BS ISO/IEC 19944-1:2020

BSI Standards Publication

Cloud computing and distributed platforms — Data flow, data categories and data use

Part 1: Fundamentals

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19944-1:2020

National foreword

This British Standard is the UK implementation of ISO/IEC 19944-1:2020. It supersedes BS ISO/IEC 19944:2017, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/38, Cloud Computing and Distributed Platforms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 06768 2

ICS 35.210

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19944-1:2020

INTERNATIONAL STANDARD

ISO/IEC 19944-1

First edition
2020-10

Cloud computing and distributed platforms — Data flow, data categories and data use —

Part 1: Fundamentals

Informatique en nuage et plates-formes distribuées — Flux de données, catégories de données et utilisation des données —

Partie 1: Principes de base

Reference number
ISO/IEC 19944-1:2020(E)

Documents
Document Sharing Hub
© ISO/IEC 2020

Full document details: BS ISO/IEC 19944-1:2020

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19944-1:2020

Contents

Page

Foreword ... **vi**

Introduction ... **vii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**
3.1 Terms related to data categories ... 2
3.2 Terms related to cloud services and devices ecosystem ... 2
3.3 Terms related to privacy ... 3
3.4 Terms related to organizational data ... 3
3.5 Terms related to artificial intelligence ... 4
3.6 General terms ... 6

4 Abbreviated terms ... **6**

5 Structure of this document ... **7**
5.1 Document organization ... 7
5.2 Overview and reference architecture ... 7
5.3 Data taxonomies, data categories and data use statement structure ... 7

6 Overview of devices and cloud services ecosystems ... **7**
6.1 Background and context — Impact of devices and personalized cloud services ... 7
6.2 Ecosystem of devices and cloud services ... 8
6.3 Devices and multiple user sub-roles ... 9
6.3.1 General ... 9
6.3.2 Bring your own device ... 10

7 Extending the CCRA to the devices and cloud services ecosystem ... **12**
7.1 Overview ... 12
7.2 Personal and organizational environments ... 12
7.3 Device impact on the CCRA: User view ... 12
7.3.1 Cloud service provider ... 12
7.3.2 Cloud service customer ... 13
7.4 Device impact on the CCRA: functional view ... 14
7.4.1 General ... 14
7.4.2 Functional components in the functional view ... 15
7.4.3 Functional view: data flows ... 16

8 Data taxonomy ... **18**
8.1 Overview ... 18
8.2 Data categories ... 19
8.2.1 General ... 19
8.2.2 Customer content data ... 20
8.2.3 Derived data ... 21
8.2.4 Cloud service provider data ... 23
8.2.5 Account data ... 24
8.3 Data identification qualifiers ... 24
8.3.1 General ... 24
8.3.2 Identified data ... 25
8.3.3 Pseudonymized data ... 25
8.3.4 Unlinked pseudonymized data ... 25
8.3.5 Anonymized data ... 25
8.3.6 Aggregated data ... 25
8.4 Orthogonal facets of data ... 26
8.4.1 General ... 26
8.4.2 Perspective used in the definition of data facets ... 28
8.4.3 Common orthogonal data facets ... 28

AVA Documents
Document Sharing Hub

© ISO/IEC 2020 – All rights reserved

Full document details: BS ISO/IEC 19944-1:2020

8.4.4 Use of data facets to describe data taxonomy ... 34

9 Data processing and use categories ... 34
9.1 Overview ... 34
9.2 Data processing categories ... 34
9.2.1 General ... 34
9.2.2 Data partitioning ... 35
9.2.3 Data integration ... 35
9.2.4 Data fusion ... 36
9.2.5 Data improvement ... 36
9.2.6 Encryption ... 36
9.2.7 Replication ... 36
9.2.8 Data Deletion ... 36
9.2.9 Re-identification ... 37
9.3 Data use categories ... 37
9.3.1 General ... 37
9.3.2 Provide ... 38
9.3.3 Improve ... 38
9.3.4 Personalize ... 39
9.3.5 Offer upgrades or upsell ... 39
9.3.6 Market/advertize/promote ... 39
9.3.7 Share ... 40
9.3.8 Collect ... 41
9.3.9 Train (AI system) ... 41
9.4 Scopes: Boundaries of collection and use of data ... 41
9.4.1 Scope concepts ... 41
9.4.2 Scope types ... 41
9.4.3 Scope characteristics ... 43
9.4.4 Network connection between scopes ... 43
9.4.5 Control of source scope over result scope ... 44

