DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 19944-1

ISO/IEC JTC **1**/SC **38**

Secretariat: **ANSI**

Voting begins on:
2019-12-04

Voting terminates on:
2020-02-26

Cloud computing – Cloud services and devices: data flow, data categories and data use —

Part 1:
Fundamentals

ICS: 35.210

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 19944-1:2019(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

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.

This revision 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.

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

Cloud computing – Cloud services and devices: 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 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
personal data
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

3.21
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 (3.26).

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

3.22
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.

Note 2 to entry: Customer content data is 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 (3.26).

3.23
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[7] 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.

3.24
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 both subtle and varies between jurisdictions. Readers should make themselves aware of the specific legal situation as it may apply to them.

3.25
non-personal data
class of data objects that does not contain PII (3.16)

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

3.26
mixed dataset
set of data objects that contain both PII (3.16) and non-personal data (3.25)

3.27
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]

3.28
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 WD 22989]

3.29
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 WD 22989]

[Editor’s NOTE] Need to check whether need to have two definitions for AI or select one which proper in this document.

3.30
artificial intelligence system
AI system
Technical system that uses artificial intelligence to solve problems

[SOURCE: ISO/IEC WD 22989]