International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4553

(03/2016)

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

Internet of things and smart cities and communities – Services, applications, computation and data processing

Requirements of smartphone as sink node for IoT applications and services

Recommendation ITU-T Y.4553

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	**Y.4550–Y.4699**
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899

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

Recommendation ITU-T Y.4553

Requirements of smartphone as sink node for IoT applications and services

Summary

Recommendation ITU-T Y.4553 provides common requirements of a smartphone working as a sink node (SPSN) for Internet of things (IoT) applications and services. Recommendation ITU-T Y.4553 clarifies the concept of a sink node in the IoT domain, and identifies the characteristics, work modes and the high level functional requirements of the SPSN. Cases of use are provided in an appendix.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4553	2016-03-15	20	11.1002/1000/12779

Keywords

Mobile network, sensor network, sink node, smart phone.

---

* 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

Introduction

With the enormous growth in numbers of mobile phone subscribers, smartphones are being deployed as display terminals for many Internet of things (IoT) applications and services. The use of a smartphone as a sink node to collect various pieces of information from the IoT is becoming more and more popular. For example, a near-field communication- (NFC)-enabled smartphone can be paired with NFC tags or stickers that can be programmed by NFC APPs to automate tasks. In E-commerce, smartphones are used to obtain credit card information and operate as point of sale (POS) terminals. With the powerful computing, communication and storage capacities of these mobile terminals, it is anticipated that the smartphone will act as one of the key devices in the IoT system. The objective of this Recommendation is to develop common requirements for the smartphone as a sink node for IoT applications and services.

Recommendation ITU-T Y.4553

Requirements of smartphone as sink node for IoT applications and services

1 Scope

This Recommendation specifies common requirements for a smartphone acting as a sink node as well as an end user terminal and a mobile gateway for IoT applications and services. More specifically, this Recommendation covers:

– the concept and characteristics of a sink node of the IoT system;

– work modes of a smartphone as a sink node (SPSN) for IoT applications and services;

– requirements for the use of a smartphone as a sink node for IoT applications and services.

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*.

[ITU-T Y.4101] Recommendation ITU-T Y.4101/Y.2067 (2014), *Common requirements and capabilities of a gateway for Internet of things applications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 gateway [ITU-T Y.4101]: A unit in the Internet of things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

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 – 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 sink node: A node in IoT which collects and/or transfers information from/to a group of Internet of things devices (e.g., wearable sensors) in an end user network.

3.2.2 smartphone as a sink node: A smart phone that supports the functionalities of a sink node.

NOTE 1 – In local service mode, a smartphone as a sink node can process collected information locally (e.g., data sorting, format changing, and forwarding), and is the last unit in the flow of information processing (i.e., the smartphone consumes the collected information and does not forward it to a control centre or external entities).

NOTE 2 – In remote service mode, a smartphone as a sink node can forward collected information to remote IoT applications and services through communication networks (i.e., the smartphone does not consume the collected information, but forwards it to other entities over an communication network).

NOTE 3 – A smartphone as a sink node can support local and remote service modes simultaneously.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G second Generation

3G third Generation

4G fourth Generation

API Application Programming Interface

DM Device Management

IoT Internet of Things

IP Internet Protocol

MAC Media Access Control

NFC Near-Field Communication

OS Operating System

PHY Physical

POS Point Of Sale

REST Representational State Transfer

SPSN Smartphone as a Sink Node

UI User Interface

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 Description and characteristics of SPSN

6.1 Descriptions

Typically, full-pledged IoT devices (e.g., smartphones) collect the information in either the physical or information world, and then send the information to IoT applications and services through communication networks. However, many kinds of constrained IoT devices in end user networks (e.g., wearable devices, devices in the home or vehicle) cannot connect to communication networks directly. In this case, a smartphone can act as a sink node to provide those types of connectivity capabilities for IoT devices.

Figure 6-1 shows a typical deployment scenario of an SPSN for IoT applications and services, which lies in the device layer of the IoT reference model [ITU-T Y.4000], along with a gateway with sink node functionality. The SPSN performs as a "mobile" sink node to detect and access various types of sensing nodes in an end user network with different types of communication technologies, such as Bluetooth, Wi-Fi and NFC.