10 Data use statements ... 44
10.1 Overview ... 44
10.2 Data use statement structure ... 45
10.2.1 Structure definition ... 45
10.2.2 Describing the scope of applications and cloud services that apply to use statements ... 47
10.2.3 Assumptions about when data are collected and used ... 47
10.2.4 Defining promotion targets ... 48
10.2.5 Data types ... 48
10.2.6 Data qualifiers for data types ... 49
10.2.7 Examples of statements about data flow in the devices and cloud services ecosystem ... 49
10.2.8 Exceptional use statements ... 50
10.2.9 Data sharing ... 53
10.3 Use of orthogonal data facets in data use statement ... 54
10.3.1 General ... 54
10.3.2 Use of elements in the data facets as attributes ... 54
10.3.3 Hierarchy of elements/attributes of data based on facets ... 55
10.3.4 Use of attributes to describe PII ... 55
10.3.5 Use of attributes to tag IP data ... 56
10.3.6 Use of attributes to tag IP data from shared pools, while respecting partner IP ... 57

11 Data lineage and data provenance ... 59
11.1 General ... 59
11.2 Tracing data lineage ... 59

12 Use of taxonomy and data use statement in other computing environments ... 60

13 Use of data taxonomy and use statements in Artificial Intelligence scenarios ... 60

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

Annex A (informative) **Diagrams of data categories and data identification qualifiers** **63**
Bibliography **64**

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

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.

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) or the IEC list of patent declarations received (see https://patents.iec.c).

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology,* Subcommittee SC 38, *Cloud Computing and Distributed Platforms.*

This first edition of ISO/IEC 19944-1, along with ISO/IEC 19944-2[1)] cancels and replaces ISO/IEC 19944:2017, which has been technically revised.

The main changes compared to the previous edition are as follows:

— provides additional material which principally deals with organizational data and the need to treat some organizational data in particular ways in order to ensure confidentiality, integrity and so on,

— the new concept of data facets is introduced and data facets are used to extend the expressiveness of data use statements, including adding the concept of which individuals or organizations have control over data,

— the new data use categories are introduced, including some that address the newer uses of data associated with artificial intelligence systems.

A list of all parts in the ISO/IEC 19944 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

1) Under preparation. Stage at the time of publication: ISO/IEC PWI 19944-2:2020.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

Introduction

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 are 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 may be used in several ways including, but not limited to:

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 organisations 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 organisation, 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 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 are used in an ecosystem of devices and cloud services.

This document also 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.

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 are 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.

This version of ISO/IEC 19944 contains additional material which principally deals with organizational data and the need to treat some organizational data in particular ways in order to ensure confidentiality, integrity and so on.

To assist with this, the new concept of data facets is introduced and data facets are used to extend the expressiveness of data use statements, including adding the concept of which individuals or organizations have control over data.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

New data use categories are introduced, including some that address the newer uses of data associated with artificial intelligence systems.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

Cloud computing and distributed platforms — Data flow, data categories and data use —

Part 1: Fundamentals

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 organisation involved in legal, policy, technical or other implications of data flows between devices and cloud services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 17789:2014, *Information technology — Cloud computing — Reference architecture*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788 and the following apply.

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

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

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

3.1 Terms related to data categories

3.1.1
account data
class of data specific to each CSC that is required to administer the *cloud service*

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 the CSC, such as name, address, telephone, etc.

