INTERNATIONAL STANDARD

ISO/IEC 19944

First edition
2017-09

Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use

Technologies de l'information — Informatique en nuage — Services et dispositifs en nuage : Débits, catégories et utilisation des données

Reference number
ISO/IEC 19944:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

Introduction

Objective and target audience

This document provides a description of the ecosystem of devices and cloud services and the related flows of data between cloud services, cloud service customers, cloud service users and their devices. These are necessary to provide guidance about how data is used on the devices in the context of the cloud computing ecosystem and the associated location and identity issues that emerge from such use.

This document proposes a scheme for the structure of data use statements that can be used by cloud service providers to help cloud service customers understand and protect the privacy and confidentiality of their data and their users' data through increased transparency of policies and practices.

This document can be used in several ways including, but not limited to, the following:

a) by cloud service providers and application developers to guide them in describing what they intend to do with data in their designs, so as to simplify privacy and data use reviews and to communicate this information to non-technical departments such as internal compliance, marketing and legal teams;

b) by organizations drawing up data use statements as part of drafting cloud service agreements and application contracts, privacy statements, etc., which could apply to documents internal to an organization, in addition to public or legal documents;

c) by government regulators and agencies to advise on suitable ways of describing data flow and use;

d) by those preparing information on data flow and data use for communication to the press and the public.

This document is descriptive and not prescriptive. It cannot be used for compliance directly. Instead, it provides a set of concepts and definitions, including a data taxonomy and data use statement structure, that can be used for transparency about how data is used in an ecosystem of devices and cloud services.

Providing a clear description of data flows

This document aims to improve the understanding of the data flows that take place in an ecosystem consisting of devices accessing cloud services. It does this through an extended cloud computing reference architecture (CCRA) (based on the architecture described in ISO/IEC 17789) that describes the impact of devices on cloud service ecosystems and the impact of cloud services on devices. It also describes the data flows that take place within the extended reference architecture.

Providing transparency to all stakeholders

To maintain a relationship of trust between the stakeholders of the ecosystem of devices and cloud services and also to meet the demands of laws and regulations, it is necessary for the device platform providers and the cloud service providers to be transparent about how they make use of the various data types that flow within the ecosystem.

There is a particular need to provide simple and clear statements to end users about what is done with data that relates to them. The data may be personally identifiable information (PII) and may be sensitive, in other words, this can be a privacy issue. Cloud service customers are likely to be concerned about how their data is used, even when the customer is an organization rather than an individual. The cloud service customer may be a data controller, holding personal data about their employees or their customers; in such a role, the cloud service customer has obligations relating to the processing of that data.

To assist cloud service providers and device platform providers in being transparent about their use of data, this document defines a simple language for making statements about data use, which can be used to create clear notification to end users and other interested parties.

Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use

1 Scope

This document

— extends the existing cloud computing vocabulary and reference architecture in ISO/IEC 17788 and ISO/IEC 17789 to describe an ecosystem involving devices using cloud services,

— describes the various types of data flowing within the devices and cloud computing ecosystem,

— describes the impact of connected devices on the data that flow within the cloud computing ecosystem,

— describes flows of data between cloud services, cloud service customers and cloud service users,

— provides foundational concepts, including a data taxonomy, and

— identifies the categories of data that flow across the cloud service customer devices and cloud services.

This document is applicable primarily to cloud service providers, cloud service customers and cloud service users, but also to any person or organization involved in legal, policy, technical or other implications of data flows between devices and cloud services.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
cloud service
one or more capabilities offered through cloud computing invoked using a defined interface

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.2
cloud service customer
party which is in a business relationship for the purpose of using *cloud services* (3.1)

Note 1 to entry: A business relationship does not necessarily imply financial agreements.

[SOURCE: ISO/IEC 17788:2014, 3.2.11]

3.3
cloud service partner
party which is engaged in support of, or auxiliary to, activities of either the *cloud service provider* (3.4) or the *cloud service customer* (3.2), or both

[SOURCE: ISO/IEC 17788:2014, 3.2.14]

3.4
cloud service provider
party which makes *cloud services* (3.1) available

[SOURCE: ISO/IEC 17788:2014, 3.2.15]

3.5
cloud service user
natural person, or entity acting on their behalf, associated with a *cloud service customer* (3.2) that uses *cloud services* (3.1)

Note 1 to entry: Examples of such entities include devices and applications.

