Cloud Standards Coordination

Final Report

November 2013

VERSION 1.0

Executive Summary

The European Commission Communication on the European Cloud strategy identifies a key action for standardisation in this context:

> *Key action 1: Cutting through the jungle of standards [...]*
>
> - *Promote trusted and reliable cloud offerings by tasking ETSI to coordinate with stakeholders in a transparent and open way to identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility).*
> - *Enhance trust in cloud computing services by recognising at EU-level technical specifications in the field of information and communication technologies for the protection of personal information in accordance with the new Regulation on European Standardisation.*

Following the request from the European Commission, ETSI launched the Cloud Standards Coordination (CSC) initiative in a fully open and transparent way, open for all stakeholders.

After an analysis of major aspects of cloud computing standardization, the final Report provides:

- A definition of roles in cloud computing;
- The collection and classification of over 100 cloud computing Use Cases;
- A list of around 20 relevant organizations in cloud computing Standardization and a selection of around 150 associated documents, Standards & Specifications as well as Reports & White Papers produced by these organizations;
- A classification of activities that need to be undertaken by Cloud Service Customers or Cloud Service Providers over the whole Cloud Service Life-Cycle;
- A mapping of the selected cloud computing documents (in particular Standards & Specifications) on these activities.

Based on these technical results, conclusions regarding the status of Cloud Standardization at the time of this writing have been developed, concerning general aspects (fragmentation, etc.) and more specific topics of Interoperability, Security & Privacy and Service Level Agreements.

> Regarding fragmentation, the analysis has concluded that cloud standardization is much more focused that anticipated. In short: the Cloud Standards landscape is complex but not chaotic and by no means a 'jungle'.
>
> Though several cloud computing standards have seen successful adoption in small-scale and research projects, cloud computing-specific standards are not seen widespread adoption by cloud providers to date. However, given its dynamism, Cloud Standardization will likely mature in the next 18 months. Adoption may be encouraged if mechanisms are found for domain-specific stakeholders to agree on shared vocabularies and formal definitions that are machine readable.
>
> Important gaps in the cloud computing standards landscape have been identified. New cloud computing standards, or cloud computing specific extensions to existing standards that fill these gaps should be encouraged.
>
> The legal environment for cloud computing is highly challenging. Research into standardized ways of describing, advertising, consuming and verifying legal requirements is necessary. Solutions need to accommodate both national and international (e.g. EU) legal requirements.

This analysis also shows that standards are maturing in some areas (for example, for IaaS machine control, vocabularies, SLA or security) while maturation is slower in other areas.

Table of contents

History of document

Version	Date	Content
0.0.4	27/06/2013	Version for distribution to the European Commission
1.0	27/11/2013	Final version for distribution to the European Commission

1. Introduction

1.1 Objectives of this report

The European Commission Communication on the European Cloud strategy, "Unleashing the Potential of Cloud Computing in Europe", identifies a key action for standardisation in the context of promoting the uptake of cloud computing technologies:

> *Key action 1: Cutting through the jungle of standards [...]*
>
> - *Promote trusted and reliable cloud offerings by tasking ETSI to coordinate with stakeholders in a transparent and open way to identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility).*
> - *Enhance trust in cloud computing services by recognising at EU-level technical specifications in the field of information and communication technologies for the protection of personal information in accordance with the new Regulation on European Standardisation.*
>
> *[...].*[1]

To answer the request from the European Commission, ETSI launched the Cloud Standards Coordination (CSC). Its overall objective is to present a report which is useful for its target audience and which effectively supports the European Commission's work on implementing its Cloud strategy and therefore the broad uptake of standards-based cloud computing technologies in Europe – driving innovation and growth with the Cloud.

This document is the CSC final report.

1.2 Target audience

The audience for the CSC report includes

- Cloud service providers who should be able to use it to understand which standards and specifications they may wish to select and apply to their services.
- Cloud service customers, who should be able, from knowing the standards and specifications applied by a cloud service provider, to understand how their requirements can be covered by the current and future offerings and to have confidence in the service offering.
- All sizes of cloud service providers and cloud service customers from small businesses to public procurers and multinationals.
- Administrations that have to act as cloud service customer.
- Governmental authorities that have to act as cloud regulators.

