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

SPECIAL REPORT

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 Certifies 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.

In order to be able to act on the CSC's request, at minimum the following requirements and capabilities most likely have to be supported:

1) Cloud Service Level Agreement (Cloud SLA):

   The contract, typically manifested in a Cloud SLA, between the CSC and the CSP should define the obligations of the CSP in terms of providing the CSC's data, with definitions of e.g. response time, data categories and taxonomies covered by the agreement, exchange and removal of audit trail (log) data and more. A particular important aspect of the Cloud SLA pertinent to this scenario is that it should also define the obligations of the CSP regarding safe erasure of all data of the CSC after the CSC has moved off its data from this CSP's infrastructure, including both data belonging to the CSC as well as derived data resulting from using the CSP's cloud service (such as audit trails etc.). Besides the cost of storing the data, the Cloud SLA should also stipulate the cost model for moving off the data.

2) Data portability:

   A basic prerequisite for this scenario is that the requirements for data portability have been met, between the CSP and the CSC (use case 1) and between the old CSP and the new CSP (use case 2), respectively. To facilitate data portability, adequate interoperability need to exist. Interoperability at semantic, syntactical and technical levels will facilitate an effortless transfer of data. Even if only semantic interoperability exists, data portability at syntactical level and technical can be achieved using data mapping tools (mapping data from one syntax to another, e.g. from XML to semi colon delimited text file formats) and transport protocol mapping tools. However, if the data models defining the data semantic are substantially different, the data transfer will most likely be difficult and cumbersome to achieve. Aspects of data portability and interoperability are detailed in the upcoming ISO/IEC 19941 standard [i.9].

3) Data ownership and data definitions:

   In order to offer transfer of data, the data itself need, of course, to be defined, stored and generally handled in such a way that a migration of data can be executed without any significant extra work. In order to achieve this, semantic, syntactical and technical interoperability have to be ensured and to exist in order to facilitate data portability. This in turn requires both the CSC and CSP to establish and agree upon on some basic data classification and taxonomy principles, including (but not restricted to):

   - defining data ownership, i.e. defining the data that belongs to the CSC and the CSP, respectively,
   - classification of data (e.g. according to criticality),
   - defining and enforcing data integrity and security policies.

   As pointed out above, in order to define and establish a clear separation between the CSC data and data that belongs to the CSP, all aspects of ownership of data need to be understood. Concepts such as "derived data" and "audit trails" (resulting from data operations) are particularly critical in this respect. The responsibilities pertinent to data management are generally captured in the Cloud SLA, but it falls on both the CSC and the CSP to ensure that all aspects of secure and controlled data management are in place before the Cloud service offered by the CSP becomes operational.

4) Data protection:

   Ensuring that the data belonging to the CSC is well protected by the CSP that provides the Cloud service used by the CSC is a fundamental key capability in Cloud Computing. In the relationship between the CSC and the CSP, the responsibilities and related measures needed to ensure that the CSC's data is secure and protected is typically described in the Cloud SLA (or other form of contract between the parties involved in the Cloud service). A particularly important aspect is the potential use of encryption (together with key management) to further secure and protect the data of the CSC, both during the operation of the cloud service provided by the CSP as well as during the transfer of data (as defined in the two use cases comprising this scenario). As with the definition of Data, it is important that the responsibilities and tasks are well defined and understood by all stakeholders (including the use of any third party vendors providing, e.g. solutions for encryption of data).

   The CSP should offer security and privacy enhanced mechanisms for data protection providing capabilities that allows the CSC to monitor the use and encryption of data owned by the CSC.

   Finally, Data protection also involves ensuring that back-up data is well protected, typically as part of as disaster-recovery or contingency plan.

5) Identity and Access Management (IAM)

Identity and Access Management (IAM) is concerned with the following:

- Authorization and security policy management:

  This function is further described in clause 9.5.2.2.2 of the Cloud Computing Reference Architecture standards commonly published as ISO/IEC 17789 [i.74] and Recommendation ITU-T Y.3502 [i.76].

  A critical aspect of data exchange in Cloud scenarios is the provision and use of authorization and security policy management. This aspect covers e.g. who is authorized to access data, how the authorization should be carried out, integration with and enforcement of the CSC's security policies, general data management and more. Authorization and security policy management belong to the security systems related multi-layer functions according to the Cloud Computing Reference Architecture standard (see Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74]).

- Authentication and identity management:

  This function is further described in clause 9.5.2.2.1 of the Cloud Computing Reference Architecture standards commonly published as ISO/IEC 17789 [i.74] and Recommendation ITU-T Y.3502 [i.76].

  A secondary function of data management is the authentication and identity management functionality provided by the CSP. This function allows the CSC to securely access the services and related data provided by the CSP. Authentication and identity management belong to the security systems related multi-layer functions according to the Cloud Computing Reference Architecture standard (see Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74]).

- Access control:

  Access control is the collective term for the function that governs and controls the access of users to Cloud services. "Access control limits users to the use of particular services. Principally, access control involves the authentication of a user through the presentation and validation of credentials, followed by the authorization of this authenticated user to use specific services. Associated with this is identity management" (quote from the Cloud Computing Reference Architecture standard, Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74]). Access control in the access layer uses capabilities of the multi-layer functions manifested as functional components (e.g. those described above in the previous bullet items). All aspects of access control need to be defined in the Cloud SLA or similar contract that defines the obligations and responsibilities of the CSP (and the CSC).

6) Certification:

For CSCs, it is necessary to be able to rely on the Certification of CSPs as a step towards selecting only those CSPs that offer Cloud Services that meet the criteria necessary to ensure a smooth data migration. Certification allows the CSP to provide commitments on aspects such as security, and privacy, portability and interoperability enabling a CSP to pick a suitable CSP.

The level of complexity in this scenario will obviously depend on the type of data that is subject to migration. Data transfer of critical and sensitive information will obviously require more attention and most likely more work than migration of low value and non-critical data. When planning for the data transfer, existing data classification and data categorizations might provide valuable reference points for assessing the workload and subsequent activities needed for the transfer. The data volume and the infrastructure (such as available bandwidth) also factor in.

Core concepts covered by the scenario:

Disclaimer: please note that the core concepts (cross cutting aspects) presented in this clause are examples of concerns. Other concerns might also be relevant. The list of core concepts is presented to illustrate the issue presented in the respective clauses, without the intention to provide an exhaustive and complete list of core concepts.

Data Portability, Data Integrity, Data Protection, Interoperability (primary semantic and syntactical), Certification, Identity and Access Management (IAM), Cloud SLA.

Other aspects:

Contract, Conformance, legislations/legality.

Conclusions and remarks:

This scenario exposes the many facets of data portability and security in Cloud Computing, where complex dependencies and many different requirements need to be understood and met. Given the multi stakeholder nature of Cloud Computing, the requirements might not only concern one single actor, but typically span several actors, roles, sub roles and activities, adding to the complexity.

Interoperability, in particular, but also the capabilities (or limitations) of Portability and Security are inherent to Cloud Computing. It can be argued that for Cloud Computing to be successful, all aspects of Interoperability, Portability and Security have to be fully understood, addressed and covered. This, in turn, demands the availability of mature, transparent, easy-to-use and fully covered functionality support manifested in standards and certification schemes that are adopted by all users and providers of Cloud services.

5.3 Scenario 2: Retrieving Customer data in case of Service Provider failure

Example of questions to illustrate the scenario:

- "What happens to my data when the Cloud Service is no longer available"
- "I want to retrieve my data when the Cloud vendor has gone bankrupt"

Scenario description:

The scenario addresses the issue of a Cloud Service Customer (CSC) who needs to retrieve its own data in case its Cloud Service Provider (CSP) cannot provide the service for a reason that can be dealt with by a recovery plan (e.g. major natural disaster, pressing financial difficulties, legal obligations) or may be hard to deal with at all (e.g. bankruptcy).

High-level requirements:

In this scenario, there is a need to move data from the "problematic" CSP back to the environment controlled by the CSC: this is largely dealt with in the previous scenario that addresses this in "nominal" conditions. To a large extent, what has been defined in that scenario also applies to this one.

However, some specific aspects of this scenario relate to the kind of "emergency action" required, which in turn lead to some specific requirements and capabilities:

1) Cloud Service Level Agreement (Cloud SLA):

   Beyond the definition of the normal obligations between the CSC and the CSP regarding the provision of the CSC's data (e.g. response time, data categories and taxonomies covered, etc.), the Cloud SLA should also define the legal obligations related to the termination of the contract in case of involuntary circumstances. The Cloud SLA should include a contingency plan that covers the activities that should be executed in case of unplanned service unavailability.

2) Data definitions:

   In order to offer transfer of data, the CSC and CSP need to agree on the way the migration of the data will be handled without any significant extra work for the CSC. In particular, it requires that the CSC and the CSP agree upon data taxonomy principles, data ownership, data classification (e.g. criticality), data integrity, security policies and more. Responsibilities regarding data management are defined in the Cloud SLA, but this work on data is a critical element of the prior work for both the CSC and the CSP.

