ETSI SR 003 391 V2.1.1 (2016-02)

Cloud Standards Coordination Phase 2;
Interoperability and Security in Cloud Computing

Reference

DSR/NTECH-00032

Keywords

Cloud computing, interoperability, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Network Technologies (NTECH).

The present document is approved by the NTECH Technical Committee and for publication on the Cloud Standards Coordination website (http://csc.etsi.org).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Cloud Computing is increasingly used as the platform for ICT infrastructure provisioning, application/systems development and end user support of a wide range of core services and applications for businesses and organizations.

Cloud Computing is drastically changing the way IT is delivered and used. However, many challenges remain to be tackled. Concerns such as security, privacy, vendor lock-in, interoperability, portability, service level agreements more oriented towards users are examples of issues that need to be addressed.

In February 2015, the Cloud Standards Coordination Phase 2 (CSC-2) was launched by ETSI to address issues left open after the Cloud Standards Coordination Phase 1 (CSC-1) work was completed at the end of 2013, with a particular focus on the point of view of the Cloud Computing users (e.g. SMEs, Administrations).

The present document addresses the question of interoperability and security in Cloud Computing. Though the availability of Cloud Computing standards related to security and their level of maturity were considered as relatively good during Cloud Standards Coordination Phase 1, some areas of concern were remaining. The present document addresses, from the user's perspective, the relationship between interoperability and security and how a global approach to both can increase the level of trust in Cloud Computing.

1 Scope

The present document presents the initial results of the analysis of interoperability and security in Cloud Computing.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI Cloud Standards Coordination, Final Report, November 2013.

NOTE: See: http://csc.etsi.org/

[i.2] ETSI SR 003 381: "Cloud Standards Coordination Phase 2; Identification of Cloud user needs".

[i.3] "Cloud Computing Schemes List (CCSL)", ENISA.

NOTE: See: https://resilience.enisa.europa.eu/cloud-computing-certification.

[i.4] "Security, Trust & Assurance Registry (STAR)", Cloud Security Alliance.

NOTE: See: https://cloudsecurityalliance.org/star/.

[i.5] "Start Audit Certification Program", EuroCloud.

[i.6] Regulation (EU) No 1025/2012 of the European Parliament and of the Council, on European standardization, 25 October 2012.

NOTE: See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025.

[i.7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

NOTE: See: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=FR.

[i.8] European Interoperability Framework (EIF), Towards Interoperability for European Public Services.

NOTE: See: http://ec.europa.eu/isa/documents/eif_brochure_2011.pdf.

[i.9] ISO/IEC 19941 standard: "Information Technology -- Cloud Computing -- Interoperability and Portability".

[i.10] Draft ISO/IEC 19041: "Information technology - Cloud computing - Interoperability and Portability".

[i.11] Draft ISO/IEC 19044: "Information technology - Cloud computing - Data and its flow across devices and cloud services".

[i.12] ISO/IEC 17203: "Information Technology - Open Virtualization Format Specification".

[i.13] ISO/IEC 17826: "Information Technology - Cloud Data Management Interface (CDMI)".

[i.14] ISO/IEC 19099: "Information Technology - Virtualization Management specification".

[i.15] ISO/IEC 19831: "Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol - An Interface for Managing Cloud Infrastructure".

[i.16] DMTF DSP0243: "Open Virtualization Format Specification".

[i.17] DMTF DSP0263: "Cloud Infrastructure Management Interface - CIMI".

[i.18] OASIS CAMP: "Cloud Application Management for Platforms".

[i.19] OASIS TOSCA: "Topology Orchestration Specification for Cloud Applications".

[i.20] OGF OCCI: "Open Cloud Computing Interface".

[i.21] SNIA CDMI: "Cloud Data Management Interface".

[i.22] ISO/IEC 27000: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.23] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[i.24] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security controls".

[i.25] ISO/IEC 27006: "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

[i.26] ISO/IEC 27014: "Information technology - Security techniques - Governance of information security".

[i.27] ISO/IEC 27031: "Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity".

[i.28] ISO/IEC 24760-1: "Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts".

[i.29] ISO/IEC 29115: "Information technology - Security techniques - Entity authentication assurance framework".

[i.30] OpenID.

[i.31] IETF RFC 6749: "The Oauth 2.0 Authorization Framework".

[i.32] Draft ISO/IEC 27017: "Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services".

[i.33] Recommendation ITU-T X.1601: "Cloud computing security - Security framework for cloud computing".