1.3 Structure of this document

The rest of this document is structured as follows:

- Chapter 2 presents the output of early Task Groups TG1 and TG2 regarding
  - Roles: a high level taxonomy of stakeholders that play a role in the provision and/or consumption of cloud services;
  - Use Cases: collection, classification and ranking of around 110 Use Cases (that are detailed in Annex 3).
- Chapter 3 present three essential elements:
  - An analysis of several Use Cases that has been undertaken by the TG3 Task Groups (TG1 to 3) or by TG3 as a whole;

[1] COM(2012) 529: Unleashing the Potential of Cloud Computing in Europe, September 2012, pp. 10-11.

  - A table of generic or specific activities across the Cloud Services Life-Cycle that has been derived from the analysis of Use Cases;
- Chapter 4 presents a detailed mapping of these activities with the list of documents from Annexes 1 (Standards & Specifications) and Annex 2 (Reports and White Papers).
- Chapter 5 provides the list of Standards Organizations that have been considered by CSC participants as most relevant to Cloud Standardization.
- Chapter 6 presents the conclusions of the CSC work.
- Chapter 7 contains References and Acronyms.

The following Annexes are added:

- Annex 1 provides the list of Standards and Specifications that have been produced by the organizations listed in Chapter 5.
- Annex 2 provides a list of other documents (essentially Reports and White Papers) that have been produced by the organizations listed in Chapter 5.
- Annex 3 provides a detailed description and classification of the Use Cases analysed by CSC TG2 and presented in section 2.2.
- Annex 4 outlines the methodology used for the production of the report.

The documents produced by the CSC can be found at: http://csc.etsi.org

2. Actors, Roles and Use Cases

This section introduces briefly the results of TG1 (Actors and Roles) and TG2 (Use Cases). More detailed content can be found in the final reports of TG1 and TG2 (both still in draft status).

2.1 Roles

The objective is to provide a high level taxonomy of stakeholders, individuals and/or organizations, that play a role in the provision and/or consumption of cloud services.

Input was collected from, in particular, the following organisations: DMTF, ITU-T and NIST.

Two main elements have been addressed: roles and parties.

Role: The following roles have been defined:

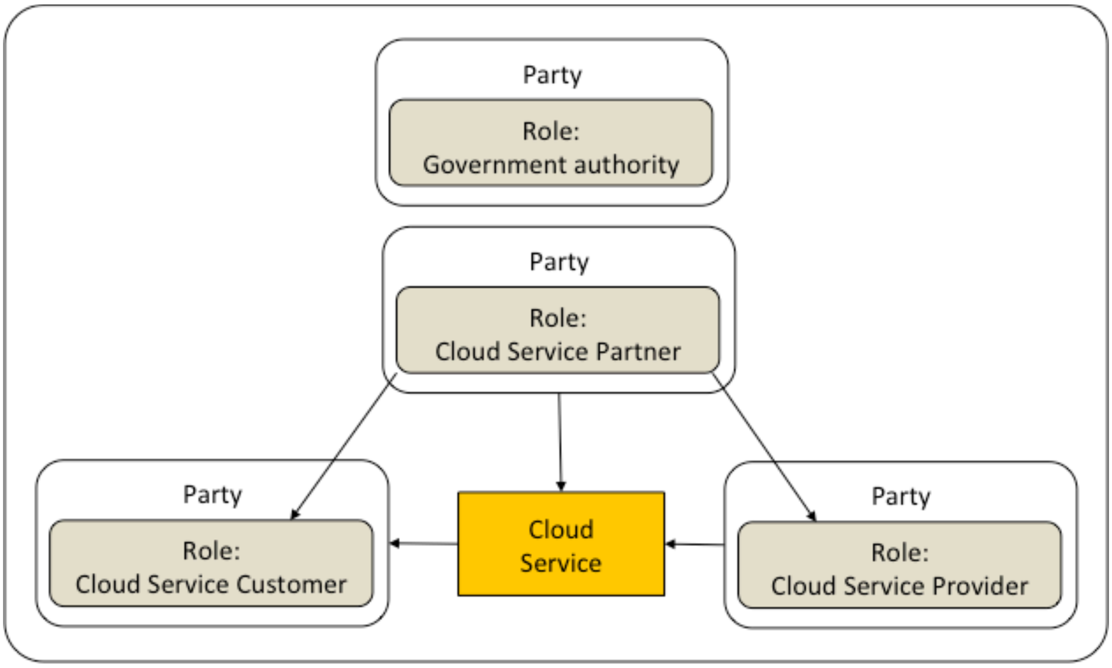
- **Cloud Service Customer**: The Cloud Service Customer role consists of those consuming one or more cloud services provided by a Cloud Service Provider.
- **Cloud Service Provider**: The Cloud Service Provider role consists of those providing cloud services to one or more Cloud Service Customers.
- **Cloud Service Partner**: The Cloud Service Partner role consists of those providing support to the provisioning of cloud services by the Cloud Service Provider, or to the consumption of cloud service by the Cloud Service Customer (e.g. service integration).
- **Government authority**: The government authority role consists of those interacting with providers, customers and partners for the purpose of regulation, law enforcement, inspection, economic stimulation, et cetera.

