International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1363

(05/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Internet of things (IoT) security

Technical framework of personally identifiable information handling in Internet of things environment

Recommendation ITU-T X.1363

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	**X.1360–X.1369**
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1363

Technical framework of personally identifiable information handling in Internet of things environment

Summary

Internet of things (IoT) devices can collect many kinds of data, including personally identifiable information (PII). Because PII data are useful for different types of services, they may be shared among multiple service providers.

It is better for users to manage their own data, including PII, in IoT environment based on their own intentions. As data usage in IoT environment with multiple service providers is complicated, user intentions for data usage should be accommodated flexibly. For example, if an IoT service provider provides the following functions, the user can appreciate that the service provider properly collects and controls data collected (including PII):

– Users can configure their own PII preferences. These preferences include a list of data allowed to be shared with other service providers.

– Collection and sharing of data are subject to controlled access based on PII preferences. Unauthorized data cannot be stored in data storage, and cannot be shared with other service providers.

– Users can check history log of data sharing among service providers. Users can also check the time at which their data has been shared.

Recommendation ITU-T X.1363 specifies a technical framework for PII handling in an IoT environment with single or multiple service providers.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1363	2020-05-29	17	11.1002/1000/14087

Keywords

IoT, Personally Identifiable Information, PII.

* 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 X.1363

Technical framework of personally identifiable information handling in Internet of things environment

1 Scope

This Recommendation specifies a technical framework of personally identifiable information (PII) handling in Internet of things (IoT) environment.

In IoT environment, some IoT devices have the capability to collect PII data. As PII data are useful for various types of services, data can be shared among multiple service providers. The technical framework specified in this Recommendation provides a mechanism to protect IoT users' PII data when collected, shared and used by one or more IoT service providers.

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 X.1058] Recommendation ITU-T X.1058 (2017) | ISO/IEC 29151:2017, *Information technology– Security techniques– Code of practice for personally identifiable information protection*.

[ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ISO/IEC 27000]: Provision of assurance that a claimed characteristic of an entity is correct.

3.1.2 access control [b-ISO/IEC 10027]: A capability to restrict the use of services accessing data to users who have been previously authorized.

3.1.3 control [b-ISO/IEC 27000]: Measure that is modifying **risk** (3.1.16).

NOTE 1 – Controls include any **process** (3.1.15), **policy** (3.1.14), device, practice, or other actions which modify **risk** (3.1.16).

NOTE 2 – It is possible that controls not always exert the intended or assumed modifying effect.

3.1.4 device [b-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.

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

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

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

3.1.6 management system [b-ISO/IEC 27000]: Set of interrelated or interacting elements of an **organization** (3.1.10) to establish **policies** (3.1.14) and **objectives** (3.1.7) and **processes** (3.1.15) to achieve those objectives.

NOTE 1 – A management system can address a single discipline or several disciplines.

NOTE 2 – The system elements include the organization's structure, roles and responsibilities, planning and operation.

NOTE 3 – The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.1.7 objective [b-ISO/IEC 27000]: Result to be achieved.

NOTE 1 – An objective can be strategic, tactical, or operational.

NOTE 2 – Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and **process** (3.1.15)].

NOTE 3 – An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 – In the context of information security management systems, information security objectives are set by the organization, consistent with the information security policy, to achieve specific results.

3.1.8 opt-in [b-ISO/TS 17975]: Process or type of policy whereby the data subject is required to take a separate action to express specific, explicit or prior consent for a specific type of processing.

3.1.9 opt-out [b-ISO/TS 17975]: Process or type of policy whereby the data subject is required to take a separate action in order to withhold or withdraw consent from a specific type of processing.

NOTE – In the case of Opt-out, Implied Consent exists for the collecting organization to process the personal information unless the individual explicitly denies or withdraws permission. Opt-out is also a process provided by a data collecting organization in order for a data subject to deny or withdraw permission to perform a specific type of processing.

3.1.10 organization [b-ISO/IEC 27000]: Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its **objectives** (3.1.7).

NOTE – The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

3.1.11 personally identifiable information [ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.12 personally identifiable information preferences [ISO/IEC 29100]: Specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose.

3.1.13 personally identifiable information principal [ISO/IEC 29100]: Natural person to whom the personally identifiable information (PII) relates.