[i.34] Draft Recommendation ITU-T X.1631: "Code of practice for information security controls based on ISO/IEC 27002 for cloud services".

[i.35] Draft ISO/IEC 19086-4: "Information technology - Cloud computing - SLA framework and terminology - Part 4: Security and Privacy".

[i.36] CSA CCM v3.0.1: " Cloud Control Matrix".

[i.37] CSA CTP: "Cloud Trust Protocol".

[i.38] CSA A6: "Cloud Audit".

[i.39] CSA CAIQ: "Consensus Assessments Initiative Questionnaire".

[i.40] CSA TCI: "Reference Architecture - Trusted Cloud Initiative".

[i.41] Draft NIST SP 500-299: "Cloud computing security reference architecture".

[i.42] NIST SP 800-125: "Guide to security for full virtualization technologies".

[i.43] NIST SP 800-144: "Guidelines on security and privacy in public cloud computing".

[i.44] ISO/IEC 29100: "Information technology - Security techniques - Privacy framework".

[i.45] ISO/IEC 29101: "Information technology - Security techniques - Privacy architecture framework".

[i.46] ISO/IEC 27018: "Information technology - Security techniques - Code of practice for PII protection in public clouds acting as PII processors".

[i.47] CSA PLA: "Privacy Level Agreement".

[i.48] OGF GFD.192: "Web services agreement specification".

[i.49] Draft OGF GFD.193: "Web services agreement negotiation specification".

[i.50] Draft ISO/IEC 19086-1: "Information technology - Cloud computing - SLA framework and terminology - Part 1: Overview and concepts".

[i.51] Draft ISO/IEC 19086-2: "Information technology - Cloud computing - SLA framework and terminology - Part 2: Metrics".

[i.52] Draft ISO/IEC 19086-3: "Information technology - Cloud computing - SLA framework and terminology - Part 3: Core requirements".

[i.53] Draft NIST SP 500-307: "Cloud Computing Service Metrics Description".

[i.54] TMF GB963: "Cloud SLA application note".

[i.55] AICPA SOC 1: "Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting".

[i.56] AICPA SOC 2: "Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy".

[i.57] AICPA SOC 3: "Trust Services Report for Service Organizations".

[i.58] Certified Cloud Service -TüV Rheinland.

[i.59] CSA Attestation - OCF Level 2.

[i.60] CSA Certification - OCF Level 2.

[i.61] CSA Self Assessment - OCF Level 1.

[i.62] EuroCloud Self Assessment.

[i.63] EuroCloud Star Audit Certification.

[i.64] Payment Card Industry (PCI) Data Security Standard v3.

[i.65] Leet Security Rating Guide.

[i.66] Cloud Industry Forum Code of Practice.

[i.67] FedRAMP.

[i.68] EIF: "European Interoperability Framework".

[i.69] ISACA COBIT: "Control Objectives for Information and related Technology".

[i.70] ISO/IEC 20000-1: "Information Technology - Service management system requirements".

[i.71] ISO 22301: "Societal security - Business Continuity Management Systems - Requirements".

[i.72] ITIL: "Information Technology Infrastructure Library".

[i.73] ISO/IEC 17788: "Information Technology - Cloud computing - Overview and vocabulary".

[i.74] ISO/IEC 17789: "Information Technology - Cloud computing - Reference architecture".

[i.75] Recommendation ITU-T Y.3500: "Information Technology - Cloud computing - Overview and vocabulary".

[i.76] Recommendation ITU-T Y.3502: "Information Technology - Cloud computing - Reference architecture".

[i.77] C-SIG: "Code of conduct".

[i.78] ISO/IEC 25010: "Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models".

[i.79] ISO/IEC 13888-1: "Information technology -- Security techniques -- Non-repudiation -- Part 1: General".

[i.80] ISO/IEC 38500: "Information technology -- Governance of IT for the organization".

[i.81] ISO 31000: "Risk management -- Principles and guidelines".

[i.82] ETSI SR 003 392: "Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

cloud service: one or more capabilities offered via cloud computing invoked using a defined interface

NOTE: Source: Recommendation ITU-T Y.3500 [i.75] | ISO/IEC 17788 [i.73], clause 3.2.8.

Cloud Service Customer (CSC): party which is in a business relationship for the purpose of using cloud services

NOTE: Source: Recommendation ITU-T Y.3500 [i.75] | ISO/IEC 17788 [i.73], clause 3.2.11.