3) Data protection:

   The data belonging to the CSC needs to be well protected. This is typically described in the Cloud SLA but important aspects such as use of encryption has to be well defined and understood by all stakeholders (including the use of any third party vendors providing, e.g. solutions for Encryption of data).

4) Certification:

A CSP involved in this scenario may not be a large actor that has a lot of protection in place against a variety of negative circumstances, but more likely a small or medium size CSP. In case a CSC wants to establish a contract with a CSP with that profile, the CSC should be able to rely on a Certification of the CSPs that meet the criteria necessary to ensure an emergency data migration.

Core concepts covered by the scenario:

Data Protection, Certification, Cloud SLA.

Other aspects:

Contract, legislations/legality.

Conclusion and remarks:

In this scenario, the definition of the Cloud SLA is critical. The applicability of the Cloud SLA will be guaranteed in the case of "emergency events" only if a prior work has been done on the nature of CSC data, a contingency plan has been carefully elaborated, and the legal obligations that apply to the CSP in this particular setting have been defined. However, even with a Cloud SLA in place and mechanisms in place to control the metrics defined in order to gauge the terms of the Cloud SLA, it might be necessary to add additional measures to safeguard against data loss. These might include continuous data back-up to the on-site IT environment of the CSC, back-up of the CSC's data to a secondary CSP and more. The data classification (i.e. the "value" of the data) will probably determine the level of additional measures that might be considered as contingency measures in order to prevent data loss in this scenario.

5.4 Scenario 3: Using on-premises identity and access management in the Cloud

Example of questions to illustrate the scenario:

- "We have got a great way of handling our co-workers access to our existing legacy system with Single-Sign-On to all systems - can I do that in the Cloud?"
- "Is any user data stored in the Cloud when we're moving our identity and access management (IAM) solutions to the Cloud?"

Scenario description:

- This scenario covers one use-case at two levels:
  - At the first level the CSC wants to extend its Single-Sign-On solution to include support for accessing systems in the Cloud and asks whether its current solution is supported in the Cloud service offered by a CSP.
  - At the second level the CSC wants to understand whether user data (related to IAM) is stored in the Cloud once its IAM solutions are moved to the Cloud and used in the Cloud.

High-level requirements:

The level of concretization increases from scenario level 1 to level 2 but the underlying criteria and high-level requirements are the same. Additionally level 2 addresses concerns related to the data protection (privacy) of the CSC's user data when its IAM solutions are used in a Cloud environment. User data here refers to the identity data artifacts needed to verify the identity of a user.

In order meet the request of the CSC, the CSP needs to provide a secure and trustworthy multi-tenant environment, where a secure environment implies isolation of the different CSCs and prevention of misuse of the Single Sign-On solution of one CSC by another CSC to gain access to privileges bound to an identity. Trustworthiness of the CSP is essential to address concerns of the CSC regarding the user data artifacts needed to verify the identity of a user that will be processed by the identity access solutions deployed into the Cloud. Potentially this data will be stored temporarily during processing (i.e. while authenticating the users) and needs to be protected against unauthorized access during that time and completely removed afterwards.

Other issues may arise from the geographical location of the Cloud infrastructure due to the different overarching legislation, e.g. in different member states within the European Union or in a country outside the EU. Related obligations and activities should be mutually agreed upon, captured in a Cloud Service Level Agreement for the CSP's Cloud service acquired by the CSC and/or a contract set up between the CSC and the CSP. In order to satisfy the CSP's request, at minimum the following requirements and capabilities most likely will have to be supported:

1) Cloud Service Level Agreement (Cloud SLA):

   The Cloud Service Level Agreement (and/or contract) between the CSC and the CSP should define the obligations of the CSP in terms of security and data protection.

   > As of mid 2015 there is no European directive on electronic contracts that specify rules for legally binding electronic Service Level Agreements. In general there are two approaches: one that considers the SLA as such as a binding contract, e.g. as proposed by the TeleManagement Forum. The other approach requires an additional binding contract and considers the SLA as the agreed-upon service description, e.g. as proposed by the C-SIG SLA.

   Standardized metrics defined with an interoperable language are required to express the level of security and data protection. As of mid 2015 these standardized metrics do not exist yet. However, there are metrics available defined and used in European projects like, e.g. metrics for data protection in OPTIMIS, or metrics for Security Level Agreements, as currently being developed in the European project SPECS together with a working group of the Cloud Security Alliance, or the related terminology proposed by the NIST RATAX working group (and also being adopted by ISO/IEC SC38 for the 19086-2 [i.51]).

2) Data protection (privacy):

   Ensuring that the CSC users' identity data is well protected is yet another fundamental key capability of Cloud services required in Cloud Computing. In the relationship between the CSC and the CSP, the responsibilities and related measures needed to ensure that the CSC's data is secure and protected is typically described in the Cloud SLA (or other form of contract between the parties involved in the Cloud service). A particularly important aspect is the potential use of encryption during data movement and potentially temporary storage of identity artifacts to further secure and protect the data of the CSC. The goal is to establish end-to-end encryption of the identity data, which should only be decrypted when processed by the CSC's identity access solutions deployed into the Cloud. Secure management of encryption is paramount and needs to have at least the same level of protection as the identity data.

3) Identity and Access Management (IAM):

   - Authorization and security policy management:

     This function is further described in clause 9.5.2.2.2 of the Cloud Computing Reference Architecture standards commonly published as ISO/IEC 17789 [i.74] and Recommendation ITU-T Y.3502 [i.76].

     - A critical aspect of data exchange in Cloud scenarios, here exchange of identity data, is the provision and use of authorization and security policy management. This aspect covers e.g. who is authorized to access data, how the authorization should be carried out, integration with and enforcement of the CSC's security policies, general data management and more. Here again Cloud SLAs and certification is a key concern.

   - Access control:

     - Access control is the collective term for the function that governs and controls the access of Cloud services, here the deployed IAM solutions of the CSC. The Access control layer of the CSP needs to reliably separate its different CSCs in the multi-tenant environment.

4) Certification:

   As described before: for Cloud Customers it is necessary to be able to rely on the certification of CSPs as a step towards selecting only those CSPs that offer Cloud Services that meet the criteria necessary to ensure a trustworthy environment that meets the required level of protection.

The level of complexity in this scenario will obviously depend on the type of IAM solutions that are used. Transfer and processing of critical and sensitive user information will obviously require more attention to the security measures taken by the CSP and the corresponding certification.

Core concepts covered by the scenario:

Disclaimer: please note that the core concepts (cross cutting aspects) presented in this clause are examples of concerns. Other concerns might also be relevant. The list of core concepts is presented to illustrate the issue presented in the respective clauses, without the intention to provide an exhaustive and complete list of core concepts.

Data Integrity, Data Protection, Identity and Access Management, Interoperability (at several levels), Portability, Certification, Cloud SLA.

Other aspects:

Contract, Conformance, legislations/legality.

Conclusions and remarks:

This scenario exposes facets of identity management in Cloud Computing when trying to integrate existing on-premises solutions with Cloud service environments.

Issues comprise the following:

- the security of the CSP's multi-tenant infrastructure,
- the Service Level Agreement between CSC and CSP to reflect the security requirements,
- the interoperability and portability required for smooth operations of the identity management solution when deploying it into the Cloud, and
- the protection of user identity data against corruption or forgery during transport or temporary storage, or the protection of identity information against intentional or unintentional theft and misuse.

Besides dedicated Cloud SLAs, the availability of CSP Certification schemes might ensure the CSC that the CSP is compliant with all aspects that are needed to verify that all security measures are in place and addressed. The CSP's level of compliance to and use of standards (where available and applicable) should also be made visible for the CSC.

5.5 Scenario 4: Ensuring security in Hybrid Cloud environments

Example of questions to illustrate the scenario:

- "How do I ensure that security is retained when I mix services that are provisioned by our own IT department and services that are provided by Cloud vendors?"

Scenario description:

This scenario relying on a "Hybrid Cloud" deployment model describes a very typical situation within companies of all size when Cloud Services get combined next to existing, own operated IT.

Typical for those Hybrid Cloud based environments is the combination of different provisioning models, where:

- Some parts of the customers "On Premise IT" may still be operated the traditional way on dedicated infrastructure.
- Other parts of customers On Premise IT may already be operated on own virtualized infrastructure and provided to the users on a consumption basis (Private Cloud).
- Further Public Cloud based services - often provided by different external CSP - may complete the customers IT landscape.

In those scenarios IT departments get challenged in their needs to ensure data privacy, data security and data integrity and the fulfilment of legal obligations. Another challenge to them is the need to monitor and manage these IT services according to the underlying service levels contracts.

High-level requirements:

1) Cloud Service Level Agreement (Cloud SLA):

   With view on the utilized Public Cloud Services the contractual Cloud SLAs are of most important and need to be considered before contract signature. Depending on CSC's sensitivity of data used or generated with a particular Cloud Service and in respect of interoperability requirements with other CSP's Public Cloud Services and/or the CSC's own operated Private Cloud or On Premise IT.