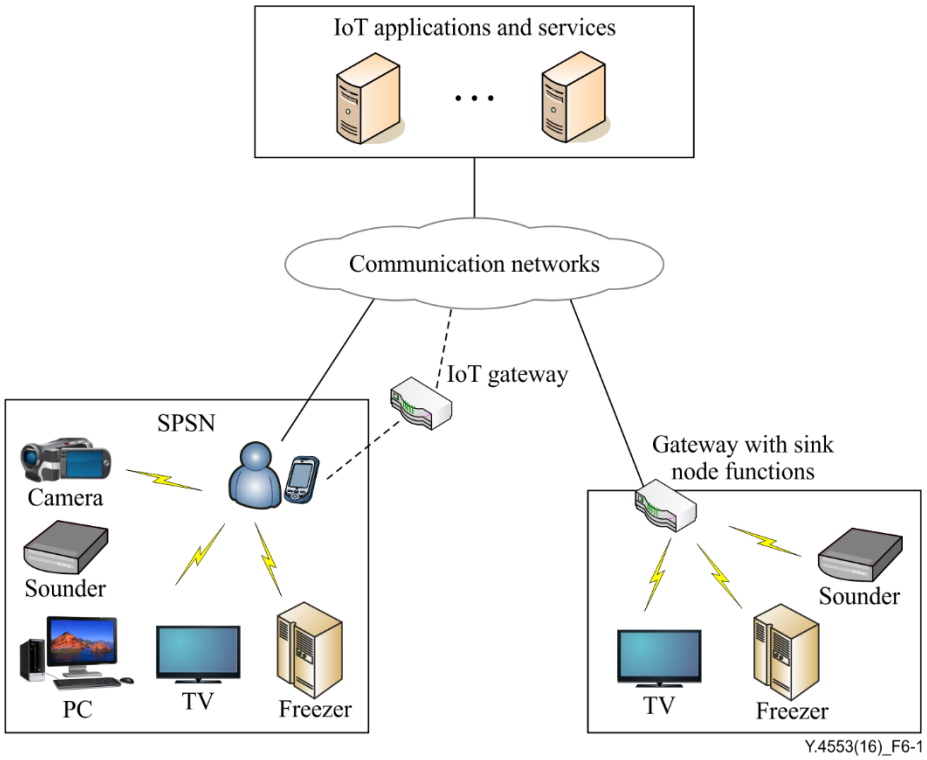

Figure 6-1 – Typical deployment scenario of SPSN

The SPSN can host various IoT applications, which can collect and process the information from IoT devices locally. For instance, the owner of an SPSN can use the IoT applications hosted in the SPSN to manage home IoT devices (e.g., sounder, TV, camera, and freezer).

IoT devices in an end user network can interact, via the SPSN, with remote IoT applications and services through communication networks. Users can remotely manage their IoT devices via their SPSN in an end user network (e.g., at home).

6.2 General characteristics

This clause provides characteristics of the SPSN for IoT applications and services. These characteristics include, but are not limited to, those described in 6.2.1 to 6.2.8.

6.2.1 Access to communication networks

An SPSN accesses communication networks directly or via the IoT gateway as described in [ITU-T Y.4101].

6.2.2 Interaction with IoT applications and services

An SPSN interacts with IoT applications and services through communication networks.

6.2.3 Access to the IoT device

An SPSN supports access to IoT devices in an end user network based on different communication technologies, such as Bluetooth, Wi-Fi and NFC.

6.2.4 Protocol translation

In an end user network, an SPSN supports data and protocol translations between IoT devices and IoT applications and services.

6.2.5 Device management characteristic

An SPSN supports the exposure of IoT devices in an end user network to allow an IoT device management (DM) service to manage the exposed IoT devices remotely.

6.2.6 Security

An SPSN provides security supports, such as IoT device authentication, data encryption and privacy protection. It is essential for the SPSN to retain security and privacy protection for its mobile characteristics.

6.2.7 Portability

An SPSN provides portability. It is expected that an SPSN provide standardized internal and external interfaces with which IoT applications can easily interact with IoT devices exposed by the SPSN.