Cloud Service Provider (CSP): party which makes cloud services available

NOTE: Source: Recommendation ITU-T Y.3500 | ISO/IEC 17788 [i.73], clause 3.2.15.

interoperability: ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

NOTE: Source: Recommendation ITU-T Y.3500 [i.75] | ISO/IEC 17788 :2014 [i.73], clause 3.1.5.

party: natural person or legal person, whether or not incorporated, or a group of either

NOTE: Source: Recommendation ITU-T Y.3500 [i.75] | ISO/IEC 17788 [i.73], clause 3.1.6.

Service Level Agreement (SLA): documented agreement between the service provider and customer that identifies services and service targets

NOTE: Source: ISO/IEC 20000-1:2011 [i.70], clause 3.29.

Standards Setting Organization (SSO): any entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining specifications and standards that address the interests of a wide base of users outside the standards development organization

Standards Development Organization (SDO): standards setting organization that has a formal recognition by international treaties, regulation, etc.

NOTE: The SDOs are a subset of the SSOs.

standard: output from an SDO (see Regulation (EU) No 1025/2012 [i.6])

specification: output from an SSO (see Regulation (EU) No 1025/2012 [i.6]) that may become a standard when ratified by an SDO

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
AUP	Acceptable Use Policy
BCP	Business Continuity Policy
CAIQ	Consensus Assessments Initiative Questionnaire
CCM	Cloud Control Matrix
CCSL	Cloud Computing Schemes List
CDMI	Cloud Data Management Interface
CIMI	Cloud Infrastructure Management Interface
COBIT	Control Objectives for Information and related Technology
CSA	Cloud Security Alliance
CSB	Cloud Service Broker
CSC	Cloud Service Customer
CSC-1	Cloud Standards Coordination Phase 1
CSC-2	Cloud Standards Coordination Phase 2
C-SIG	Cloud Select Industry Group
CSP	Cloud Service Provider
CTP	Cloud Trust Protocol
DMTF	Distributed Management Task Force
EC	European Commission
EIF	European Interoperability Framework
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
HTTPS	HyperText Transfer Protocol Secure
IAM	Identity and Access Management
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MSA	Master Service Agreement
NIST	National Institute of Science and Technology
OASIS	Advancing Open Standards for the Information Society
OCCI	Open Cloud Computing Interface
OCF	Open Certification Framework
OGF	Open Grid Forum
PaaS	Platform as a Service
PCI	Payment Card Industry
PII	Personally Identifiable Information
PLA	Privacy Level Agreement
QoS	Quality of Service
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
SDO	Standards Development Organization
SIG	Special Interest Group
SLA	Service Level Agreement
SNIA	Storage Networking Industry Association
SOC	Service Organization Control (AICPA)
SSO	Standards Setting Organization
STAR	Security, Trust & Assurance Registry
STF	Specialist Task Force

NOTE: An ETSI structure for internal projects.

STS	Security Token Service
TCI	Trusted Cloud Initiative
TMF	TeleManagement Forum
VPN	Virtual Private Network
WP	Work Package
XML	Extensible Markup Language

4 Interoperability and Security in Cloud Computing

4.1 Context

The Cloud Standards Coordination project

Cloud Standards Coordination Phase 1 (CSC-1) took place in 2013 as a community effort supported by ETSI and primarily addressed the Cloud Computing standards roadmap. In December 2013 the results were publicly presented in a workshop organized by the European Commission (EC).

The Final Report [i.1] of Cloud Standards Coordination Phase 1 provides a snapshot on the Cloud Computing standardization landscape at the end of 2013. It is available at:

- See: http://csc.etsi.org/

Cloud Standards Coordination Phase 2

Given the dynamics of the Cloud Computing market and standardization, Cloud Standards Coordination Phase 2 (CSC-2) was launched in February 2015 with, in particular, the objective of producing an updated version of the standards maturity assessment (i.e. a "snapshot") of the Cloud Computing standardization landscape. CSC-2 aims to better take into account the needs of Cloud Computing customers on their Cloud related requirements and priorities. This will help CSC-2 to further assess the maturity of Cloud Computing standards and evaluate how standards can support the Cloud Computing customers' priorities.

Interoperability and Security in Cloud Computing

Security was one of the points of attention of Cloud Standards Coordination Phase 1. Though the availability of Cloud Computing standards related to security and their level of maturity were considered as relatively good, some areas of concern were remaining.

