International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4555

(02/2019)

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 – Services, applications, computation and data processing

Service functionalities of self-quantification over Internet of things

Recommendation ITU-T Y.4555

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.4555

Service functionalities of self-quantification over Internet of things

Summary

Recommendation ITU-T Y.4555 describes service functionalities of self-quantification over Internet of things. It clarifies the concept of self-quantification services, identifies their considerations and specifies their requirements and functionalities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4555	2019-02-13	20	11.1002/1000/13862

Keywords

Functionality, IoT, requirement, self-quantification, service.

* 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.4555

Service functionalities of self-quantification over Internet of things

1 Scope

This Recommendation describes service functionalities of self-quantification over Internet of things (IoT) with the purpose of fostering interoperability of self-quantification services.

The following elements are within the scope of this Recommendation:

– Concept, technical implications and general service models to clarify the idea of self-quantification services and to categorize them into three different service models.

– Considerations to emphasize three important aspects of self-quantification services.

– Requirements to specify three different categories of requirements, which support the identified considerations.

– Functionalities to define a general functional architecture based on the identified requirements and to illustrate sequential diagrams of three different service models.

This Recommendation builds on the overview of IoT [ITU-T Y.4000] and the common requirements of the IoT [ITU-T Y.4100], providing specific requirements in support of the self-quantification application domain.

Usage scenarios of self-quantification services are provided in Appendix I.

NOTE – Regulatory, legal and business aspects are outside the scope of this Recommendation.

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 Internet of things.*

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements 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 application domain [ITU-T Y.4100]: An area of knowledge or activity applied for one specific economic, commercial, social or administrative scope.

NOTE – Transport application domain, health application domain and government application domain are examples of application domains.

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, data capture, data storage and data processing.

3.1.4 Internet of things (IoT) [ITU-T Y.4100]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

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

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

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 self-quantification: A practice of measuring, integrating and analyzing health, mental, dietary, physical, social and environmental data of a person to produce more meaningful information to the user.

NOTE 1 – Self-quantification measures ambient temperature, humidity, atmospheric pressure, etc., and relates them to users' body temperature, heart rate, etc., by means of quantifying each factor.

NOTE 2 – Self-quantification does not specify nor unify a specific way to quantify intangible status around users.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA Authentication, Authorization and Accounting

ACL Access Control List

API Application Programming Interface

BLE Bluetooth Low Energy

E2E End-to-End

HIPAA Health Insurance Portability and Accountability Act

IMT International Mobile Telecommunications

IoT Internet of Things

JSON JavaScript Object Notation

LTE Long Term Evolution

PKI Public Key Infrastructure

SI International System of units

Wi-Fi Wireless Fidelity

XML Extensible Markup Language

5 Conventions

In this Recommendation:

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

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction to self-quantification over Internet of things

This clause introduces the concept, technical implications and general service models of self-quantification over IoT.

6.1 Concept

Self-quantification, also known as quantified self or lifelogging, is a practice of measuring, integrating and analyzing health, mental, dietary, physical, social and environmental data of a person to produce more meaningful information to the user. The concept derives from a convergence of data acquisition and users' daily life to gain insight into the behaviour and habits of users. Self-quantification service provides a set of functionalities that enables and supports requirements of self-quantification.

Most recently, the culture of collecting, transmitting, analyzing and sharing data has moved from a business or marketing level to a much more personal level. Users are now tracking every aspect of their lives especially with the aid of smart wearable technologies.

Knowing where you are today and being able to measure and compare against past data is the essence of self-quantification. From a technological perspective, miniaturization of sensors and processors, ever-increasing processing power, improved battery life and ubiquitous communications infrastructure have enabled possibilities for always-on wearable devices that can be carried around all day. Other key technology drivers are cloud computing and big data computing that seamlessly facilitate communication among a number of different self-quantification services.

A wide range of sensors enables users to digitize and save information for future uses. However, if there are no current or practical sensors that can measure preferable information, for the time being, smart device applications providing self-quantification services allow users to assess their current status and input data into the applications. Typical examples include mental status or dietary consumption.

Table 1 enumerates possible data that can be measured with self-quantification services.

Table 1 – List of possible data that can be measured with self-quantification services

Category	Data
Health	Heart rate, blood glucose, body temperature, body PH, fertility, pregnancy
Mental	Mood, stress, alertness
Dietary	Calories, alcohol, nicotine, caffeine, water, medicine, drugs
Physical	Sleep, step, run, cycle power, cycle cadence, speed, time
Social	Social media uploads, social media interactions (like, love, sad, etc.)
Environmental	Temperature, geolocation (GPS location, altitude)

Practitioners of self-quantification include people with chronic medical conditions who need to track their symptoms to try and establish patterns in their state, which could help to identify correlation factors for their conditions. Sports enthusiasts, who keep track of their progress to achieve performance goals are also avid practitioners of self-quantification. Apart from the above two categories, ordinary people, who are simply curious or willing to achieve short or long-term goals also take advantage of self-quantification services. Such goals include quitting smoking, losing weight, sleeping better, and so on.

Most importantly however, the most powerful use scenarios take place when two or more different types of data combine together and provide information or insight which cannot be provided by measuring only one data. Such use scenarios can only be guaranteed by interoperability between self-quantification services. In this sense, this Recommendation aims to foster interoperability of self-quantification services.

NOTE 1 – Huge advances in sensing technology and integrating various data allow users to take advantage of collected data. It is then possible to understand personal health and fitness status by processing and visualizing them. By analyzing these data, people have a better understanding of not only their health status but also their relationship to the world around them.

NOTE 2 – The benefits of self-quantification services are as follows:

– Help users to deeply understand their health and fitness status and how to interact with the world around them.

– Learn users' behaviours and help them to adapt to their needs by risk profiling and preventing diseases.

– Find actionable intelligence in the data they collect.

– Motivate people with more serious health concerns to track multiple health aspects, which consequently could produce greater volumes and a broader range of data types.

– Capture an enormous amount of data and a broad range of data types that need to be streamed to provide feedback and trigger services in critical time frames.

– Derive valuable insight into personal habits and behaviour and could target marketing campaigns.

6.2 Technical implications

IoT is the foundation of self-quantification and self-quantification services are built upon IoT ecosystems. IoT allows self-quantification to seamlessly transfer and receive measured and processed data of users and their environment. There are necessary actors for self-quantification which correspond to the IoT elements, which are defined in [ITU-T Y.4000]; the actors include self-quantification services, sensors, users, surrounding environment and remote servers. Figure 1 shows how actors of self-quantification align with elements of IoT. It is noted that not all actors correspond to the existing elements.