6.2.8 Process of accessing data

An SPSN supports the process of collecting information from IoT devices in order to either display it on the SPSN or forward it to other elements in the communication network or IoT devices in the end user network.

7 Work modes of the SPSN

7.1 Local service mode

In local service mode, an SPSN can: host local IoT applications; collect IoT data from IoT devices in an end user network; and transfer IoT data from local IoT applications to IoT devices in the end user network. Local IoT applications on the SPSN can manage (e.g., store, process and demonstrate) collected IoT data and can forward it in processed form to IoT devices in the end user network. In this service mode, an SPSN does not need to transfer IoT data to remote IoT applications and services through communication networks. See Figure 7-1.

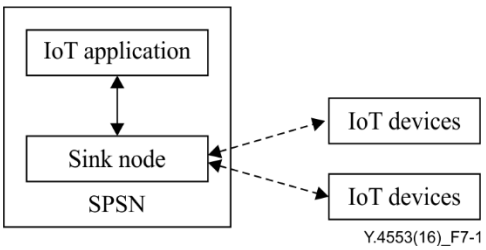

Figure 7-1 – Local service mode of the SPSN

7.2 Remote service mode

In remote service mode, an SPSN accesses IoT devices in an end user network and transfers IoT data from the SPSN to remote IoT applications and services through communication networks. Transferred IoT data can be stored and processed in such remote IoT applications and services. The users can browse and access IoT data using their terminals (e.g., smartphone, laptop, and PC) via the Internet. Additionally, in this service mode, an SPSN can forward IoT data provided by remote IoT applications and services to the IoT devices in an end user network. See Figure 7-2.

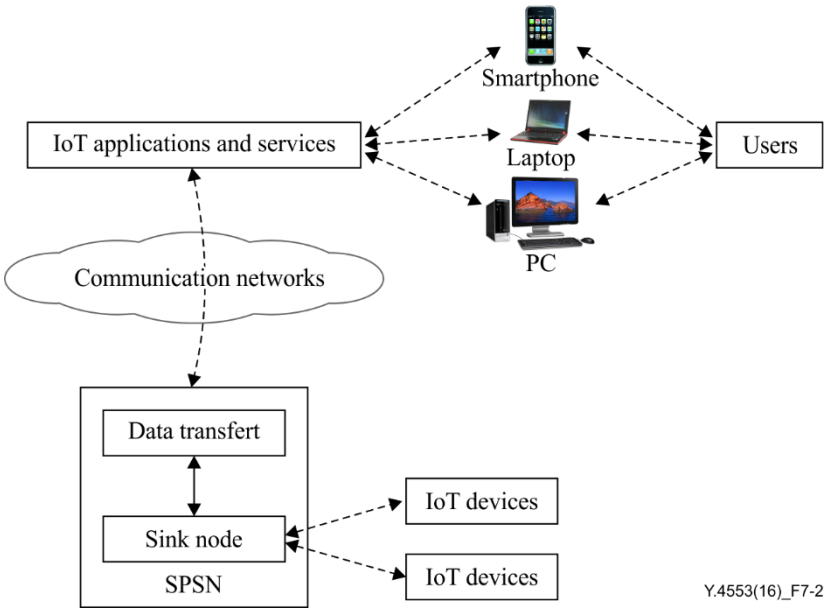

Figure 7-2 – Remote service mode of the SPSN

An SPSN may support local and remote service modes simultaneously. An SPSN can process collected IoT data from IoT devices in an end user network in order to either display it through local IoT applications on the SPSN or transfer the processed IoT data to remote IoT applications and services.

8 Requirements of the SPSN

8.1 General requirements

The general requirements of the SPSN are as follows.

1) The SPSN is required to support multiple connections of IoT devices and collaborations with other SPSNs.

2) It is recommended that the SPSN support various addressing schemes, e.g., Internet protocol (IP) and non-IP addressing schemes, to interact with the connecting or connected IoT devices.

3) The SPSN is required to provide standardized open interfaces for easy capability extensions, e.g., for integration with third party IoT applications and services.

