



DPC: 25/30480423 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 25 November 2025

Origin: International

Latest date for receipt of comments: 18 January 2026

Project No. 2023/02215

Responsible committee: IST/38 Cloud Computing and Distributed Platforms

Interested committees:

Title: Draft BS ISO/IEC 19941 Cloud computing. Part 1: Interoperability and portability.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 18 January 2026

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 19941-1

Cloud computing — Part 1: Interoperability and portability

ICS: 01.040.35; 35.210

ISO/IEC JTC 1/SC 38

Secretariat: **ANSI**

Voting begins on:
2025-11-25

Voting terminates on:
2026-02-17

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 19941-1:2025(en)

Full document details: 25/30480423 DC



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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

Contents	Page
Foreword	4
Introduction	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Abbreviated terms	9
5 Overview of cloud computing interoperability and portability	11
5.1 Description of cloud computing interoperability and portability	11
5.1.1 General.....	11
5.1.2 Considerations for cloud interoperability.....	11
5.1.3 Considerations for cloud service portability.....	13
5.1.4 Relationship between cloud interoperability and cloud portability.....	16
5.1.5 Costs associated with cloud portability	16
5.2 Cloud interoperability and portability facet models.....	17
5.2.1 Cloud interoperability facet model	17
5.2.2 Cloud data portability facet model.....	21
5.2.3 Cloud application portability facet model.....	24
5.3 Key challenges related to interoperability and portability in cloud computing.....	26
5.3.1 General.....	26
5.3.2 Security.....	27
5.3.3 Identity and Access Management	28
5.3.4 Security during migration.....	30
5.3.5 Dynamic migration	30
5.3.6 Interfaces, APIs and interoperability	30
5.3.7 Open source	31
5.3.8 Intermediary services.....	31
6 Interoperability and portability considerations related to cloud capabilities types	32
6.1 General	32
6.2 Functional components of interoperability	37
6.3 Functional components of data portability.....	38
6.4 Functional components of application portability.....	38
6.4.1 General.....	38
6.4.2 Functional views based on capabilities types.....	41
7 Cloud interoperability	46
7.1 Cloud interoperability types	46
7.1.1 General.....	46
7.1.2 Transport interoperability	49
7.1.3 Syntactic interoperability	49
7.1.4 Semantic data interoperability	49
7.1.5 Behavioural interoperability	50
7.1.6 Policy interoperability.....	51

7.1.7	Interoperability with connected devices consuming cloud services of application capabilities type.....	51
8	Cloud data portability.....	52
8.1	Cloud data portability types.....	52
8.2	Data syntactic portability.....	53
8.2.1	General.....	53
8.2.2	Data syntactic portability for infrastructure capabilities type cloud services.....	53
8.2.3	Data syntactic portability for platform capabilities type cloud services....	54
8.2.4	Data syntactic portability for application capabilities type cloud services	54
8.3	Data semantic portability.....	55
8.3.1	General.....	55
8.3.2	Data semantic portability for infrastructure capabilities type cloud services.....	55
8.3.3	Semantic data portability for platform capabilities type cloud services....	55
8.3.4	Data semantic portability for application capabilities type cloud services	56
8.4	Data policy portability.....	57
8.5	Considerations for cloud data portability of “cloud service derived data”.....	58
9	Cloud application portability.....	60
9.1	Cloud application portability types.....	60
9.2	Considerations for cloud application portability.....	60
9.3	Application portability for infrastructure capabilities type cloud services.....	64
9.3.1	Application portability from non-cloud to cloud service.....	64
9.3.2	Application portability from a cloud service to another cloud service.....	66
9.4	Application portability for platform capabilities type cloud services.....	67
9.4.1	Application portability from non-cloud to cloud service deployments.....	67
9.4.2	Application portability from one cloud service to another cloud service.	71
9.5	Application portability for application capabilities type cloud service.....	72
9.6	Application portability: Policy facet.....	72
9.6.1	General.....	72
9.6.2	Law and regulations.....	73
9.6.3	Contracts and licenses.....	73
9.6.4	Organizational policies.....	74
10	Cloud service switching.....	74
10.1	General.....	74
10.2	Benefits.....	75
10.2.1	Benefits for CSPs.....	75
10.2.2	Benefits for CSCs.....	76
10.2.3	Benefits for the cloud computing ecosystem.....	76
10.3.1	General.....	77
10.3.2	General considerations.....	77
10.3.3	Understanding their options.....	78
10.3.4	Understanding the timescale of the process.....	79
10.3.5	Identifying their existing CSC digital assets.....	80
10.3.6	Available skills at the CSC.....	81
10.3.7	Extraction of CSC digital assets.....	82
10.3.8	Identity and access management (IAM).....	83
10.3.9	Legacy architectures.....	84
10.3.10	Workload architecture and design.....	84
10.3.11	Unexpected feature mismatch.....	86

10.3.12	Data Portability and Management.....	87
10.3.13	Changing CSC priorities	87
10.3.14	Customisation by the CSC.....	87
10.3.15	Multinational aspects	88
10.3.16	Security and Compliance Frameworks.....	88
10.3.17	Network Configuration and Connectivity	88
10.3.18	3rd-party aspects.....	89
10.3.19	Automation and Orchestration	90
10.3.20	Monitoring and Observability	90
10.3.21	Contractual and Legal Considerations.....	90
10.3.22	Testing and Validation.....	91
10.4	CSC's digital assets when switching	91
10.4.1	CSC digital assets and cloud computing data.....	91
11	Interoperability considerations when using cloud services from multiple CSPs	94
11.1	General.....	94
11.2	Transport interoperability	94
11.3	Syntactic and semantic interoperability.....	94
11.4	Behaviour interoperability.....	95
11.5	Policy interoperability.....	95
12	Portability considerations when using cloud services from multiple CSPs or between an on-prem data centre and a CSP	95
12.1	General.....	95
12.2	Syntactic data portability	95
12.3	Semantic data portability.....	95
12.4	Policy portability	95
13	Cloud SLA aspects for interoperability and portability	95
13.1	General.....	95
13.2	Cloud SLOs, SQOs and components for interoperability and portability.....	95
14	Data categories for interoperability and portability	96
14.1	General.....	96
Annex A (Informative) – Relationship between cloud interoperability, portability and switching.....		97
Annex B (Informative) – How Cloud Interoperability, Portability, and Switching Support Each Other		98
Bibliography		99

1 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 ISO documents 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 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*.

16 Introduction

17 This document is intended to establish a common understanding of cloud computing interoperability and
18 portability. In particular, it is of interest to cloud stakeholders focusing on cloud service agreements
19 concerning interoperability or portability between cloud services.

20 Cloud computing is defined as a paradigm for enabling network access to a scalable and elastic pool of
21 shareable physical or virtual resources with self-service provisioning and administration on-demand.
22 ISO/IEC 22123-1, ISO/IEC 22123-2 [8] and ISO/IEC 22123-3 [9] provide a starting point for the
23 understanding of different types of interoperability and portability, relationships with activities and roles
24 and cloud capabilities types. Interoperability, data portability and application portability are essential to
25 the use of cloud services. The goal of interoperability is to enable the interaction between non-cloud and
26 cloud services, as well as between cloud services, in addition to enabling composition of new services
27 from multiple services. The goal of portability is to enable cloud service customers (CSCs) to move their
28 data or applications between non-cloud and one or more cloud services and between cloud services. The
29 benefits of interoperability include lower costs of integration and increasing the value of services through
30 enrichment or new functionality provided by composing cloud services. The benefits of portability
31 include greater efficiency by lowering the costs of migration. Both interoperability and portability offer
32 more choices to CSCs by limiting the effects of being locked into any cloud service or cloud service
33 provider (CSP). While there is no disagreement that interoperability and portability are advantages to
34 cloud computing, there is no single way of handling either capability.

35 In a greenfield project, incorporating interoperability and portability as part of business and technical
36 requirements, can be taken as a part of planning process and all design decisions and development
37 environment including application design and development are best implemented in a vendor-neutral
38 way. This way, portability and interoperability become easy across CSPs or with on premise systems. If,
39 on the other hand, switching, porting or interoperability is desired during the operation and maintenance
40 phase, the CSC ordinarily needs the assistance of an incumbent CSP for migration, tools thereof and use
41 of open interfaces and APIs at the interface, immaterial of the internal interfaces used. Additionally, CSCs
42 can use third party tools and services.