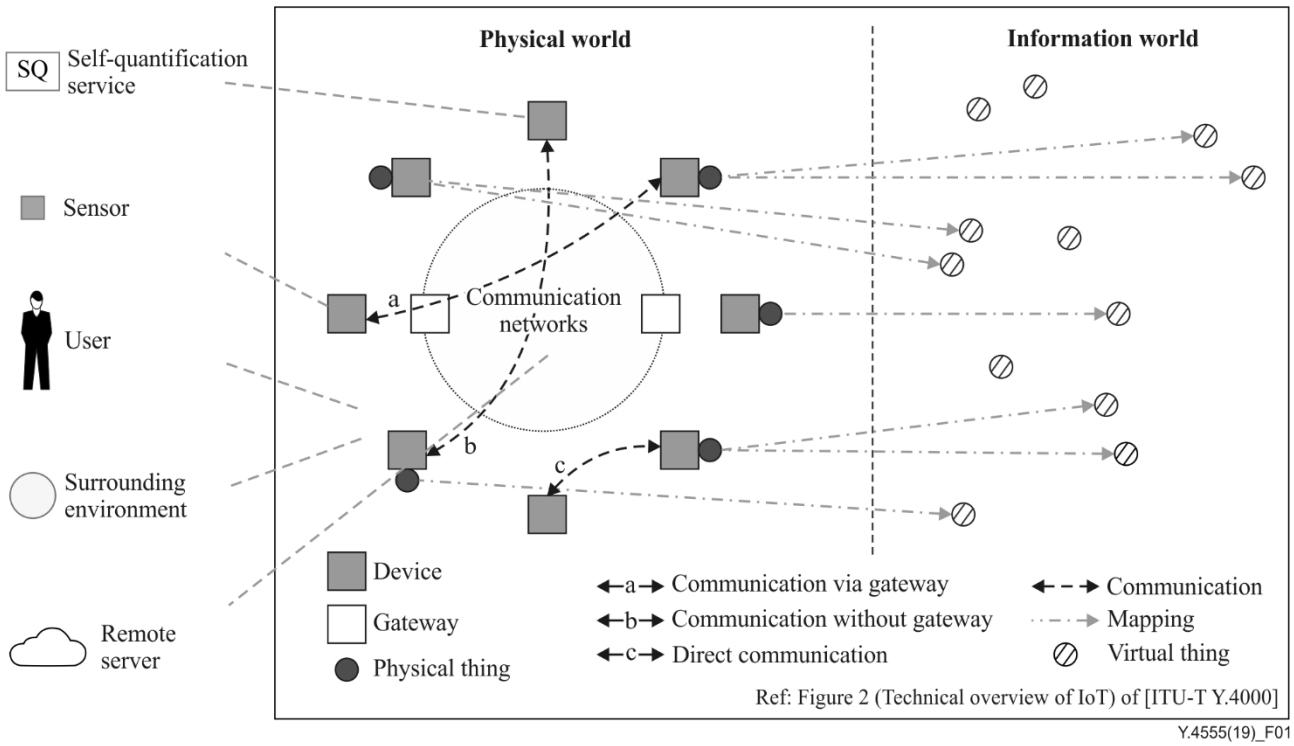

Figure 1 – Actors of self-quantification

– Self-quantification service: A set of functionalities that support and enable self-quantification. A self-quantification service corresponds to the device depicted in the technical overview of the IoT shown in Figure 2 of [ITU-T Y.4000]. A self-quantification service captures, stores and processes data but does not necessarily sense or actuate data. It is installed as applications in smart devices or independent wearable devices which support self-quantification functionalities in the physical world. It communicates with other self-quantification service elements directly at close range without a gateway or indirectly at long range via a gateway.

NOTE 1 – Technologies for close range communication include BLE, ZigBee, Wi-Fi, etc.

– Sensor: A type of device that exists in the physical world which senses or actuates data for self-quantification services. It corresponds to the device of Figure 2 in [ITU-T Y.4000]. Sensors are especially attached to a user or located in their surrounding environment to measure health, mental, dietary, physical, social and environmental data.

– User: A person, existing in the physical world, who takes advantage of self-quantification services. It corresponds to none of the elements of Figure 2 in [ITU-T Y.4000]. A user's various information is sensed by sensors and in turn, is transmitted to self-quantification services to be stored and processed.

– Surrounding environment: A location where users exist in the physical world. It corresponds to none of the elements of Figure 2 in [ITU-T Y.4000]. The ambient information is captured by sensors and transmitted to self-quantification services to be stored and processed.

– Remote server: A remote repository where information from self-quantification is transmitted and stored. It corresponds to none of the elements of Figure 2 in [ITU-T Y.4000]. When a self-quantification service cannot provide remote communication, a gateway facilitates remote communication from a self-quantification service to a remote server.

NOTE 2 – Technologies for remote communication include LTE, IMT-2020, etc.

This Recommendation extends Figure 2 of [ITU-T Y.4000] by also paying special attention to the actors that do not correspond to the existing IoT elements. Identifying this gap is necessary for the interoperability of self-quantification services. The identified gap leads to considerations provided in clause 7.

6.3 General service models

Self-quantification services are categorized into three general service models as described in Figure 2. The figure describes the relationship among actors, which are identified in clause 6.2. Clauses 7, 8 and 9 define considerations, requirements and functionalities, respectively, that the following service models support.

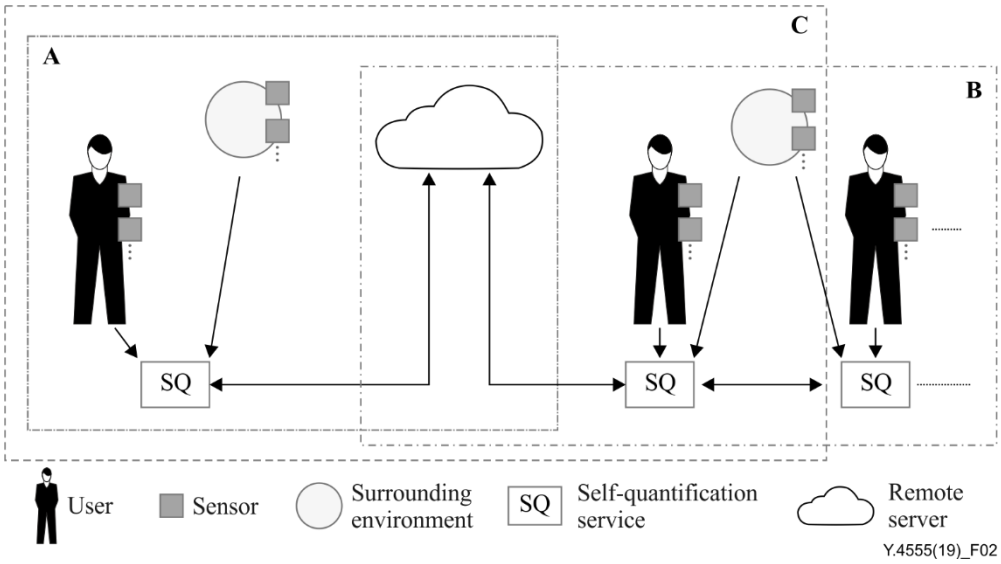

Figure 2 – General service models of self-quantification

6.3.1 Single self-quantification service

Diagram A of Figure 2 involves a self-quantification service, one or more sensors attached to a user and one or more sensors located in a surrounding environment and a remote server. Data is transmitted from sensors to the self-quantification service at close range. In the case where necessary sensors are not available, the user manually inserts data to the self-quantification service. The self-quantification service transmits data to or retrieves data from a remote server.

6.3.2 Multiple self-quantification services

Diagram B of Figure 2 is an extension of diagram A by adding one or more users with their self-quantification service. Similar to Diagram A, each user has one or more attached sensors and data is transmitted from sensors to a corresponding self-quantification service. Data is also transmitted amongst multiple self-quantification services at close range. All users are located nearby in the same surrounding environment and thus, a remote server is not required for communication among users. Each self-quantification service transmits data to or retrieves data from a remote server.

6.3.3 Multiple self-quantification services over a remote server

Diagram C of Figure 2 involves communication amongst multiple self-quantification services via remote servers. Similar to diagrams A and B, each user has one or more attached sensors and data is transmitted from sensors to a corresponding self-quantification service. In the case of diagram C, however, users are located in different environments. Hence, a remote server is necessary for communication amongst multiple self-quantification services at long range.

7 Considerations

Taking into account the aforementioned technical implications described in clause 6.2, there are several potential areas of consideration for self-quantification services. Among these areas, interoperability, security and human body safety are especially important to be considered. Interoperability aims for correct and seamless data exchange of two or more heterogeneous self-quantification services. Security ensures trustworthy communication of self-quantification services which, in most cases, involve human body information and other confidential information. Human body safety assures reliable and safe operation of self-quantification services on a human body.

Based on the high-level requirements specified in [ITU-T Y.4000], the following clauses describe considerations from a self-quantification service perspective. The considerations below are further elaborated in clause 8.