[SOURCE: ISO/IEC 17788:2014, 3.2.17]

3.6
device
physical entity that communicates directly or indirectly with one or more *cloud services* (3.1)

3.7
account data
class of data specific to each CSC that is required to administer the *cloud service* (3.1)

Note 1 to entry: Account data is typically generated when a cloud service is purchased and is under the control of the CSP.

Note 2 to entry: Account data consists of data elements provided by CSC, such as; name, address, telephone, etc.

3.8
cloud service customer data
class of data objects under the control of the *cloud service customer* (3.2) that were input to the *cloud service* (3.1), or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer through the published interface of the cloud service

Note 1 to entry: An example of legal controls is copyright.

Note 2 to entry: It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.

[SOURCE: ISO/IEC 17788:2014, 3.2.12]

3.9
cloud service derived data
class of data objects under *cloud service provider* (3.4) control that are derived as a result of interaction with the *cloud service* (3.1) by the *cloud service customer* (3.2)

Note 1 to entry: Cloud service derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities.

[SOURCE: ISO/IEC 17788:2014, 3.2.13]

3.10
cloud service provider data
class of data objects, specific to the operation of the *cloud service* (3.1), under the control of the *cloud service provider* (3.4)

Note 1 to entry: Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

[SOURCE: ISO/IEC 17788:2014, 3.2.16]

3.11
application marketplace
set of *cloud services* (3.1) providing a digital marketplace intended to offer applications and other digital content for a particular *device platform* (3.13) allowing users to browse and download applications and other content

Note 1 to entry: An application marketplace may be offered to the public, or to private groups such as a corporate environment.

Note 2 to entry: A *device* (3.6) can use more than one application marketplace.

3.12
application cloud service
cloud service (3.1) that supports applications running on a given *device* (3.6), where the cloud service is provided by a party other than the *device platform provider* (3.14)

3.13
device platform
operating system and related feature set that provide the core capabilities for a *device* (3.6)

Note 1 to entry: An *application marketplace* (3.11) is specific to a device platform.

3.14
device platform provider
device platform cloud service provider
cloud service provider (3.4) that provides *cloud services* (3.1) necessary to support a *device platform* (3.13) including managing needed digital identities

Note 1 to entry: The cloud service provider that offers the *application marketplace* (3.11) is typically the same as the device platform provider, but it is not required to be.

3.15
device platform cloud service
cloud service (3.1) offered by the *device platform provider* (3.14) to support the *device platform* (3.13)

Note 1 to entry: An *application marketplace* (3.11) can be an example of device platform cloud service.

3.16
personally identifiable information
PII
any information that a) can be used to identify the *PII principal* (3.18) to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.17
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (PII) (3.16) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others, e.g. *PII processors* (3.19) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.18
PII principal
natural person to whom the *personally identifiable information* (PII) (3.16) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.19
PII processor
privacy stakeholder that processes *personally identifiable information* (PII) (3.16) on behalf of and in accordance with the instructions of a *PII controller* (3.17)

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.20
end user identifiable information
EUII
derived data associated with a user that is captured or generated from the use of the service by that user

4 Abbreviated terms

BYOD	Bring Your Own Device
CCRA	Cloud Computing Reference Architecture
CSA	Cloud Service Agreement
CSC	Cloud Service Customer
CSN	Cloud Service partner
CSP	Cloud Service Provider
CSU	Cloud Service User
EUII	End User Identifiable Information
GPS	Global Positioning System
IaaS	Infrastructure as a Service
PII	Personally Identifiable Information
SLA	Service-Level Agreement

5 Structure of this document

This document is organized to describe two topic areas.

— Overview and reference architecture (Clauses 6 and 7).

— Data taxonomies, data categories and data use statement structure (Clauses 8, 9 and 10).