43 Interoperability is the ability of two or more systems or applications to exchange information and to
44 mutually use the information that has been exchanged. In the context of cloud computing, interoperability
45 can be viewed as the capability of public cloud services, private cloud services and other CSC systems to
46 understand each other's interfaces, configuration, forms of authentication and authorization, etc. in order
47 to cooperate and work with each other.

48 Regulators and policy makers are interested in the interoperability of cloud computing. Notably the EU
49 Data Act aims to achieve interoperability between cloud services that cover the same service type and in
50 terms of the ability to exchange data in order to perform their function.

51 Interoperability is a complex subject in the context of cloud computing because of the number of
52 interactions involved and the potential variations for each interaction. While interoperability and
53 standards add significant value and are advantageous to cloud computing, there are no comprehensive
54 solutions. Many existing IT standards contribute to enabling interoperability between CSC applications
55 and cloud services and between cloud services themselves. These standards can be de facto standards,
56 which are specifications so widely adopted in the industry that they effectively become standards, or de
57 jure standards, which are specifications for new or emerging technologies that have been formally
58 established to facilitate interoperability. Using standards can be one way to build interoperable cloud
59 services. In addition, well-documented API specifications are crucial for minimizing the costs associated
60 with developing interoperable applications.

61 Cloud computing services that enable portability using defined policies, standards or documented
62 formats can ensure that CSCs are able to get their data into or out of cloud services in a reasonably easy
63 and cost-effective manner, as this allows CSCs to move to a cloud service of another CSP and also to drive
64 integration of heterogeneous cloud services.

As presented in ISO/IEC 22123-1, portability is the ability of a CSC to move their data or their applications between two different cloud services at a low cost and with minimal disruption. Portability is significant in cloud computing since CSCs are interested in avoiding lock-in when they choose to use cloud services. Therefore, in the context of cloud computing, portability can have multiple aspects depending on what is being ported, and which cloud services are involved. For portability, there are no specific requirements for the source and target systems to be directly connected.

Portability in a cloud computing environment is not a binary concept. It would be a mistake to think of cloud services and the associated cloud applications and data as being either 100% portable or not portable at all. Almost all applications running in a cloud service can be ported to another cloud service offering equivalent capabilities, if the necessary resources are invested. The critical considerations for portability discussions are the porting cost, the risks associated with the porting and how to control the costs and risks compared to the expected benefits.

78 Cloud computing – Part 1: Interoperability and Portability

79 1 Scope

80 This document specifies cloud computing interoperability and portability types, the relationship and
81 interactions between these two cross-cutting aspects of cloud computing and distributed platforms, as
82 well as common terminology and concepts used to discuss interoperability and portability, particularly
83 relating to cloud services.

84 This document is related to other standards, including, ISO/IEC 22123 series, ISO/IEC 19086-1, ISO/IEC
85 19944-1, ISO/IEC 5140 and in particular, references the cross-cutting aspects and components identified
86 in ISO/IEC 22123-1 and ISO/IEC 22123-3 respectively.

87 The goal of this document is to ensure that all parties involved in cloud computing, particularly CSCs,
88 CSPs and CSNs acting as cloud service developers, have a common understanding of interoperability and
89 portability for their specific needs – including switching service provision from one CSP to another. This
90 common understanding helps to achieve interoperability and portability in cloud computing by
91 establishing common terminology and concepts.

92 2 Normative references

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

96 ISO/IEC 22123-1, *I Cloud computing – Part 1: Vocabulary*

97 3 Terms and definitions

98 For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1 and the
99 following apply.

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

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

102 — IEC Electropedia: available at <https://www.electropedia.org/>

103 3.1

104 cloud service switching

105 process whereby a CSC changes the provisioning of a cloud service from the current cloud service
106 provider to another cloud service provider

107
108 Note 1 to entry: To move the provisioning of a cloud service to an on-premises service, the other CSP can
109 be the same party as the CSC.

111 3.2

112 CSC-provided code

113 software code artefacts created by CSDs acting on the CSC's behalf, that are designed to execute within a
114 cloud service to meet the needs of the CSC

115 Note 1 to entry: Such code artefacts can be supplemented by data or metadata.

116 Note 2 to entry: The CSDs creating the code can be employees or contractors of the CSC, or of another
117 organization such as a vendor, partner, or contractor to the CSC.

118 [Source: ISO/IEC TS 7339:2024(en), 3.2]

119 **3.3**
120 **Metadata**
121 data that defines and describes other data

122 Note 1 to entry: Metadata can include many different kinds of attributes of the data it describes. Some
123 metadata fields are almost universal, such as date of creation and last change, type of file or object,
124 permissions, and ownership. Other metadata can be specific to the type of object, such as the camera
125 settings of a digital image, the author's name for a document, the version of a code artefact, etc.

126 Note 2 to entry: Some metadata can be directly attached to (or embedded within) the data to which it
127 relates and will always move with it. Other metadata can be stored separately and associated with the
128 data by reference or other means.

129 [SOURCE: ISO/IEC TS 7339:2024(en), 3.3]

130 **3.4**
131 **CSC digital asset**

132
133 class of data objects that includes CSC data and a subset of cloud service derived data essential for the
134 effective use of the cloud service

135 Note 1 to entry: Examples of cloud service derived data that are part of CSC digital asset are configuration
136 settings, security, and access and control rights management. Such cloud service derived data is
137 sometimes referred to as CSC metadata (3.3).

138 Note 2 to entry: Examples of cloud service derived data that are not part of CSC digital asset are those
139 covered by the intellectual property rights of others, or that constitute a trade secret of another party, or
140 that can compromise the security and integrity of the cloud service.

141 Note 3 to entry: CSPs and CSNs also have their own digital assets, (not defined in this document).

142 Note 4 to entry: CSC digital assets are in digital form, limited to that for which the CSC has control and is
143 independent from its contractual relationship with the CSP.

144
145 **3.5**
146 **<cloud computing> jurisdiction**
147 geographical or corporate area over which a cloud computing policy extends

148 Note 1 to entry: In a government policy context this will generally be the geographical area over which
149 the body enacting the policy has legal authority either as government or as authorised regulator. However,
150 in an enterprise or government agency environment, the jurisdiction of a policy can cover a business
151 function, department, agency, or other organisational area of responsibility not tied to geography.

152 [Source: ISO/IEC TR 22678:2019 3.2]

153 **3.6**
154 **Observed derived data**

155 subset of cloud service derived data consisting of records of interactions that the CSC has had with a cloud
156 service

157 Note 1 to entry: Examples of observed derived data are service configurations, access logs, call logs,
158 change records, and audit records.

159 3.7

160 **Inferred derived data**

161 subset of cloud service derived data created by the CSP through analysis of the cloud service and its usage

162 Note 1 to entry: Inferred derived data is often a subjective and approximate estimate rather than an
163 objectively calculated derivative.

164 Note 2 to entry: Inferred derived data is often (though not exclusively) used to estimate CSC attributes,
165 interests, and potential behaviours.

166 Note 3 to entry: Examples of using inferred derived data include product recommendations.

167

168

169 4 Abbreviated terms

ACL	Access Control List
AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
BPEL	Business Process Execution Language
BPML	Business Process Management Language
CD	Continuous Deployment
CI	Continuous Integration
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSC	Cloud Service Customer
CSD	Cloud Service Developer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
CSV	Comma-separated Values
DSP	Data Space Protocol
EC	European Commission
ERP	Enterprise Resource Planning

ESB	Enterprise Service Bus
EU	European Union
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation (EU)
GPU	Graphics Processing UNit
HCM	Human Capital Management
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICT	Information & Communication Technology
IDAM	Identity and Access Management
IDaaS	Identity as a Service
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
LCIM	Levels of Conceptual Interoperability Model
MIME	Multipurpose Internet Mail Extensions
MQTT	Message Queuing Telemetry Transport
OVF	Open Virtualization Format
OWL	Web Ontology Language
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry – Data Security Standard
PII	Personally identifiable information
RDF	Resource Description Framework
REST	Representational State Transfer
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SLA	Service Level Agreement
SLO	Service Level Objective
SOAP	Simple Object Access Protocol
SPARQL	SPARQL Protocol and RDF Query Language

SQO	Service Qualitative Objective
SSO	Single Sign-On
TAR	Tape Archive
TCK	Technology Compatibility Kit
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UML	Unified Modeling Language
VM	Virtual Machine
VPN	Virtual Private Network
XML	eXtensible Markup Language
YAML	Yet Another Mark-Up Language

5 Overview of cloud computing interoperability and portability

5.1 Description of cloud computing interoperability and portability

5.1.1 General

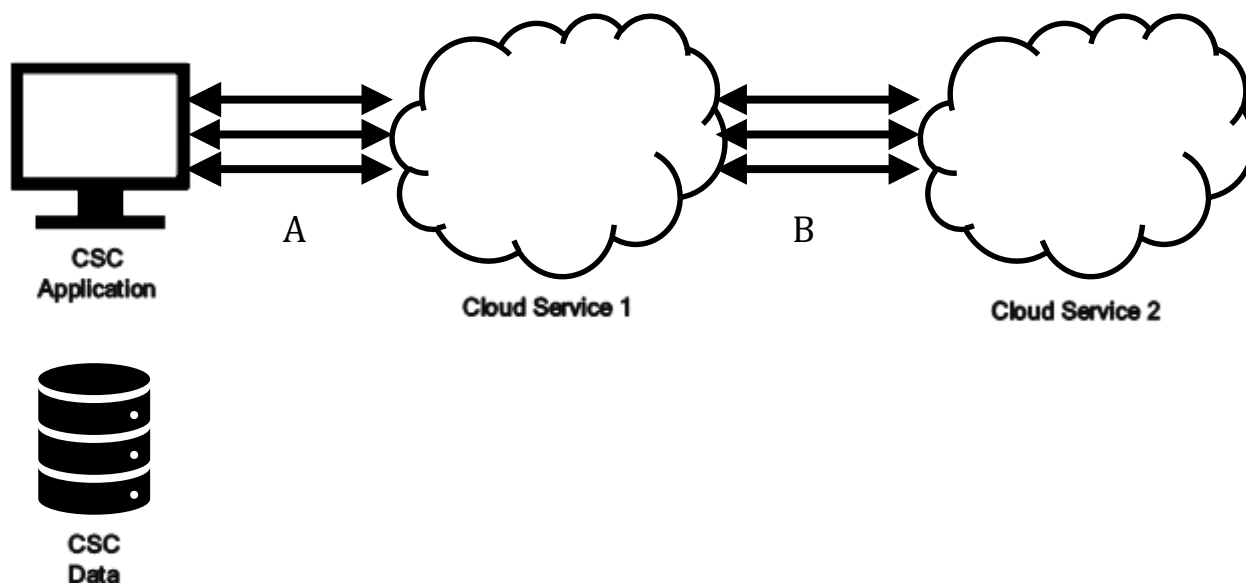
This clause provides an overview and models (known as “facet models”; refer to 5.2.1, 5.2.2 and 5.2.3 for details) for cloud interoperability, cloud data portability and cloud application portability. There are various perspectives of interoperability and portability that need to be considered. These perspectives are called “facets”.

Interoperability and portability in cloud computing involve interactions affected by technological, information and human aspects. NOTE portability in this document includes both data portability and application portability. Interoperability and portability related challenges are likely to intensify and become more difficult to manage as systems grow more complex and interconnected. In cloud computing environments with internationally interconnected systems, the complexities also include matters of corporate policy, regulation and laws of applicable jurisdictions (3.5).

For information on cloud service switching (3.1), see clause 10.

5.1.2 Considerations for cloud interoperability

ISO/IEC 22123-1 defines interoperability as “the ability for two or more systems or applications to exchange information and mutually use the information that has been exchanged”. In the context of cloud computing, interoperability is further described as a cross-cutting aspect providing the ability for a CSC’s on-premises system to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results (see ISO/IEC 22123-2: 2023, 7.5 [8]). Interoperability also includes the ability for one cloud service to interact with other cloud services (see ISO/IEC 22123-3: 2023, 8.3.4 [9]). Figure 1 illustrates that cloud interoperability takes place both between a CSC’s application and cloud services (A) and also between cloud services (B). There are typically multiple interactions involved in both of these cases, as indicated by the multiple arrows. The interactions can be for different services or for multiple instances of the same cloud service. In Figure 1 the arrows indicate that the information to be exchanged is bi-directional, with either end able to initiate the interaction



Key
A application to/from cloud service
B cloud service to/from cloud service

Figure 1 — High-level view of cloud interoperability

NOTE 1 Figure 1 illustrates basic interaction styles only. Other configurations, such as using Cloud 1 as a relay or intermediary for indirect interactions between the CSC application and Cloud 2, are possible.

NOTE 2 Interoperability in cloud computing has multi-faceted requirements that demand consideration, such as clearly defined IT capabilities and interoperability requirements, realistic expectations, flexibility in approach, commitment of necessary resources, informed decision making, a long-term perspective, and active participation to determine and implement effective solutions.

In its simplest form, cloud interoperability means the useful exchange of information between a system and a cloud service so that the systems work together to provide the targeted IT capability.

However, as described further in this document, the degree and usefulness of interoperability between the systems will be determined by many factors including what information needs to be sent to the other system, how that information is interpreted and used by the other system – and ultimately – whether the other system’s actions reflect the needs and expectations of the CSC. These are more than simple syntax or even technology factors - since interoperability also requires validation that all facets, including behavioural and policy facets, are respectively interoperable.

Therefore, the CSC should understand the degree of interoperability between systems that is required to meet their needs – and the costs of all facets of achieving such interoperability. The degree of interoperability with existing and future systems is likely to be an important consideration when choosing cloud services. CSPs should align to appropriate standards for interoperability and provide the relevant information about their offered cloud services to assist in these choices.

There are many considerations when addressing cloud interoperability. These include:

- the ability of a CSC to interact with a cloud service by exchanging information according to a prescribed method obtaining predictable results;

- 221 — the ability for a cloud service to work with other cloud services, within the same CSP, or other CSPs,
222 or on-premises systems;
- 223 — properties needed to facilitate successful interactions between an organization's ICT facilities and a
224 cloud service;
- 225 — roles and activities as defined in ISO/IEC 22123-3 [9];
- 226 — cloud capabilities types as defined in ISO/IEC 22123-1 and described in ISO/IEC 22123-2 [8];
- 227 — interfaces between different functional components as defined in ISO/IEC 22123-3, 9.2 [9].

228 By taking these considerations into account, this document promotes better understanding of
229 interoperable cloud services.

230 **5.1.3 Considerations for cloud service portability**

231 **5.1.3.1 General**

232 This document distinguishes between cloud application portability and cloud data portability. In the
233 context of cloud computing, portability refers to the ability of a CSC to move and suitably adapt their
234 applications and data between the CSC's on-premises systems and cloud services, between different
235 cloud deployment models, and between cloud services of different CSPs.

236 When the CSC has moved the applications or data, they can be deleted from the source CSP's cloud system.

237 Portability is multifaceted. It involves a nuanced evaluation of potential costs and benefits associated with
238 migration. While initial considerations such as switching costs are pertinent, it is important to approach
239 these deliberations pragmatically. Assessing the alignment between CSC and CSP extends beyond mere
240 cost reduction; it aims for operational optimization. Transitions can necessitate effort and can entail
241 some level of risk. However, by adopting a strategic outlook and recognizing opportunities for growth,
242 organizations can effectively navigate these transitions. Ultimately, informed decision-making that
243 prioritizes long-term viability and success is key.