   Next to the typical SLA's like service availability, response time, data categories and other typical taxonomies also the Cloud specific SLA requirements have to be taken into account: The legal obligations, the location of the involved datacenter(s), the format and method of how CSC's data get returned at contract end or in case of unforeseen circumstances. The complexity of monitoring the Cloud SLA fulfilment rises, as far as several CSPs are providing different Cloud services with different Cloud SLAs and may be further affected in case of data exchange between those Public Cloud Services and the own operated Private Cloud and/or the own operated traditional On Premise IT.

2) Data definitions:

   Large enterprises might have defined, classified and categorized the data used by the organization. For SMEs this is more rarely the case. With the introduction of Cloud Services in general, but specifically for Hybrid Cloud environments, having control of data and understanding the nature of the data and its importance based on categorization, definition (taxonomies) and classification is however a critical factor. In order to set the appropriate data protection levels and to contractually state the corresponding terms in the Cloud SLA, one needs to understand and be able to discriminate all relevant data aspects needed according with the aspects mentioned in this paragraph.

3) Data protection:

   Typically CSCs base their decision for a single Cloud Service on the identification of functional requirements and involved financial means, while the classification and qualification of derived and user data is not always taken into account. But when data protection aspects need to be considered, there is no way around a serious data classification and qualification, specifically in a Hybrid Cloud environment with data exchange between Private and Public Cloud.

   The more sensitive the data, the more focus should be placed on data protection of course, which in Hybrid Cloud environments very likely results in specific requirements that are imposed on the involved CSPs to ensure the necessary levels of Cloud SLA data protection, e.g. by applying data encryption. At the same time the quality level of the involved IAM) solution(s) and the network security between the CSC and the CSP need to be considered.

4) Identity and Access Management (IAM):

   - Authorization and security policy management:

     In On-Premise IT environments (specifically when data is exchanged internally or externally), the need for a well defined IAM and Security Policy Management is given. However, the need increases when Cloud services are introduced. This is especially true in complex Hybrid Cloud environments, where Private and Public Cloud Services are combined and integrated with On-Premise IT. Subsequently, the need for the enforcement of clearly defined IAM and Security Policies becomes mandatory (including definitions of who is allowed to do what and when under which preconditions).

   - Authentication and Identity Management:

   - Hybrid Cloud environments often require a high level of authentication to be provided by the involved Identity and Access Management (IAM). CSPs are well advised to provide adequate interfaces to connect to IAM solutions.

   - Next to the higher level of authentication security, IAM allows a defined permission management for a wide range of connected services and usually allows access control. At least in large CSC organizations the IAM appears to be part of an operational framework, which allows the management of the entire IT landscape.

5) Certification:

Hybrid Cloud environments, specifically the combination of Private and Public Cloud Services easily become complex and appear as challenge for non-IT experienced customers in their identification of reliable and trustworthy cloud providers.

Customers are responsible for their own data. In some European countries customers are legally obliged to prove the trustworthiness of a provider before signing a contract. But how at all are CSCs able to verify the trustworthiness of CSPs, as quite often a particular Cloud Service is provided due to the collaboration of various (internationally spread) partners along the value chain? Large enterprises typically can rely on internal IT expertise for such an assessment, while SMEs mostly are unable to meet their (legal) obligations in this regard.

Quality Cloud Certifications with a defined scope and audited by accredited experts can be most helpful in the decision phase for a Cloud Service from a reliable and trustworthy CSP.

Next to the important Data Security and Data privacy aspects, Cloud Certifications need to cover the embodiment of legal and contractual aspects, specifically the coverage of Cloud SLAs and the processes across all partners involved in the provision of a particular cloud service.

Under the first objective of the EU Cloud Strategy, the EC together with the Cloud Select Industry Group (C-SIG) and ENISA have setup the Cloud Certification Schemes List (CCSL) [i.3].

Core concepts covered by the scenario:

Cloud SLA, Identity and Access Management, Trust, Data Integrity, Data privacy, Interoperability, Certification.

Other aspects:

Conformance, contract, legislations/legality.

Conclusions and remarks:

The Hybrid Cloud Scenario is probably the most commonly used, as the combination of Private and Public Cloud Services together with remaining parts of the traditional dedicated IT landscape and might be further completed by aspects as described in the other use case scenarios.

Documented so far is the impact on the organization providing the combined service, where the traditional role of IT departments as the operator and administrator of the internal IT changes. With Cloud Services, it is likely that the IT department will change its role to become an IT Broker, who on the one hand needs to orchestrate a broad range of Private and Public cloud services, while obligated to stay flexible in order to meet the growing needs and requirements of the enterprise's operational departments. This, in turn, will probably require new or updated frameworks for governance and lifecycle management, supporting the production, provision and management of ICT services that are both internal as well as external to the organization responsible for governance and life cycle management. To securely "mix and match" cloud services that run in both private and public cloud environments, the control of all resources compromising the cloud services need to be fully supervised and managed. The overarching control should be monitored and measured against the terms laid out in a SLA, where in particular the Privacy and Security requirements are given special attention.

5.6 Scenario 5: Ensuring portability and interoperability when migrating from a PaaS Cloud Service Provider to another

Example of questions to illustrate the scenario:

- "If I choose to run my development of innovative solutions based on a single Cloud Vendor's platform, how do I secure that the solutions developed are useful in other 'Clouds' as well?"

Scenario description:

This scenario covers the following use case:

> The Cloud Service Customer (CSC) develops, tests and runs an innovative application using the PaaS services provided by a Cloud Service Provider (CSP), called here "origin PaaS CSP". The CSC wants that this developed innovative application can be deployed and run in other "target PaaS CSPs", i.e. that this application be then easily portable to cloud platforms of other CSPs.

The set of services provided by the "origin PaaS CSP" and the ones provided by a "target PaaS CSP" may be different potentially leading to modifications being necessary to the application software developed by the CSC when migrating the application from the "origin PaaS CSP" to the "target PaaS CSP" in order to deal with these differences.

In some cases, the "origin PaaS CSP" may support only limited and sometimes proprietary languages, libraries, etc. thus forcing the CSC to develop application architectures dictated by features offered by the "origin PaaS CSP". The CSC might face having its developed application being locked to that "origin PaaS CSP" and therefore being almost impossible to port it to other "target PaaS CSPs".

Furthermore, the application execution environment of the platforms used by the "origin PaaS CSP" and the ones used by the "target PaaS CSP" can also substantially differ making portability of the application difficult. The interface between cloud applications and the Cloud Computing platform they run on is known as the Application Programming Interface (API). It is the mechanism by which a cloud application actually uses the features and services provided by the Cloud Computing platform. If the PaaS platform is proprietary, services running on top of it will run exclusively (have high dependencies) on that Cloud Computing platform. If compatible PaaS platforms are offered by multiple cloud service providers, CSCs that run cloud based applications on that platform can move their applications across cloud platforms providing the same PaaS interfaces with relative ease.

In this context, the ability to easily transfer the application developed by the CSC from the "origin PaaS CSP" to another "target PaaS CSP" and run this application in the "target PaaS CSP" corresponds to what is called "application portability" which becomes a key requirement in this scenario. What should be avoided is the necessity of making significant changes to the application software when migrating between different CSPs. If the "origin PaaS CSP" provides the CSC developing an application with access to "commonly" used runtime execution environments, programming languages and middleware, then the risk of having application portability issues may decrease.

Other aspects to consider include:

- The potential differences in terms of the PaaS APIs exposed by the "origin PaaS CSP" and the "target PaaS CSP" which may lead the CSC to have to adapt when migrating between such PaaS CSPs.
- Data portability issues when migrating from the "origin PaaS CSP" to a "target PaaS CSP" which should in any case be considered although for PaaS, the CSC is typically in control of data managed by the application.

High-level requirements:

Concerning the described scenario, at minimum the following requirements and capabilities most likely have to be supported:

1) Interoperability:

   This covers interoperability of PaaS APIs and corresponding tools used by the CSC to develop, upload, deploy and manage the application (and its code) in a PaaS CSP. When migrating from the "origin PaaS CSP" to another "target PaaS CSP", the tools used by the CSC which are consuming the PaaS APIs provided by "origin PaaS CSP" need to be able to connect to the PaaS APIs provided by the "target PaaS CSP".

2) Application portability:

   The ability to deploy and run a CSC's application from one PaaS CSP to another PaaS CSP with minimal disruptions is a key requirement.

3) Certification:

   For the CSC it is important to be able to rely on the Certification of PaaS CSPs as a step towards selecting only those CSPs that offer PaaS services that meet in particular the criteria necessary to ensure appropriate application portability requirements of the CSC.

Core concepts covered by the scenario:

Interoperability, Application Portability, Certification.

Other aspects:

Contract, legislations/legality, Conformance.

Conclusions and remarks:

This scenario presents some critical aspects of interoperability and application portability issues when moving a CSC developed application from one cloud PaaS platform to another one.

Formal (standard based) or informal (provider specific) "conformance" procedures might be set up to ensure that, in this context, the portability through the PaaS API can be validated and verified before the actual transfer (migration) is executed. Validation of standards and/or openly available specifications that are used to offer portability can be provided by the organization that is responsible for the standard/specification on which the API is constructed. Validation and verification tools might also be provided through third party vendors. Conformance can of course also be part of and supported by certification schemes, where conformance testing might be included in the accreditation process.