3.1.2
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

3.2 Terms related to cloud services and devices ecosystem

3.2.1
device
physical entity that communicates directly or indirectly with one or more *cloud services*

3.2.2
application marketplace
set of *cloud services* providing a digital marketplace intended to offer applications and other digital content for a particular *device platform* (3.2.4) 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* (3.2.1) can use more than one application marketplace.

3.2.3
application cloud service
cloud service that supports applications running on a given *device* (3.2.1), where the cloud service is provided by a party other than the *device platform provider* (3.2.5)

3.2.4
device platform
operating system and related feature set that provides the core capabilities for a *device* (3.2.1)

Note 1 to entry: An *application marketplace* (3.2.2) is specific to a device platform.

3.2.5
device platform provider
device platform cloud service provider
cloud service provider that provides *cloud services* necessary to support a *device platform* (3.2.4) including managing needed digital identities

Note 1 to entry: The cloud service provider that offers the *application marketplace* (3.2.2) is typically the same as the device platform provider, but it is not required to be.

3.2.6
device platform cloud service
cloud service offered by the *device platform provider* (3.2.5) to support the *device platform* (3.2.4)

Note 1 to entry: An *application marketplace* (3.2.2) can be an example of device platform cloud service.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

3.3 Terms related to privacy

3.3.1
personally identifiable information
PII
personal data
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the PII principal (3.3.3). 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 establish the link between the set of PII and the natural person.

Note 2 to entry: This definition is included to define the term PII as used in this document. A public cloud PII processor (3.3.2) is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.

[SOURCE: ISO/IEC 29100:2011/Amd1:2018, 2.9]

3.3.2
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (PII) (3.3.1) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others, e.g. *PII processors* (3.3.4) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

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

3.3.3
PII principal
natural person to whom the *personally identifiable information* (PII) (3.3.1) 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]

3.3.4
PII processor
privacy stakeholder that processes *personally identifiable information* (PII) (3.3.1) on behalf of and in accordance with the instructions of a *PII controller* (3.3.2)

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

3.4 Terms related to organizational data

3.4.1
individual data
class of data objects under the control, by legal or other reasons, of a natural person

Note 1 to entry: Individual data can be a mixed dataset (3.4.6).

Note 2 to entry: Customer content data is individual data when the CSC is a natural person.

3.4.2
organizational data
class of data objects under the control, by legal, contractual or other reasons, of an organization

Note 1 to entry: An organization can be a for-profit company, a non-profit organization, a public or government agency, a non-governmental organization or an international organization, and can be small, medium or large.

© ISO/IEC 2020 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

Note 2 to entry: Customer content organizational data when the CSC is an organization and thus not a natural person.

Note 3 to entry: Cloud service provider data (ISO/IEC 17788) is always organizational data by nature.

Note 4 to entry: Organizational data can be a *mixed dataset* (3.4.6).

3.4.3
organizational protected data
OPD
organizational data whose protection is required based on the policies established by governance of data process

Note 1 to entry: Organizations have policies that govern the data under their control. ISO/IEC 38505-1 identifies and examines higher level governance concerns regarding the use of data which is relevant from the perspective of governance of data.

Note 2 to entry: Organizational data can contain OPD and PII.

3.4.4
public domain data
class of data objects over which nobody holds or can hold copyright or other intellectual property

Note 1 to entry: Data can be in the public domain in some jurisdictions, while not in others.

Note 2 to entry: The concept of public domain and the difference between this and "publicly available" is subtle and varies between jurisdictions. Readers should make themselves aware of the specific legal situation as it may apply to them.

3.4.5
non-personal data
class of data objects that does not contain *PII* (3.3.1)

Note 1 to entry: data objects that were originally PII and were later made anonymous are non-personal data.

3.4.6
mixed dataset
set of data objects that contain both *PII* (3.3.1) and *non-personal data* (3.4.5)

3.4.7
data principal
entity to which data relates

Note 1 to entry: The term “data principal” is broader than “PII principal” (or “data subject” as used elsewhere) and is able to denote any entity such as a person, an organization, a device, or a software application.