Overview and reference architecture

— Clause 6 provides the foundation of the document covering the "Overview of devices and cloud services ecosystems". The clause describes the ecosystem and stakeholders where devices and cloud services operate.

— Clause 7, "Extending the cloud computing reference architecture to the devices and cloud services ecosystem" covers an extension of the architecture specified in ISO/IEC 17789[2] to include devices and the flow of data between devices and cloud services.

Data taxonomies, data categories and data use statement structure (applicable to data exchanges between devices and cloud services)

— Clause 8, "Data taxonomies" describes categories of data that can be captured, processed, used and shared. This taxonomy extends the definitions in ISO/IEC 17788[1] of cloud service customer data, cloud service derived data, cloud service provider data and account data. The taxonomy described in this clause is used in creating data use statements covered in Clause 10.

— Clause 9, "Data processing and use categories" describes the various categories of data processing and operations. "Data use categories" and related "scopes" described in this clause are required for understanding of the data use statements structure covered in Clause 10.

— Clause 10, "Data use statements" describes the syntax and statement structure for expressing how data is used by CSPs and their partners.

6 Overview of devices and cloud services ecosystems

6.1 Background and context — Impact of devices and personalized cloud services

This document builds on the foundation provided by the CCRA, ISO/IEC 17789, to accommodate data and its flow within the ecosystem of devices and cloud services.

Many kinds of devices are used as clients for accessing cloud services. These devices rely on support from cloud services which have an association between the device and the cloud service. Unique identifiers are created and maintained to enable that association. The interaction between the device and the cloud service requires an understanding of the flow of data between devices, cloud services, cloud service customer and cloud service providers. This interaction also makes the discussion of data classification, access and use more complex.

NOTE This document uses the term "device" in the context of a cloud service user as defined in ISO/IEC 17788:2014, 3.2.17, which includes natural person, or entity acting on their behalf. Examples of such entities include devices and applications. This document is written such that there is no conceptual difference between types of devices, provided the device is acting as a cloud service user using cloud services.

Cloud service providers offering device specific cloud services typically require a unique identifier and a cloud service user account in order to provide those cloud services. This identifier and user combination becomes the cloud service user's key to their own personalized cloud services which can offer an array of services, access to applications, rich advertising and retail infrastructure.

The always-on, always-with-me nature of some devices drives a new class of applications for personal use that strive to assist users with every aspect of their daily lives by making useful suggestions based on a trail of information flowing from the device and from applications running on the device.

For example, a mobile device user's interaction with the device platform cloud services may offer the device platform provider a very detailed trail of behavioural data, including user communications, contacts, calendar, whereabouts and searches and purchases.

6.2 Ecosystem of devices and cloud services

This clause describes an ecosystem of cloud-supported devices and cloud services. Figure 1 depicts a common way of how a device may operate in a cloud environment. The cloud services used by devices come in several categories. The categories of cloud services used by devices and covered in this document are as follows.

— **Device platform cloud service** (see 3.15) which can include application marketplace (see 3.11). These "core" cloud services are offered by the device platform provider and used to configure the device and register the customer (and where appropriate, the primary user of the device) with the application marketplace and associated cloud services, including online user identity management. This is depicted by the upper cloud in the diagram in Figure 1 and corresponds with the sub-role "device platform provider" defined in 7.3.1.1.2.

— **Application cloud service** (see 3.12) which supports the applications developed and supported by cloud service providers (e.g. social networking, weather, news or organization-specific applications) that are not the device platform CSP. Such applications interact with their own cloud services, distinct from the cloud services provided to support the device platform. This is depicted by the lower cloud in the diagram in Figure 1 and corresponds with the role of cloud service provider defined in ISO/IEC 17789:2014, 8.3.1.

Both categories involve interactions with the device and carry data traffic, potentially including cloud service customer data or end user identifiable information (EUII). For example, the application marketplace knows which applications have been downloaded on the device and the device platform knows how often they are invoked and how long they are used.