Roles can be refined into sub-roles.

Party: An individual or an organization. Parties can play one or more roles.

Note that one party can play several roles at the same time. Consider for example an SME that deploys a specific piece of software on a PaaS cloud service, offering the Software as a Service to other SMEs. In this case, the SME plays both the roles of Cloud Service Customer, as well as Cloud Service Provider. Consider as a second example a government agency which could play the role of provider (offering a governmental cloud appstore, for instance) or play the role of customer (consuming an email as a service solution, for example). Each party may have either or both of the responsibilities of data processor or data controller depending on use case.

The relations between the roles (and parties) are depicted in the figure below.



2.2 Use Cases

Use Cases have been collected from several Organizations (see Annex 3).

The collection phase has led to the identification of 110 Use Cases that have then been

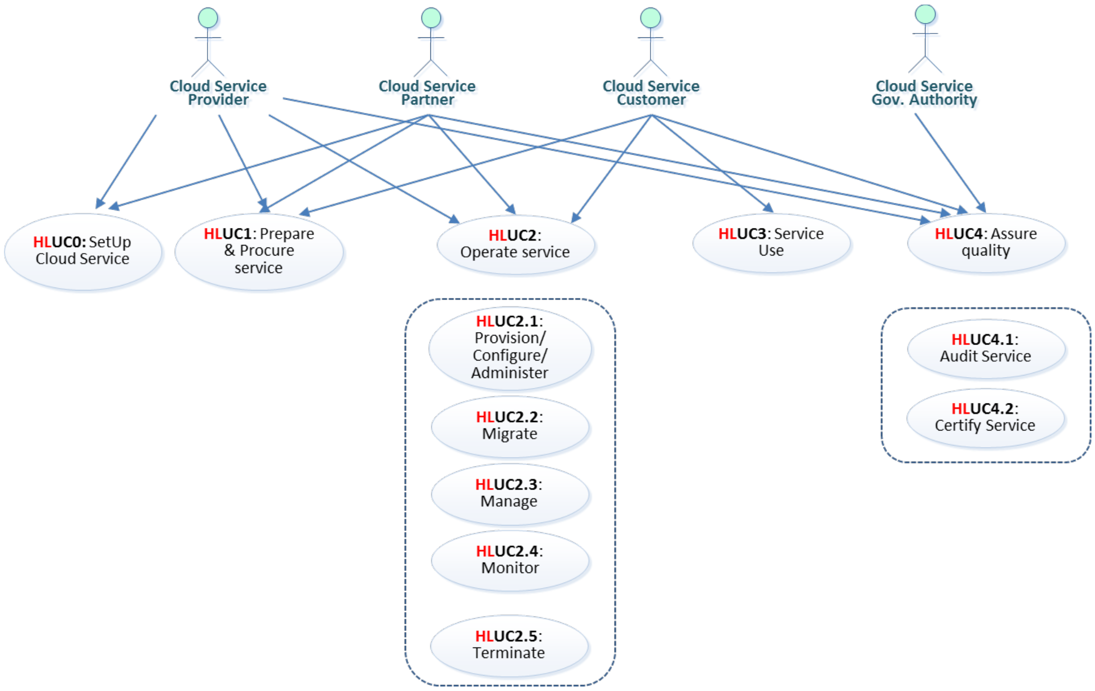
- categorized according to criteria that could help in the following phases of the activity, i.e. Data Security and Privacy, Service Level Agreements, Interoperability, Data Portability, Reversibility, Support EU Policies, Based on Real life situations, and
- ranked on a four level scale indicating their relevance (not a UC, broad UC, UC, detailed UC).

By filtering out the collected UCs ranked "not a UC", the total number of UCs was reduced to 90.