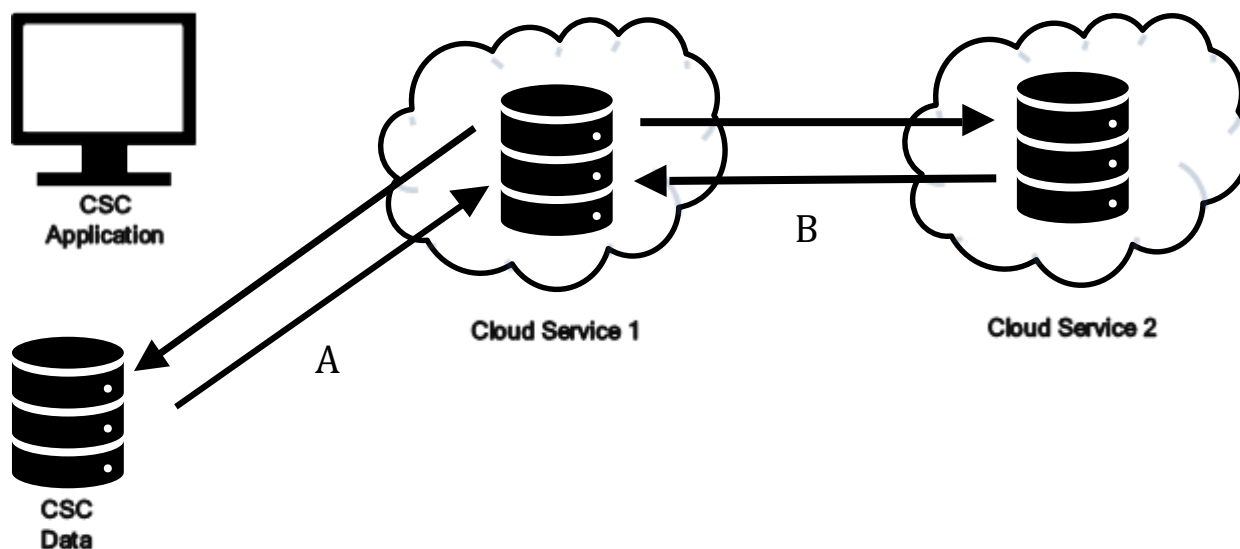
244 There are many considerations when addressing portability in cloud computing. These include:

- 245 — allowing CSCs to migrate applications and data in response to business needs such as faster service,
246 lower cost, greater reliability or disaster recovery needs;
- 247 — wider availability of application and data allowing access to a broader market;
- 248 — time and effort required for porting both applications and data, however, such overhead can be
249 reduced using common programming languages, standards, tools, frameworks, models, run times
250 and APIs;
- 251 — limiting of lock-in situations where the CSC is tied to the cloud services of one CSP.

252 Portability is an aspect of the more general topic of migration. Other issues related to migration are not
253 considered further in this document.

254 **5.1.3.2 Cloud data portability**

255 Cloud data portability is the ability to transfer data from one cloud service to another cloud service or
256 between a CSC's on-premises system and a cloud service. Note: A CSC's on-premises system can be hosted
257 by another organization (e.g. hosted physical machines, dedicated private cloud service). Figure 2
258 illustrates the porting of data between a CSC's on-premises system and a cloud service and porting of data
259 from one cloud service to another. The arrows in both directions indicate the potential to port data to and
260 from any of those places.



Key

- A CSC system to/from cloud service
- B cloud service to/from cloud service

Figure 2 — High-level view of cloud data portability

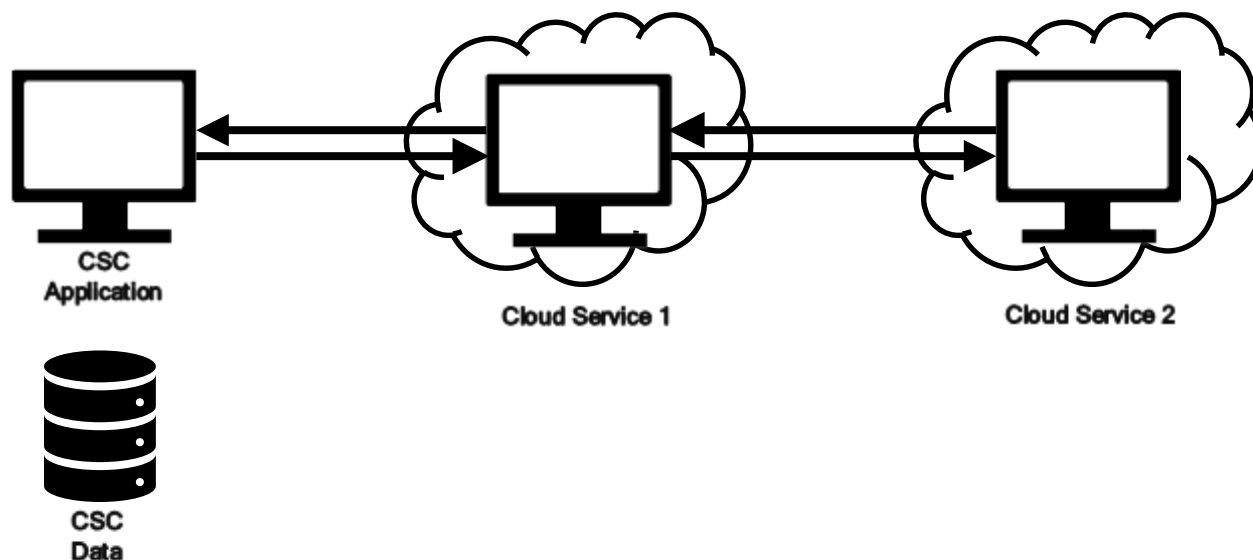
Considerations relating to cloud data portability include:

- **Retrieval of CSC data:** capability to retrieve CSC data from the source cloud service is needed and a capability to import CSC data into the target cloud service. Cloud data is frequently large enough to tax available bandwidth between systems and data and can therefore be moved by the physical movement of physical storage media. In some cases, data is moved electronically.
- **Syntax of the data:** ideally the same for the source service and the target service. However, if the syntax does not match, e.g. the source uses JSON syntax, but the target uses XML, it can be possible to map the data using commonly available tools.
- **Semantics of the data:** commonly expressed by an ontology. Compatible ontologies simplify the porting of data between source and target services. If the ontologies are incompatible, additional resources can be applied to detect inconsistencies. These inconsistencies can be resolved, or fidelity of the data can be reduced to enable the data to be ported.

5.1.3.3 Cloud application portability

Cloud application portability is the ability to migrate applications from a CSC's on-premises system to a cloud service or from one cloud service to another including migration between instances of cloud deployment models (private, public, community and hybrid). Figure 3 illustrates the porting of an application between a CSC's on-premises system and a cloud service and porting of an application between two cloud services. The arrows in both directions indicate the potential to port applications to and from any of those places.

284



285

286 **Key**

- A CSC system to/from cloud service
- B cloud service to/from cloud service

287

Figure 3 — High level view of cloud application portability

288 Considerations relating to cloud application portability include the following:

- 289 — Cloud application portability can require the movement of one or more application components that
290 form part of a larger, multi-cloud application. For instance, in addition to application logic, it can be
291 necessary to port and/or reconfigure the cloud application and/or the components upon which it
292 depends, e.g. libraries, databases and web servers. The sequence of virtual machine and/or
293 component start-up can also be important.
- 294 — Portability of complex applications can also require CSPs to share application metadata (3.3). This
295 metadata (3.3) can be acquired by capturing expert knowledge and best practices related to that
296 application's deployment and subsequent management throughout its lifecycle, by automated
297 inspection or discovery or by other means. Common examples of this metadata (3.3) are details
298 regarding the relationships and dependencies between various application components,
299 requirements such as the acceptable range of component versions, start-up sequence, network and
300 firewall configuration, processing capacity, co-location rules and load balancing requirements.
- 301 — Cloud application portability requires that interfaces needed by the application in the source
302 environment are also available in the target environment. These interfaces, for example, can enable
303 the application to use service discovery and communication protocols implemented by the
304 environment, as well as providing access to the environment capabilities that support the
305 application. In some environments, the interfaces also enable applications to manage the underlying
306 resources. In cases where an application is being ported between two cloud services within the same
307 CSP or between two different CSPs, the ability of a target cloud service to replicate the environment

that the source cloud service has for the application/service or at least create an environment that similarly satisfies the dependencies of the application, is a major consideration.

- The reduced disruption and increased choice enabled by cloud application portability provide CSCs with the capability to mitigate risks. Cloud application portability can facilitate greater business agility by enabling more rapid redeployment of cloud applications and services to alternative or complementary CSPs in response to changing business conditions and technical trends.
- Cloud application portability requires that the identified activities of CSC and CSN and their sub-roles that are supported in the source system are also supported, with acceptable fidelity, by the target system and its components. In practice, different cloud services rarely provide identical capabilities to support all of the activities for all sub-roles. The effort necessary to adjust for these differences and the potential benefits need to be considered. For example, a cloud application implemented on an infrastructure capabilities type cloud service (ISO/IEC 22123-1: 2023, 3.5.3) moved to a different cloud service of the same type can provide identical capabilities to support the activities of the CSC:Cloud service user sub-role deploying and operating the application, but very different capabilities for the CSC:Cloud service administrator sub-role managing the use of the cloud service.

5.1.4 Relationship between cloud interoperability and cloud portability

It is important to understand that portability and interoperability are not synonymous. While interoperability and portability are often discussed in parallel and are related concepts, they are in fact separate concepts without direct dependencies.

