

IEEE Guide for Cloud Portability and Interoperability Profiles (CPIP)

IEEE Computer Society

Developed by the
Cloud Computing Standards Committee (C/CCSC)

IEEE Std 2301™-2020

STANDARDS

IEEE Guide for Cloud Portability and Interoperability Profiles (CPIP)

Developed by the

Cloud Computing Standards Committee (C/CCSC)
of the
IEEE Computer Society

Approved 30 January 2020

IEEE SA Standards Board

Abstract: Advice is given for cloud computing ecosystem participants (cloud vendors, service providers, and users) of standards-based choices in areas such as application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conventions. These choices are grouped into multiple logical profiles, which are organized to address different cloud roles.

Keywords: cloud customers, cloud management, cloud profiles, cloud service providers, consent interoperability, data portability, IEEE 2301™, interoperability, privacy, security

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 13 August 2020. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-6464-2 STD24064
Print: ISBN 978-1-5044-6465-9 STDPD24064

*IEEE prohibits discrimination, harassment, and bullying.
For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/ipr/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for IEEE standards can be accessed via <https://standards.ieee.org/standard/index.html>. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore: <https://ieeexplore.ieee.org/browse/standards/collection/ieee/>. Users are encouraged to periodically check for errata.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE guide was completed, the Cloud Profiles WG (CPWG) Working Group had the following membership:

Brian D'Andrade, *Chair*
Hosnieh Rafiee, *Vice Chair*

Nicolas Batara
Dipankar Chakrabarti
Victor Danilchenko
Sujatha Dantuluri

Hiroki Kashiwazaki
Zachary Lochner
Andrews Offei Nyanteh
Lair Martes Jr.

Sonal Phan
Matthew Pooley
Nancy Rivera
Alan Sill

The following members of the individual Standards Association balloting group voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

Demetrio Bucaneg Jr.
Dipankar Chakrabarti
Ioannis Chatzigiannakis
Keith Chow
Charles Cook
Benjamin Cotts
Michael Crusoe
Brian D'Andrade
Victor Danilchenko
Sujatha Dantuluri
David Fuschi
Randall Groves
Richard Hafner

Werner Hoelzl
Noriyuki Ikeuchi
Atsushi Ito
Piotr Karocki
Stuart Kerry
Yongbum Kim
Krishna M. Kumar
Thomas Kurihara
Marc Lacroix
Sajeev Manikoth
Arumugam Paventhan
Hosnieh Rafiee
Maximilian Riegel
Robert Robinson

Hamadou Saliah-Hassane
Stephen Schwarm
Kendall Southwick
Thomas Starai
Walter Struppler
Ganesh Subramanian
Thomas Tullia
Mark-Rene Uchida
John Vergis
Karl Weber
Oren Yuen
Daidi Zhong

When the IEEE SA Standards Board approved this guide on 30 January 2020, it had the following membership:

Gary Hoffman, *Chair*
Vacant Position, *Vice Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
J.Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*
John D. Kulick
David J. Law

Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Jon Walter Rosdahl

Dorothy Stanley
Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2301-2020, IEEE Guide for Cloud Portability and Interoperability Profiles (CPIP).

The purpose of this guide is to assist cloud computing vendors and users in developing, building, and using standards-based cloud computing products and services, which should enable increased portability, commonality, and interoperability. Cloud computing systems contain many disparate elements. For each element there are often multiple options, each with different externally visible interfaces, file formats, and operational conventions. In many cases these visible interfaces, formats, and conventions have different semantics. This guide enumerates those options, grouped in a logical fashion called *profiles* for such definitions of interfaces, formats, and conventions, from a variety of sources.

IEEE Standards downloads and executable files

Files are available in the IEEE Std 2301-2020 directory located at <https://standards.ieee.org/downloads>.