NOTE – Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

3.1.14 policy [b-ISO/IEC 27000]: Intentions and direction of an **organization** (3.1.10), as formally expressed by its **top management** (3.1.18).

3.1.15 process [b-ISO/IEC 27000]: Set of interrelated or interacting activities which transforms inputs into outputs.

3.1.16 risk [b-ISO/IEC 27000]: Effect of uncertainty on **objectives** (3.1.7).

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

3.1.18 top management [b-ISO/IEC 27000]: Person or group of people who directs and controls an **organization** (3.1.10) at the highest level.

NOTE 1 – Top management has the power to delegate authority and provide resources within the organization.

NOTE 2 – If the scope of the management system (3.1.6) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

NOTE 3 – Top management is sometimes called executive management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACT Access Control Table

IoT Internet of Things

PII Personally Identifiable Information

T&C Terms and Conditions

5 Conventions

None.

6 Overview

There are many types of IoT devices and some of them are capable to collect PII data. Because PII data are useful for various types of services, service providers tend to collect many kinds of PII data from users. Moreover, such collected PII data can be shared by one service provider with other service providers to collectively provide services that are more useful to users. In this case, there are two types of service providers, one who collects (PII) data from users, and the other who provides various services using data collected by other service providers.

From users' point of view, their PII data should be handled appropriately by these service providers. It is recommended for users to specify their intentions of how their data could be handled, including PII, in the IoT environment. Because data usage situation is complicated in IoT environment with multiple service providers, user intentions for data usage should be accommodated flexibly. For example, if an IoT service provider provides the following functions, users can appreciate that this service provider collects data and handles PII data properly:

– Users can configure their own PII preferences. These preferences include a list of data that is permitted to be shared with other service providers.
– Collection and sharing of data are subject to controlled access based on PII preferences. Unauthorized data cannot be stored in data storage, cannot be shared with other service providers.
– Users can check history log of data sharing among service providers. Users can also check the time at which their data has been shared.

7 IoT service model with single or multiple service providers

Figure 1 is an IoT service model showing a service provided by one service provider. In this case, the service provider collects several kinds of data (including PII) and retains the information in a data storage that is managed by the service provider. The service provider provides various application(s) to users who provide their data (including PII) to the service provider.

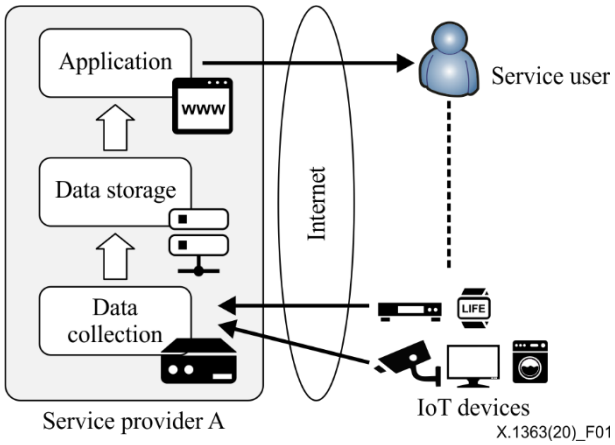

Figure 1 – Single service provider model

In this IoT service model, the sole service provider handles the collected data, and users use the application(s) under consented terms and conditions (T&C).

Figure 2 is a model showing multiple service providers sharing data collected from IoT devices. In this case, there are two kinds of service providers, 'data service provider' and 'application service provider'. In Figure 2, Service provider A collects data (including PII) from IoT devices, and shares it with other service providers (Service provider B and Service provider C). Service provider A is categorized as 'data service provider', and Service providers B and C are categorized as 'application service provider'. A service provider can be both 'data service provider' and 'application service provider'.