8.2 Network connectivity

The SPSN provides logical connectivity between IoT devices in end user networks and communication networks.

The network connectivity requirements of the SPSN are as follows.

1) The SPSN is required to be able to connect to communication networks through communication technologies (e.g., 2G/3G/4G/Wi-Fi).
2) The SPSN is required to support data exchange between IoT devices and IoT applications and services.
3) It is recommended that the SPSN translate data and protocols between IoT devices and IoT applications and services.

8.3 Local information processing

The SPSN can support information processing locally. With IoT applications in the SPSN, IoT data can be collected, stored, processed and demonstrated in the SPSN directly.

The local information processing requirements of the SPSN are as follows.

1) The SPSN is required to install the IoT applications locally.
2) It is recommended that the SPSN store data locally.
3) It is recommended that the SPSN compute IoT data locally (e.g., data averaging).
4) It is recommended that the SPSN support the user interface (UI) for connected IoT devices.
5) It is recommended that the SPSN support standardized Web-based interfaces [e.g., representational state transfer- (REST)-ful application programming interfaces (APIs)] with which remote IoT applications and services interact with connected IoT devices.

8.4 Devices connectivity

When the SPSN joins an end user network, it can detect the IoT devices in that end user network, and the IoT devices can also actively detect and connect to the SPSN.

The devices connectivity requirements of the SPSN are as follows.

1) The SPSN is required to be able to discover and connect to the IoT devices in an end user network, subject to the user's request.
2) The SPSN is required to allow access to the connected IoT devices and to allow access from the connected IoT devices, according to pre-defined polices.
3) The SPSN is required to connect and disconnect the IoT devices actively, if necessary.

8.5 Data exchanging

When an SPSN establishes connections with IoT devices in an end user network, it can exchange data with those devices.

The data exchange requirements of the SPSN are as follows.

1) The SPSN is required to collect data from IoT devices.
2) The SPSN is required to send or dispatch data to IoT devices.
3) It is recommended that the SPSN adapt policy to data collection or data transfer according to users' requests.

8.6 Support of multiple communication protocols

IoT devices in an end user network can support various communication protocols. An SPSN can provide protocol adoption functions to support interactions with IoT devices.

The related requirements of the SPSN are as follows.

1) The SPSN is required to support multiple communication protocols, such as Bluetooth, Wi-Fi and NFC, in order for smartphones to connect to IoT devices.
2) It is recommended that the SPSN dynamically support various protocols.

8.7 DM requirements

The DM server can remotely manage an SPSN and connected IoT devices.

The DM requirements of the SPSN are as follows.

1) It is recommended that the SPSN support remote DM service to manage the IoT devices exposed by the SPSN.
2) It is recommended that the SPSN support remote DM service to manage the SPSN.

8.8 Security and privacy

An SPSN can participate in or leave an end user network casually, therefore it is essential to guarantee the security and privacy of the SPSN and connected IoT devices.

The security and privacy requirements of the SPSN are as follows.

1) An SPSN is required to support mutual or one-way authentication with IoT devices.
2) An SPSN is required to support mutual authentication with communication networks.
3) An SPSN is required to support mutual authentication with IoT applications and services.
4) An SPSN is required to securely store data or transfer the its own data and that of connected IoT devices.
5) An SPSN is required to protect its own data privacy and that of connected IoT devices.

Appendix I

Use cases of the SPSN for IoT applications and services

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

This appendix describes typical SPSN scenarios for IoT applications and services.

I.1 SPSN for commercial merchant service

In this scenario, an SPSN can be used to manage supplier service information. In commercial service, suppliers need to collect information about products, order data and the purchasers' account information required to complete transactions. On one hand, an SPSN has sensors for gathering information including identity data, transaction sensitive data and geographical position data that is acquired through various technologies, such as NFC, sounder and Bluetooth. On the other hand, an SPSN has a big screen to display real information for both suppliers and purchasers. Therefore, it is natural that suppliers use SPSNs to gather information. See Figure I.1.

Suppliers or retailers can use SPSNs to access and control each IoT device using related IoT applications installed on them. The SPSN performs identity recognition and information acquisition during the transaction process.