[SOURCE: ISO/IEC 20889:2018, 3.4]

3.5 Terms related to artificial intelligence

3.5.1
artificial intelligence
<system> capability of an engineered system to acquire, process and apply knowledge and skills

Note 1 to entry: knowledge are facts, information, and skills acquired through experience or education.

[SOURCE: ISO/IEC CD 22989[2)]]

2) Under preparation. Stage at the time of publication: ISO/IEC CD 22989:2020.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

3.5.2
artificial intelligence
<engineering discipline>discipline which studies the engineering of systems with the capability to acquire, process and apply knowledge and skills

Note 1 to entry: knowledge are facts, information, and skills acquired through experience or education.

[SOURCE: ISO/IEC CD 22989]

3.5.3
artificial intelligence system
AI system
system using AI

[SOURCE: ISO/IEC CD 22989]

3.5.4
machine learning
ML
process using computational techniques to enable systems to learn from data or experience

[SOURCE: ISO/IEC CD 23053[3)]]

3.5.5
machine learning model
mathematical construct that generates an inference, or prediction, based on input data

Note 1 to entry: for supervised learning, a machine learning model results from the training or a machine learning algorithm

Note 2 to entry: for example, if a univariate linear function (y = w0 + w1(x)) has been trained using linear regression, the resulting model could be y = 3 + 7(x).

[SOURCE: ISO/IEC CD 23053]

3.5.6
model training
<machine learning> task of determining optimal model parameters from a given dataset

[SOURCE: ISO/IEC CD 23053]

3.5.7
trained model
result of model training

[SOURCE: ISO/IEC CD 23053]

3.5.8
training data
samples used to fit a machine learning model

[SOURCE: ISO/IEC CD 23053]

3) Under preparation. Stage at the time of publication: ISO/IEC CD 23053:2020.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

3.6 General terms

3.6.1
lifecycle
evolution of a system, product, service, project or other human-made entity, from conception through retirement

[SOURCE: ISO/IEC 29110-4-3:2018, 3.15]

3.6.2
transparency
open, comprehensive and understandable presentation of information

[SOURCE: ISO 21931-2:2019, 3.33]

4 Abbreviated terms

AI	Artificial Intelligence
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
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
ML	Machine Learning
OPD	Organizational Protected Data
PII	Personally Identifiable Information
SLA	Service Level Agreement
USB	Universal Serial Bus

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

5 Structure of this document

5.1 Document organization

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).

5.2 Overview and reference architecture

Overview and reference architecture are covered as follows.

— 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 to include devices and the flow of data between devices and cloud services.

5.3 Data taxonomies, data categories and data use statement structure

Data taxonomies, data categories and data use statement structure (applicable to data exchanges between devices and cloud services) are covered as follows.

— 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 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 are 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 customers and cloud service providers. This interaction also makes the discussion of data classification and access and use become 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.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

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** which can include application marketplaces. 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** 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.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