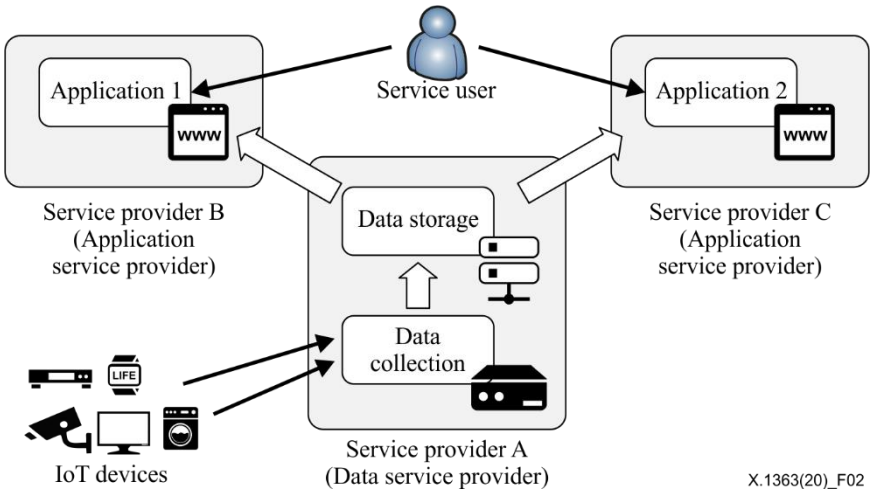

Figure 2 – Multiple service provider model

Normally, the list of data shared with other service providers is included in the T&C of a data service provider, and users need to consent to them before they can use this service provider's service(s).

The main difference between the single service provider model and the multiple service provider model is whether data collected by IoT devices are shared with other application service providers or not. In the case of the multiple service provider model, data collected by IoT devices are transferred to other application service providers.

8 Issues concerning PII data handling by IoT services

IoT service providers should consider the following issues when handling PII data:

– Purpose of PII data collection.

In order to avoid unnecessary data collection from a user's standpoint, users need to know the purpose of data collection and the nature of data collected for an IoT service.

– Mandatory consent to PII data collection.

When users subscribe to an IoT service, the data service provider needs to acquire their consent to the collection of several kinds of PII data. Normally this information is written in the T&C of the data service provider, and users must consent to it before they can subscribe to the service.

– Transferring PII data to third parties.

Data collected from IoT devices can be shared with third parties, i.e., other service providers. In this case, the data service provider needs to acquire explicit consent from users on transferring their PII data to third parties before the provider can send PII data to other service providers. In most cases, users cannot control PII data transfer. For example, users cannot select third parties to which they permit their PII data to be transferred, nor configure which kinds of PII data to be shared. Moreover, users cannot know what kinds of PII data are sent to third parties.

– Opt-in and Opt-out of consent to PII data collection/transfer.

When a service employs user PII data, the data service provider needs to acquire consent from the user both to collect PII data from the user and to transfer it to the third party. Not only the timing of receipt of consent is important, but also the method of getting it (opt-in or opt-out).

9 Principles for PII data handling by IoT services

PII protection principles and controls are specified in [ISO/IEC 29100] and [ITU-T X.1058], and developed based on various existing PII protection principles in a number of countries, states and international organizations, such as the Organization for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC).

Clauses 9.1 and 9.2 list principles for handling of PII data by IoT services to satisfy these principles in [ISO/IEC 29100] and [ITU-T X.1058].

9.1 General principles for PII data handling by IoT services

PII can be used to identify, contact or locate a specific individual. Disclosure of such information can lead to identity theft or other fraudulent usages, resulting in substantial harm, embarrassment and inconvenience to individuals [b-GAO-08-343]. Therefore, handling of PII data by an IoT service should meet the following general principles:

1) Encryption of PII data

All PII stored in IoT devices or in service databases shall be encrypted. Additionally, all PII shall be encrypted during transmission within and among all IoT service components (i.e., IoT device, data storage and application).

2) Access control/authentication

If PII data are stored on IoT devices or in service databases (data storage), appropriate access controls shall apply. Authorization to access PII shall be limited solely to fulfilling the purpose of its use for which the request of consent has been made by the service provider. This purpose of use shall be included in the T&C for which the service provider has obtained user consent. Access shall also be restricted when there is a potential for link-ability among stored data sets that would result in unauthorized identification or inference of additional PII.

3) Logging

Creation of computer-readable data extracts that include PII shall be maintained in an official log including creator, date, type of information, the purpose for extraction and user. Any PII that is included in these logs (e.g. username) shall be encrypted and subject to access controls.

4) Encryption for communication

PII data shall be encrypted or masked if it is shared among multiple service providers.

5) Notification of data compromise

If PII data are compromised due to data breach, leak, misuse or mishandling at any point in an IoT service, the service provider shall notify affected users and relevant service providers immediately following discovery of the compromise.