NOTE: Conformance, in general, is problematic since Cloud services might be conformant at certain levels (e.g. technical and semantic levels), while still non-conformant at others (e.g. process and legal levels). However problematic, the issue of conformance including support for validation and verification of the technologies involved in securing the portability between PaaS platforms should be addressed when the CSC is procuring a Cloud service. Conformance might also be implemented partially, for example conformance in terms of moving data between different PaaS platforms only but not for application portability.

5.7 Scenario 6: The Cloud as an hybrid innovation platform

Example of questions to illustrate the scenario:

- "Can I have a specific Cloud environment that is extensible to accommodate for my own devices?"

Scenario description:

Cloud Computing is often presented as a new innovation platform, in particular for enterprises. For example, Cloud Computing allows users to employ the resources of a Cloud Service Provider for hosting (a part of) its Research and Development environments. In some cases, it may be necessary to share the resources between those that will be provided by the CSP (e.g. simulation, massive computing, large-scale testing, etc.) and those that will be on the Cloud Service Customer premises (e.g. specific appliances, "things", etc.) for reasons of confidentiality.

High-level requirements:

In the "simple" case where the Cloud Service Customer (CSC) wants to use the Cloud Service Provider (CSP) environment to outsource a part of its R&D, a number of requirements have to be met regarding the CSLA, the Data Protection, etc. This is a rather classical setting for a CSC to CSP relationship.

In the "hybrid innovation platform" scenario, a number of additional requirements have to be met to satisfy the more complex CSC requests. Some resources have to be interoperable across the CSC and CSP environments in a secure and trustworthy manner. This means that the supported levels of interoperability (e.g. networking, data models) have to be defined and guaranteed. On top of this, the access to some confidential user data (appliances or applications characteristics, settings, configurations, etc.) and the transient presence of this information on the CSP environment has to be controlled, in order to ensure that it will be securely processed, stored and removed. This is involving the following requirements and capabilities:

1) Cloud Service Level Agreement (Cloud SLA):

   The Cloud SLA between the CSC and the CSP should define the obligations of the CSP in terms of interoperability, data protection and security. This should be supported by defining values for standardized metrics in those aspects.

2) Interoperability:

The required interoperability of devices across the CSC and CSP environments will result in the need for the CSP to support a certain number of protocols and data models. In some cases, these elements may not be in the basic offering of the CSP and may require additional efforts from the CSC and Cloud SLA adaptations.

3) Data protection:

Beyond what is described in the Cloud SLA, an important key capability that needs to be defined to ensure that the CSC data is well protected is the CSP's technical support to data protection coming from the potential use of encryption during data movement, or temporary data storage in order to support end-to-end encryption of the CSC data (including the CSC user's data). To support this, certification may be needed.

4) Identity and Access Management (IAM):

IAM is a key element in this scenario: who is authorized to access data, how the authorization is carried out and enforced within the CSP's environment. Cloud SLAs and certification schemes could support this core concept.

5) Certification:

As described above, the certification of CSPs regarding Data Protection, Authorization, etc. is an important element in the selection of the CSPs that support this scenario.

Core concepts covered by the scenario:

Data integrity, Data privacy, Interoperability, Identity and Access Management, Certification, Cloud SLA.

Conclusions and remarks:

For this scenario, as for many of those that involve the need for a high level trust from the CSC in the CSP, the CSP's measures for protection of sensitive data is a key criterion for the set-up of a successful solution. It is expected that certification of the CSP will provide decision support for the CSC.

Another aspect of this scenario is the support of interoperability and what is required to support a large range of protocols and data models in a hybrid deployment model. The basic question here is whether or not it is profitable for a CSP to go beyond the "one-size-fits-all" schema supporting basic protocols and data models.

5.8 Scenario 7: Conformance of Cloud Service Providers to Data Protection Regulation

Remark:

This scenario differs from the other scenarios in the present document and is in essence rather an "analysis" than a scenario, that highlights some, but far from all implications of the new General Data Protection Regulation that need to be understood by Cloud Computing stakeholders, in particular Cloud Service Providers.

Example of questions to illustrate the scenario:

- "How can I trust the Cloud service provider to be conformant to the EU's proposed General Data Protection Regulation?"

Scenario description:

This scenario concentrates on one of the major changes between the between the existing Data Protection Directive and the proposed EU General Data Protection Regulation (GDPR) which is the extension of the responsibilities for Personal Data from the data owner, e.g. the Cloud Service Customer (CSC) to all third parties processing such data, i.e. the Cloud Service Provider (CSP). This and further changes due to the proposed Regulation lead to modifications in the relationship between the CSC and CSP in regards to the adequacy of the provided Cloud services with respect to legal aspects.

NOTE: Personal Data is defined in EU Data Protection directive (see article 2a, [i.7]) as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Another term similar to "personal data" is "Personally identifiable information (PII)" as defined in ISO/IEC 27018 [i.46].

High-level requirements:

Due to the proposed EU GDPR there are new requirements on the CSPs. This will make it necessary to renew the SLA between the CSC and the CSP.

1) Changes incurred by the proposed GDPR on existing SLAs:

   Major amendments that might have to be added to a new SLA include:

   a) A clear statement identifying the responsibility of the CSP for all Personal Data handled through the contracted services. This also applies if the CSP resides outside the legislation of the EU.

   b) Any terms related to compensation payments in case of data loss have to be carefully reviewed to ensure full damage cover as foreseen in the proposed Regulation.

   c) The SLA should detail the whole chain of potential cloud sub-providers sub-contracted by the CSP with which the CSC has a contract. All those third party subcontractors have to also fulfil the requirements of the proposed Regulation.

   d) Special care has to be taken if data (especially Personal Data) is stored outside of the European Economic Area (the European Economic Area includes the member states of the European Union plus Iceland, Norway and Liechtenstein**)**. The CSP has to assure the adequate level of privacy protection.

      a) Third party subcontractors in that respect have to be considered safe.

      b) National legislation outside the EU Data protection Regulation have also to be considered.

2) Proof of compliance to the proposed GDPR:

   All the above points may require a new set of certification schemes to allow CSPs to provide evidence supporting their compliance to the proposed EU Data Protection Regulation as to give the CSCs the necessary confidence to hand over Personal Data with minimized risk of legal breaches related to the regulation.

   This may include that CSPs will have to prove that their third party subcontractors also conform to the proposed EU Regulation.

Core concepts covered by the scenario:

Data protection, Data privacy, Trust, Cloud SLA, Compliance.

Other aspects:

Contract, Conformance, legislations/legality, Code of Conduct (CoC).

Conclusions and remarks:

This scenario exposes the significant impact the proposed GDPR will have on the Cloud Computing industry, especially on CSPs. CSPs will be forced to allow a significantly higher level of transparency about the legally-significant elements of their internal sub-structures. Third party subcontractors should be made visible and potentially have their conformance towards the EU Regulation's requirements checked and certified. Special care has to be taken for CSPs that use sub-contractors and/or infrastructure located outside the legal jurisdiction of the EU to store Personal Data. In this case, the main contracting CSP has still to prove complete compliance with all regulations towards the CSC. The work done by C-SIG on "Code of Conduct" should also be mentioned and referenced in this context. The recommendations following the C-SIG efforts provide valuable guidelines and support for measures related to data protection.

There is a potential risk that the CSCs may end up between those two "lines of fire". Therefore a comprehensive (set of) certification schemes is needed to give the users of Cloud Computing the necessary confidence to act legally correct when handing over Personal Data to a CSP and to allow the CSP to prove their compliance in regards to the proposed EU GDPR.

5.9 Scenario 8: Cloud SLA in brokered, multi CSP use cases

Example of questions to illustrate the scenario:

- "In scenarios where several Cloud Services from different Cloud Service providers are used, how do you as a Cloud Broker ensure that my data is processed according to the contract/SLA?"
- "How do you as a Cloud Service Provider monitor and keep an audit trail of my activities?"

Scenario description:

In this scenario, a CSC has procured the service of a Cloud Service Broker, CSB. The CSB has in turn procured a number of different Cloud services on behalf of the CSC, services that might come from one or more different CSP's.

High-level requirements:

In this scenario, it is critical to understand the responsibilities of the CSC, the CSB and the CSP (one or more) to ensure that the terms and conditions manifested in the individual Cloud SLAs for the Cloud services offered by the CSP(s) are met.

Most of the criteria, needs and capabilities listed in the above scenarios also apply for the "Cloud SLA in brokered, multi CSP use cases" scenario. In particular, clarifying the role of the CSB and its responsibilities in regard of the data protection and data storage aspects is key.