Contents

1. Overview	9
1.1 Scope	9
1.2 Purpose	9
1.3 Word usage	9
2. Normative references	10
3. Cloud standards	10
3.1 Introduction	10
3.2 Collections of cloud standards	10
3.3 Categories of cloud standards	10
4. Cloud profiles	23
5. Cloud service provider (CSP)	23
5.1 Description	23
5.2 Sub-role: Inter-cloud provider	23
5.3 Sub-role: Cloud Service Operations Manager	36
5.4 Sub-role: Cloud Service Deployment Manager	36
5.5 Sub-role: Cloud Service Manager	36
5.6 Sub-role: Cloud Service Business Manager	36
5.7 Sub-role: Customer Support and Care	36
5.8 Sub-role: Cloud Service Security and Risk Manager	37
5.9 Sub-role: Network Provider	37
6. Cloud service partner	37
6.1 Introduction	37
6.2 Sub-role: Cloud Service Developer	37
6.3 Sub-role: Cloud Auditor	37
6.4 Sub-role: Cloud Service Broker	37
7. Cloud service customer	40
7.1 Description	40
7.2 Sub-role: cloud service user	40
7.3 Sub-role: cloud service administrator	40
7.4 Sub-role: business manager	40
7.5 Sub-role: cloud service integrator (CSI)	40
8. Cloud standard use cases	42
8.1 IoT use cases	42
8.2 Cloud computing in automotive applications	46
8.3 Cloud computing in financial markets	47
9. Cloud open source	48
Annex A (informative) Bibliography	49

IEEE Guide for Cloud Portability and Interoperability Profiles (CPIP)

1. Overview

1.1 Scope

This guide advises cloud computing ecosystem participants (cloud vendors, service providers, and users) of standards-based choices in areas such as application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conventions. This guide groups these choices into multiple logical profiles, which are organized to address different cloud roles.

1.2 Purpose

The purpose of this guide is to assist cloud computing vendors and users in developing, building, and using standards-based cloud computing products and services, which should lead to increased portability, commonality, and interoperability. Cloud computing systems contain many disparate elements. For each element there are often multiple options, each with different externally visible interfaces, file formats, and operational conventions. In many cases these visible interfaces, formats, and conventions have different semantics. This guide enumerates options, grouped in a logical fashion, called *profiles*, for such definitions of interfaces, formats, and conventions from a variety of sources. In this way, cloud ecosystem participants will tend toward more portability, commonality, and interoperability, growing the cloud computing adoption rate overall.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{1, 2}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

¹The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

²The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3. Cloud standards

3.1 Introduction

Standards are already available in support of many of the functions and requirements for cloud computing. While many of these standards were developed in support of pre-cloud computing technologies, such as those designed for web services and the Internet, they also support the functions and requirements of cloud computing. Other standards are now being developed in specific support of cloud computing functions and requirements, such as virtualization.

The National Institute of Standards and Technology (NIST) initiated a public working group to identify all the existing cloud computing standards in development. The group's findings were then published in the NIST Special Publication 500-291 [B73].^{3,4} Using a taxonomy developed by the NIST Cloud Computing Reference Architecture and Taxonomy Working Group and published in NIST-SP 500-292 [B74], cloud computing relevant standards were mapped into categories based on the requirements of portability, interoperability, and security. IEEE members continue working on NIST's result to make it useful for cloud stakeholders in all countries over the world. The categorization scheme is not meant to be a definitive single hierarchy, as there could be different perspectives to categorize the standards. However, these categories should be useful in helping cloud stakeholders identify a class of standards relevant to their areas of interest.

3.2 Collections of cloud standards

There have been several activities focusing on cloud computing standards. Three of the more significant efforts include the ITU-T Joint Cloud Activity (JCA), the INCITS Technical Committee on Cloud Computing and Distributed Platforms, which serves as the U.S. TAG to ISO/IEC JTC 1/SC 38, Cloud Computing and Distributed Platforms, and the NIST Cloud Computing Standards Roadmap Working Group. Efforts have been keeping track of and developing standards that could have a significant impact on cloud computing. For the purposes of providing a catalog of cloud standards to align with the cloud profiles, the NIST standards roadmap work (as published in NIST-SP 500-291 [B73]) was selected. The deciding factor was that the NIST special publication had defined categorization of cloud standards.

3.3 Categories of cloud standards

3.3.1 Introduction

This is the list of cloud standards categories that were identified in NIST-SP 500-291 [B73]. Many of these proposed categories were derived from the cloud computing special publications. This is not an extensive list and is intended to illustrate the functional areas that users need to be aware of. As well, standards, regulations, and guidelines will continue to evolve, and users should understand that the requirements will change and will have to adapt as necessary to implement and update their systems.