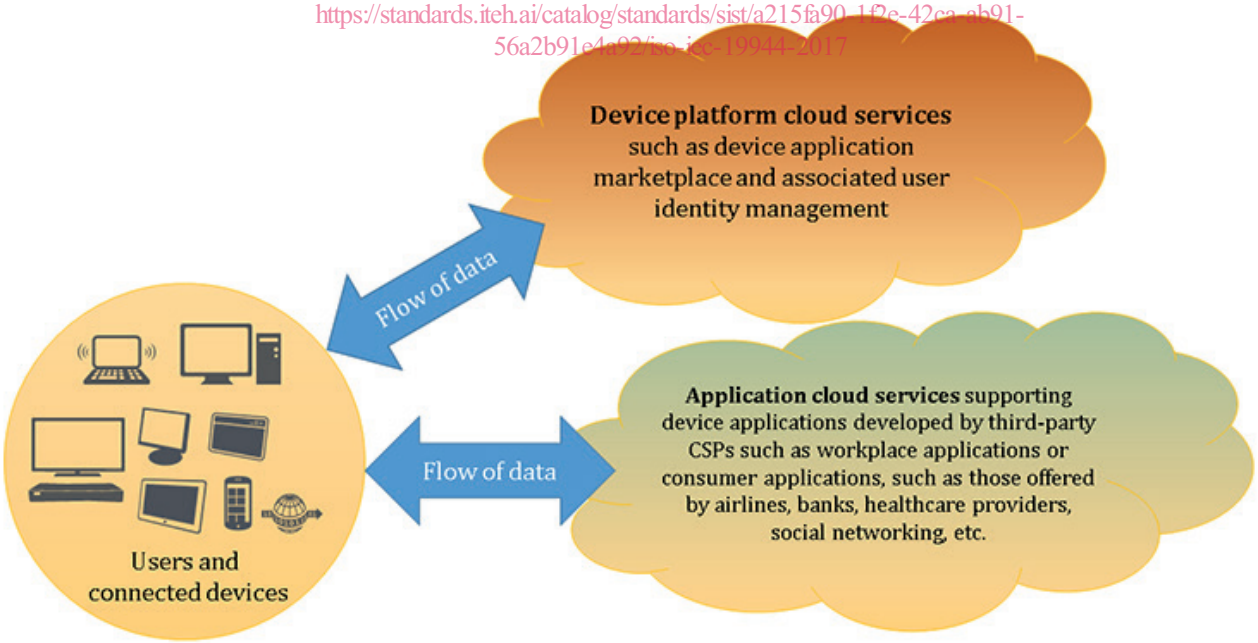

Figure 1 — Devices and cloud services ecosystem

Most tablets, smartphones and other connected devices are often connected to their device platform cloud services in order to be fully functional. This connectivity and flow of data is depicted by the arrow to the upper cloud in Figure 1, although some IoT devices may not communicate to the device platform cloud services directly. At the same time, the devices are also connected to various cloud services,

depicted in the diagram by the lower cloud, that support the applications developed and supported by cloud service providers. This connectivity and flow of data is shown by the arrow to the lower cloud in Figure 1.

6.3 Devices and multiple user sub-roles

6.3.1 General

Device users typically use the same device while assuming various roles in their daily lives, often concurrently as shown Figure 2, a citizen/voter consuming city/government services, a patient receiving medical services at a doctor's office or a hospital, a student attending school, a motorist or commuter on the road, a consumer in a mall/coffee shop/store, a passenger in the airport or train station, in addition to being an employee.

Citizens, students, patients and employees, for example, each have unique requirements and needs for data and privacy protection. Nevertheless, each user sub-role will use the same personal device including the device's local storage, which can potentially be part of the same device application marketplace(s) ecosystem and will use the same device services offered by the device's operating system.

Device provider, device services and applications, as well as cloud service providers providing the applications on the device may have visibility into the device users' actions, data and their use of applications and services. Such visibility to user data could continue as users assume multiple sub-roles throughout their use of the device and use multiple applications such as those developed for workplace use (employees), government and citizen use (voters, taxpayers, etc.), schools (students) or healthcare (patients). The user's data may be collected, stored, processed and used by the cloud service providers. In contrast, for some applications and some cloud services, the user might take the sub-role of anonymous user, where the user wants the right to use the application and cloud services in a private manner, where the user's identity and the user's personal information are deliberately not shared with the application and with the cloud service. While technologies such as application containers/sandboxes, application-specific encryption and application-specific VPNs can mitigate this, there is still a need for a data taxonomy that categorizes data in a harmonized and consistent fashion so as to enable a meaningful conversation between the cloud service customers, the cloud service providers, regulators and other stakeholders about this data.