7.1 Interoperability

Ensuring interoperability allows self-quantification services to communicate with a limitless number of sensors and other self-quantification services. Different self-quantification services provide different methods for data collection, transmission, saving and so on. It is important to note that such self-quantification services cannot support all existing sensors, data, or functionalities.

Possible risks of lack of interoperability among self-quantification services are incompatible, inconsistent, disconnected, incomplete or inaccurate information due to different protocols, data formats, inefficient processes, barriers to the development of new services, excessive manual work by users which also leads to inaccurate data and even decline of safety through a series of unintended consequences.

In this sense, self-quantification services seek ways to ensure interoperability by taking advantage of other resources of neighbouring or remote self-quantification services by reusing data and functionalities. Ensuring interoperability starts from data collection and transmission and leads to data saving and storage. Data translation, integration, analysis and visualization are necessary for compatible future processes. Data sharing is also an important aspect of interoperability for remote server access. Interoperability of data itself also takes into account from the schema, naming, measured units, observability, granularity and validation perspectives.

7.2 Security

Assuring security and confidentiality of self-quantification services comprises secure data transaction among all actors of self-quantification services. Needless to say that self-quantification services will result in a plethora of private information transmitted via and stored at remote servers while users unconsciously track their data.

Expected risks of insecure self-quantification services are excessive information gathering, identity theft, profiling, stalking, extortion and so on. These risks are mostly attributed to unintentional data leakage during data communication among sensors and self-quantification services and remote servers or even at rest.

In addition, the more self-quantification services are connected to sensors and other self-quantification services, the more the possibility of attack increases and eventually introducing unexpected risks and challenges. From data collection, transmission to data sharing, trustworthy end-to-end (E2E) security is vital. Lack of security and confidentiality results in insecure and unreliable connections among actors.

7.3 Human body safety

Guaranteeing human body safety allows self-quantification services to be accessed by people of all ages. In a number of cases, self-quantification services are supported by wearable, patchable, or even implantable sensors and devices that communicate wirelessly. Thus, reliable safe operation on

the human body can be realized by complying with associated safety guidelines. Lack of human body safety results in unexpected damage and harm to human body.

8 Requirements

In this clause, the requirements of self-quantification services are specified to support the considerations identified in clause 7. The requirements are built on and thus, extend the common requirements of the IoT [ITU-T Y.4100] to specifically support the self-quantification application domain.

8.1 Interoperability

Interoperability is a vital requirement for service functionalities of self-quantification over IoT. The existing [ITU-T Y.4100] described interoperability as a non-functional requirement as those which are not derived from general use cases of IoT described in clause 6.

This clause specifically extends and elaborates interoperability from the existing [ITU-T Y.4100], which is to be ensured among heterogeneous IoT implementations, under non-functional requirements from a self-quantification service perspective. Requirements are divided into five categories, all of which are directly aligned to layers of general functional architecture defined in clause 9.1.

8.1.1 Collection requirements

Collection requirements address the way data is collected from sensors, remote servers and other self-quantification services.

8.1.1.1 Collection

Collection is the beginning of all self-quantification services where sensed data, which is described in Notes 1 to 5 below, is retrieved to self-quantification services.

– Self-quantification services are required to receive data from sensors, other self-quantification services and remote servers.

– Data collected by self-quantification services is required to pass through necessary security checks to ensure security.

– Self-quantification services can optionally prevent data from being automatically received from other self-quantification services or to a remote server.

NOTE 1 – Sensors and actuators such as glucose meter, accelerometer, thermometer, hygrometer, and others are used to measure and collect raw data.

NOTE 2 – Human body information includes body weight and height, body status, electromyography, respiration, skin temperature, galvanic skin response, pulse rate, heart rate, etc.

NOTE 3 – Physiological status includes stress, emotion, mood, brain activities, bio-signals, etc.

NOTE 4 – Indoor or outdoor activities includes exercising, eating, sleeping, dosing, watching television, studying, web searching, etc.

NOTE 5 – Environmental factors include location, weather, temperature, electricity/water consumption, etc.

8.1.1.2 Saving

Saving takes place when data is temporarily located in volatile memory such as random access memory because the data is received but has yet to be processed or translated.

– Self-quantification services are required to save raw, processed, or untranslated data temporarily to use them directly and immediately during process or translation.

8.1.1.3 Storage

Storage takes place when users prefer to cumulatively analyze a large amount of data in one process or non-understandable data is waiting for software update of self-quantification services. Non-volatile memories are used to store data in the format of JavaScript Object Notation (JSON), Extensible Markup Language (XML), etc. depending on self-quantification services.

– Self-quantification services are required to store raw, processed, or untranslated data inside their non-volatile memories to use them anytime.

– When self-quantification services are installed in constrained devices with limited resources, self-quantification services can optionally compress data to minimize the required space for storage.

8.1.1.4 Observability

Observability allows self-quantification services to look for data which can be sensed nearby.

– Self-quantification services are recommended to observe environmental information and to transfer this information automatically or manually to other self-quantification services and/or remote servers.

– Self-quantification services can optionally ask for permission from the host of non-observable data, which cannot be identified spontaneously, in order to access and retrieve the data.

8.1.1.5 Schema

The schema sets the rules on how data is designed or described in self-quantification services.

– Self-quantification services are recommended to comply with pre-defined and pre-installed schema specified by service providers to validate received data if it can be directly parsed and to be processed.

NOTE – Self-quantification services sharing the same platform or complying with the same specification are likely to have data types which are derived from an identical schema.

8.1.1.6 Validation

Validation takes place upon retrieval of data from sensors, remote servers, or other self-quantification services to verify if data can be correctly processed by self-quantification services without further translation or modification.

– Self-quantification services are required to, upon reception, check if the data can be correctly parsed, understood and be further processed based on its pre-defined default schema.

– Self-quantification services can optionally discard unnecessary data to save space.

8.1.2 Process requirements

Process requirements address the way data is processed.

8.1.2.1 Integration

Integration takes place when synchronizing a number of different data since self-quantification services receive a plethora of data including human body information, physiological status, environmental factors, etc.

– Self-quantification services are recommended to be able to integrate such various data, which could be received anytime by anybody, based on the timestamp and user identity.

8.1.2.2 Analysis

Analysis is a process where data becomes useful information to users of self-quantification services.

– Self-quantification services are required to provide the necessary applications or algorithms to process raw data and extract information requested or required by users.

NOTE – It is possible that the result of analysis differs from application to application since specific methods and algorithms to analyze data could be different.

8.1.2.3 Visualization

Visualization allows users to better understand the processed data by providing refined information.

– Self-quantification services are recommended to display digits or elaborate complicated information using graphs, tables, or pictures if possible.

– If possible or if necessary, self-quantification services can optionally extend to second screens nearby to display the visualized information.

8.1.2.4 Timestamp

Timestamp records the moment when the data is measured to integrate and synchronize multiple measurements from different sensors or different self-quantification services.

– Self-quantification services are recommended to link timestamp information with the measured data so that the actual measured data and its timestamp can be accessed as a group.

NOTE – It is noted that individual access to the actual measured data and its timestamp is likely to cause unnecessary fragmentation of data.

8.1.2.5 User identity

User identity recognizes users of self-quantification services to integrate and synchronize multiple measurements from different sensors or different self-quantification services by multiple users.

– Self-quantification services are recommended to link user identity information with the measured data so that the actual measured data and its user identity can be accessed as a group.

8.1.3 Transmission requirements

Transmission requirements address the way data is transmitted to remote servers and other self-quantification services.

8.1.3.1 Transmission

Transmission is a way to send raw, processed, or untranslated data to other actors such as self-quantification services or remote servers. Self-quantification takes advantage of conventional wired or wireless transmission protocols for stable transmission. Defining or redefining such transmission protocols is outside the scope of this Recommendation.

– Self-quantification services are required to send data to other self-quantification services or to a remote server.

– Data transmitted from self-quantification services is required to pass through necessary security checks to ensure security.