Subsequently, information is transferred to a data processing centre, through a special network, such as the Internet, cable network or wireless network.

Finally, information processing centres deployed in banks and third parties undertake information analysis, decision-making, sharing, publishing and provision to users of an instant intelligence acquisition service.

For instance, when a customer wants to buy products and pay for them, the merchant could use the SPSN to scan tags to collect the products' information, swipe the contactless bank card to get the account information or even swipe the customer's mobile phone if he or she has a mobile wallet. As a result, the SPSN collects all the data together just as the sink node does. It sends the data to a processing centre through the network and also transmits feedback to the merchant and customers.

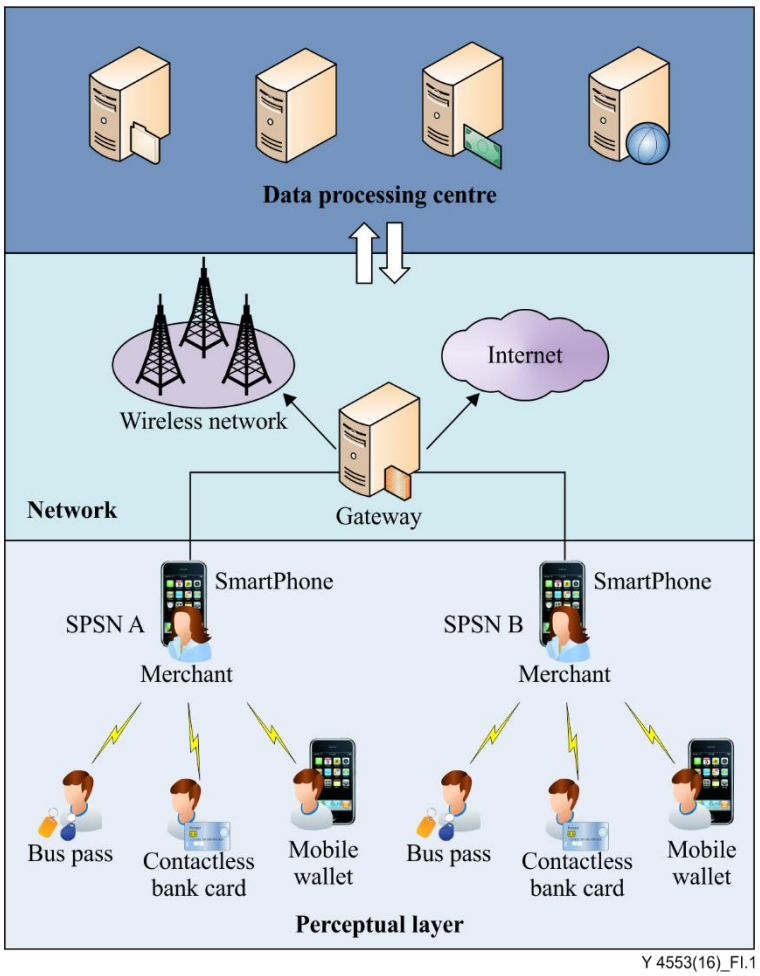

Figure I.1 – Scenario of the SPSN used for commercial merchant

I.2 SPSN for home services

The SPSN can be used at home, where occupiers can connect and manage IoT devices (e.g., sounder, freezer, and camera). With the support of an occupier's SPSN, IoT devices in home network can communicate with remote IoT applications and services through a communication network. Additionally, IoT devices can interact with local IoT applications hosted on the SPSN. Figure I.2 shows the scenario for SPSN use in the home.

When an occupier returns home carrying his or her SPSN, the device can automatically (or mutually) discover and connect to domestic IoT devices. Then the occupier can control these devices through the IoT application hosted on the SPSN. Furthermore, an occupier can leave the SPSN at home and remotely control his or her domestic IoT devices through the SPSN via communication networks, for example from an office.