The Cloud Service Broker role is defined and described in the Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74] standard as follows (clause 8.4.1.3 Cloud service broker):

> *"The cloud service broker is a sub-role of cloud service partner that negotiates relationships between cloud service customers and cloud service providers. The cloud service broker is not itself a cloud service provider and should not be confused with the role of inter-cloud provider (see clause 8.3.1.6). The cloud service broker role could be combined with or operate independently of the role of inter-cloud provider.*

The Cloud Computing activities of a cloud service broker include:

- *acquire and assess customers (clause 8.4.2.6);*
- *assess marketplace (clause 8.4.2.7);*
- *set up legal agreement (clause 8.4.2.8);*

The marketplace assessment can happen prior to customer acquisition, creating pre-agreements with cloud service providers and this can enable cloud service customers to select cloud service providers from a service catalogue, possibly negotiating service details (e.g. service level objectives) at selection time.

In either case, the cloud service broker only acts during the contracting phase of the service, between the cloud service customer and cloud service provider. The cloud service broker is not involved during the consumption of the service. In such cases, the activities involve cloud service provider's activities".

Furthermore, setting up legal agreements is defined in clause 8.4.2.8 of the Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74] standard as follows:

> *"The set up legal agreement activity concerns the service agreement between the cloud service customer and the chosen cloud service provider(s). This involves negotiating the service agreement between the cloud service customer and the chosen cloud service provider(s), aiming to meet the customer's needs."*

Based on the Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74] standard, it is the CSB that will assume the responsibility of negotiating the terms and conditions of the individual Cloud SLA with all involved CSPs, but the actual Cloud SLA will be still set up between the CSC and the CSP (one or more).

Core concepts covered by the scenario:

Disclaimer: please note that the core concepts (cross cutting aspects) presented in this clause are examples of concerns. Other concerns might also be relevant. The list of core concepts is presented to illustrate the issue presented in the respective clauses, without the intention to provide an exhaustive and complete list of core concepts.

Data Integrity, Data Protection, Interoperability (at several levels), Portability, Certification, Cloud SLA.

Other aspects:

Contract, conformance, legislations/legality.

Conclusions and remarks:

The Cloud Service Broker role is defined in international standards and the role and activities as well as the responsibilities linked to the roles should be followed in order to ensure that all relevant aspects necessary to understand and adhere to are covered.

Multi Cloud scenarios with multiple CSPs involved obviously create challenges but also conversely underscore the necessity of a strict contract framework. The Cloud Service Broker role will probably develop as an increasing number of Cloud Service Customer start using Cloud Computing based services.

The inherent nature of the Cloud supports using multiple Cloud Services, independent of each other or used in combination. Therefore the complexity of defining and ensuring full compliance with the contracts that govern and restrict the use of the CSP's data should not be underestimated.

6 Core concepts

6.1 Introduction

Core concepts are key "system-wide" aspects that need to be coordinated and implemented consistently in a Cloud Computing system. These core concepts have an impact on the different stakeholders (CSCs, CSPs) involved in a Cloud Computing system and thus represent shared concerns that need to be addressed when designing, implementing and deploying a Cloud Computing system.

This clause provides a description of core concepts as applicable in the context of Cloud Computing. It also discusses the relationships between these core concepts.

6.2 Interoperability

Generally speaking, interoperability can be defined as a measure of the degree to which various kinds of systems or components interact successfully. ITU-T and ISO/IEC define 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 can be further described as the "*capability of public clouds, private clouds, and any other systems in the enterprise to understand each other's application and service interfaces, configuration, forms of authentication and authorization, data formats etc. in order to cooperate and interoperate with each other*" (from the draft of ISO/IEC 19941 [i.9] Interoperability & Portability in Cloud Computing).

In the Cloud Computing space, interoperability is even more critical as the CSC is expected to be able to exchange information (data) with and between Cloud services by design, i.e. as a built-in general capability of Cloud Computing. This capability is however still not universally available and many outstanding challenges remain before generally approved and used APIs exist across all available Cloud services. Adding to the challenge of attaining "full interoperability" is the fact that interoperability takes on different meaning on different levels (read the European Interoperability Framework, EIF, [i.8] as a reference in this respect).

Work is however underway to address the need to establish common terminology and reference points that will hopefully over time increase the support for interoperability and portability in the Cloud Computing space. The work in ISO/IEC on 19941 [i.9] ("Information Technology - Cloud Computing - Interoperability and Portability") is an example of an important effort in this respect.

6.3 Portability

Portability in Cloud Computing allows users to move applications and data between different CSPs and their Cloud services. In a way, portability is (or should be) built into the very fabric of Cloud Computing. From a CSC point of view, portability increases the confidence of the CSC in particular as portability (and interoperability) can help the CSC to select the most cost-effective solutions without the risk of vendor-lock in.

However, portability, as interoperability has different meaning depending on the type of Cloud service offered and the type of elements that are subject to a move from a Cloud service to another. There are sometimes unique capabilities offered in a Cloud service, capabilities that might impact the level of portability. For example, application portability (aka workload portability) for Cloud Computing systems can be achieved by use of popular programming languages, standards, tools, frameworks, runtime elements and API specification.

Data portability concerns the ability to easily transfer data from one source cloud service to a target cloud service, without being required to re-enter the data. Important aspects to consider for data portability include the syntax and semantics of the transferred data. Data portability can still be achieved if the syntax is different between the source cloud service and target cloud service, since tools (including standard ones) can be used to perform some data transformations. If the semantics of the transferred data does not match between the source cloud service and the target cloud service then data portability is likely to be more difficult or even sometimes impossible. Application portability defines the degree to which an application can be moved from one provider (CSP) to another, with a minimum of changes made to the application in question. As with interoperability, application portability can be achieved at different levels, similar to the ones mentioned above. A variant of application portability is "behaviour" portability, where the behaviour of an application is mimicked in the receiving application, but the underlying elements that form the application might be completely different (in terms of technologies used, etc.).

As mentioned above, portability is typically not offered as "either-or". Depending on the type of Cloud service and/or constituents that are going to be ported, the effort involved might be easy or complex. To address the many aspects of portability in the Cloud, significant work is probably required both in terms of providing international standards that can be referenced as well as collaborations for non-standard oriented solutions between the dominant Cloud vendors. In particular the vendors that provide the Cloud service category, "Platform as a Service" (PaaS) need to agree on the exchange and API mechanisms that can be used to safely and easily create Cloud solutions that can be ported between different CSPs and CSCs.

Finally, the cost of providing full Cloud portability should be weighed against the actual business value. It is recommended that CSCs demanding portability first assess the cost and value ratio, also factoring in other requirements that make it justifiable to request the Cloud service to be portable.

6.4 Security

6.4.1 Introduction

One of many challenges with Security as a concept is the fact that Security comes in many different flavours, i.e. Security is a broad topic that encompasses many domains and individual areas. Below a list of some, but certainly not all areas that can be linked or related to Security, is presented.

Security related to Cloud Computing is described in the international standard "Information Technology - Cloud Computing - Reference Architecture, ISO/IEC 17789 [i.74] - ITU-T recommendation Y.3502" as follows:

*"**Cloud computing** systems can address security requirements such as authentication, authorization, **availability**, **confidentiality**, non-repudiation, identity management, **integrity**, audit, security monitoring, incident response, and security policy management. This clause describes **cloud computing** specific perspectives to help analyse and implement security in a **cloud computing** system.*

*Security capabilities for **cloud services** include: access control, **confidentiality**, **integrity** and **availability**. Security for **cloud computing** is described in detail in other specifications.*

*Security capabilities also include the management and administration functions which are used to control **cloud services**, underlying resources and the use of **cloud services**, with particular attention applied to access control for users of these functions. This is in addition to:*

- *facilities to enable early detection, diagnosis and fixing of **cloud service** and resource related problems;*
- *secure logging of access records, activity reports, session monitoring and packet inspections on the network;*

- *provision of firewalling, and malicious attack detection and prevention for the* ***cloud service providers'*** *systems.*

One user should not be able to disrupt other users' use of ***cloud services****.*

Intranet level security should be provided on the network connecting the ***cloud service customer*** *to the* ***cloud service provider*** *(for example, through the use of VPN capabilities).*

Security measures in ***cloud computing*** *exist to address a series of threats that relate to the use of* ***cloud services*** *by* ***cloud service customers****, which affect both* ***cloud service customers*** *and* ***cloud service providers****. These threats are more fully described in other specifications, such as ISO/IEC 27018 [i.46]."*

When discussing cloud security, it is useful to distinguish between "information security" and "privacy". While there are some significant overlaps between these two domains, they are almost always treated distinctly by practitioners and standard setting organizations.

6.4.2 Information security

Information security broadly covers the protection of the confidentiality, integrity and availability (some also add the property of "non-repudiation" to the other three).of information assets, where:

- Confidentiality describes the "property that information is not disclosed to unauthorized individuals, entities or processes" (ISO/IEC 27000 [i.22]).
- Integrity describes "the property of accuracy and completeness" of information and the processes that manage it (ISO/IEC 27000 [i.22]).
- Availability describes "the property of being accessible and usable upon demand by an authorized entity" (ISO/IEC 27000 [i.22]).

Assets may include software, customer data, intellectual property and more generally "*anything that has value to an organization"* (see [i.9]*)*.