The focus of interoperability is the ability to exchange information between a CSC's on-premises system and a cloud service or between a cloud service and another cloud service, resulting in the ability to mutually use the information that has been exchanged. A cloud service that is interoperable does not necessarily support portability of applications and/or data.

Portability is the ability to migrate data or applications from one cloud service to another or between a CSC's on-premises system and a cloud service. The degree of effectiveness and efficiency of the migration is considered as the ability to execute the application or use the data with few or no manual changes in the migration process. (see ISO/IEC 22123-2: 2023 7.8 [8]). The focus of portability is the ease of migration of the data and application. A cloud service that supports portability is not necessarily interoperable.

Annex A and Annex B present relationships and dependencies between cloud interoperability, portability and switching.

5.1.5 Costs associated with cloud portability

Cloud portability, especially when it involves switching from one CSP to another, can involve costs to the CSC which are related to the CSC's own past decisions and business needs, which can vary considerably.

Examples of such costs can include, but are not limited to, the following:

- Management of the portability or switching process. CSC management and staff will potentially need to spend considerable human time and effort on:
 - evaluating;
 - making the business case;
 - choosing a new CSP;
 - choosing or negotiating a new CSA;
 - determining the technical changes required;

- 350 — determining the human resources required for the transition;
- 351 — determining acceptable application downtime;
- 352 — notifying affected application users;
- 353 — planning mitigations for problems, and planning how they are to be accomplished.
- 354 — Use of consultants who have experience with this type of portability project.
- 355 — Training or recruiting staff to cover any skills or capacity shortfall for engineering and executing the
- 356 process.
- 357 — Redesigning and recoding the CSC's workload either to enable the porting process, and to reduce the
- 358 cost of any future porting decisions.
- 359 — Insurance for any business risk associated with the process.
- 360 — Training or recruiting for user support services for the transition and new environment.
- 361 — Exit or egress charges imposed by the original CSP.
- 362 — In practice these, where they exist at all, tend to be a small part of the overall costs.
- 363 — There can be charges associated with any early termination of a CSA. This is highly dependent on
- 364 past choices made by the CSC.

365 Some of these costs can be anticipated by good CSC planning when first adopting the source CSP and
 366 designing the CSC workload. If they are not anticipated and planned for, there is increased risk that the
 367 switching project will not be successful or offer the expected return on investment.

368 **5.2 Cloud interoperability and portability facet models**

369 **5.2.1 Cloud interoperability facet model**

370 **5.2.1.1 General**

371 Interoperability transcends a mere binary classification of yes or no, representing a multifaceted
 372 landscape with multiple opportunities for collaboration and advancement. At its core, interoperability
 373 encompasses various components, from the fundamental exchange of data bytes to fostering a deep
 374 understanding of exchanged information's semantics, harmonizing business processes, behaviours, and
 375 policies across entities engaged in the exchange. While technical aspects like data transmission are
 376 pivotal, recognizing that semantic, behavioural, and policy interoperability pose significant challenges is
 377 an invitation to explore and innovate. Interoperability in cloud computing leads to enhanced
 378 collaboration which can drive technology progress and foster synergies among users and systems.
 379 Interoperability can be viewed as a way to unlock new possibilities through the use of cloud computing.
 380 The interoperability facet model described in this document defines five facets within the context of cloud
 381 interoperability. These five facets, shown in Figure 4, are transport, syntactic, semantic data, behavioural
 382 and policy. This model is derived by combining and abstracting the European Interoperability
 383 Framework [18] and the LCIM [19].

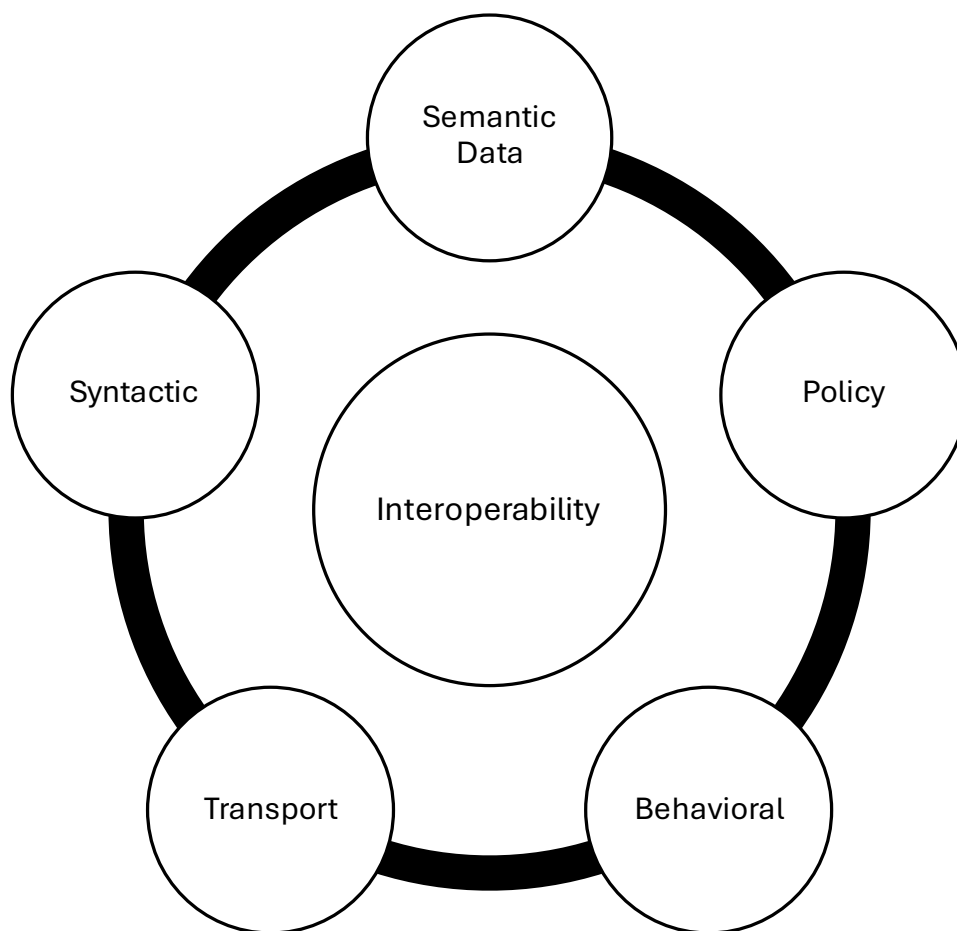


Figure 4 — Facets of cloud interoperability

5.2.1.2 Transport interoperability

Transport interoperability means the commonality of the communication infrastructure established to exchange data between systems. In the context of cloud computing, transport interoperability is the transfer mechanism between various cloud computing components, either between CSC components and CSP components or between CSP components related to different cloud services. Examples include HTTP/S, SOAP, AMQP and MQTT.

5.2.1.3 Syntactic interoperability

Syntactic interoperability is the ability of two or more systems or services to understand the structure of exchanged information, which is an encoding of the domain concepts as defined by the semantic data facet. Examples of encoding syntaxes include JSON, XML and syntaxes described in ASN.1.

5.2.1.4 Semantic data interoperability

Semantic data interoperability is the ability for the systems exchanging information to understand the meaning of the data model within the context of a subject area. Domain concepts in a cloud computing context are dictated by the type of cloud service offering.

Semantic data interoperability is based on the data models of the information being exchanged at the time of that exchange. At the infrastructure level, this concerns VMs, containers, storage and networking

concepts and their management. At the platform level, this concerns applications, the execution and deployment environment and their management. At the application level, the domain concepts are dictated by the application itself, such as HCM, CRM, ERP, etc.

At the business domain level, semantic data interoperability concerns the ability for discrete domain concepts to be shared and understood between applications, e.g. the concept of “customer” in insurance versus the concept of “patient” in healthcare. Example approaches include the construction of ontologies using, for example, OWL, and the use of semantic query languages like SPARQL.

5.2.1.5 Behavioural interoperability

Behavioural interoperability is where the results of the use of the exchanged information matches the expected outcome. A cloud service, like any other software component is designed for a particular purpose or intention. However, its actual use by a CSC can have a different intention without violating the other facets of interoperability. For example, the web architecture was originally intended to serve static web pages but over time and without significant architectural redesigns, many different dynamic and interactive models have emerged.

Behavioural interoperability of a cloud service is defined in the service description. The service description includes a declaration of the interface provided by the service, often referred to as an API. The interface declaration describes the service in terms of a set of operations provided by the service and the inputs and outputs for each operation. In terms of the service description, behavioural interoperability requires additional information to be supplied in terms of the expected results of each operation, including elements such as pre-conditions, post-conditions and any sequences of operations that are necessary for successful use of the service.

Behavioural interoperability is defined in terms of:

- Intended use as described by the CSP. This description is a characterization of the functionality provided by the service.
- Expected results as defined by the cloud service description include:
 - pre-conditions as stated by the CSP which need to be fulfilled prior to operation;
 - post-conditions which reflect the state of the service upon completion of the operation;
 - orchestration and dependencies with respect to other services required by the CSP to assure correct operation.

The behavioral interoperability facet abstracts from implementation details and describes the behaviour of software components without relying on specific formats or structures.

If the result of an operation against an interface is coherent with the CSC expectations for two different cloud services, the cloud services are considered interoperable, assuming identical policies have been applied.

As an example, if the CSC's current order processing system automatically waits for approval of a submitted order by a listed authority, while a new system assumes that such an order is already approved, the behaviour is very different and problems will arise, although both process the same order data otherwise correctly.

5.2.1.6 Policy interoperability

Policy interoperability is defined as the ability of two or more systems to interoperate while complying with the legal, organizational and policy frameworks applicable to the participating systems and the applicable jurisdictions (3.5). This facet concerns governmental laws and regulations, CSP and CSC policy terms and conditions and organizational policies covering the interactions. Governmental regulations

and organizational policies are outside the scope of this document.

Clause 7.1.6 provides an example of policy interoperability.

5.2.1.7 Issues affecting cloud interoperability

The most significant aspect of interoperability is the mutual understanding of the semantic data and behavioural interoperability which express concepts from a domain of interest.

Full interoperability between two interacting systems requires that all interoperability facets are satisfied. However, practically speaking, two systems can still interact successfully even if interoperability is not possible to achieve for all facets. However, some interoperability facets are more challenging than others when there are mismatches between the systems involved. It is worth noting that a mismatch in one interoperability facet does not imply that other interoperability facets do not match; the facets are chosen because they are largely independent of one another.

For the transport interoperability facet, if one system communicates using a REST HTTP protocol while another system communicates using the MQTT protocol, transport interoperability can still be achieved by using a protocol adapter between the systems, such as an ESB.

Similarly, if the two systems differ in relation to the syntactic interoperability facet, it can be possible to enable them to interoperate using a syntax translator; an example is a syntax mapping between data encoded in XML versus data encoded in JSON.

Challenges related to the semantics of data, the intended use and the organizational realities of people and processes and the constraints of legal or regulatory frameworks tend to be far more difficult to address. For example, transport interoperability can make it possible to deliver data from one system to another but policy, legal or regulatory restrictions can make the data practically unavailable. A lack of agreement on governance structures can impose legal risks that prevent the sharing of that data.

Systems that differ in data semantics pose significant issues for interoperability. If two systems have different types of data artefacts or the meaning of data artefacts differs between the systems, the data from one system has no meaning or is unusable by the other system. In addition, it isn't always possible to create semantic adapters to enable the two systems to connect meaningfully. It can be possible to create metadata (3.3) or semantic mappings to provide a form (full or partial) of semantic equivalency.

In order to achieve successful behavioural interoperability, it is necessary that the processes or activities of the CSC's on-premises systems are aligned with the processes or activities of the relevant cloud services, otherwise, the CSP's cloud services possibly won't provide the features and functionalities expected by the CSC. Lack of behavioural interoperability between two systems can be a very significant barrier to enabling full interoperability between the systems. The implication is that the actual behaviour of one system does not match the expectations of the other system, even if the service interface (or API) matches between the systems. It can be possible to create some form of behavioural adapter to deal with the behavioural differences, but this can be a significant challenge for more complex behavioural mismatches.

Policy interoperability can be one of the most challenging and difficult to resolve. If there is a legal prohibition on a CSC using a cloud service because the service runs in a different jurisdiction (3.5), for example, then it is not possible for a CSC to use that cloud service even if all the other facets of interoperability are satisfied. CSC policies concerning data placement, e.g. for sensitive data, can also be a significant barrier to policy interoperability. CSC enterprise policies can also have an impact, for example, where specific accessibility capabilities are required (as in ISO 9241-171:2008, 3.2). In some cases, the CSC can negotiate with the CSP to offer the cloud service in a different way that overcomes the regulatory or policy issues, for example, a public cloud service can be alternatively offered as a private cloud service (with dedicated resources for that CSC) in order to satisfy the security policies of the CSC.

5.2.1.8 Summary of cloud interoperability facet model

Table 1 provides a brief summary of the information provided in 5.2.1 but does not replace or alter 5.2.1.1 to 5.2.1.7.

Table 1 — Summary of different facets of cloud interoperability

Facets	Aim	Objects	Requirements	Examples
Transport	Data transfer between systems	Signals	Protocols of data transfer	REST-based HTTP/S, MQTT
Syntactic	Receive data in an understood format	Data	Standardized data exchange formats	JSON, XML, ASN.1
Semantic data	Receive data using an understood data model	Programmatic interface	Common interpretation of data model	OData, shared understanding and meaning, OWL
Behavioural	Obtain expected outcomes to service requests	Information	Behavioural models for the cloud service	UML models, pre and post conditions, constraint specifications
Policy	Assurance that interoperating systems follow applicable regulatory and organizational policies	Regulatory and organizational policies and interoperation context	Conditions and control for use and access	CSC security policies, restriction on cross-border data transfer, regulations controlling PII, intellectual property rights

5.2.2 Cloud data portability facet model

5.2.2.1 General

Cloud data portability is the ability to transfer data from one cloud service to another cloud service or between a CSC's on-premises system and a cloud service using a machine-readable format. Like interoperability, data portability can be observed from different facets, where each facet focuses on a single dimension. To achieve data portability, all facets need to be understood and mutually agreed upon or sufficiently understood so that it is clear what facet can need attention when porting data.

This document defines three facets of data portability within the context of cloud computing. These facets are called data policy, data syntactic and data semantic as shown in Figure 5. This model is based on the cloud interoperability model in 5.2.1, adapted to focus on the different concerns of cloud data portability.

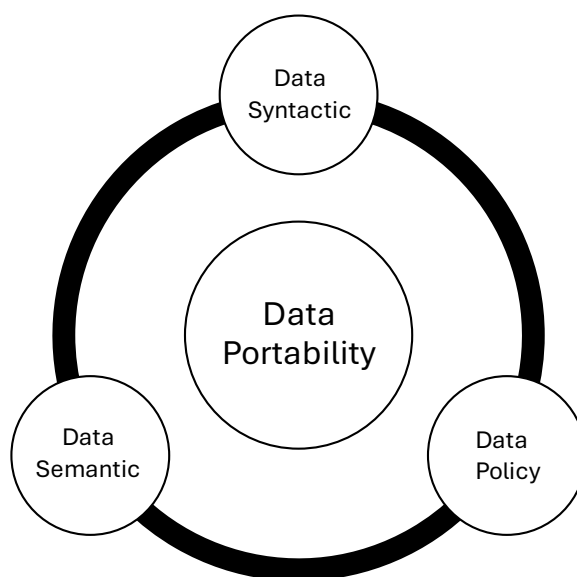


Figure 5 — Facets of cloud data portability

NOTE Although a transport facet for portability has not been included, data transport is needed to achieve data or application portability.

5.2.2.2 Data syntactic portability

Data syntactic portability is defined as transferring data from a source system to a target system using data formats that can be decoded on the target system, using a particular syntax for encoding the data, such as XML or encapsulating the data in a packaging format, such as OVF [3] or ISO/IEC 21320-1 [8]

5.2.2.3 Data semantic portability

Data semantic portability is defined as transferring data to a target such that the meaning of the data model is understood within the context of a subject area by the target. A (logical) data model, sometimes called a meta-model, expresses the data items, their attributes, logical structures and relationships between data items. Data models in a cloud context are dictated by the type of cloud service offering. At the infrastructure level, data models concern VMs, containers, storage and networking metadata (3.3). At the platform level, the data models concern applications intended to be installed. At the application level, the domain concepts and data model will be dictated by the application itself, such as HCM, CRM and ERP.

5.2.2.4 Data policy portability

Data policy portability is defined as the ability to transfer data between a source and a target while complying with the legal, organizational and policy frameworks applicable to the source and target and the applicable jurisdictions (3.5). This includes regulations on data locality, rights to access, use and share data, and mutual responsibilities with respect to security and privacy between a CSP and a CSC. For some specific issues that can affect compliance for privacy and confidentiality during migration, see 5.3.4.

5.2.2.5 Issues affecting cloud data portability

The core of cloud data portability is a mutual understanding of the semantics as captured in a data model. Semantics can be encoded into different syntaxes, but providing the different parties have a mutual

understanding of the data model, translations between syntaxes will result in minimal information loss. Similarly, policies can change but semantic data portability ensures consistency.

Data portability is a key consideration when considering lock-in to a specific cloud service. Although application portability (see 5.2.3) can affect the cost of migrating between systems, application migration is largely a cost issue and although economic lock-in is a real possibility, it can be mitigated. However, if key data is unavailable outside of a system, it can be impossible for a CSC to leave that system, and they are locked into that system. Data syntactic incompatibilities can increase costs involved in moving data between systems, but they are rarely a cause of lock-in for cloud services. It is necessary to focus on semantic portability of key data when considering the feasibility of data portability since loss of access to meaningful information in the data can make the target system unable to provide supporting activities important for CSC and CSN roles. In addition, an absence of data policy portability can make it impossible to access the data and key information.

EXAMPLE

An enterprise CSC uses a SaaS offering for CRM and the commercial terms for use of that offering become unattractive compared with other SaaS offerings. The CSC data held by the SaaS offering is crucial to the enterprise's operation. However, the CSC discovers that the data semantics are specific to their current CRM service and cannot be easily ported to a competitor.

In many such cases, porting will be very difficult. The structure of the data is often designed to fit a particular form of application processing which has developed over years of operation, and a significant transformation is needed to produce data that can be handled by a different cloud service. This problem can be greatly amplified if the CSC has employed customisation capabilities of the source cloud service thereby adding to or changing the data elements that are present and consequently need to be ported to the destination, since the published schemas of the source cloud service potentially no longer correctly describe the data itself.

Data formats define syntax and convey semantics, so it is important to consider the role of data formats within data portability. In addition to interfaces, application programs and software packages acquire, store and process data using structures, which are optimized by the software developer. Following the principle that compatible interfaces are important in a cloud environment, two implementations of the same service do not have to be created in the same way and can store data very differently. Data storage methods and formats will also need to change as innovation brings new features or performance improvements to a service. It is likely that internal data storage methods and format will change dramatically over the life cycle of the service. In general, it is not possible to “freeze” the internal data storage methods or formats without also blocking future innovations.

Without proper definitions of import and export formats, a set of data from one cloud service will probably be meaningless when imported into another cloud service. This problem clearly has an impact on data portability between CSPs. Software is available in many different business domains. Therefore, data interchange formats will need to be considered for specific domains such as administration, finance, healthcare, etc. This issue is of particular concern at the SaaS level.

Regardless of the domain, special attention has to be given to personal information. For example, according to GDPR [21], the data subject has the right to receive personal data in machine-readable, structured and commonly used formats. Personal data can be described by a number of categories. Information regarding these data categories can be found in ISO/IEC 19944-1 [11]. Furthermore, data in any category can provide or contribute to information that can be linked to an individual, referred to in this document as PII. The extent to which individuals are directly identified in the data and how easy it is to associate a set of characteristics in the data to an individual is important to individuals, CSCs and policy makers as they assess the use of that data category. Therefore, the specification of data often includes not only the type of that data, but also a description of the degree to which the data can identify an individual (ISO/IEC 19944:2017, 8.3 [11]).

Standards that define the semantics of some elements of the data can help ensure semantics portability. For example, Dublin Core [5] schema is a vocabulary that describes web resources.

5.2.2.6 Summary of cloud data portability facet model

Table 2 provides a summary of the information in 5.2.2.

Table 2 — Summary of different facets of cloud data portability

Facets	Aim	Objects	Requirements	Examples
Data syntactic	Receiving data in a machine readable, structured and commonly used format	Data	Common machine-readable data format	XML, CSV, JSON, Parquet
Data semantic	Assured meaning of data	Data schemas and ontologies	Mutually understood ontologies and metadata (3.3)	OWL, Dublin Core schema [5]
Data policy	Adhering to all applicable regulations and organizational policies	Regulatory and organizational policy	Agreed set of applicable regulations and organizational policies	Confidentiality levels, privacy rights, cross border transfer, intellectual property rights

5.2.3 Cloud application portability facet model

5.2.3.1 General

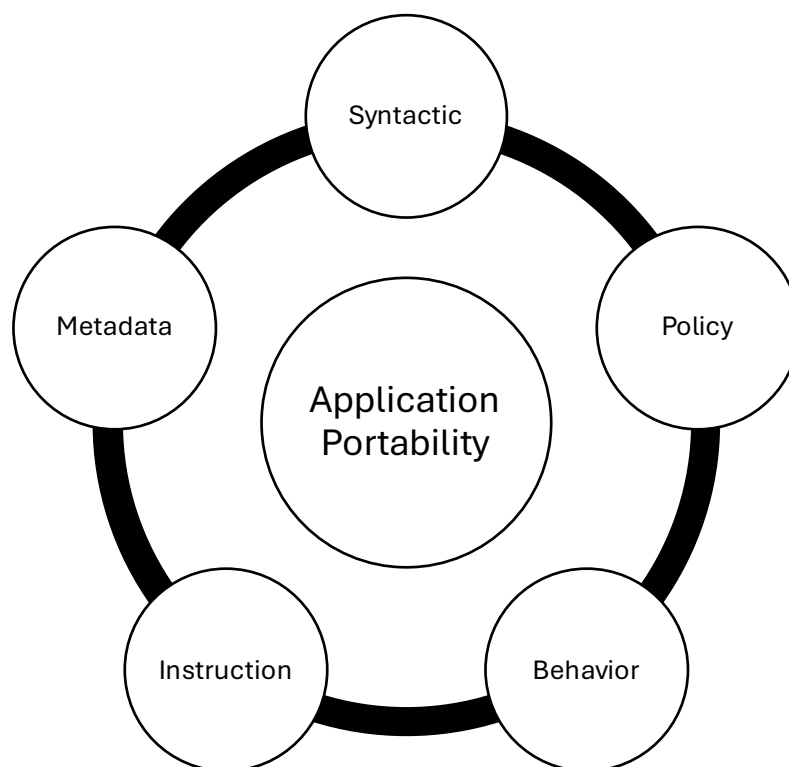
Cloud application portability is the ability to migrate CSC-provided code (3.2) from one cloud service to another cloud service or between a CSC's on-premises system and a cloud service. The objective is that once ported, the CSC-provided code (3.2) provides equivalent functionality in the destination environment as it did on the source environment. To achieve application portability, all facets need to be sufficiently understood so that it is clear what facet(s) need attention when porting CSC-provided code (3.2).

NOTE 1 Application portability does not imply any right of a CSC to move or take copies of CSP-owned code or executables unless explicit permission has been granted to do so, since CSP-owned code and applications will generally be covered by applicable copyright and property law. This document defines five facets of cloud application portability within the context of cloud computing. These facets as shown in Figure 6 are application syntactic, application instruction, application metadata (3.3), application behaviour and application policy. The cloud application portability facet model is inspired by the cloud interoperability facet model described in 5.2.1 and adapted to focus on the different considerations related to cloud application portability.

NOTE 2 Although a Transport facet for portability has not been included, data transport (e.g. over-the-wire protocol, physical media such as magnetic tape, optical disk, hard disk or other portable persistent

602

memory device) is needed to achieve data or application portability.



603

604

605

Figure 6 — Facets of cloud application portability

606

5.2.3.2 Application syntactic portability

607

Application syntactic portability is migrating an application from a source system to a target system in a format that can be decoded on the target system. Similar to data syntactic portability, application artefacts and metadata (3.3) are structured according to a domain model for applications and are encoded using a particular syntax and packaging format.

611

5.2.3.3 Application instruction portability

612

Application instruction portability is migrating an application from a source system to a target system so that its instruction set executes on the target system. Once ported, the software artefacts, orchestration instructions and other scripts that comprise an application need to be executed on an infrastructure that appears to the application as similar to the system for which it was designed. This means ensuring all the necessary interpreters and execution engines are available.

617

5.2.3.4 Application metadata portability

618

Application metadata (3.3) portability is migrating an application from a source system to a target system so that the application metadata (3.3) is understood on the target system. Similar to semantic data portability, the domain model for an application needs to be mutually understood if an application is ported from one system to another. The domain model for an application typically includes metadata (3.3) about the application, including what resources the application needs, how it can be configured, initialization data, etc.

623

5.2.3.5 Application behaviour portability

Application behaviour portability is migrating an application from a source to a target so that execution on the target produces equivalent results to those produced on the source. An application ported from one system to another possibly won't exactly exhibit the same behaviour in the target system due to the differences in the execution environment. For example, fast clock speeds can cause threading and locking issues or there can be an increase in response times to a user request causing HTTP timeouts. Such problems are usually a result of legacy application design, e.g. out-dated latency assumptions, and need to be addressed by the CSC in the application, since the CSP has no control over such behaviours. This is much less of an issue for applications developed for cloud service deployment.

5.2.3.6 Application policy portability

Application policy portability is defined as migrating an application from a source system to a target system while complying with the applicable legal, organizational and policy frameworks of both the source and target systems and the applicable jurisdiction(s) (3.5). Application policy portability can be affected by a number of factors, for example, lack of payment for the cloud service, lack of a license to run the application in the target system, regulations preventing running an application in a certain jurisdiction (3.5), etc.

5.2.3.7 Summary of cloud application portability facet model

Table 3 provides a summary of the information in 5.2.3

Table 3 — Summary of different facets of cloud application portability

Facets	Aim	Objects	Requirements	Examples
Application syntactic	Received application in an understood format	Application	Common packaging format	Zip, TAR, jar
Application instruction	Ability to execute application instructions in functional equivalent manner	Application instructions	Supported runtime environment	C++, Java, C#, BPEL,
Application metadata (3.3)	Mutual understanding of environmental dependencies needed for proper execution of application	Application metadata (3.3)	Shared metadata (3.3) model	XML, JSON, YAML
Application behaviour	Ability to execute an application to produce expected results	Application functional and non-functional requirements	Shared assumptions on environment	Application test suites
Application policy	Agreed set of regulatory and organizational policy constraints on application use	Regulatory and organizational policy	Conditions and control for use and access	Licenses, applicable regulations, enterprise policies

5.3 Key challenges related to interoperability and portability in cloud computing

5.3.1 General

The following key challenges need to be carefully considered, even in cases where identical software is used in both the source and the target system.

5.3.2 Security

Security is a key concern for all CSCs when using cloud services, both in terms of interoperability and also, in terms of data portability and application portability.

For interoperability, concerns include the security controls, for example, as defined in ISO/IEC 27000 [13] series of standards, applied to the interfaces between the CSC's on-premises systems and the cloud service. These controls include the confidentiality of communications between the CSC's on-premises systems and the cloud service, typically enabled using encryption of some form. Confidentiality controls can include encrypted protocols such as HTTPS or TLS or can take the form of a VPN between the CSC's on-premises systems and the cloud service. There are a number of standards in this area, which can make interoperability possible from the point of view of this security concern.

A second concern for interoperability is that of identity and access management, covered in 5.3.3.

For data portability, the movement of CSC data from a CSC's on-premises system to a cloud service or from one cloud service to another cloud service raises a series of security concerns. The essential question is whether the security controls in place in the target cloud service meet the CSC requirements for the data concerned. The CSC needs to classify the data; more sensitive data need a higher level of security controls applied. Factors affecting data classification include:

- whether the data contains PII;
- if the data contains PII, whether any of the PII is sensitive data;
- whether the data contains confidential data, such as financial records or data supplied by third parties under a restrictive license (e.g. data which is subject to digital rights management);
- whether the data is subject to regulation and if so, what restrictions or requirements are imposed by the regulation.

Data of all classifications can need security controls in place to ensure availability. How this is done can vary but suitable backup and restore facilities are typically required and/or data replication and redundancy capabilities. How these capabilities are provided can vary widely. In some cases, the capabilities are built into the cloud service and in other cases, the CSC needs to set up the capabilities.

Data classified as low risk can be placed into a cloud service with a relatively small set of security controls, although even this data can need protection from tampering or destruction by unauthorized users. Data classified at a higher level of risk is likely to need more security controls. These controls are likely to include encryption of the data at rest, e.g. when stored in a database, encryption of the data when in motion over any communication link and granular control over access to the data (see 5.3.3).

Once encryption is necessary, consideration needs to be given to the form of encryption, e.g. does the encryption meet the requirements of a standard such as FIPS 140-2[22] and also to the mechanisms used to handle the encryption keys. Encryption key handling can include key storage services and the use of hardware encryption modules. It is possible that the encryption capabilities differ between the CSC's on-premises systems and the cloud service or between cloud services and these differences should be accounted for during the porting process.

More sensitive data usually also requires close monitoring, with requirements for recording all access to the data and recording all changes made to the data.

A key question for all these controls is who is responsible for applying and operating the controls. This is likely to vary depending on the cloud capabilities type of the cloud service. For application capabilities cloud services, most of the controls are likely to be in the hands of the CSP, although the CSC can select the appropriate configuration of the cloud service. For infrastructure capabilities cloud services, many of the controls are likely to be in the hands of the CSC, except for general data centre controls such as

physical security. For platform capabilities cloud services, there can be a mix of responsibilities depending on the platform capabilities used by the CSC.

For application portability, key security considerations concern the security controls which enable the CSC to assure that the ported application artefacts are not subject to tampering, destruction or theft. There are also the security controls relating to the operation of the application (firewalls, authentication, encryption and so on). Protection of the application artefacts relates to both protection when in motion between CSC's on-premises systems and the cloud service and also at rest when stored within the cloud service. Encryption and strict access control are capabilities likely to be necessary. For the operation of the application, it is typical that the CSC needs to arrange for all the necessary capabilities to be in place (as applies where the application runs on CSC in-house systems). For some cloud services, it can be the case that some security capabilities are supplied by the cloud service, either automatically or through configuration, e.g. firewalls, in this case, the CSC needs to understand the capabilities available including their responsibilities for configuring and operating them.

In all cases, interoperability and portability are improved where the target cloud service meets the security requirements of the CSC, ideally with minimal configuration and change on the part of the CSC.

5.3.2.1 Data Integrity and Availability

Achieving true data portability and system interoperability critically hinges on maintaining robust data integrity throughout any data movement or exchange process. Whether porting data between cloud services, or enabling different services to interoperate by sharing information, the data needs to retain its accuracy, completeness, consistency, and semantic meaning. Without guaranteed data integrity, ported data can become corrupted, incomplete, or misinterpreted, rendering interoperable processes unreliable and potentially leading to flawed business outcomes or compliance violations, thereby undermining the core benefits of portability and interoperability.

In the context of cloud portability and interoperability, availability becomes a critical security concern because the very processes designed to enhance flexibility can inadvertently introduce new points of failure or increase susceptibility to disruptions. During data or application portability, improperly managed migration processes can lead to extended downtime or loss of access to services if source or target systems become unavailable or if data is in an unusable state mid-transfer. Similarly, with interoperability, the tight coupling or dependencies between different cloud services mean that the unavailability of one critical service can cascade, rendering other interconnected services inaccessible to authorized users, akin to a denial-of-service impact, thereby compromising the overall operational continuity and security posture.

5.3.3 Identity and Access Management

Important aspects of identity and access management include:

- **Enabler of Interoperability:** Digital identity is central to enabling syntactic, semantic, behavioral, and policy interoperability as defined in this document. For cloud services to interoperate, they need to recognize and authenticate users, systems, and services in a consistent and secure manner. This requires standardized digital identity management practices.
- **Identity and Access Management (IdAM):** This document references IdAM as a key aspect, ensuring that identities (users, services, devices) can be securely and reliably managed, authenticated, and authorized across different cloud environments. This is essential for both interoperability (interaction between systems) and portability (moving data/applications while preserving access controls).
- **Policy Interoperability:** Digital identity also plays a role in policy interoperability, where compliance with legal, organizational, and policy frameworks is necessary. Consistent digital identity management ensures that access policies and user permissions remain enforceable when services or data move between different CSPs.
- **Portability Considerations:** When data or applications are ported from one cloud service to another, maintaining the integrity and continuity of digital identities and their associated