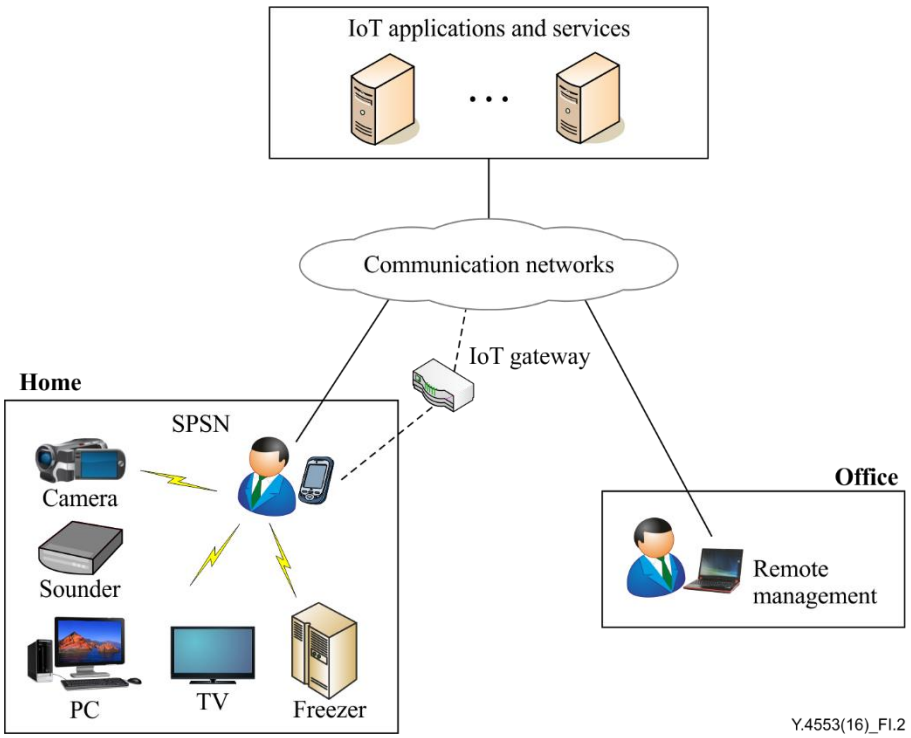

Figure I.2 – Scenario for SPSN use in the home

I.3 SPSN for environment-monitoring services

The SPSN can be used to monitor the environment. Environment-monitoring staff can collect sensing data with the SPSN and control the local sensor network in the outdoor environment. In this scenario, the SPSN is used as a processor as well as an information aggregator.

Figure I.3 illustrates this scenario. A temperature sensor, moisture sensor, hydro sensor and outdoor watering equipment are located at specific places to monitor temperature, humidity and hydration of the ground. All these sensors are equipped with a Bluetooth (or Wi-Fi) module.

A specific application installed on the SPSN can detect these environment-monitoring devices through Bluetooth and recognize them via the media access control (MAC) addresses of the devices. It can also transform raw data from the sensor to a readable form for the user to interpret easily.

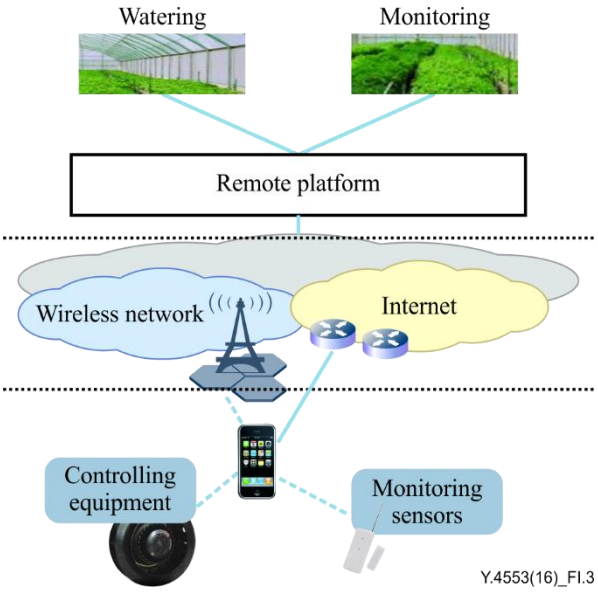

Figure I.3 – Scenario for SPSN use for environment monitoring

When environment-monitoring staff wish to check the status of a specific place, they turn on the monitoring application and the SPSN discovers sensors close to the SPSN with a Bluetooth-equipped sensor, connects to them and collects data automatically. The SPSN then asks for the temperature, moisture and water sensor data and displays them as programmed.