6) Data minimization procedures for retention

Any storage of PII data, whether collected or produced as outputs of data handling carried out by a service provider, shall be limited solely to the specified purpose for which the service provider has obtained explicit consent. The service provider shall set a maximum period for retention of PII data that is limited based on the specified purpose of its use, the potential for any link-ability among stored data sets that would result in identification or inference of additional PII and any applicable national laws and regulations.

9.2 Principles for PII data handling

Data service providers that collect PII data from IoT devices also should handle them appropriately. In particular, if data are used by services and shared with other service providers, its handling should satisfy user intentions. Therefore, handling of PII data by IoT service providers should meet the following principles:

1) Explanation of purpose for PII data collection

In order to collect minimum necessary PII data from users for providing an IoT service, the service provider shall explain in the T&C the purpose of its collection and the retention period for any PII collected.

2) Explicit consent to collect and share PII data from users

When a service provider supplies services that collect PII data from users, it shall obtain explicit user consent in data collection and sharing. In particular, the service provider shall implement an opt-in model wherever possible to obtain consent.

3) Transparency of PII data usage

When PII data, including any PII produced as data handling outputs carried out by a service provider, are shared among other service providers, the service provider shall provide transparency of PII management mechanism to allow users to check their own PII data usage. The IoT service shall also provide a redress mechanism that users can employ if data misattribution occurs.

4) Control of own preference

PII data shall be handled based on PII preferences configured by users.

10 PII data handling in IoT environment

10.1 Basic framework for PII data handling in an IoT environment

Figure 3 shows a basic framework for PII data handling in an IoT environment.

First, users decide their preference for PII data handling and reflect it as their PII preference in PII preference manager. The data (including PII) provided by users are controlled based on PII preferences.

PII preferences may include the following items:

– Kinds of data collected by IoT devices – IoT devices should collect only PII data that users specifically consented to in their PII preferences.

– Timing of data collection by IoT devices (e.g., weekday between 9:00 and 17:30) – Users do not want to send their PII data any time, hence such timing needs to be configured in PII preferences.

– Permitted service providers with which PII data can be shared – Users can choose application service providers that can access their PII data. Users can also choose the kinds of PII data that application service providers can access, including data that are collected from IoT devices or produced as outputs of data handling carried out by the primary service provider.

When IoT service components such as IoT device, data storage, application, etc. start to collect and use data, they should check PII preferences and handle data accordingly.

Second, access control information is generated based on the PII preference, and the access control table (ACT) is updated by using this information.

Third, each component refers to this ACT in case it collects or transfers PII data. The access control information in ACT is used to control what kind of PII data can be transferred among IoT service components.

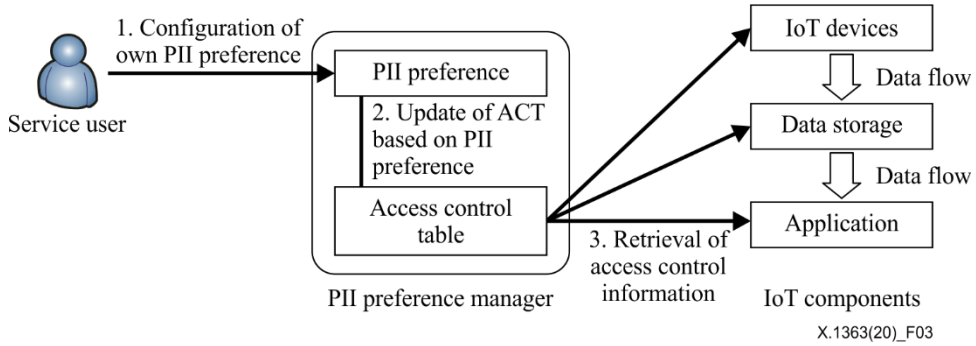

Figure 3 – Basic framework for PII data handling

10.2 Principles for a user interface to configure PII preferences

In order to implement this basic framework, service providers should provide a user interface for users to configure their PII preferences. This user interface should meet the following principles:

1) Easy access for all users

All users shall be able to access the user interface easily. For example, the first screen of the provided services should have a link to this user interface.

2) Proper access control to the user interface

Each service user has its own PII preference. Therefore, each user shall have a unique user account and shall be authenticated in a secure manner, for example, by using two factor authentication, before allowing him/her to access his/her user account.