³The numbers in brackets correspond to those of the bibliography in Annex A.

⁴Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

Authentication & Authorization—Check the identity of the entity that would like to access any resources in the cloud service provider or manage cloud services. Further check whether this entity can access/modify the resources.

Confidentiality—Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity—Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

Identity Management—The management of individuals, their authentication, and authorization.

Security Monitoring & Incident Response—The monitoring of security and privacy incidents to help protect cloud customers' data and services from any data leakage, or to identify any malicious activities or cyber-attacks to immediately respond to incidents and recover from the problems.

Security Controls—Safeguards and countermeasures used to minimize security risks.

Security Policy Management—Managing a controllable set of security rules.

Availability—Ensuring timely and reliable access to and use of information.⁵

Service Interoperability—The capability to communicate, execute programs, or transfer data among various cloud services under specified conditions.⁶

Data Portability—The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.⁷

Service Portability—The ability of a service to run on more than one type or size of cloud.⁸

Service Agreements—The agreement between the cloud service provider and cloud service customer that governs the covered service.

Accessibility—The ability of services to be usable by people with disabilities.

Privacy & Data Protection—The privacy regulation of different countries regarding the storage, transfer, deletion, usage, and retention of cloud data. It is the responsibility of the cloud solution provider as well as the owner of the data to understand and be in compliance with applicable regulations. Timely reporting in compliance with the applicable regulatory bodies after discovery of breaches of security associated with personally identifiable information (PII) is the responsibility of the cloud solution provider and the owner of the data.

Subclauses 3.3.2 through 3.3.16 explain the related standards in detail. These standards are applicable to most cloud profiles that are explained in detail in Clause 4. When there is any exception, the whole related standard will be repeated under that subclause.

3.3.2 Authentication & Authorization

Relevant materials in this domain are as follows:

⁵From Title III of the E-Government Act, The Federal Information Security Management Act of 2002 (FISMA) [B12].

⁶Modified from American National Standard Dictionary of Information Technology (ANSDIT).

⁷From Federal Standard 1037C, Telecommunications: Glossary of Telecommunication Terms.

⁸Modified from Federal Standard 1037C.

- IETF RFC 5246 [B27]: Specifies the transport layer security (TLS) that provides communication security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. This RFC is obsoleted by RFC 8446 [B32].
- IETF RFC 8446 [B32]: TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.
- IETF RFC 3820 [B26]: Forms a certificate profile for proxy certificates based on X.509 Public Key Infrastructure (PKI) certificates for use in the Internet. A proxy certificate is a certificate that is derived from, and signed by, a normal X.509 Public Key End Entity Certificate or by another proxy certificate for the purpose of providing restricted proxying and delegation within a PKI-based authentication system.
- IETF RFC 5280 [B28]: Internet X.509 profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet. The X.509 v3 certificate format is described in detail with additional information regarding the format and semantics of Internet name forms. The X.509 v2 CRL format is described in detail along with standard and Internet-specific extensions.
- IETF RFC 5849 [B29]: Describes the OAuth 1.0 protocol. OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user). It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair), using user-agent redirections. The OAuth protocol was originally created by a small community of web developers from a variety of websites and other Internet services who wanted to solve the common problem of enabling delegated access to protected resources. This RFC is obsoleted by RFC 6749 [B30].
- IETF RFC 6749 [B30]: The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849 [B29].
- IETF RFC 8252 [B31]: OAuth 2.0 authorization requests from native apps should only be made through external user-agents, primarily the user's browser. This RFC details the security and usability reasons why this is the case, and how native apps and authorization servers can implement this best practice.
- ISO/IEC 29115:2013 [B60]: Many electronic transactions within or between ICT systems have security requirements which depend on an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access for which an access control mechanism might be used, and/or for the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.
- Recommendation ITU-T X.1254 [B64] provides a framework for entity authentication assurance. Assurance within this recommendation refers to the confidence placed in all of the processes, management activities, and technologies used to establish and manage the identity of an entity for use in authentication transactions.
- OpenID Authentication [B88]: OpenID is a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. OpenID allows clients of all types, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, allowing participants to use optional features, such as encryption of identity data, discovery of OpenID providers, and session management, when it makes sense for them.