– Self-quantification services can optionally prevent data from being automatically transmitted to other self-quantification services or to remote servers.

8.1.3.2 Sharing

Sharing is an integral part of self-quantification services because users send or request, for example, environmental factors sensed with self-quantification services that they need.

– Self-quantification services are recommended to share or distribute user's measured data to other self-quantification services directly or via remote servers.

– Self-quantification services can optionally share or distribute such measured data, especially non-confidential information, by attaching a timestamp to ensure synchronization.

8.1.3.3 Granularity

Granularity means that processed data, which is ready to be transmitted to other self-quantification services or remote servers, is simple and can be re-constructed to compose more complex information to prevent unnecessary duplication of data.

– Self-quantification services are recommended to send data in a minimally viable way.

8.1.3.4 Naming

Naming is a convention of assigning human readable names to computer data. However, long names result in unnecessary payloads during data transmission.

– Self-quantification services are recommended to use abbreviations or acronyms for data names to eventually reduce the amount of actual data to be transmitted on the wire.

NOTE – Excessive contraction causes difficulty for other self-quantification services to understand the data.

8.1.4 Virtual server requirements

Virtual server requirements address the way data is properly mapped.

8.1.4.1 Mapping

Mapping is a process wherein a certain property correctly corresponds to its identical information of a different name especially in the case when self-quantification services receive a collection of data that cannot be immediately parsed.

– Self-quantification services are required to provide a mapping table which allows self-quantification services to automatically or manually convert unknown properties into different names that self-quantification services can actually parse and process.

8.1.4.2 Measured units

Measured units are standards for measurement of physical quantities to express the definite magnitude of a quantity of human body information, activities and other information.

– Self-quantification services are recommended to use the international system of units (SI).

8.1.5 Translation requirements

Translation requirements address the way data is translated.

8.1.5.1 Translation

Translation converts data formats or types into those which can be understood and parsed by a specific self-quantification service.

– Self-quantification services are required to provide specific methods to convert data formats or types into those which can be understood by the self-quantification service which performs translation.

– Self-quantification services can optionally select automatic or manual mapping for translation.

8.2 Security

The existing [ITU-T Y.4100] described security and privacy protection requirements as functional requirements during capturing, storing, transferring, aggregating and processing the data of things, as well as to the provision of services which involve things. These requirements are related to all the IoT actors.

The purpose of security requirements is to protect data vulnerable from outside attacks. Common security requirements are as follows.

– All data of self-quantification services are required to pass through the corresponding security layer, which is the transport and connectivity abstraction layer agnostic, before data is collected and after data is transmitted.

– Vendors of self-quantification services are recommended to look for privacy and security statements and compliance with standards, where appropriate.

NOTE 1 – Privacy and security statements can include, for example, those of iCloud, Fitbit, Jawbone, etc.

NOTE 2 – Standards with which self-quantification services comply can include the Health Insurance Portability and Accountability Act (HIPAA), ISO 27001, etc.

The following requirements are minimal requirements to be supported by all self-quantification services whose sensors are highly probable to be constrained. Although the minimal requirements are specified in this Recommendation, vendors and manufacturers are responsible for checking appropriate security, human body safety, environmental and applicable regulatory requirements from national authorities.

8.2.1 Anonymity

Anonymity allows self-quantification services to hide user identity from random adjacent self-quantification services because when certain data is observable, it is difficult to selectively make certain self-quantification services be able to discover that certain data.

– Self-quantification services are required to anonymize user identity to others when personal information or any privacy issues are linked to that user identity.

– Appropriate authentication and authorization are required between self-quantification services to inform user identity.

NOTE – Environmental data, which is less useful to attackers, does not always have to be anonymized when it exists independently. However, when it is linked with personal information, it could easily be used to track a user's current location.

8.2.2 Unlinkability

Unlinkability makes third-party entities incapable of tracing the relation between two self-quantification services to ensure that attackers in the middle cannot make any decisions nor actions based on the stolen data since the data is encrypted.

– Self-quantification services are required to prevent attackers from spoofing data in the middle of communication between two actors.

NOTE – One typical example of such attacks is man-in-the-middle attacks.

8.2.3 Access control

Access control defines a set of rules for querying self-quantification services, sensors and remote servers whether they have the correct rights to access destination self-quantification services.

– Self-quantification services are required to use an access control list (ACL), which is stored locally in self-quantification services, to assert the identity of another self-quantification service which requests information.

NOTE – If a self-quantification service hopes to verify if it matches the policy of a requesting self-quantification service, then asserting the identity of the requestor requires an authentication process. The requester then permits the requests of outside actors.

8.2.4 Authentication, authorization and accounting (AAA)

Authentication, authorization and accounting (AAA) are a process for verifying the identity of accessing self-quantification services and for granting specific rights to provide certain types of data specified in the access control list.

– Self-quantification services are required to provide relevant information such as public key infrastructure (PKI), which consists of a pair of asymmetric public and private keys.

8.2.5 Encryption and decryption

Encryption and decryption are ways to protect data spontaneously exposed by self-quantification services to mitigate risk traffic sniffing, which lets attackers collect all transmitted data and man-in-the-middle and redirection attacks, which could cause data to be sent to the wrong destination.

– Self-quantification services are required to encrypt data before transmitting data outside and to decrypt data after receiving data.

8.3 Human body safety

The existing [ITU-T Y.4100] described reliable and secure human body connectivity services as part of service requirements related to the service providers, IoT users and things. Common human body safety requirements are as follows.

– Self-quantification services, especially physical devices which are used attached to a human body, are required to pass local or regional safety tests or inspections.

NOTE – Different countries have different regulatory requirements for testing and thus, such regulatory requirements are outside the scope of this Recommendation.

9 Functionalities

In this clause, a general functional architecture and three sequential diagrams of self-quantification services are specified to support the requirements identified in clause 8.

9.1 General functional architecture

Based on the three service models, which are illustrated in clause 6, the functionalities are defined with the following general functional architecture.

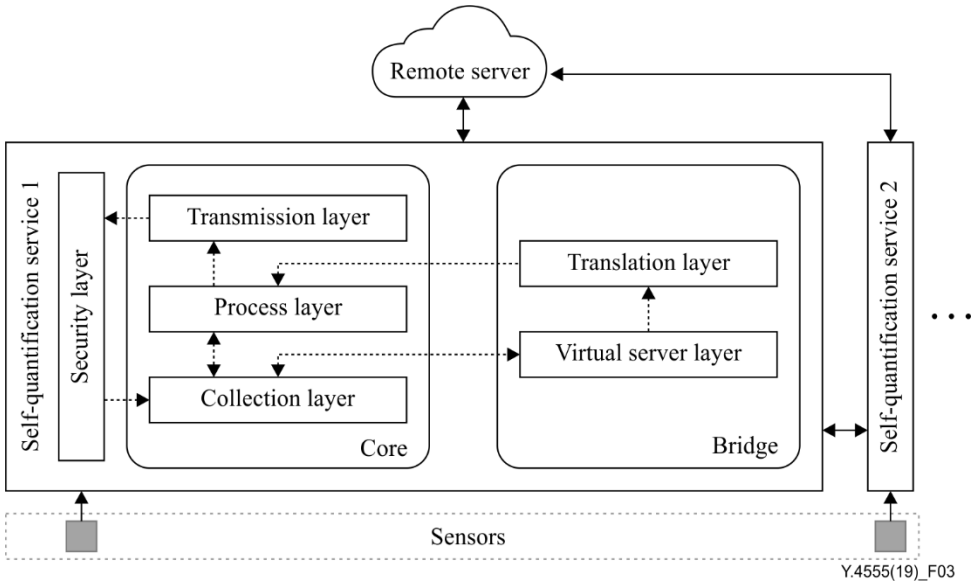

Figure 3 – General functional architecture of self-quantification services

Figure 3 describes a general functional architecture of self-quantification services. Self-quantification service 1 is a typical self-quantification service of which each layer corresponds to specific requirements that are identified in clause 8. The layers of self-quantification service 2, whose general functional architecture is identical to that of self-quantification 1, are omitted intentionally for simplicity.