3) Comprehensive

The user interface shall manage all PII preferences, including both on PII collection and sharing, of one user in one place.

4) Easy to use

The user interface shall be easy and straightforward to allow users to configure their PII preferences.

11 Technical framework for PII data handling in an IoT environment

This clause shows how to apply the basic framework specified in clause 10 for PII data handling in both single and multiple service provider environments.

11.1 PII data handling of IoT services by single service provider

11.1.1 Reference model for IoT services provided by single service provider

Figure 4 is a reference model showing IoT services provided by a single service provider. In this case, one service provider provides all functions for IoT services. The service provider collects data (including PII) from IoT devices, and stores it in its data storage. Application services can be provided to users using the collected data.

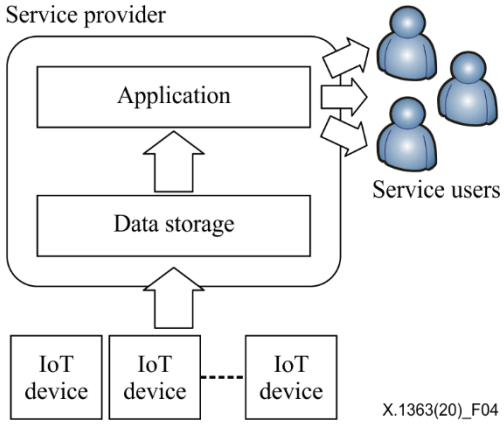

Figure 4 – Reference model for IoT services by single service provider

11.1.2 Technical framework for PII data handling by single service provider

Figure 5 is a technical framework showing a service provider that has a PII preference manager which manages users' PII preferences. Users configure their PII preferences with this PII preference manager, and IoT service components, such as IoT device, data storage and application, handle PII data based on that configuration. For example, if a user wants to limit specific PII data collected from IoT devices, then as the result IoT devices should not send such PII data to data storage.

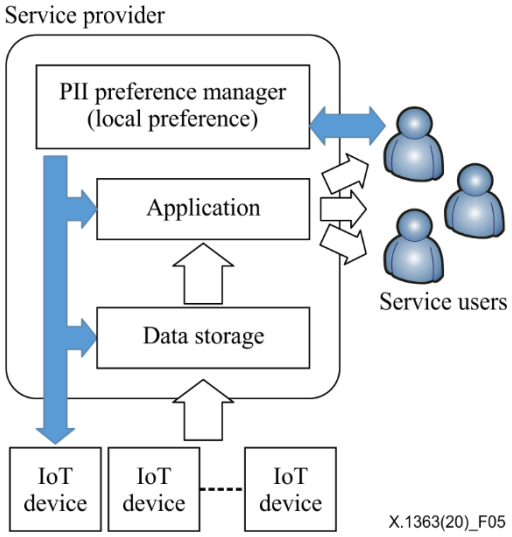

Figure 5 – Technical framework for PII data handling by single service provider

11.1.3 Technical framework for PII data handling by single provider with a common PII preference management portal

When IoT services are provided by a single provider, the data collected by IoT devices are not shared with other service providers whose IoT services are not used by this user. However, it could be necessary to share some common basic items of PII preference among service providers, as it may take too much time for users to configure their PII preferences for each individual IoT service. If users can specify common PII preferences for any kinds of IoT services, configuring PII preferences for each individual service will be easier and more efficient. To implement this, there are two types of PII preference manager.

Figure 6 is a technical framework showing there are two PII preference manager components, one is still the PII preference manager located in a service provider, and the other is a PII preference

management portal that is used to manage common preferences for any IoT services and for access by other service providers.

In this case, the user's common preferences for any services are stored in the PII preference management portal, whereas his/her specific preferences for each individual service are stored in the PII preference manager managed by each service provider. When a user starts to subscribe to a new service, the local PII preference manager in the data service provider retrieves his/her common preferences from the PII preference management portal, which could be managed by a third party and configured in advance by the user. Although users still need to configure their PII preferences with the local PII preference manager for this specific service, they do not need to configure every time their common preferences that are stored in the PII preference management portal. IoT service components, such as IoT device, data storage and application, control PII data based on local preferences in the PII preference manager.

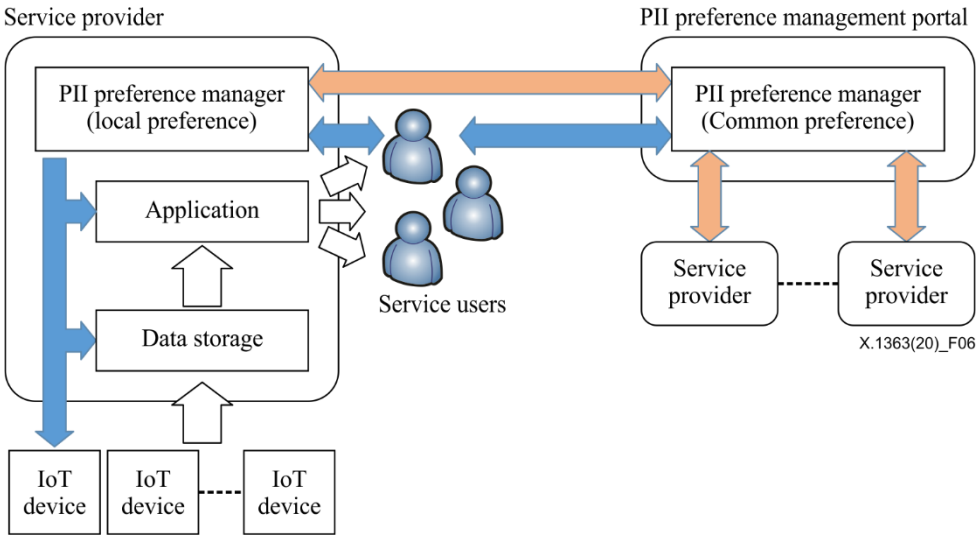

Figure 6 – Technical framework for PII data handling on IoT services by single service provider with a common PII preference management portal

11.2 PII data handling of IoT service by multiple service providers

11.2.1 Reference model for IoT services by multiple service providers

Figure 7 is a reference model showing IoT services provided by multiple service providers. In this case, an IoT service consists of multiple service providers (application service provider and data service provider), and each application service provider provides its own service(s) to users by using data collected by other data service provider. Therefore, service providers that collect data (including PII) from IoT devices (data service provider) can be different from those that only provide services to users (application service provider). In Figure 7, there are two types of service providers, one is a 'data service provider' that collects data (including PII) from IoT devices and the others are 'application service provider' that provides application services to users using the collected data.

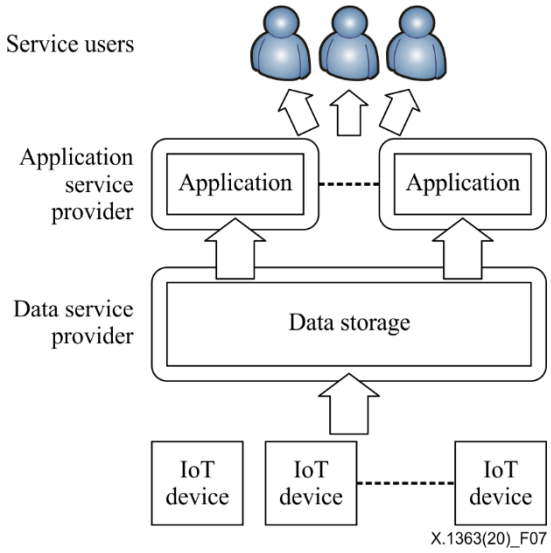

Figure 1 – Reference model for IoT services by multiple service providers

11.2.2 Technical framework for PII data handling by multiple service providers

Figure 8 is a technical framework showing a data service provider has a PII preference manager and all the user preferences for handling PII data are managed at this local management component. Users configure their local preferences with the PII preference manager. IoT service components (including applications provided by other application service providers) handle PII data based on the local preferences in the data service provider's PII preference manager.

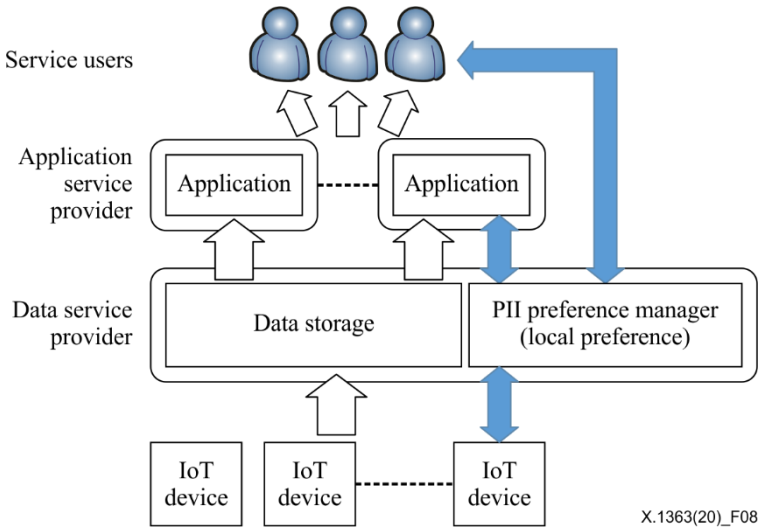

Figure 8 – Technical framework for PII data handling for IoT services by multiple service providers

11.2.3 Technical framework for PII data handling on IoT services by multiple service providers with a common PII preference management portal

Figure 9 is a technical framework showing multiple service providers use both PII preferences stored in a common PII preference management portal and in data service providers' local PII preference managers.

In this case, common preferences for any services are stored in a common PII preference management portal, whereas specific preferences for each service are stored in a local PII preference manager

managed by each data service provider. When a user starts to subscribe to a new service, the local PII preference manager of the service provider retrieves common preferences from the PII preference management portal. Although this user still needs to configure his/her PII preferences in the local PII preference manager, he/she does not need to configure the common PII preferences stored in the PII preference management portal repeatedly. IoT service components control PII data based on local preferences in the PII preference manager.

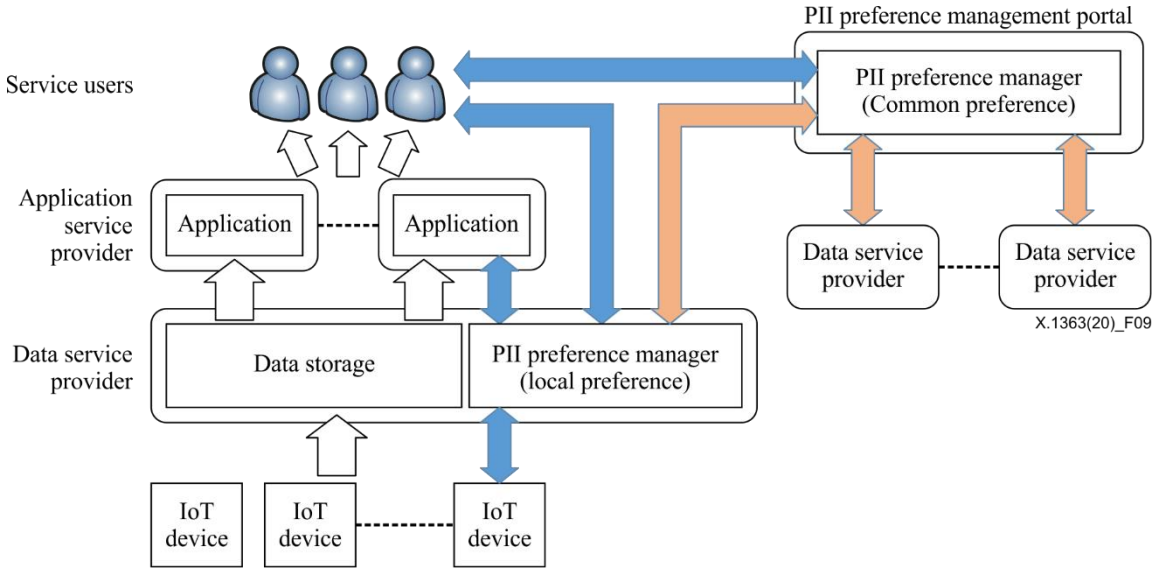

Figure 9 – Technical framework for PII data handling one IoT services by multiple service providers with a common PII preference management portal

Bibliography

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

[b-ISO/IEC 10027] ISO/IEC 10027:1990 *Information technology – Information Resource Dictionary System (IRDS) framework*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/TS 17975] ISO/TS 17975:2015, *Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information.*

[b-GAO-08-343] GAO-08-343 (2008). *Information security: Protecting personally identifiable information*. Washington, DC: United States Government Accountability Office. 34 pp.

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, 2020