In this scenario, the SPSN collects the information from various sensors, processes the data locally to the required form, and finally uploads all the information to the monitoring centre.

I.4 SPSN for wearable smart devices

Wearable smart devices (e.g., watches, glasses, headbands and belts) are becoming more and more popular. Generally, wearable smart devices allow the owner to access information in real-time or non-real-time.

Due to the high mobility of smartphones, SPSN can be the most common tool for owners to access and manage their wearable smart devices.

An SPSN can be used to connect and manage users' constrained wearable smart devices through personal communication technologies, such as ZigBee, NFC, Bluetooth, Wi-Fi or USB. Figure I.4 shows the scenario for SPSN use for wearable smart devices.

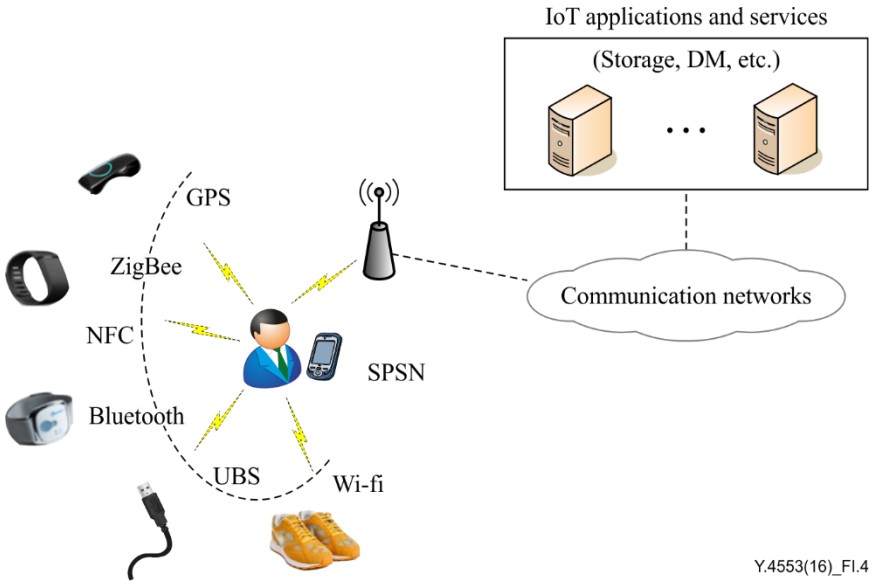

Figure I.4 – Scenario for SPSN use for wearable smart devices

In Figure I.4, the user has several wearable smart devices, such as a hairpin, a bracelet, a watch, a pair of glasses and a pair of shoes. These wearable smart devices connect to the user's SPSN through personal communication technologies.

Users can use their SPSNs to detect and connect to their wearable smart devices, through relevant IoT applications installed on the SPSN.

The SPSN collects and synchronizes information (including device capabilities) of the connected wearable smart devices with local stores or network repositories (such as cloud stores). The data collection can be real-time or non-real-time, depending the communication technology used and the device's capabilities.

Furthermore, the SPSN can process the devices' information locally with local relevant IoT applications.

At any time, the owner can use the SPSN to configure any of the wearable smart devices connected to it.

Appendix II

Example of sink node related functions of an SPSN

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

NOTE – This appendix takes the Android operating system (OS) platform as an example to illustrate the sink node-related functions of an SPSN. Note that each type of OS platform for SPSNs may have their own relevant implementation mechanisms.

The sink node-related functions of an SPSN include four logical function groups generally: adaptation functions, supporting functions, applications, and security and management functions. Those functions are part of the smartphone. See Figure II.1.

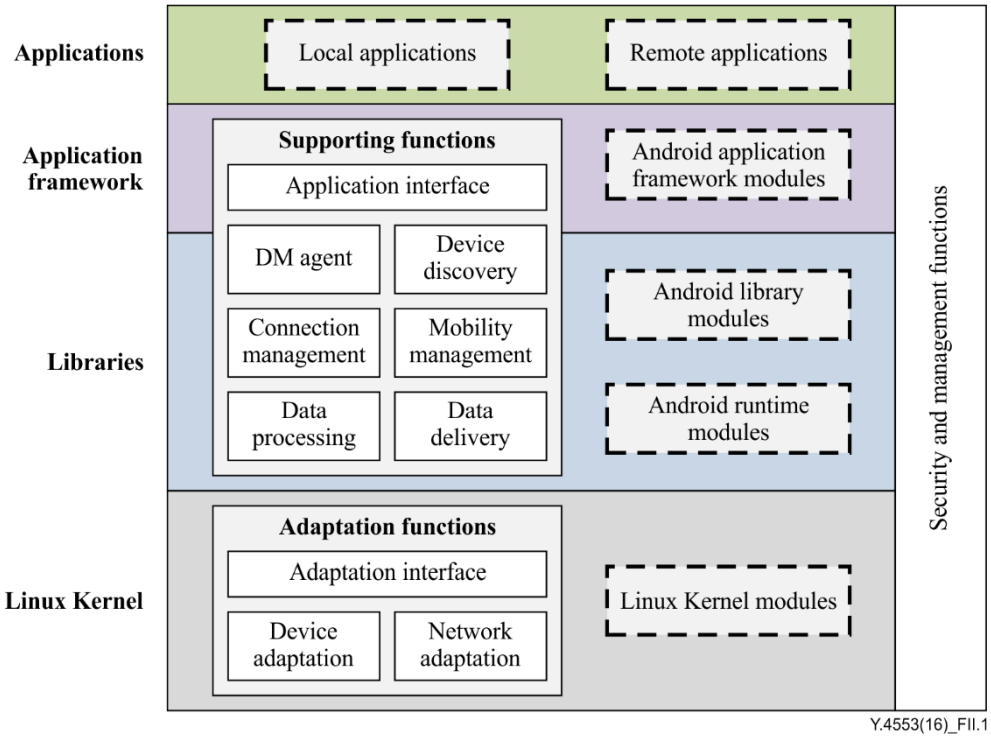

Figure II.1 – Example of sink node-related functions of an SPSN

The adaptation functions group in the Linux kernel layer of the Android OS includes communication-related functions of the SPSN to interact with the IoT devices (via device adaptation), and to communicate with the IoT applications and services (via network adaptation). This functional group includes at least the following functions.

– Device adaptation, which provides implementation of connecting IoT devices in the end user network and maps the device information according to the abstract adaptation interface.

– Network adaptation, which provides PHY/MAC layer adaptations for the SPSN to interact with the IoT devices in an end user network or the IoT applications and services via the communication networks, respectively.

– Adaptation interface, which provides an abstract interface to support the upper supporting functions and applications to access IoT devices, or the IoT applications and services, respectively.

The supporting functions group, across the libraries layer and application framework layer of the Android OS, provides functionalities including DM and discovery, connection management, mobility management, data processing and data delivery. This functions group includes at least the following functions.

– A DM agent, which supports local or remote IoT device management applications to manage the IoT devices exposed by the SPSN.
– Device discovery, which discovers the IoT devices in an end user network actively and processes active connection requests from the IoT devices.
– Connection management, which establishes and manages the connections, including the connections between IoT devices and the SPSN, and the connections between the SPSN and IoT applications and service.
– Authentication management, which manages the mobility of the SPSN. When the SPSN joins or leaves an end user network the SPSN manages the authentications and authorities to IoT devices and end user networks.
– Data processing, which collects and processes IoT data from IoT devices locally.
– Data delivery, which delivers IoT data (including locally processed IoT data) to other entities in communication networks or back to IoT devices.
– Application interface, which provides an abstract interface to support local and remote IoT applications and services to access the IoT devices exposed by the SPSN, with standard and uniform logical methods (e.g., web-based interfaces).

The local or remote IoT applications and service use the application interfaces and adaptation interfaces mentioned above to discover, access and manage IoT devices in the end user network.

The security and management functions group, cooperating closely with all the layers of the Android OS, provides capabilities for supporting security of data and communications.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2016