Given the large number and the lack of homogeneity of the Use Cases, it has been agreed to provide a high level view of UCs over which to map all the submitted ones, in order to provide a clearer representation for Cloud Services Use Cases. This is achieved with the definition of High-Level Use Cases (HLUC)

- Set-Up Cloud Service,
- Prepare & Procure service,
- Operate the service,
- Use Service, and
- Assure Quality.

These HLUCs (and a refinement for some of them) are represented in the figure below.



In parallel, the UCs were grouped by family and for each of the families, a "master" UC was identified. With this, it was possible to filter the list of (90) UCs down to 21 very representative UCs, that could be mapped with the HLUCs[2].

The full list of UCs is provided in Annex 3 and also on the CSC website at:
http://csc.etsi.org/Application/documentapp/downloadLatestRevision/?docId=185

[2] This list of 21 UCs an be extracted by filtering from the Use Case spreadsheet that is delivered together with the report.

3. Use Cases Analysis

3.1 Phases and Activities

The Use Cases analysis as well as the mapping to Standards & Specifications have been done by using a common set of Phases (i.e. major part of the Cloud Service Life-cycle) and identifying activities within these phases.

The three phases, common to all Use Cases are:

- Phase 1: Acquisition of Cloud Service
- Phase 2: Operation of Cloud Service
- Phase 3: Termination of Cloud Service

3.2 Perspectives for Use Case Analysis

3.2.1 The Service Level Agreement Perspective

Public cloud services generally involve a formal Customer Agreement (sometimes called a “Master Agreement” or “Terms of Service”) between the cloud service customer and the cloud service provider. The customer agreement may be a fixed set of terms prepared by the provider alone, or it may be the result of negotiations between the customer and the provider, depending on the nature of the cloud service offered by the provider and the customer’s power to negotiate.

Associated with the Customer Agreement are typically an “Acceptable Use Policy” (AUP) and a “Service Level Agreement” (SLA). Service Level Agreements are formal documents, accepted by both the customer and the provider, that define a set of service level objectives and related key performance indicators (KPI). These objectives concern aspects of the cloud service including availability, performance, security and compliance/privacy. The service level objectives define measurable thresholds of service attributes, which the cloud service provider aims to meet in respect of the cloud service to be delivered. However, the most common service level target offered by commercial cloud service providers today is that for availability, typically described in terms of the percentage uptime - 99.999%, for example.

SLAs are of importance during three distinct phases of the lifecycle of a cloud service.

- Advertisement of a Cloud Service offering and acquisition of Cloud Service
  In the first phase the cloud provider advertises its offerings for potential customers and the customers may check whether a particular service offering meets their business and technical requirements and how a service offering compares with other offerings in the market.
- Operation of Cloud Service
  The second phase covers the use of the cloud service by the cloud customer. The emphasis is on determining whether the cloud service is meeting each of the defined service level objectives and on taking corrective actions for the operation of the cloud service if it fails to meet one or more service level objectives. This phase also includes monitoring of the state of KPIs defined in the SLA and the state of the SLA as a whole.
- Termination of Cloud Service
  In the third phase during the termination of a cloud service both provider and customer may evaluate whether the SLA has been fulfilled or is violated. Potentially, discrepancies in the perception of the state of the SLA are disputed. Return of customer data to the customer and the deletion of customer data from the provider’s systems completes this phase. This includes but is not limited to Reversibility.

The key concern relating to SLAs in the acquisition phase is that the customer must retrieve information about all the service level objectives and related metrics pertaining to the cloud service and that each service level target must be:

- **Well-defined.** The parameter definition is not ambiguous. Suppliers must not be able to interpret measures differently - this reduces comparability and degrades consumer trust.
- **Determinate.** Multiple measurements of identical systems in identical states must give the same result. For example, measures which result in random results are of no value.
- **Correlated to business value.** Service level objectives must be strongly correlated with perceived value to consumers. For example, clock speed for CPUs is not a useful measure unless it is strongly correlated to real-world performance on typical consumer tasks.
- **Comparable.** Metrics must reflect the same quantity across different measurement targets. For example, if the scope of measurement is not well defined, one cloud provider might report the availability of a cloud service as a percentage of total time in a period, while another may exclude significant periods of time in a period such as specified maintenance windows. In this case, the measurements are not comparable.

It is important that each service level target uses such consistent terminology and also has commonly understood metrics, so that the cloud service customer can understand what is being claimed for the cloud service and relate the claims to their own requirements.