The protection of confidentiality, integrity and availability is built on several foundations, in particular:

- Trust:

  Trust has several standardized definitions that might be applicable to the context in which trust is mentioned in the present document:

  > *"degree to which a user or other stakeholder has confidence that a product or system will behave as intended"* (ISO/IEC 25010 [i.78] 4.1.3.2)

  or

  > *"relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not vio-late the given security policy"* (ISO/IEC 13888-1 [i.79], section 3.59).

In a broader sense, "trust" can also mean "can I trust this Cloud service?" or even "Can I trust this Cloud service provider"?

Furthermore, several different Trust models exist, e.g. attribute certification, evidence-based trust and policy-based trust. To ensure the level of Trust agreed upon between the CSP and the CSC, several measures need to be taken. E.g. the use of data encryption when necessary for the safe transfer over data, using HTTPS (or similar technologies) to securely exchange information between the CSC and the CSP's Cloud service.

Depending on the model of trust, trust can be verified (validated) in a number of different ways. The Cloud SLA is one way to ensure that trust model is verified with monitoring mechanisms in place to make sure that the quality of service (QoS) as stated in the Cloud SLA is met in the actual delivery of the Cloud service. Trust in Cloud Computing requires a high degree of transparency in the Cloud services offered by CSPs.

Certification can also help in addressing transparency and accountability and building trust in the Cloud Computing space. See for example the "Security, Trust & Assurance Registry (STAR)" [i.4] from the Cloud Security Alliance (CSA) and the EuroCloud's STAR Audit for cloud services (ECSA) [i.5].

Identity and Access Management (IAM)

Identity and Access Management (IAM) involves the management of individuals and ICT resources in an organization and the definition and enforcement of policies for the authentication and resource authorization of these individuals and ICT resources. IAM might be specific to and only cover entities within a specific organization, but can only span and comprise management across the boundaries of a particular organization. The goal of IAM is to secure that ICT resources are made available only to those entities that have been allocated rights to the resources of the organization (internal or external to the organization in question) according to the security policies in effect.

In other words IAM is the umbrella term for the policies, technologies, roles and activities that together provide support for the identification and authorization of individuals and ICT resources (hardware and software). The purpose of IAM is to securely (and often based on set policies) allocate, verify and protect identities and the rights allocated to a specific identity. In the Cloud environment, IAM becomes even more complex, as the identity systems might span over several systems boundaries, across several Clouds and also include the use of Cloud services that represent aggregations of several different, independently provisioned Cloud services.

Among the individual technologies, available services, solutions and core elements that relate to and comprise IAM one can find for example:

- Directory services
- Digital cards
- Service providers
- Identity providers
- Web services
- Access control, such as Role Based Access Control (RBAC)
- Digital identities
- Password managers
- Single Sign-on
- Security tokens
- Security Token Services (STS)
- Workflows
- OpenID (See http://openid.net/foundation/)
- WS-Security
- WS-Trust
- SAML 2.0
- Oauth (Open Authorization, developed by the IETF, See http://oauth.net)

Even though IAM is a non-specific aspect of Cloud Computing, it is still a critical element needed to build confidence in Cloud Computing. Organizations with existing IAM solutions, especially large organizations and enterprises, need to be able to trust that existing IAM solutions can be moved to or used in a Cloud context.

Two important aspects of IAM are:

1) Authentication

   Authentication is a security activity that serves the purpose of verifying the authenticity of the identity of any user of a service, application or function provided by a CSC (in this context). Authentication might be done in several steps and can also be done to service the continued authorization to not just one but multiple services and applications. Authentication is a key feature of a safe Cloud Computing environment, critical to ensuring full reliability of its users.

A number of individual technologies are available for authentication. Though they have been developed without regard to Cloud Computing many of them are also useful for Cloud Computing scenarios. In the Cloud Computing space, using individual Service Providers authentication mechanisms to facilitate simple authentication is growing in popularity, e.g. using Facebook, Google or Office/Live accounts to authenticate users not only for the mentioned services but for other services as well. From a CSC point of view, this ensures a simple authentication step. One of the openly available protocols used in the Cloud Computing industry by CSPs is OpenID, developed by the OpenID Foundation. One of the openly available protocols used in the Cloud Computing industry by CSPs is OpenID, developed by the OpenID Foundation. OpenID is used by many service providers who have implemented authentication solutions based on OpenID.

2) Authorization

Authorization involves granting the access to resources for individual users (human or machine resources) based on defined authorization policies. The resources for which access is granted might be for example hardware elements, data, applications and/or services (e.g. Cloud Computing services). The authorization is typically linked to and based on a Role Based Access Control (RBAC) system, where the access to resources is dependent on the actual role of the user who is attempting to access a particular resource. The role of the user is determined by the identity management system. Authorization typically involves defining the authorization policy and the enforcement of the policy. A widely used authorization protocol with growing use in the Cloud Computing space is "Oauth", developed by the IETF.

Cryptography

Cryptographic tools for encryption can be used to secure data during transit in a network and when stored at the CSPs' resources. There are several commonly used (and standardized) approaches (both for data in transit or at rest) that mainly differ in the level of (long-term) security and the effort needed to apply them. All of them have been developed for distributed environments (some of them already decades ago) but without a focus on Cloud Computing. However, they are also applicable in the Cloud Computing space.

Approaches can be classified in symmetric (one common key is use for encryption), asymmetric (based on a key pair where one key is public and the other one private) and hybrid techniques (a use of both symmetric and asymmetric keys). One important issue the CSC should particularly pay attention to when encryption is used in Cloud Computing is the secure management of the private keys which need to be available in the Cloud environment in order to decrypt the data (or the symmetric key in the case of the hybrid approach. Besides encryption to protect the data digital signatures can be used to verify the identity of the person or instance providing the data. As the other cryptographic techniques digital signatures have not been developed for Cloud Computing but are easily applicable in this domain also, Encryption to protect data while it is in storage is potentially particularly important in the case of multi-tenant clouds, such as Public clouds, where data could be accidently made available to third-parties as a result of storage allocation operations or hardware maintenance.

Security policy management

Security policies might cover many different areas, such as policies for Authentication and Authorization, data management policies, policies for Cloud Service access and more. Handling the security policy (and other related policies) requires a well-structured and formal approach integrated into and made part of the Cloud Service management. Security policy management is handled by the "multi-layer functions" according to the Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74] standard on Cloud Computing reference architecture.

The above information security list of elements is by no means limitative, and others could also be added such as:

- Governance and risk management (see ISO/IEC 38500 [i.80] "Information technology - Governance of IT for the organization" and ISO 31000 [i.81] "Risk management").
- Business continuity (backups and redundancy), captured in a disaster recovery or contingency plan. The term used in the upcoming ISO/IEC Cloud SLA standard is "Business Continuity Policy (BCP)" - see clause 6.4 for more information.
- Change control, asset classification and configuration management.
- Audit assurance and compliance.
- Application and interface security.
- Cloud tenant isolation and virtualization security.

- Datacenter security.
- Incident management and forensics.
- Accountability and supply chain management.

6.4.3 Privacy

Privacy or data protection broadly covers the protection and processing of personal data, where personal data refers to "*any information relating to an identified or identifiable natural person"*, as defined in article 2 of Directive 95/46/EC [i.7] (personal data is also sometimes referred to as Personally Identifiable Information or PII, as used in ISO/IEC 29100:2011 [i.44]).

The foundational principles of data protection, notably described in Directive 95/46/EC [i.7] or the Convention 108 of the Council of Europe, include:

- Security of personal data (confidentiality, integrity and availability).
- The fairness and lawfulness of processing.
- Data adequacy and minimization.
- Preserving data in identifiable form for no longer than necessary.
- User rights (access, rectification and deletion).
- Specific safeguards for special categories of data (racial/ethnic origin, political opinions, religious/philosophical beliefs, trade-union membership, health and sex life).
- Safeguards for trans-border data flows.

The EU Directive 95/46/EC [i.7] will be replaced by the General Data Protection Regulation, which is currently in the final phase of coordination between the EC, the European Parliament and the European Council.

Taking into considerations related to the new draft General Data Protection Regulation, this list could also be expanded to include accountability, personal data breach notifications, "privacy by design" and certification, which are all elements that have been identified as important areas to support in the upcoming data protection regulation.

Maintaining data privacy and data integrity is increasingly becoming an important but also problematic and complex issue as the value of data and information increases and the sheer data volumes are becoming enormous in size.

6.4.4 Other concerns

Data Breach:

Of special interest is of course Data Breach, which is non-authorized access to data. In light of the upcoming General Data Protection Regulation, aligning existing security policies with the new rules to be enforced following the implementation of the Data Regulation throughout Europe, is one of many critical measures necessary to ensure and comply to data protection and data privacy legislation and defined policies. For more information, see also scenario 7.

Isolation of virtual resources:

The implementation of Cloud Computing services often relies on the use of virtualization technologies, where a single physical resource is shared to implement multiple instances of a service, each visible to the user as if it were implemented on dedicated physical resources. It is essential that the virtualization technologies implement all required measures and mechanisms to guarantee the isolation of the various service instances, i.e. that there is no possibility for the user of one instance to obtain any information on the data stored or processed in any other instance implemented on the same physical resource.