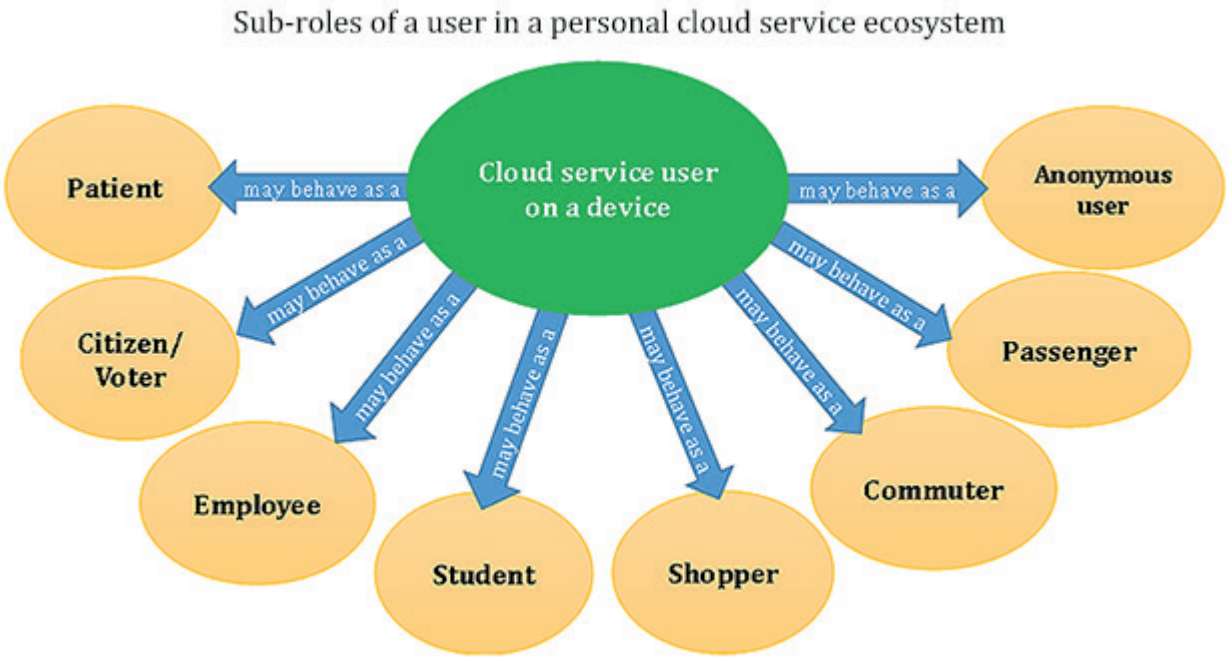

Figure 2 — Example of roles a user can assume in device use scenarios

The following is a non-exhaustive and informative list of sub-roles that help describe device scenarios and issues.

— Patient: patients are under healthcare privacy laws.

— Citizen: all aspects of an individual's relationship with government and public authorities, including voting and obligations to and benefits received from government.

— Employee: they should follow the organization’s policies to protect the organization’s confidential assets.

— Students: many students are under-age and therefore they are under stricter privacy and commercial advertisement laws.

— Shopper: data, such as payment instrument data, personal favourites, shopping locations, personal financial information, can be collected and processed during shopping. Such data can be relevant to privacy.

— Commuter: the flow of commuter’s personal data could also be examined while the user utilizes data services offered while in transit.

— Passenger: passengers are in public transportation hubs like airports, and therefore, certain rules may apply.

— Anonymous user: where the user does not wish to share any personal data with the application and with the cloud services, including identity.