The topic of Security in Cloud Standards Coordination Phase 2 was addressed in several of the questions included in the CSC-2 web survey report (see [i.2]). Security is consistently ranked as one of the top user concern. The following remark is made in the report:

"Security" in general is without doubt a major concern for most users, customers and providers alike, in particular in a Cloud setting, as the resources typically are shared and the data integrity as a consequence needs additional attention to ensure a retained confidence in regard of the ownership of data aspects. Many users are concerned about "losing the control of data", in many cases probably justifiably so. Unless Security - all relevant aspects of Security related to Cloud Computing - is fully addressed and the users are made aware of available options and existing protocols and standards that can be used to build reliable Cloud Computing offerings, the adoption of Cloud Computing is likely to continue to grow slowly".

The present document addresses interoperability and security in Cloud Computing. The analysis is based on a number of high-level user scenarios and a description of core concepts identified as relevant for all user scenarios. The present document further presents existing standards relevant for the high-level user scenarios and the core concepts identified.

4.2 Objectives

The main objectives are to:

- Identify and present high-level user scenarios that together provide a sufficient base for presentation of role and importance of and relationship between interoperability and security.
- Identify and present the core concepts covered by the user scenarios.
- Present related existing standards.
- Provide conclusions based on the analysis presented before.

4.3 Content of the present document

Clause 5 of the present document presents some high-level user scenarios in the present document that are included to illustrate and describe the role and importance of and relationship between the core concepts interoperability and security in particular.

Clause 6 presents the core concepts referred to in clause 5, namely Interoperability, Portability, Security, and its sub-areas, and Service Level Agreements.

Clause 7 lists identified existing standards and certification schemes for Interoperability, Portability, Security and Service Level Agreements.

Clause 8 highlights preliminary conclusions and recommendations from the analysis presented in the present document.

Clause 9 suggests some areas for further work.

5 High-level user scenarios for interoperability and security

5.1 Introduction

This clause presents some high-level user scenarios that are included in the present document in order to illustrate and describe the role and importance of the relationship between interoperability and security. Please note that the list of scenarios obviously is far from exhaustive. It only serves the purpose of highlighting some but certainly not all of the cases where security and interoperability are important issues in the Cloud Computing space.

The purpose of the clause is to place the "core concepts" in context. Core concepts are key "transversal" aspects (sometimes called "non-functional" or "cross cutting aspects") that need to be coordinated and implemented consistently in a Cloud Computing system. These core concepts typically have an impact on many areas in a Cloud Computing system, such as Cloud services, business processes, operational systems, and have to be considered in all engineering phases of a Cloud Computing system (i.e. from supported use cases, required capabilities and their design, implementation and deployment). The Core Concepts are further elaborated in clause 6.

NOTE: The purpose of scenarios presented is not to present a comprehensive list of use cases, concepts, requirements and concerns related to the core concepts listed in the scenarios. The purpose is to illustrate and disclose how some well-known aspects need to be understood and in most cases addressed through the provision of standards, solutions and/or certification schemes that target individual areas of the scenarios.

For the following presentation the same structure is used for describing the scenarios:

- Questions are included to prepare the ground for a more elaborate description of the scenarios, presented as high-level use cases and followed by a presentation of high-level requirements.
- Based on this the core concepts covered by the scenario and other relevant aspects are identified.
- Finally, conclusions and remarks summarize the scenario.

5.2 Scenario 1: Moving data from and between Cloud Service Providers

Example of questions to illustrate the scenario:

- "I want to retrieve my data from my Cloud Service Provider".
- "I would like to move from a Cloud Service provider to another - can I move my data?"

Scenario description:

This scenario covers two different use cases:

1) In the first Use Case, the Cloud Service Customer (CSC) wants to retrieve all data that is handled by the Cloud Service Provider (CSP), physically moving the data from the CSP to the CSC's own systems (either on-site or to a designated outsourcing partner).

2) In the second Use Case, the CSC wants to move its data residing at a particular CSP from the current CSP to another CSP.

High- level requirements:

The motive for the data transfer is different in the two Use Cases, but the underlying criteria, needs and requirements are quite similar. In order to meet the request of the CSC, many individual capabilities of the Cloud service have to exist and the related obligations and activities should be mutually agreed upon, captured in a Cloud Service Level Agreement (SLA) or corresponding agreement (contract) set up between the CSC and the CSP. It is also critical to understand the implications of any legislation or regulation in effect, that is relevant for the data migration. This is particularly important if the data is to be moved over geographies with different overarching legislation, e.g. from any member states within the European Union to a country outside the EU.