6.4.5 Conclusions on Security aspects

Several of the above listed security areas are either overlapping or perhaps even concepts that need to be defined and handled separately from the Security issues. The point here though is that one needs to understand both what applies in terms of Security in the Cloud Computing context as well as how different aspects of come together to address all relevant Security concerns at hand. It is also important to again underline that any Security related measure should be applied according to the CSC's actual need and the topography of the requested Cloud service. The type of data to be processed also dictates the levels of trust and security that need to be considered. Security aspects should be defined as part of the Cloud SLA.

6.5 Cloud Service Level Agreement (Cloud SLA)

A Service Level Agreement (SLA) is a documented agreement between the service provider and customer that identifies services and service level objectives [SOURCE: ISO/IEC 20000-1:2011[i.70], 3.29]. The Cloud Service Level Agreement (Cloud SLA) is a contract framework that defines the terms and conditions necessary to fulfill the obligations of a CSP for the service(s) offered to a CSC. The service offered can either be a standard service provided by the CSP ("off the shelf") or an offer based on specific requirements of a CSC (probably resulting from a negotiation between CSC and CSP). The Cloud SLA defines the attributes and metrics necessary to monitor the Quality of Service (QoS) of a service as well as activities necessary to ensure that the cross cutting aspects (non-functional requirements) are handled in accordance with the terms defined for the service in question. Non-functional requirements include, e.g. data protection, various facets of security, privacy, IPR protection, resiliency, contingency procedures, data erasure procedures, exit procedures, and more. In the Cloud SLA the QoS metric attributes and their respective set values are listed. These might be, e.g. access time, number of transactions per time unit (for data transfer) and number of users that can simultaneously access the service.

While the demand for Cloud SLAs defining functional and non-functional properties of a Cloud service is in general recognized (at least on the side of the CSC), standardization of terms (attributes) and metrics is still under development with different levels of maturity already achieved. Mid 2015 the most advanced standardization efforts being the work of the ISO/IEC JTC1 SC38 WG3 on ISO/IEC 19086 ([i.35], [i.50], [i.51] and [i.52]) and the work of the Cloud Security Alliance (CSA) on metrics for trust and security.

ISO/IEC 19086 consists of the following parts, under the general title Information technology - Cloud computing - Service Level Agreement (SLA) framework:

- Part 1: Overview and concepts
- Part 2: Metrics
- Part 3: Core requirements
- Part 4: Security & Privacy

The purpose of the Cloud SLA is to complement existing standard SLA frameworks with those elements that are particular to Cloud Computing. The Cloud SLA will of course be different from service to service, depending on the complexity of the service offered, the criticality and type of data handled by the service and a number of other factors.

The Cloud SLA might be one of several elements of a Master Service Agreement (MSA). Other elements of the MSA might be:

- **Acceptable Use Policy (AUP):** defines and restricts the CSC's use of the CSP's service.
- **Security Policy:** defines those responsibilities of the CSC and CSP that are necessary in order ensure the defined security objectives (potentially profiled according to the topography of the service in question, taking data classification and other parameters into account).
- **Privacy Policy:** the Privacy Policy is either a part of the Security Policy or a stand-alone policy (again, potentially dependent on the nature of the data handled by the service). The privacy policy might include definition of the Data Protection measures necessary to maintain the stated privacy policy objectives and privacy certifications and standards used to enforce the objectives. In particular, the European Regulation on Data Protection needs to be acknowledged and the Privacy Policy aligned to the upcoming regulation, where necessary.

- **Business Continuity Policy (BCP):** the BCP defines measures necessary to ensure Cloud service resiliency, including contingency planning and disruption mitigation. The BCP defines the activities implemented by the CSP to avoid data loss and to deal with outages, such as backups and redundant components.

- **Service Description:** the service description provides a functional account of the service offered by the CSC including e.g. interfaces, input formats, output formats, metadata, etc.

By applying and basing the Cloud SLA on standard elements, structures and terminology, a stable and measurable situation will be created that over time will build user confidence in Cloud Computing. Bringing the work done within the European C-SIG project into the ongoing ISO/IEC standardization effort will hopefully guarantee that relevant European level considerations are covered by the upcoming international standard (ISO/IEC 19086 ([i.35], [i.50], [i.51] and [i.52])) currently being developed.

6.6 Relationship between core concepts

The core concepts presented in clauses 6.1 to 6.4 are all relevant, irrespective of the Cloud services to which core concepts apply. Cloud Computing relies on the ability for its users to easily, securely and transparently be able to procure, to use and to discontinue the use of Cloud services without compromising the user's availability to the service and its data. This, in turn, underscores the significance and relevance for the provision and availability of standards and certification schemes that address and fully cover all aspects of the core concepts presented in the present document. The inherent nature of Cloud Computing in terms of multi tenancy (sharing resources among several different users), self-provisioning and other key characteristics, calls for interoperability, portability and security aspects to be supported and captured in well-structured Cloud Service Level Agreement framework standards.

In terms of relationship between the different core concepts, it is obviously challenging to come up with a single description of the relationships due to the many dependencies that exist, but also because of the many different facets and levels that come into play given the type of Cloud service subject to use by the CSC. As pointed out in earlier clauses, the core concepts that apply for a particular Cloud service will vary depending on the "topography" of the Cloud service in question. Factors such as data criticality/classification, number of users, dependencies across multiple Cloud services, security policies, legal framework and legislation, Cloud deployment models and Cloud service categories are all example of factors that come together to determine how core concepts need to be defined, related and cross referenced.

Cloud SLA frameworks that assist the CSC and CSP in determining the appropriate levels for the core concepts included in the contract between the CSC and CSP will hopefully significantly lead to an increased awareness of the core concepts themselves as well as the relationships between the core concepts. Understanding the core concepts will eventually and ultimately increase the confidence in Cloud Computing in general, thus accelerating the adoption of Cloud Computing. Standards and certification schemes play an important role in this process. But there are other factors that need to be understood and addressed as well, for instance the general high level business rationales (potentially manifested as business requirements and process descriptions), functional support and the end user's expected support for individual activities.

7 Standards, certifications and frameworks for Interoperability and Security

7.1 Introduction

This clause identifies the standards and specifications for interoperability and security classified taking into account the core concepts presented in clause 6. For each core concept, the identified standards and specifications are categorized as being "cloud specific" or "non Cloud specific".

For the ones classified as "Cloud specific", please refer to the WP4 report (ETSI SR 003 392 [i.82]) for further information. These are either available as published standards or draft standards.

The standards classified as "non Cloud specific", are not meant to constitute an exhaustive list but included in the present document because they have been assessed to be relevant for consideration in the context of the core concepts listed in the present document.

7.2 Interoperability and Portability

Cloud specific:

- Draft ISO/IEC 19041 [i.10]: "Information technology - Cloud computing - Interoperability and Portability".
- Draft ISO/IEC 19044 [i.11]: "Information technology - Cloud computing - Data and its flow across devices and cloud services".
- ISO/IEC 17203 [i.12]: "Information Technology - Open Virtualization Format Specification".
- ISO/IEC 17826 [i.13]: "Information Technology - Cloud Data Management Interface (CDMI)".
- ISO/IEC 19099 [i.14]: "Information Technology - Virtualization Management specification".
- ISO/IEC 19831 [i.15]: "Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol - An Interface for Managing Cloud Infrastructure".
- DMTF DSP0243 [i.16]: "Open Virtualization Format Specification".
- DMTF DSP0263 [i.17]: "Cloud Infrastructure Management Interface - CIMI".
- OASIS CAMP [i.18]: "Cloud Application Management for Platforms".
- OASIS TOSCA [i.19]: "Topology Orchestration Specification for Cloud Applications".
- OGF OCCI [i.20] "Open Cloud Computing Interface".
- SNIA CDMI [i.21]: "Cloud Data Management Interface".

7.3 Information security

Non Cloud specific:

- ISO/IEC 27000 [i.22]: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".
- ISO/IEC 27001 [i.23]: "Information technology - Security techniques - Information security management systems - Requirements".
- ISO/IEC 27002 [i.24]: "Information technology - Security techniques - Code of practice for information security controls".
- ISO/IEC 27006 [i.25]: "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".
- ISO/IEC 27014 [i.26]: "Information technology - Security techniques - Governance of information security".
- ISO/IEC 27031 [i.27]: " Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity".
- ISO/IEC 24760-1 [i.28]: ""Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts".
- ISO/IEC 29115 [i.29]: "Information technology - Security techniques - Entity authentication assurance framework".
- OpenID [i.30]: see specification at http://openid.net/developers/specs/.
- IETF RFC 6749 [i.31]: "The Oauth 2.0 Authorization Framework".

Cloud specific:

- Draft ISO/IEC 27017 [i.32]: "Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 [i.24] for cloud services".

The ISO/IEC 27017 [i.32] - Recommendation ITU-T X.1631 [i.34] standard was approved as an International Standard on the 1st of October 2015 following balloting. The standard however has yet to be formally published as a standard and will for this reason remain as 'draft' when referenced in the present document.