3.2.2 The Interoperability Perspective

Interoperability in the context of cloud computing includes the ability of a cloud service customer to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results. Typically, interoperability implies that the cloud service operates according to an agreed specification, one that is possibly standardized. The cloud service customer should be able to use widely available ICT facilities in-house when interacting with the cloud services, avoiding the need to use proprietary or highly specialized software.

Interoperability also includes the ability for one cloud service to work with other cloud services, either where the cloud service of one provider works directly with a cloud service of another provider, or where a cloud service customer uses multiple different cloud services in some form of composition to achieve their business goals.

Portability is also significant in cloud computing since prospective cloud service customers are interested to avoid lock-in when they choose to use cloud services. Cloud service customers need to know that they can move cloud service customer data or their applications between multiple cloud service providers at low cost and with minimal disruption."

Significant stakeholders in cloud computing have identified lack of interoperability as being a substantial barrier to cloud adoption. These include the Open Data Center Alliance [ODCA] and the European Commissioner for the Digital Agenda, Neelie Kroes [DA].

Interoperability through the appropriate standardization of APIs, data models, data formats and vocabularies will help automate business processes surrounding cloud computing procurement, enable straightforward technical integration between the client and provider, and allow for flexible and dynamic application deployments across multiple clouds.

Given that cloud computing is rapidly evolving, it is important that any solutions adopted are able to accommodate new cloud functionality and concepts as they become relevant. Standards must be extensible and flexible. Practical examples of this can already be seen in the infrastructure extension to OGF's OCCI, the discoverable capabilities in SNIA's CDMI, and the support for custom properties in DMTF's CIMI.

A truly interoperable cloud will encourage potential cloud customers to on-board, safe in the knowledge that they can change providers, or use multiple providers, without significant technical challenges or effort. This will expand the size of markets in which cloud providers operate. Additionally, if standards are suitably defined, the unique selling propositions of cloud providers can all be exposed.

Interoperability is a significant challenge in cloud computing, but if addressed appropriately will offer new business opportunities for cloud customers and providers alike.

3.2.3 The Security Perspective

One of the main challenges, when it comes to cloud computing, consists of building trust and confidence in cloud computing services. The variety of existing standards, with a varying degree of maturity, as well as the lack of clarity around the suitability of currently available certification schemes, are not really helpful in these trust building efforts. Concerns are being voiced about compliance issues as well as the effectiveness and efficiency of traditional security governance and protection mechanisms applied to the cloud computing.

In this document, we provide an analysis of on-going standardization initiatives in cloud security with specific focus on security, data protection and privacy and cyber forensics.

3.2.3.1 Context setting: Security and Clouds

In the following sections, we present the main challenges, risks, objectives concerning security in cloud as well as requirements from a legal, regulatory and standards compliance standpoint. We detail also main gaps and concerns when addressing cloud security.

3.2.3.2 Challenges, risks and potential benefits

The cloud computing service delivery model is subject to a number of security challenges and risks which have been highlighted in a number of studies, see for instance the report produced by the European Network and Information Security Agency (Ref: Cloud Risk Assessment [DC1]), by independent industry organizations such as Cloud Security Alliance (Ref: Cloud Top Threats [DC2]) and the Cloud Standards Customer Council (Ref: Security for Cloud computing [DC3]).

The underlying cause of many of the risks and challenges associated with cloud computing is that the cloud service customer passes over responsibility for data and for applications to the cloud service provider and the provider has an environment in which resources are shared (the multi-tenant model).

Typical risks and challenges concern:

- Availability of services and/or data
- Lack of data classification mechanisms
- Integrity of services and/or data
- Confidentiality concerns
- Regulatory Compliance
- Repudiability and lack of forensic capability
- Loss of control of services and/or data
- Responsibility ambiguity
- Lack of liability of providers in case of security incidents
- Cost and difficulty of migration to the cloud (legacy software, etc.)
- Vendor lock-in

As with other applications of ICT, the cloud computing threat sources include accidents, natural disasters, hostile governments, criminal organizations, terrorist groups, intentional and unintentional introduction of vulnerabilities through internal and external authorized and unauthorized human, and system access, including but not limited to employees and intruders.

In addition to the many economic and technological advantages that cloud computing offers to our society, there are also significant security benefits in migrating applications and usage to the cloud, as noted by ENISA in their reports on cloud computing. The shared resources available in clouds also potentially include rare expertise, shared best practices and advanced security technologies, beyond the means or abilities of the vast majority of SMEs, most larger companies and even many government bodies, to provide for their in-house systems.