- XACML [B78]: Extensible Access Control Markup Language (XACML) is an Extensible Markup Language (XML) defining policy language, used for description of general access control requirements. It also defines an access control decision request/response language which allows users to form a query to ask whether or not a given action should be allowed, and interpret the result. The response always includes an answer about whether the request should be allowed using one of four values: Permit, Deny, Indeterminate (an error occurred or some required value was missing, so a decision cannot be made), or Not Applicable (the request cannot be answered by this service).
- SAML [B92]: The Security Assertion Markup Language is an XML-based framework for communicating user authentication, entitlement, and attribute information. It allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. SAML is a flexible and extensible protocol designed to be used—and customized if necessary—by other standards.

3.3.3 Confidentiality

Relevant materials in this domain are as follows:

- OASIS Key Management Interoperability Protocol (KMIP) TC [B79]: It is an Organization for the Advancement of Structured Information Standards (OASIS) standard that defines a single, comprehensive protocol for communication between encryption systems and a broad range of new and legacy enterprise applications, including email, databases, and storage devices. By removing redundant, incompatible key management processes, KMIP will provide better data security while at the same time reducing expenditures on multiple products.
- XML: Extensible Markup Language is a W3 standard [B15]. It is a simple, very flexible text format derived from SGML (ISO 8879:1986 [B38]). XML was designed to meet the challenges of large-scale electronic publishing and as an important means to exchange a wide variety of data over the Internet. For confidentiality purposes, the data are usually encrypted or anonymized, which disallows any further process on data. XML standards likely to use as a means on working with encrypted or anonymized data (processing, categorizing, searching).

3.3.4 Integrity

Relevant materials in this domain are as follows:

- XML Signature Syntax and Processing Version 1.1 [B102]: This W3 standard provides integrity, message authentication, and signer authenticity check for data in XML or any other formats.
- Federal Information Processing Standard (FIPS) 180-4 [B17]: The Secure Hash Standard (SHS) is a NIST standard that specifies secure hash algorithms that includes SHA2, SHA3, etc.
- FIPS 186-4 [B18]: The Digital Signature Standard (DSS) specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Rivest-Shamir Adelman Algorithm (RSA).
- FIPS 198-1 [B19]: The Keyed-Hash Message Authentication Code (HMAC) is a mechanism for message authentication using cryptographic hash functions. Its purpose is to authenticate both the source of a message and its integrity without the use of any additional mechanisms.

3.3.5 Identity Management

Relevant materials in this domain are as follows:

- FIPS 201-2 [B22]: Personal Identity Verification (PIV) of Federal Employees and Contractors provides security requirements for security of identity verification systems. This standard does not include descriptions of security policies, but rather it describes the card elements, system interfaces, and security control to help securely store, process, and retrieve identity credentials from the card.
- ISO/IEC 24760-1:2011 [B49]: Information Technology—Security Techniques—A Framework for Identity Management—Part 1: Terminology and Concepts is an ISO standard that defines terms for identity management. It specifies core concepts of identity and identity management and their relationships. ISO/IEC 24760-1 is applicable to any information system that processes identity information.
- ISO/IEC 24760-2:2015 [B50]: Information Technology—Security Techniques—A Framework for Identity Management—Part 2: Reference Architecture and Requirements is an ISO standard that provides guidelines for the implementation of systems for the management of identity information, and specifies requirements for the implementation and operation of a framework for identity management. ISO/IEC 24760-2 is applicable to any information system where information relating to identity is processed or stored.
- ISO/IEC 24760-3:2016 [B51]: Information Technology—Security Techniques—A Framework for Identity Management—Part 3: Practice is an ISO standard that provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1:2011 [B49] and ISO/IEC 24760-2:2015 [B50]. ISO/IEC 24760-3 is applicable to an identity management system where identifiers or personally identifiable information (PII) relating to entities are acquired, processed, stored, transferred, or used for the purposes of identifying or authenticating entities and/or for the purpose of decision making using attributes of entities.
- OASIS WS-Federation [B82]: WS-Federation extends WS-Trust to provide a flexible, federated identity architecture with clean separation between trust mechanisms, security token formats, and the protocol for obtaining tokens. The goal of federation is to allow security principal identities and attributes to be shared across trust boundaries according to established policies. This framework leverages the WS-* specifications to create an evolutionary federation path allowing services to use only what they need and leverage existing infrastructures and investments.
- OASIS WS-Trust 1.3 [B83]: WS-Trust 1.3 defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Using the tokens issued, applications can engage in secure communication designed to work with the general web services framework, including WSDL service descriptions, UDDI business services and binding templates, and Simple Object Access Protocol (SOAP) and SOAP2 messages.
- SAML [B92]: Single sign-on to access an inter-cloud application that spans multiple cloud systems will require federated identity management, delegation of trust, and virtual organizations. The Security Assertion Markup Language SAML V2.0 defines how two providers can establish and subsequently manage the pseudonym(s) for the principals for whom they are operating. It is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.
- SPML v.2 [B81]: Service Provisioning Markup Language is an XML-based request and response language developed by OASIS. The purpose is to allow entities fast and secure setup of user interfaces for web services and applications where service centers generate provisioning requests within and across entities.
- OpenID Authentication [B88]: OpenID is a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. OpenID allows clients of all types, including web-based, mobile, and JavaScript clients to request and receive information about authenticated sessions and end-users.

The specification suite is extensible, allowing participants to use optional features, such as encryption of identity data, discovery of OpenID Providers, and session management, when it makes sense for them.

3.3.6 Security Monitoring & Incident Response

Relevant materials in this domain are as follows:

- ISO/IEC 27039:2015 [B58]: Information technology—Security techniques—Selection, Deployment, and Operation of Intrusion Detection and Prevention Systems (IDPS) is an ISO standard that provides guidelines to assist organisations in preparing to deploy IDPS. In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived.
- PCI DSS [B91]: The Payment Card Industry Data Security Standard explains the minimum set of requirements that every merchant or service provider must follow in order to help protect the cardholder data of their customers during processing and storage. It enumerates 12 security requirements, for example: How to install and maintain firewall configuration, default password requirements, encrypt on transmission, protect for systems, and restrictions on access to card holder data by the rule of need to know. It assists in the protection and security of cardholder information.
- ITU-T X.1500 [B65]: This ITU standard describes techniques to exchange cyber-security information. These techniques can be used alone or in combination with other techniques. The list of these techniques were introduced to augment this document. Some examples include: techniques to rate vulnerabilities based on Common Vulnerabilities and Exposures (CVE) and Common Vulnerabilities Scoring System (CVSS), Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), Critical Security Controls for Effective Cyber Defense (CSC), Open Vulnerability and Assessment Language (OVAL), and Common Platform Enumeration (CPE).

3.3.7 Security Controls

Relevant materials in this domain are as follows:

- Open Trust Protocol [B89]: Open Trust Protocol is a protocol to install, update, and delete applications and to manage security configuration in a Trusted Execution Environment (TEE).
- ITU-T X.509 [B63]: This is a ITU-T standard for public key infrastructure (PKI) to manage digital certificates and public-key encryption. This standard is a key part of the Transport Layer Security protocol used to secure web and email communication.
- ISO/IEC 27001:2013 [B52]: Information Technology—Security Techniques—Information Security Management Systems is the series of standards for information security management systems (ISMS) which give a framework to legal and regulatory requirements. It helps to identify information assets and do the risk management by identifying the risks to these assets and the approach to help reduce the impact of the risk in order to protect information. It needs the engagement of all internal and external stakeholders and puts the requirement to communicate the ISMS policy to them.
- ISO/IEC 27017:2015 [B54]: Information Technology—Security Techniques—Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services provides guidance on the information security aspects of cloud computing. It recommends and assists with the implementation of cloud-specific information security controls which supplement the guidance in ISO/IEC 27002:2013 [B53].
- ISO/IEC 27018:2014 [B55]: Information Technology—Security Techniques—Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors deals with the privacy of the customers at public cloud service providers. It provides controls within the

process of implementing a cloud computing information security management system based on ISO/IEC 27001:2013 [B52].