Self-quantification service 1 comprises of a core and a bridge. The core collects, processes and transmits data while the bridge converts data from a non-understandable format to an understandable format. These two components are separated because, in some cases, the bridge is not used because data translation is not necessary.

Dotted lines indicate data flow inside a self-quantification service and solid lines indicate data flow between a self-quantification service and outer actors (e.g., sensors, remote server and other self-quantification services). Human body safety requirement is not supported by any of the layers of the general functional architecture since this general functional architecture is specified to support interoperability and security requirements. As specified in clause 8.3, different countries have different regulatory requirements for testing and thus, such regulatory requirements for human body safety are outside the scope of this general functional architecture.

9.1.1 Sensors

Sensors transmit data to a security layer of self-quantification services. The data includes a person's physical information (e.g., body temperature, height, weight, etc.), activity log (e.g., step count, distance, etc.), ambient information (e.g., GPS, humidity, etc.), social information (e.g., product, marketing, social media information, music, etc.) or other useful information to self-quantification services. Sensors collect data periodically or whenever they detect or recognize changes of movement or environment, etc. Sensors also record timestamps to track the moment when data is measured. Sensors transmit information only if they are requested by self-quantification services in raw format or extracted format. Sensors are separate physical devices or are installed inside the same devices where self-quantification services are also installed.

9.1.2 Core

The core comprises collection, process and transmission layers.

9.1.2.1 Collection layer

The collection layer receives data (e.g., physical data, activity data, or ambient data, etc.) from sensors, remote servers, or other self-quantification services via a security layer. Figure 4 describes six functional blocks within the collection layer.

– The collection layer observes data which are transmitted from nearby sensors (Observability).
– The collection layer automatically retrieves data periodically from nearby sensors or manually asks for data (Collection).
– The collection layer then validates data (Validation) based on pre-defined schema (Schema) and categorizes data into understandable or non-understandable data so that they can be selectively forwarded to a process or virtual server layer, respectively.
– Before or after sending data to the process or virtual server layer, the collection layer saves data temporarily (Saving) or stores it permanently (Storage).

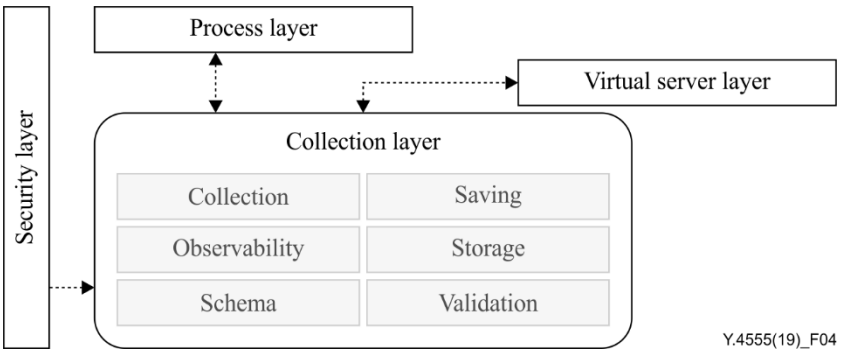

Figure 4 – Collection layer of self-quantification services

9.1.2.2 Process layer

The process layer receives data from the collection layer and translation layer. Figure 5 describes five functional blocks within the process layer.

– The process layer extracts the activity log of users to integrate (Integration) and analyze (Analysis) data which was received by the transmitting actors in order to produce users' pattern.

– When integrating and analyzing data, timestamp (Timestamp) and user ID (User identity) play an important role in self-quantification services since the process layer receives similar data having little difference of timestamp from various users. In this case, in order for the process layer to easily rearrange data based on the timestamp and user ID, self-quantification services deal with this dataset as a batch, where measured data, timestamp and user ID are analyzed together in one package of information.

– Information is then visualized (Visualization). When visualizing data, the process layer selectively displays processed information with respect to time, geolocation, or to other parameters.

– After processing data, the process layer sends data back to the collection layer to store or save.

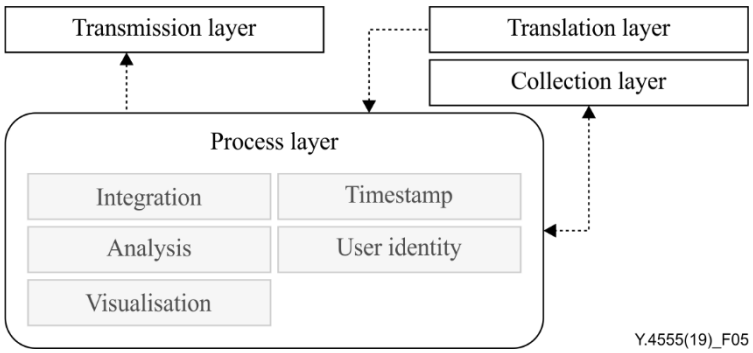

Figure 5 – Process layer of self-quantification services

9.1.2.3 Transmission layer

The transmission layer receives processed data from the process layer and sends the data to remote servers or other self-quantification services through a security layer. Figure 6 describes four functional blocks within the transmission layer.

– The transmission layer transmits data to actors outside its self-quantification service (Transmission) and sometimes shares data to other users (Sharing). When recipients do not allow data to be received automatically, the transmission layer asks for the recipient's permission to transmit. At times, remote servers or other self-quantification services request for data.

– Data, which is ready to be sent, is minimally viable and is easily re-composed by other self-quantification services to prevent unnecessary duplication of data (Granularity).
– Self-quantification services simplify or subtract the length of property or resource names to reduce payload (Naming).

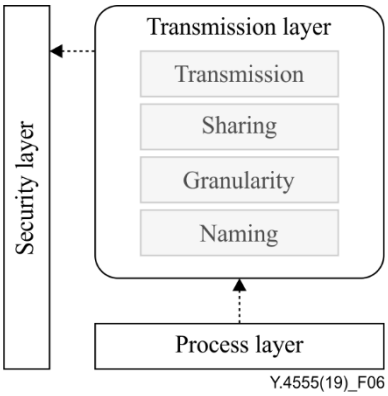

Figure 6 – Transmission layer of self-quantification services

9.1.3 Bridge

The bridge comprises virtual server and translation layers.

9.1.3.1 Virtual server layer

The virtual server layer receives the collected data, which is not understandable to the self-quantification service. Figure 7 describes two functional blocks within the virtual server layer.

– The virtual server layer provides a common list or mapping table of the semantics of predefined data models which allows different representations of properties of resources to be recognized identically (Mapping).

NOTE – For example, a person's heart rate could be expressed as follows: heartrate, heart-rate, heart_rate, hr, etc.

– Having a separate repository for units complements self-quantification services because different regions or applications use different units (Measured units).
– The virtual server layer sends data, which does not correspond to any other types listed in the common semantics list, back to the collection layer and asks for updating of the list to correctly parse the returned data in the future.

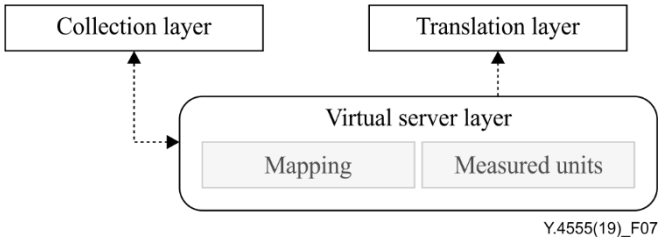

Figure 7 – Virtual server layer of self-quantification services

9.1.3.2 Translation layer

The translation layer converts the received data from the virtual server layer using the common semantics list provided by the virtual server layer. Figure 8 describes a functional block within the translation layer.

– Translation takes place only if properties and values of data from other self-quantification services can be correctly mapped to the intrinsic data types (Translation). After translation, the converted data is sent back to the process layer.

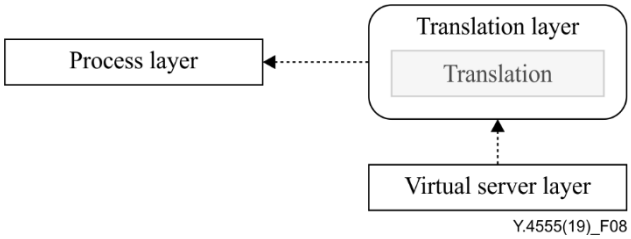

Figure 8 – Translation layer of self-quantification services

9.1.4 Security layer

The security layer ensures secure communications of self-quantification services. The security layer is supported by security requirements of self-quantification services especially when two or more different services communicate among them. Figure 9 describes five functional blocks within the security layer. All data and information transferred to/from self-quantification services pass through the security layer. The security layer encapsulates payload being transmitted to/from outside sensors, self-quantification services and remote servers. Each functional block strengthens the overall security of self-quantification services. Functional blocks are aligned with the requirements from the security perspective defined in clause 8.2. However, it is possible that additional security features are added depending on hardware and software specifications of self-quantification services.

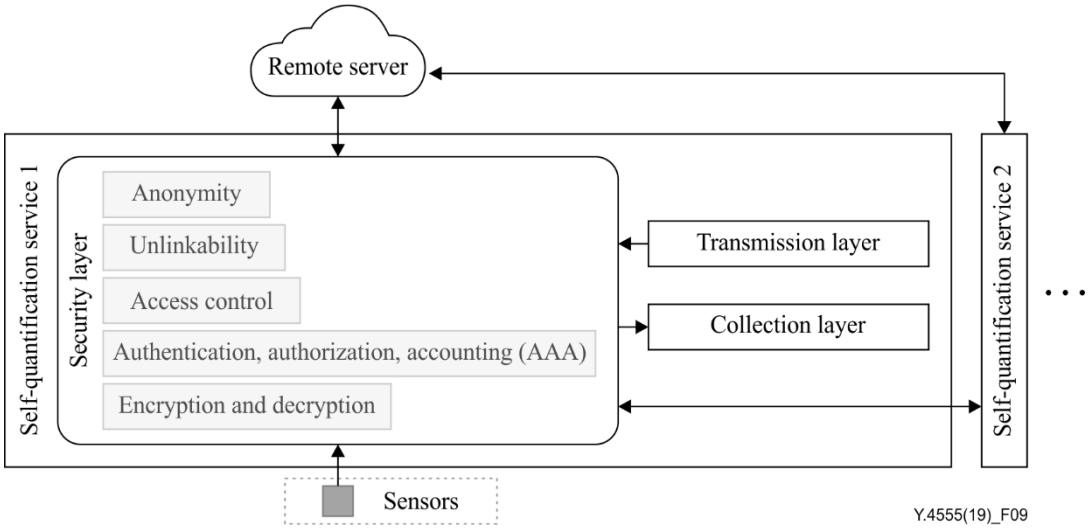

Figure 9 – Security layer of self-quantification services

9.1.5 Remote server

Remote servers receive data from self-quantification services. Remote servers engage in permission for data communication between two or more self-quantification services. Remote servers store data of self-quantification services under the agreement and permission of users. Remote servers can also be provided by third-party service providers that do not provide any self-quantification services. In such cases, self-quantification services allow self-quantification service user's account to third-party remote server providers without exposing any confidential user information. Such an authentication method can be carried out with other standards such as OAuth (Open Authorization). It could also be possible for data to be transmitted between remote servers. However, interactions among more than two different remote servers are outside the scope of this Recommendation.

9.2 Sequence diagrams of self-quantification services

In this clause, three sequence diagrams of self-quantification services are specified. The sequence diagrams are illustrated based on the general service models in clause 6.3 and the general functional architecture in clause 9.1. Similar to the general functional architecture, dotted lines indicate data flow inside a self-quantification service 1 and solid lines indicate data flow between a self-quantification service 1 and outer actors (e.g., sensors, remote server and other self-quantification services). The security layer is not specified in any of the sequence diagrams in this clause because the purpose of the security layer is common to all types of sequence diagrams.

9.2.1 Single self-quantification service

Figure 10 describes the sequence diagram of a typical single self-quantification service that collects data from sensors attached to one or more person and sensors located in the surrounding environment.

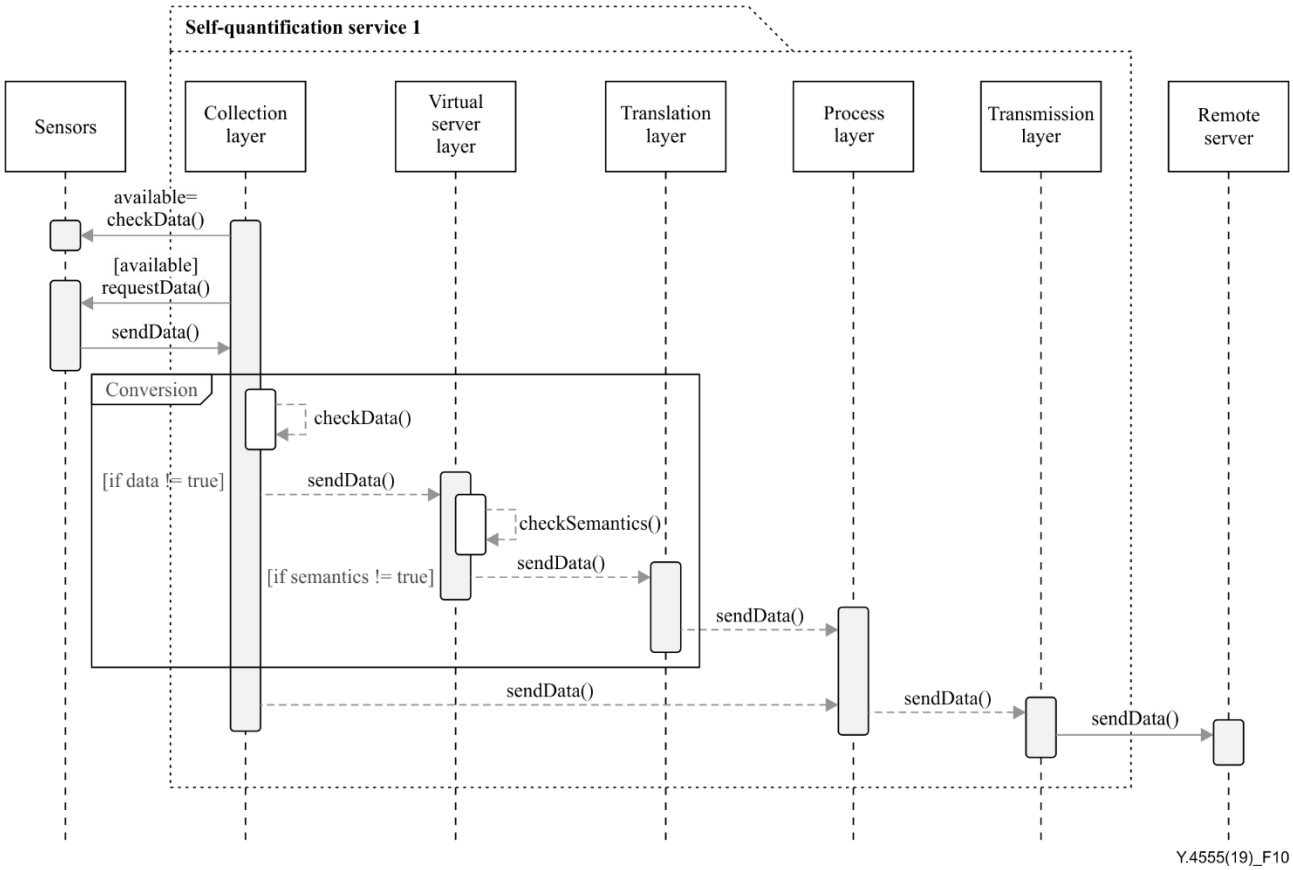

Figure 10 – Sequence diagram of single self-quantification service

1) Collection layer checks directly the adjacent sensors and asks for the availability of particular data.
2) If available, the collection layer requests for that data and retrieves it.
3) Collection layer checks if the data can be parsed and directly be forwarded to the process layer without conversion; i.e., if conversion is not required, the data is directly sent to the process layer.
4) If a conversion is required, the data is sent to the virtual server layer and the virtual server layer checks the semantics of the received data. If the virtual server layer finds proper semantics to the received data, then the data is sent to the translation layer to be mapped into a format which complies with the internal schema. The data is then sent to the process layer.

5) Process layer receives data from the collection layer or the translation layer and integrates, analyzes, visualizes, or stores data to produce a meaningful information to users. If users want to send the data to remote servers, the data is sent to the transmission layer.

6) Transmission layer sends data to the remote server only if deemed necessary.

9.2.2 Multiple self-quantification services

Figure 11 describes the sequence diagram of multiple self-quantification services where a single self-quantification service collects data not only from sensors attached to more than one person or surrounding environment but also other self-quantification services.

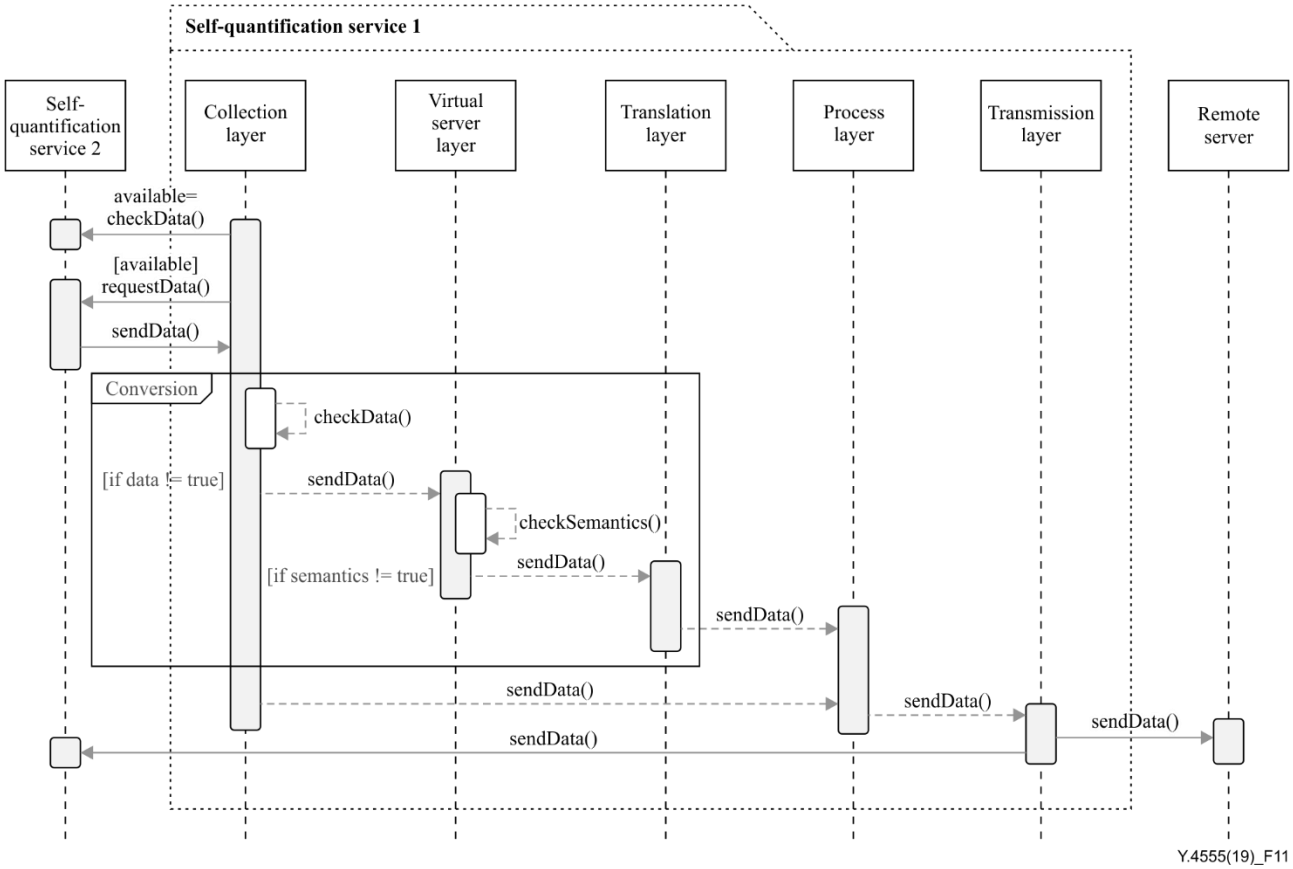

Figure 11 – Sequence diagram of multiple self-quantification services

1) Collection layer checks directly the adjacent self-quantification service 2 and asks for the availability of particular data.

2) If available, the collection layer requests for that data and retrieves it.

3) Collection layer checks if the data can be parsed and directly forwarded to the process layer without conversion; i.e., if conversion is not required, the data is directly sent to the process layer.

4) If a conversion is required, the data is sent to the virtual server layer and the virtual server layer checks the semantics of the received data. If the virtual server layer finds proper semantics to the received data, then the data is sent to the translation layer to be mapped into a format which complies with the internal schema. The data is then sent to the process layer.

5) Process layer receives data from the collection layer or translation layer and integrates, analyzes, visualizes, or stores data to produce a meaningful information to users. If users want to send the data to a remote server, the data is sent to the transmission layer.

6) Transmission layer sends data to the remote server only if deemed necessary or back to the self-quantification service 2 if self-quantification service 2 desires.

9.2.3 Multiple self-quantification services over a remote server

Figure 12 describes the sequence diagram of multiple self-quantification services where a single self-quantification service collects data not only from sensors attached to more than one person or surrounding environment but also other self-quantification services. In this case, however, communication between self-quantification services takes place at long range via remote servers.

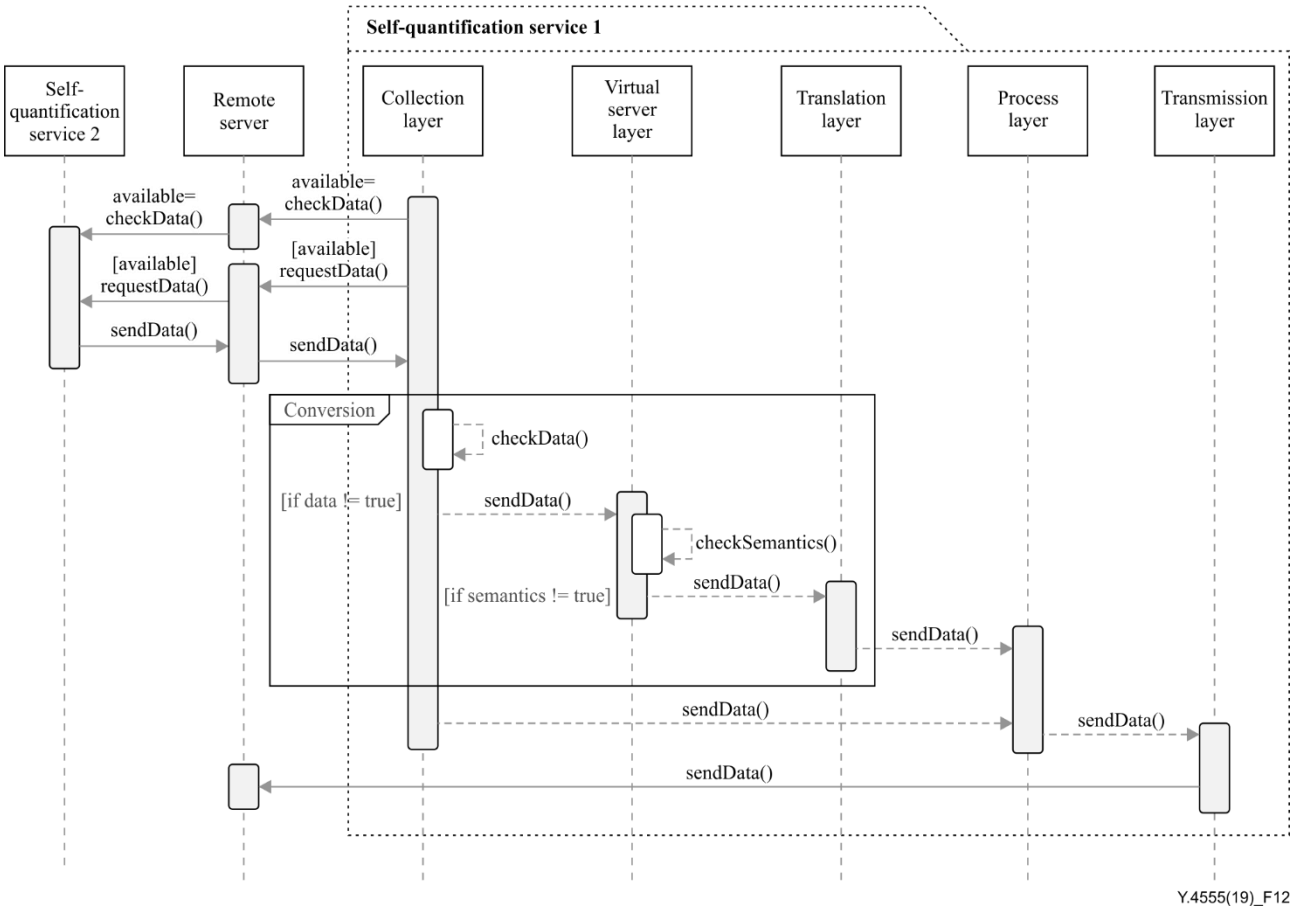

Figure 12 – Sequence diagram of multiple self-quantification services over a remote server

1) Collection layer checks directly remote servers and asks for the availability of particular data of self-quantification service 2. Remote servers then ask the self-quantification service 2 for the particular data.
2) If available, the collection layer requests for that data to remote servers and consequently, remote servers ask for that data to the self-quantification service 2.
3) Collection layer checks if the data can be parsed and directly forwarded to the process layer without conversion; i.e., if conversion is not required, the data is directly sent to the process layer.
4) If a conversion is required, the data is sent to the virtual server layer and the virtual server layer checks the semantics of the received data. If the virtual server layer finds proper semantics to the received data, then the data is sent to the translation layer to be mapped into a format which complies with the internal schema. The data is then sent to the process layer.

5) Process layer receives data from the collection layer or the translation layer and integrates, analyzes, visualizes, or stores data to produce a meaningful information to users. If users want to send the data to a remote server, the data is sent to the transmission layer.

6) Transmission layer sends data to a remote server only if deemed necessary.

Appendix I

Usage scenarios of self-quantification services

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

This appendix illustrates various usage scenarios of different numbers of self-quantification devices and users.

I.1 Usage scenario for one-user and one-device

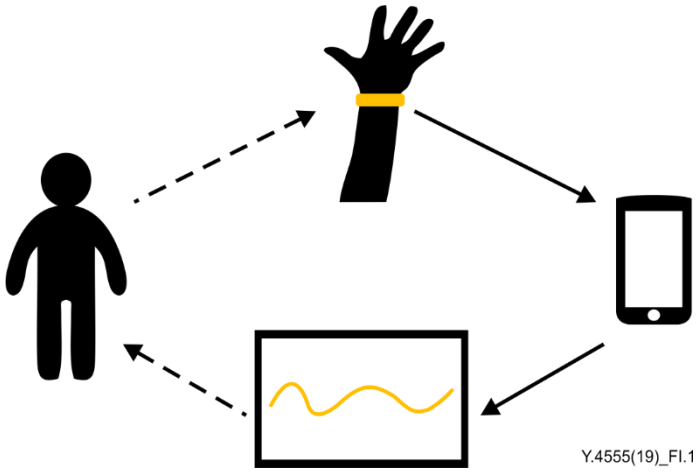

Figure I.1 – Usage scenario for one-user and one-device

1) CHA purchases a smart wristband to track his heart rate while jogging.
2) The smart band tracks his heart rate every specific time interval and transmits it to his smartphone to be stored.
3) His smartphone application then processes the data into a human-friendly information which can soon be visualized when requested.
4) After jogging, CHA returns back home and checks a chart that illustrates his heart rate fluctuation over time.
5) CHA shares his records through social media and stores his records in order to compare with his records in the future.

I.2 Usage scenario for one-user and two-devices

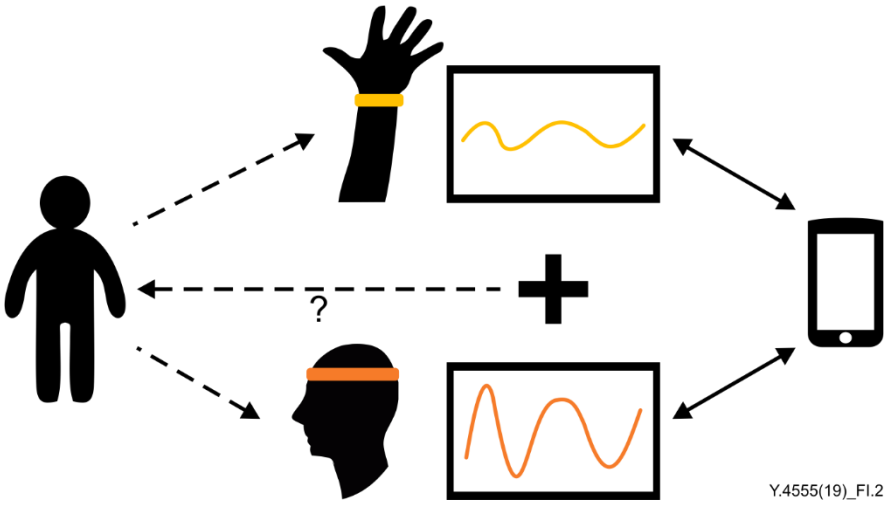

Figure I.2 – Usage scenario one-user and two-devices

1) CHA, who has already bought a smart wristband, purchases an additional smart headband to understand his sleep patterns and its relationship with his heart rate.
   – The smart headband measures the brain's electrical signals and provides a quantitative sleep quality value.
2) CHA's smartphone receives data from his devices and the corresponding applications for the wristband and the headband process and visualizes the result.
3) CHA now has two results but he cannot retrieve any information on the relationship between his sleep pattern and his heart rate because each of the results cannot represent any semantics to another. (Lack of interoperability)
4) CHA realizes these services support different rules of expressing and transmitting data since each device runs on different platforms. (Platform-dependency)
5) CHA, from an engineer's point of view, finds out there could also be an unnecessary duplication of functionalities since each device cannot use another device's functionalities when required for further data analysis. (Redundancy in functionality)
6) CHA hopes for an interoperable approach to be able to synthesize the results.
7) In other words, CHA wonders about the possibility of more insight and intelligence from direct communication between his wristband and headband by providing necessary protocols and guidelines.
8) CHA questions any other possible ways to overcome this problem.

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, 2019