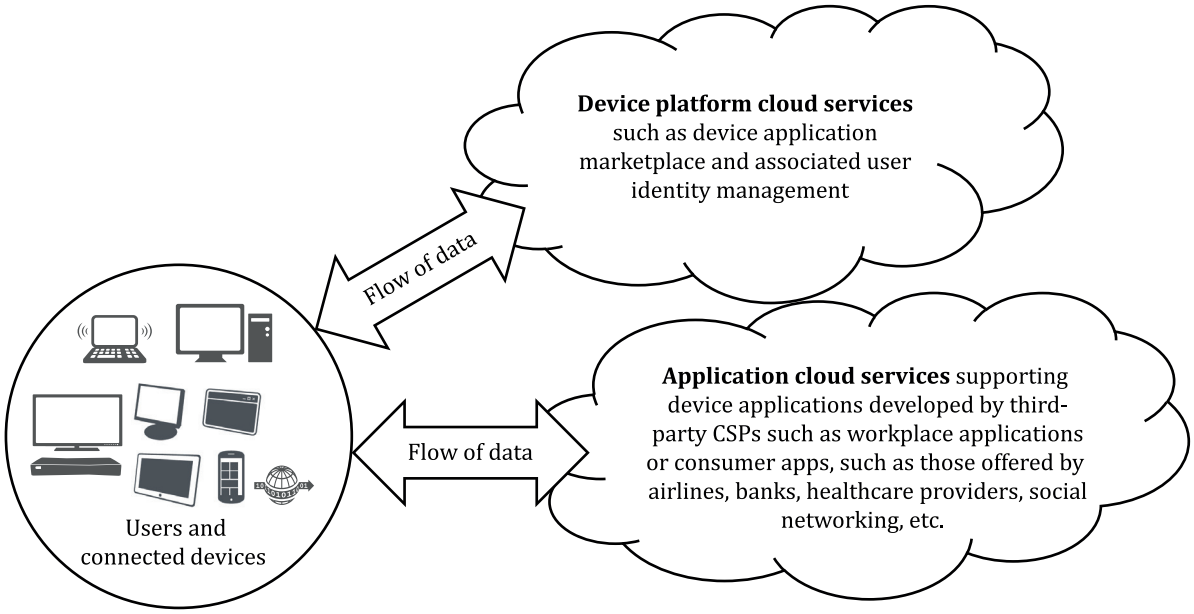

Figure 1 — Devices and cloud services ecosystem

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 are 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 are 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 in Figure 2. Examples include 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, or 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 may take the sub-role of anonymous user, where the user wants the right to use the application and cloud services in a private manner and 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

© ISO/IEC 2020 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

meaningful conversation between the cloud service customers, the cloud service providers, regulators and other stakeholders about this data.

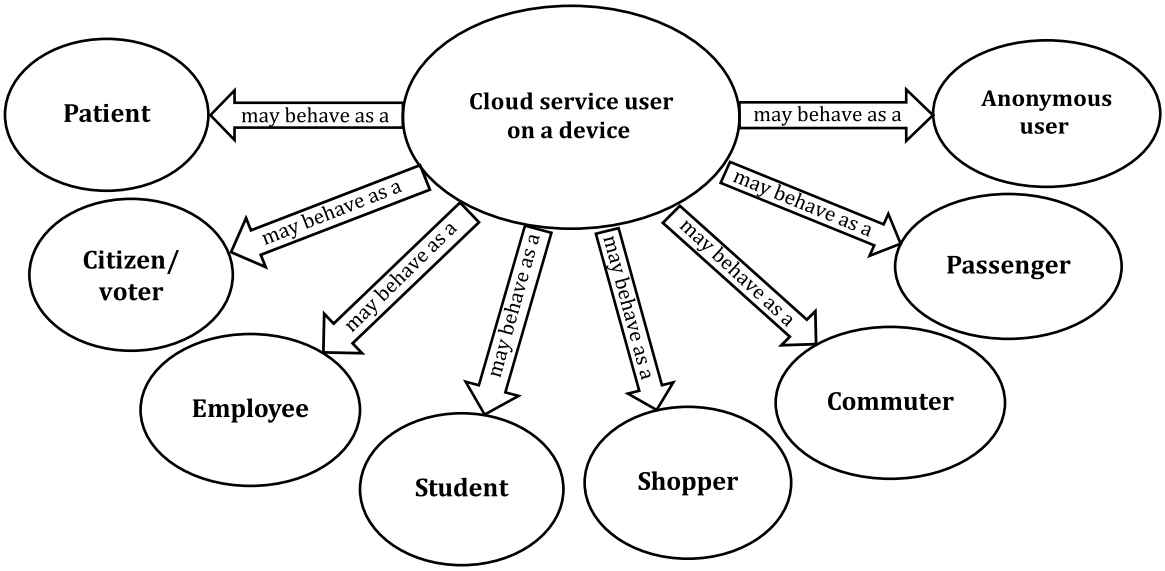

Figure 2 — Example of roles a user can assume in device use scenarios

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

— Patient: patients are subject to 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: employees should follow the organization's policies to protect the organization's confidential assets.