- ISO/IEC CD 27030 [B62]: Information Technology—Security Techniques—Guidelines for Security and Privacy in Internet of Things (IoT) is an in-development ISO draft standard that provides guidelines and recommendations for the handling of information security and privacy in IoT devices, complementing ISO/IEC 27001:2013 [B52].
- ISO/IEC 27036-4:2016 [B56]: IT Security—Security Techniques—Information Security for Supplier Relationships provides guidelines on evaluating and handling the information risks involved in the acquisition of goods and services from suppliers. This includes B2B relationships (e.g., IT outsourcing and cloud computing service).
- NEN 7510:2011 [B72]: This standard, developed by the Dutch Standardisation Institute, is an extension of ISO/IEC 27001 (information security). It has been developed for the health care industry with specific attention to privacy protection.
- OASIS PKCS#11 [B80]: Public-Key Cryptography Standards (PKCS) is an OASIS standard. This standard has overlap with KMIP. The PKCS#11 standard specifies an application programming interface (API) called *Cryptoki* for devices that hold cryptographic information and perform cryptographic functions. Cryptoki follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a *cryptographic token*.

3.3.8 Security Policy Management

Relevant materials in this domain are as follows:

- FIPS Pub 199 [B20]: Standards for Security Categorization of Federal Information and Information Systems describes the standards to be used for categorization of all information to provide an appropriate level of information security according to a range of risk levels. It also provides guidelines and recommendations on the type of information and explains how to categorize based on the information content.
- FIPS Pub 200 [B21]: Minimum Security Requirements for Federal Information and Information Systems provides minimum state-of-the-practice safeguards and countermeasures for information systems where federal agencies must meet this requirement.
- ISO/IEC 27002:2013 [B53]: Information Technology—Security Techniques—Code of Practice for Information Security Controls is another series of ISMS which adds suitable information security control on ISO/IEC 27001 in the form of recommendations. This standard also focuses on different sizes of organizations. The area of its focus is information security policies, cryptography, access control, asset management, communication security, information security incident management, physical and environmental security, compliance, human resource security, and organization of information security.
- OASIS XACML [B78]: Developed by OASIS, cloud entry point should be protected by policy enforcement point (PEP) and XACML implements attribute-based PEPs. PEPs that conform to v2.0 of XACML are required to deny access unless they understand and can discharge all of the <Obligations> elements associated with the applicable policy. <Obligations> elements are returned to the PEP for enforcement. XACML can be vulnerable to certain threats and hence should be used in conjunction with other trust mechanisms as applicable.
- ATIS-0200008 [B3]: ATIS Trusted Information Exchange (TIE) describes the Trusted Information Exchange requirements for ATIS CSF (Cloud Services Forum)—defined services.

- Y.3520 [B66]: ITU Cloud Computing Framework for End-to-End Resource Management describes general concepts on end-to-end management of software and resources in cloud computing and in multi-cloud.

3.3.9 Service Interoperability

Relevant materials in this domain are as follows:

- CIMI [B11]: Cloud Infrastructure Management Interface describes protocol and models to provide management interfaces to allow interactions between infrastructure as a service (IaaS) providers and their customers. The application management is out of scope of this standard.
- CAMP [B77]: Cloud Application Management for Platform is an OASIS standard that provides protocols and interfaces that can be used for self-service provisioning, monitoring, and control and allows cloud developers to more easily package and deploy their application. It adds additional value to REST.
- OCCI [B86]: Open Cloud Computing Interface is an API and protocol for all kinds of management tasks in the cloud. The idea behind it was to create a remote management API for IaaS. The current release is suitable for IaaS, PaaS, and SaaS.
- DFDL [B10]: Data Format Description Language is an Open Grid Forum standard that introduces a language for describing text and binary data formats. A DFDL description allows any text or binary data to be read from its native format and to be presented as an instance of an information set. DFDL also allows data to be taken from an instance of an information set and written out to its native format. DFDL achieves this by leveraging W3C XML Schema Definition Language (XSDL) 1.0. It is therefore very easy to use DFDL to convert text and binary data to a corresponding XML document.
- TOSCA Version 1.0 [B100]: This standard developed by OASIS, Topology and Orchestration Specification for Cloud Applications, describes service components and their relationship using service topology that describes management procedures.
- IEEE Std 1905.1a™-2014 [B24]: This standard defines an abstraction layer for multiple home networking technologies that provides a common interface to widely deployed home networking technologies: IEEE Std 1901™ over power lines, IEEE Std 802.11™ for wireless; ethernet over twisted pair cable; and MoCA 1.1 over coax. Additional network technologies are supported by an extensible mechanism using an IEEE organizationally unique identifier (OUI) and an XML-formatted document. Connectivity selection for transmission of packets arriving from any interface or application is supported by the IEEE 1905 abstraction layer. Modification to the underlying home networking technologies is not required by the IEEE 1905 abstraction layer, and hence it does not change the behavior or implementation of existing home networking technologies.
- IEEE Std 802.15.4-2015: This standard intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed, ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The emphasis is on very low-cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.
- ISO/IEC 17826:2016 [B47]: Information technology—Cloud Data Management Interface (CDMI) specifies the interface to access cloud storage and to manage the stored data such as delete, update, retrieve, and create. This interface is also used by administrative and management applications to manage containers, accounts, security access, and monitoring/billing.
- OASIS PKCS#11 [B80]: Public-Key Cryptography Standards is an OASIS standard. This standard has overlap with KMIP. The PKCS#11 standard specifies an application programming interface (API) called *Cryptoki* for devices that hold cryptographic information and perform cryptographic functions. Cryptoki follows a simple object-based approach, addressing the goals of technology independence

(any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a *cryptographic token*.

3.3.10 Data Portability

Relevant materials in this domain are as follows:

- ISO/IEC 17826:2016 [B47]: Information technology—Cloud Data Management Interface (CDMI) specifies the interface to access cloud storage and to manage the stored data such as delete, update, retrieve, and create. This interface is also used by administrative and management applications to manage containers, accounts, security access, and monitoring/billing.
- Kantara Initiative Consent Receipt Specification V 1.0 [B67]: This specification provides a common standard digital format for providing a record to individuals about privacy and what they have consented to. The standardized format promotes a consistent, machine- and human-understandable consent receipt, facilitating consent interoperability between systems and enabling data portability.
- ISO 32000-1:2008 [B40]: Document Management—Portable Document Format—Part 1: PDF 1.7 specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed. It is intended for the developer of software that creates Portable Document Format (PDF) files (conforming writers), software that reads existing PDF files and interprets their contents for display and interaction (conforming readers), and PDF products that read and/or write PDF files for a variety of other purposes (conforming products).
- ISO 19005-1:2005 [B39]: Document Management—Electronic Document File Format for Long-Term Preservation—Part 1: Use of PDF 1.4 (PDF/A-1) specifies how to use PDF 1.4 for long-term preservation of electronic documents. It is applicable to documents containing combinations of character, raster, and vector data.
- ISO/IEC 9075-1:2016 [B44]: Information Technology—Database Languages—SQL—Part 1: Framework (SQL/Framework) describes the conceptual framework used in other parts of ISO/IEC 9075 to specify the grammar of SQL and the result of processing statements in that language by an SQL-implementation. ISO/IEC 9075-1 also defines terms and notation used in the other parts of ISO/IEC 9075.

3.3.11 Service Portability

Relevant materials in this domain are as follows:

- ISO/IEC 17203:2011 [B46]: Information Technology—Open Virtualization Format (OVF) specification provides requirements for an open, secure, portable, efficient, and extensible format for the packaging and distribution of software to be run in virtual machines.
- Open Virtualization Format (OVF) 2.0: This DMTF open standard is similar to its version 1.0 that was adopted by ISO. Version 2.0 differs from 1.0 in that it also applies to cloud use cases and it also improves network configuration support and package encryption capabilities.
- TOSCA Version 1.0 [B100]: Topology and Orchestration Specification for Cloud Applications provides OASIS standard language to describe service components and its relationship using service topology that describes management procedures.

3.3.12 Service Agreements

Relevant materials in this domain are as follows: