTE – This appendix takes an operating system (OS) platform as an implementaton example to illustrate the reference architecture of the IoT DCE. Note that each type of OS platform for IoT DCE may have specific proprietary implementation mechanisms.

As an example, an IoT DCE can work both the application framework layer and libraries layer, as shown in Figure II.1.

The device proxies and Auth agents can utilize functions provided by the application framework and libraries and underlying infrastructure, to interact with the connected IoT devices (e.g., home devices, wearable devices), or to interact with external Auth servers respectively.

The AM-FC exposes a group of APIs, the interface DCE-1, subject to the rules of the application framework. When using these APIs, IoT applications can discover, subscribe and access the published device capabilities of the IoT devices.

The IoT DCE can utilize the security and management functions provided by OS to provide security protection.

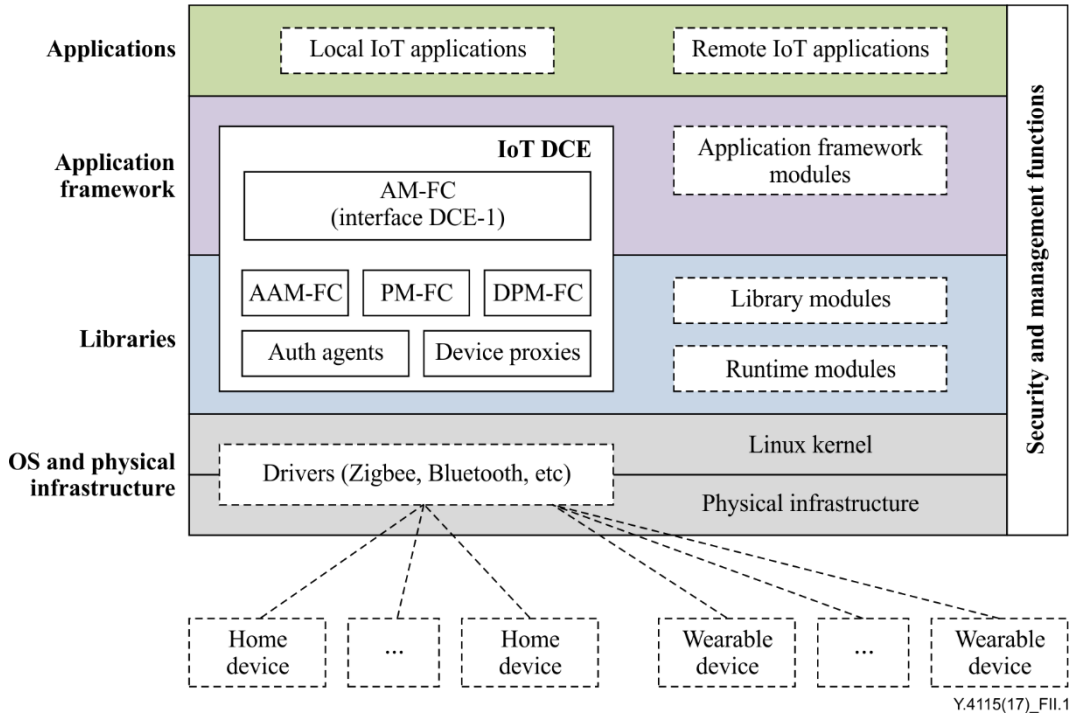

Figure II.1 – Implementation example of IoT DCE

Bibliography

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

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