- Recommendation ITU-T X.1601 [i.33]: "Cloud computing security - Security framework for cloud computing".
- Draft Recommendation ITU-T X.1631 [i.34]: "Code of practice for information security controls based on ISO/IEC 27002 [i.24] for cloud services".

NOTE: Same as ISO/IEC 27017 [i.32].

- Draft ISO/IEC 19086-4 [i.35]: "Information technology - Cloud computing - SLA framework and terminology - Part 4: Security and Privacy".
- CSA CCM [i.36]: V3.0.1, " Cloud Control Matrix".
- CSA CTP [i.37]: " Cloud Trust Protocol".
- CSA A6 [i.38]: "Cloud Audit".
- CSA CAIQ [i.39]: "Consensus Assessments Initiative Questionnaire".
- CSA TCI [i.40]: "Reference Architecture - Trusted Cloud Initiative".
- Draft NIST SP 500-299 [i.41]: "Cloud computing security reference architecture".
- NIST SP 800-125 [i.42]: "Guide to security for full virtualization technologies".
- NIST SP 800-144 [i.43]: "Guidelines on security and privacy in public cloud computing".

7.4 Privacy

Non Cloud specific

- ISO/IEC 29100 [i.44]: "Information technology - Security techniques - Privacy framework".
- ISO/IEC 29101 [i.45]: "Information technology - Security techniques - Privacy architecture framework".

Cloud specific:

- Draft ISO/IEC 19086-4 [i.35]: "Information technology - Cloud computing - SLA framework and terminology - Part 4: Security and Privacy".
- ISO/IEC 27018 [i.46]: "Information technology - Security techniques - Code of practice for PII protection in public clouds acting as PII processors".
- CSA PLA [i.47]: "Privacy Level Agreement".
- NIST SP 800-144 [i.43]: "Guidelines on security and privacy in public cloud computing".

7.5 SLA

Non Cloud specific:

- OGF GFD.192 [i.48]: "Web services agreement specification".
- Draft OGF GFD.193 [i.49]: "Web services agreement negotiation specification".

Cloud specific:

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

- Draft ISO/IEC 19086-2 [i.51]: "Information technology - Cloud computing - SLA framework and terminology - Part 2: Metrics".
- Draft ISO/IEC 19086-3 [i.52]: "Information technology - Cloud computing - SLA framework and terminology - Part 3: Core requirements".
- Draft NIST SP 500-307 [i.53]: "Cloud Computing Service Metrics Description".
- TMF GB963 [i.54]: "Cloud SLA application note".

7.6 Certification

Cloud specific:

- AICPA SOC 1 [i.55].
- AICPA SOC 2 [i.56].
- AICPA SOC 3 [i.57].
- Certified Cloud Service -TüV Rheinland [i.58].
- CSA Attestation - OCF Level 2 [i.59].
- CSA Certification - OCF Level 2 [i.60].
- CSA Self Assessment - OCF Level 1 [i.61].
- EuroCloud Self Assessment [i.62].
- EuroCloud Star Audit Certification [i.63].
- ISO/IEC 27001 [i.23] Certification.
- Payment Card Industry (PCI) Data Security Standard v3 [i.64].
- Leet Security Rating Guide [i.65].
- Cloud Industry Forum Code of Practice [i.66].
- FedRAMP [i.67].

7.7 Other relevant standards, frameworks and legislation

Non Cloud specific:

- Directive 95/46/EC [i.7]: "EU's Data Protection Directive".
- EIF: "European Interoperability Framework" [i.68].
- ISACA COBIT: "Control Objectives for Information and related Technology".
- ISO/IEC 20000-1 [i.70]: "Information Technology - Service management system requirements".
- ISO 22301 [i.71]: "Societal security - Business Continuity Management Systems - Requirements".
- ITIL: "Information Technology Infrastructure Library" [i.72].

Cloud specific:

- C-SIG "Code of conduct" (see note 1) [i.77].

NOTE 1: See http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=11194.

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

- ISO/IEC 17789 [i.74]: "Information Technology - Cloud computing - Reference architecture".
- Recommendation ITU-T Y.3500 [i.75]: "Information Technology - Cloud computing - Overview and vocabulary".

NOTE 2: Same as ISO/IEC 17788 [i.73].

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

NOTE 3: Same as ISO/IEC 17789 [i.74].

8 Conclusions and recommendations

Risks

Cloud Computing covers many areas and introduces some new challenges. Even though Cloud Computing builds on existing technologies and architectures, the width and depth of service categories, deployment models and geographical coverage accentuate the demand for structure, alignment and stability in many areas. Unless the main stakeholders of Cloud Computing can continue to or even accelerate the efforts needed to develop (where necessary) and map existing (where available) standards to Cloud Computing, the overarching risk is that the potential Cloud Computing users will hold back, not realizing and tapping into the assessed value of Cloud Computing.

Outstanding gaps

While gaps exist in many areas, work is progressing to address these gaps. Among these gaps are interoperability and portability standards that will allow CSCs to effortless move their data and applications between different CSPs Cloud Services offered on various Cloud platforms. Understanding and clarifying the significance of national, regional and global legislations that restrict and govern the use of personal and/or corporate data also need to be fully understood and addressed. This is not fully the case among all stakeholders of Cloud Computing.

Despite the undisputed advantages of Cloud computing, customers (in particular small and medium enterprises - SMEs) are still in need of understanding the implications of security and privacy concerns and the challenges that the Cloud introduces. Risk management frameworks might assist the users (and providers) in assessing if Cloud services are secure enough based on the security requirements at hand. Cloud-specific risk management frameworks are, however, still missing. Risk management frameworks could help the CSC understand and set the levels appropriate levels of security and privacy where applicable.

Please note there are important concepts that have not been covered in this report, such as the concept of "Containers", concepts that might warrant more attention and that are equally important to understand and to map to Cloud Computing as those included in the report. There is definitely a need for further work, specifically for information security, that have to be in-depth, exhaustive and authoritative.

Finally, standardized and machine-readable specifications are required to improve both interoperability and security in Cloud computing, in particular related to the adoption of realistic levels of automation in areas like Cloud SLA management.

Awareness, dissemination and marketing

As mentioned in the "recommendations" paragraph, below, raising the awareness among both users and providers of Cloud Computing through dissemination and education concerning the availability of Cloud Computing standards, certification schemes and available solutions is probably one of the key efforts necessary to propagate and encourage the use of Cloud Computing. Existing and already available solutions that address the concerns related to the core concepts discussed in the present document should be communicated to Cloud Computing stakeholders.

Recommendations

The CSC-2 Survey report (see [i.2]) clearly showcases the importance of the main core concepts (security, interoperability, portability, security and Cloud SLA) presented in the present document. The concerns raised by current and future CSCs in the WP 1 report underscore the importance and relevance of accelerating ongoing efforts to develop new standards to address the concerns related to the core concepts. There is also a need to map already existing standards and solutions to Cloud Computing and the related core concepts presented in the present document. As shown in the WP 1 report [i.2], awareness on the already existing possibilities and solutions is important in addition to develop new standards to fill any identified gap.

The same need can be applied to certifications; well-structured, continuously updated and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the CSCs' confidence in the Cloud. But it is imperative that available Cloud Computing standards and certification schemes are made publicly known. No matter how well constructed the standards and certifications are or how good the coverage of any area is, without the knowledge of their existence, the value is lessened.

The relevance and potential high-value use of the upcoming framework for Cloud SLA (ISO/IEC 19086 Part 1 to 4 [i.35], [i.50], [i.51] and [i.52]) should also be mentioned as part of the list of recommendations; using the Cloud SLA to identify and populate core concepts with content relevant for the Cloud service for which the Cloud SLA is created will hopefully substantially alleviate the burden of keeping track of all relevant areas that need to be included in the Cloud SLA. The availability of standardized metrics that can be populated with values set in the Cloud SLA will obviously provide better visibility in terms of the level of quality of the Cloud services provided, thus establishing better trust and confidence in the Cloud Computing space. Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture (Recommendation ITU-T Y.3502 [i.76] | ISO/IEC 17789 [i.74]) will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in the present document.

All Cloud Computing stakeholders, SSOs, Cloud Open Source communities, certification providers and Cloud industry communities should collaborate with the overarching goal to significantly increase the potential Cloud user and customer awareness of what can be achieved and done today in order to address and mitigate the concerns related to interoperability and security.

9 Areas for further study

Areas for further study include:

- Development of existing and new scenarios used for a more detailed identification of requirements and description of core concepts;
- Analysis of scenarios with respect to their support by available security standards and identification of potential gaps;
- Description of core concepts identified in clause 5 and not covered in clause 6;
- More detailed analysis regarding the relationship between core concepts;
- More scoped and technical oriented recommendations, including recommendations useful for a CSC or a CSP.

Annex A:
Change History

Date	Version	Information about changes
July 2015	1.0.0	First publication of the SR for comments
November 2015	2.0.0	Final publication based on the changes provided by: - Comments from the NTECH Technical Committee review - Comments from the public review gathered on http://csc.etsi.org - Additional changes proposed during the final review workshop

History

Document history		
V2.1.1	February 2016	Publication