— Student: many students are under legal age and are therefore subject to stricter privacy and commercial advertisement laws.

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

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

— Passenger: passengers are located in public transportation hubs, like airports. Certain rules may therefore 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

"Bring your own device" (BYOD) is defined as the practice of allowing employees of an organisation 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 organisations to provide the devices that employees used mainly or even exclusively for work purposes, and those devices were connected to the organization's networks

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

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. 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, as a personal device may be shared with others.

— Vulnerability of organization data which is downloaded and stored on the device, as 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.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

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.

Organizational use applications and cloud services by contrast very likely separate out the interfaces for the different roles for a cloud service customer, since it is highly likely that the end user is not the same person as the cloud service administrator, for example.

7.3 Device impact on the CCRA: User view

7.3.1 Cloud service provider

7.3.1.1 Sub-roles

7.3.1.1.1 General

The cloud service provider role is defined in ISO/IEC 17789:2014, 8.3.1. A cloud service provider can make cloud services which are usable with any device. However, devices usually have a special relationship with one particular cloud service provider, the device platform provider; therefore, there is the need to define a new sub-role to accommodate this.

7.3.1.1.2 CSP:device platform provider

The CSP:device platform provider is a sub-role of cloud service provider that provides the set of cloud services necessary to support the device platform. The party that offers the cloud services for the application marketplace is typically the same as the party that plays the CSP:device platform provider sub-role, but this is not necessarily the case.

The CSP:device platform provider typically offers the cloud services necessary to provide identity management for the user of the device. This is usually done in conjunction with the application marketplace.

The device platform provider's cloud computing activities include:

— providing data and applications;

— sharing data with third parties;

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020

— processing and using data;

— providing application marketplace;

— providing device platform cloud services;

— providing data related services.

7.3.1.2 Cloud computing activities

In addition to the cloud computing activities specified in ISO/IEC 17789:2014, 8.3.2, the following activities apply to the sub-roles of CSP.

— Providing data and applications: makes provider data and applications available to cloud service customers under a cloud service agreement.

— Sharing data: makes customer content data and derived data available to third party organizations under an agreement, for business purposes of the cloud service provider.

— Processing and using data: processes customer content data and derived data for certain purposes, for instance advertising, business intelligence, security and privacy, under terms stated in the cloud service agreement.

— Providing application marketplace: provide and maintain the application marketplace. This includes the applications which run on devices and the set of cloud services which support the application.

— Providing device platform cloud services: provide the set of cloud services necessary to support a device platform.

— Providing data related services: involves the providing of data related services to cloud service customers and cloud service users such as online advertisements or business intelligence.

7.3.2 Cloud service customer

7.3.2.1 Sub-roles

7.3.2.1.1 General

ISO/IEC 17789:2014, 8.2.1 and 8.2.1.1 specify the role of cloud service customer and its sub-role CSC: cloud service user. Both apply to this document.

According to ISO/IEC 17788 and ISO/IEC 17789, the cloud service customer is a party in a business relationship for the purpose of using cloud services, whereas the cloud service user, as the actual person using a particular device, is a sub-role of cloud service customer which uses the cloud services. In organization scenarios, the cloud service customer is the organization and the cloud service users are the individual employees of the organization.

There are other cases where the cloud service users may not be employed by the organization but have another type of relationship with the cloud service customer, for example, the cloud service users may be customers of the cloud service customer organization.

In other cases, one person may be the customer of a cloud service but the cloud service users are a number of people who have a non-business relationship with the customer (such as a home movie streaming service).

There are consumer scenarios where the cloud service customer is the same person as the cloud service user and, in this case, devices, applications and services are all linked to the device users through their customer accounts.

The term “CSC:cloud service user” is synonymous with “device user” used elsewhere in this document

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19944-1:2020