6.3.2 Bring your own device (BYOD)

“Bring your own device” (BYOD) is defined as the practice of allowing employees of an organization to use their own computers, smartphones, tablets or other devices for work purposes. BYOD is a particular case of mixing different roles when using a device where the user has the role of an employee or partner of an organization.

In the past, it was common for organizations to provide the devices that employees used mainly or even exclusively for work purposes and those devices were connected to the organization’s networks and used the organization applications and systems. Organization-owned devices are typically tightly controlled in terms of the installed software, both in terms of the software that can be installed by employees and in the requirement to run a variety of management and security components including firewalls, malware checking programs, encryption of stored data and so on.

The main concern for organizations is to ensure that the organization’s applications, systems and data are secure and are only used for authorized purposes, so any employee devices with access to corporate assets are controlled to ensure the integrity of organization systems.

The introduction of mobile devices such as smartphones and tablets changed the IT landscape significantly. These mobile devices are very popular and employees see them as helping them do productive work both outside the office and within the office. This leads to a demand from employees to use their personal/private mobile devices to access the organization’s applications and systems. Employees do not want to have multiple different devices (one their own, another owned by the organization) since this can be burdensome and difficult to manage.

BYOD encompasses not only employees but also other users with a close relationship to the organization, such as business partners.

A mobile device user remains connected to their personalized cloud services even when they bring their own device into an organizational setting where they use organization-specific applications, systems and networks even as the device runs applications not belonging to the organization and connects with cloud services not belonging to the organization. The organization’s own client applications running on the device may also use functions and rely on services from the device platform cloud services or elsewhere. That interaction is also captured and associated with the user’s digital identity or the

device's identifier. Instead of a simple client-server interaction, there is the potential for intertwined flow of data between the device, the device platform cloud services, organization applications, other applications installed by the user and the organization's cloud services. The major issues are the potential for leakage of enterprise data and the potential for data of doubtful provenance to be transmitted to the organizations' cloud services and/or internal systems.

Organizational Information Technology (IT) managers need to protect intellectual property and confidential data against unauthorized disclosure or leakage and, as such, may demand tight control over a user's own device when that person is interacting with the organization as an employee or in another role. Additional information on the security threats can be found in ISO/IEC 27033-3:2010, Clause 13[5] Organizational users and their IT managers would benefit from deeper understanding of BYOD scenarios affecting security and confidentiality of organizational data when device users assume other roles when using the same device (for example, as an employee, a student, a patient, a consumer). Effectively, the need is to partition the use of the device, with organization applications and data separated by secure boundaries from other applications and data.

For organizations, BYOD brings some challenges, mostly relating to the security of organization applications and data when personal devices are used. The main risks can be summarized as follows.

— Loss of control over access to organization applications from the device, a personal device may be shared with others.

— Vulnerability of organization data which is downloaded and stored on the device, there is potential for loss, theft and unauthorized alteration of the data.

— Use of non-organization applications and cloud services on the device:

  a) to use or transmit or share or store organization data

  b) which may be used to access organization systems and applications.

— Malware on the device stealing important data including identities and credentials.

7 Extending the CCRA to the devices and cloud services ecosystem

7.1 Overview

The devices and cloud services ecosystem requires extensions to the CCRA described in ISO/IEC 17789.

Expansion of the description of the functional components in the User layer is required in order to describe a number of components which relate to mobile devices. This is particularly important to understand the data flows that take place within the ecosystem. There is an associated expansion in the cloud service customer role and its sub-roles to describe additional activities and responsibilities that exist when devices are used with cloud services. Similar extensions of the cloud service provider role and its sub-roles are also necessary.

7.2 Personal and organizational environments

The cloud services and associated applications are designed for a variety of uses. Applications and cloud services designed for the personal use of the end user form part of the "personalized cloud services" of the end user. Applications and cloud services, designed for use as part of the function of an organization to which the end user has a relationship (e.g. employee or partner), can be described as "business capabilities" or "organizational capabilities".

Personal use applications and cloud services are very likely to involve the case where the end user performs all of the roles defined for a cloud service customer, with a need for simple interfaces to allow necessary administration and management capabilities.