On the longer-term, in particular once better certification schemes will have been put in place (based on the available set of security standards) and legal obligations will be better enforced, the variety and coverage of services available with the right level of security will be enlarged and offer significant business opportunities to the consumers. Many EU and international efforts are being aimed towards improving security, assurance and transparency with the purpose of creating these trustworthy clouds.

With regard to standards: current international security standards, such as the ISO/IEC 27000 series, are already widely used (with adaption where necessary) by global cloud providers, and increasingly used by smaller providers. New standards and certification schemes, including cloud-specific ones, are also being developed and brought into use, with the explicit intent of encouraging & further illuminating good practice by providers, in a form that is comprehensible to current and potential future cloud consumers.

3.2.3.3 Security and Privacy objectives

The challenges relating to cloud computing highlight the need to consider data and systems protection in the context of logical as well as physical boundaries. Major security objectives for cloud computing are the following:

- Protect data from unauthorized access, disclosure and modification
- Prevent unauthorized access to cloud computing resources
- Ensure isolation
- Ensure service availability
- Ensure effective governance, control and compliance processes are in place
- Ensure appropriate security provisions for cloud applications
- Ensure security of cloud connections and networks
- Enforce privacy policies
- Ensure incident prevention, detection and response

Key issues that need to be addressed when assessing security standards for cloud computing are

- Cross-border legal issues, including variations in data protection regulations
- Conflict of interest between cloud customers and national security of the hosting country
- Visibility and transparency
- Assurance and trust
- Certification, audit and testing
- Identity and Access Management
- Provider use of the services of other providers
- Virtualization and multi-tenancy risks
- Data location control
- Secure data deletion and the exit process

Many new standards have been developed or are under development to address some of these objectives and key issues. It should be noted though that with the exception of cloud computing governance and assurance standards which are specifically developed for and aimed at the cloud, existing standards were built with ‘traditional IT and security’ in mind and therefore may not completely satisfy cloud specific needs.

Although cloud computing is fundamentally a new business and service delivery model, it also has implications for the technology used to deliver such services. For example, the use of multi-tenancy environments, virtualization, shared data storage and the ease of data being transferred on a global scale.

3.3 Description of Use Cases Analyzed

Some Use Cases have been developed by TG3 to define the list of activities that serve for the mapping of relevant documents (listed in Annex 1 and Annex 2). These Use Cases can be mapped (fully or partly) with the UC developed by TG2 that are listed in Annex 3.

The mapping between the Use Cases described below and these listed in Annex 3 is the following:

UC	Title	UC in Annex 3	Focus
AC	App on a Cloud	Based on UC 78	SLA
CB	Cloud Bursting	UC 85	IOP
SD	Processing Sensitive Data	Based on UC 71	SEC
DI	Data Integrity	Based on UC 71	SEC
HA	High Availability	UC 26	SEC

3.3.1 UC AC: App on a Cloud

An Enterprise develops an App on a Cloud Service for their end users
Focus: Service Level Agreement
Related TG2 UC: based on UC 78

An organization chooses to develop a cloud computing application with components that run on multiple clouds simultaneously. This may include a computing cloud node that uses services of a storage Cloud Service Provider at run time to store/access data, and probably further services hosted by other clouds. We focus on the computing cloud which must support certified levels of assurance regarding key non-functional properties like security and dependability, so that customers can preserve the desired assurance level across multiple provisioning. Besides the non-functional properties the customer (the enterprise) should be able to request the QoS of the cloud service necessary to satisfy the performance requirements of their end-users.

In this use-case, the cloud service provider is assumed maintaining a repository of service level agreement templates reflecting different offerings in terms of non-functional and QoS parameters as a starting point for creating SLAs. Its customer can select the most appropriate one regarding its requirements. The template either relates to a cloud service offered under a fixed set of terms or would be the base for further negotiations with the cloud service provider. Based on the template, a Service Level Agreement for the cloud service can be created between the customer and the provider and the provider will provision the resources needed by the customer to deploy its application with the performance properties as needed for their end-users.

The roles involved here are the cloud service customer (the Enterprise), the cloud service provider and the end-user service customer. Sub-roles within the cloud service customer are the customer business manager and the customer cloud service administrator. Sub-roles within the cloud service provider include the business manager, the cloud service manager and the cloud service administrator.

The assumption is that the application is owned or acquired by the cloud service customer and that the cloud service is either an IaaS service or a PaaS service which enables the customer to deploy the application onto the provider's compute, storage and networking resources and to make the application available from there for the customer's end users.

3.3.2 UC CB: Cloud Bursting

Cloud Bursting across multiple clouds
Focus: Interoperability
Related TG2 UC: 85

The cloud bursting use case describes the scenario where multiple clouds have to work together. The typical example is the coexistence of public and private cloud and the possibility to do some “offload” between them.

The focus in this use case will be on the Infrastructure as a Service (IaaS). For illustration, we will consider the example of a private cloud of a company, with running virtual machines (VMs), that needs an extra computational power from a public cloud (add new VMs): (a) to enlarge the VMs Cluster (b) to disparate set of VMs. The difference between the two cases is explained as below:
(a) this case corresponds to a well managed set of VMs over the same virtual network
(b) this case corresponds to disparate VMs connected in non structured/managed way

In the description below, we will focus on the case (b) in a first phase.

In this cloud bursting scenario, we can distinguish the following phases:

Phase 1: Acquisition of Cloud Service
The principal activities in this phase are to setup the ability to burst from cloud A (Private) to cloud B (Public). This includes, firstly, the selection of a second provider and then the agreement on SLA. The latter should consider an agreement between the provider and customer on common management interfaces to enable interoperability and common formats of the data (e.g. VMs image).

Phase 2: Operation of Cloud Service
This phase will start with the Creation of a VM image for the public cloud (B) corresponding to the exact functional objectives of the VM image running on the private cloud (A), for a coordinated use on A and B. This requires knowing exactly what functional differences could exist between B and A (if any).

Then the provision of (set of) VMs starts This will include the upload of the VM image onto the public cloud (B), the start of the technical process that will be able to start VM instances on B when required or the start the VM instances on B. Note that this activity (i.e. CB_2.2) can be either done in one atomic operation or separately depending on the interfaces provided.

Finally, the runtime management & administration will operate. The objective is to allow the customer to have an overview and control of the running phase. The customer should then be able to monitor VMs. This includes the compliance with SLA and the possibility to reconfigure resources (e.g. re-scaling CPU and memory resources). Specific interfaces to allow for that are then required.

Phase 3: Termination of Cloud service
Two activities should be done according to the atomicity of the phase 2: the first is to kill individual VMs, and the second, to remove the image from the cloud B.

Note that the use case can be extended to workload migration which could generate more advanced and complex steps.

3.3.3 UC SD: Processing Sensitive Data

An enterprise wants to use an online cloud application (SaaS) to process sensitive data, including Personally Identifiable Information (PII).
Focus: Security & Privacy
Related TG2 UC: Based on UC 71

The following section describes a simple use case which is addressing in very simple terms one of the key issues related to security and privacy in cloud computing.

The use case focuses mainly on data protection compliance. The assumption is that through this use case the analysis will be able to identify both the main privacy and security standard requirements. In other terms, a potential Cloud Service Customer should be able to obtain enough details on which technical and governance security measures are implemented by the cloud service provider to satisfy the legal and technical requirements for data protection compliance.

3.3.3.1 Use Case Description

The enterprise looks forward to the additional features some cloud services have to offer, but at the same time has to be careful to fulfill its obligations under Data Protection (DP) legislation as a data controller.

The roles involved in this use case are:

- Cloud Service Customer
    - business manager
    - cloud service administrator
- Cloud Service Provider
- Cloud Service Partner
    - cloud auditor

Phase 1: Acquisition of Cloud Service
In this phase, the customer examines different service offerings, particularly focusing on legal obligation regarding PII, and selects the service of one SaaS provider.

Phase 2: Operation of Cloud Service
In this phase, the service is operational.

Phase 3: Termination of Cloud Service
In this phase, the customer terminates its use of the cloud service.

3.3.4 UC DI: Data Integrity

Move three-tier application from on-premises to cloud
Focus: Security
Related TG2 UC: Based on UC 71

An organization (customer) moves a three-tier application from an on-premises data center to a cloud infrastructure provider (Cloud Service Provider) that will run the application off-premises.

A three-tier application consists of the frontend web server, back-end database, and middle-tier business logic that services data requests between the user and the database.

The data associated with the application is sensitive and confidential and it is necessary to assure its integrity.

Issues to be considered include:

- suitable SLA/certificate,
- responsibility for the provision and application of encryption,
- key management processes
- data validation
- etc.

As a side scenario, the organization (Cloud Service Customer) can also evaluate the possibility of substituting the in-house developed software with existing cloud applications and services in the process of migrating from on-premises to cloud, thus taking full advantages of the potential of cloud computing. This “shop around for services” scenario requires the ability to evaluate non-functional properties of existing cloud-based services (e.g., performance, security, availability) possibly expressed via Service Level Agreements (SLAs)/certificates.

The roles involved here are the Cloud Service Customer (the Enterprise) and the Cloud Service Provider.

3.3.5 UC HA: High Availability

Provide high availability in the event of a disaster or a large-scale failure
Focus: Security
Related TG2 UC: 26

The cloud system of Municipality A (here Cloud Service Provider) is damaged due to a natural disaster, and cannot continue to provide its services.

It autonomously examines the impact of the disaster and determines that it is unable to continue to provide services, and performs disaster recovery by using the resources (applications, middleware, database servers, etc.) of the remote Municipalities B, C, and D pre-arranged for such service recovery (Cloud Service Providers for those services).

Services that are normally provided by Municipality A are now temporarily provided by other municipalities, and consumers (second level Cloud Customers) can continue to access the services.

If the resources required for recovery are too huge to provide high availability for all the services, those that are given high priority in providing high availability, such as Service 1, are recovered using the resources of a municipality that can provide high availability.

Services that require early recovery (even when part of their quality requirements are satisfied only on a best-effort basis, such as Service 2) are recovered using the resources of a municipality that can achieve early recovery.

The roles involved here are several Cloud Service Providers: Municipality A which suffers from a disaster and needs to migrate all services (that now becomes a Customer of the other Municipalities) to other Cloud Service Providers (Municipalities B, C and D), the Cloud Service Provider (Municipality A) and the cloud service customers (the clients of Municipality A).

The specific characteristic of this use case is that the cloud provider A has a double role: Firstly, A is a service provider providing services to its customers hosted on its own cloud resources. Secondly, A is a customer of cloud providers B, C, and D with whom A negotiates and creates Service Level Agreements for the use of fallback resources in order to be prepared for a local outage due to a disaster.

From the perspective of provider A the providers B, C, and D form a federation where A can deploy data and services to the members of the federation taking into account their capabilities and guaranteed QoS, and the requirements of its services.

From a security standpoint, the assumptions are that:

- Sensitive data and confidential data (possibly also including PII)
- External services provided by Municipality A contain some tables with encrypted data. The corresponding application has the key to decrypt and present this data to the end-user, and this set-up must remain unchanged when moving to the other cloud providers.
- Municipality A’s admin users access the cloud services (e.g., for maintenance purposes), using a VPN gateway.
- The cloud service is provided through an IaaS platform, where existing (legacy) software and data (databases) are installed on VMs. For availability reasons, those VMs are then moved to the other selected cloud providers B, C, D in regular intervals.

3.4 Phases and activities in Use Cases

From the analysis of each of the five Use Cases above, a list of activities in each of the three phases (1 to 3, see section 3.1) have been identified. These five lists have been consolidated and, whenever it was possible, some generic activities (common to two or more of the Use Cases) were identified.

In the remainder of this section, the naming convention for the activities is the following:

GENx.y   means a GENeric activity that apply to the Use Cases listed in the right-most column;
UCx.y   means a specific activity only applicable to the UC (where UC can be AC, CB, etc.).

3.4.1 Pre-condition to all phases

Pre-condition	Short Summary	Description	UC
ALL_1.0	Terminology and Metrics	It is a precondition for the following steps that each service level objective uses consistent and widely accepted and agreed terminology as well as clearly defined KQIs and metrics.	AC, DI, HA, SD

3.4.2 Phase 1: Acquisition of Cloud Service

The principal activities of the cloud service customer in this phase are service selection and purchase, performed by the customer business manager subrole, which involves:

Activity	Short Summary	Description	UC
GEN_1.0	Requirements specification	Functional requirements of a cloud service are specified by means of a service description. Non-functional requirements are specified by means of SLAs/certificates. The same applies for one or multiple provider(s). These requirements will be matched with the provider capabilities in GEN_1.1.	AC, DI, HA, SD

Activity	Short Summary	Description	UC
GEN_1.0a	Security & Privacy Requirements specification	The customer must analyze its Data Privacy obligations with respect to the PII (if any) that will be processed by the cloud services, and build a set of security and privacy requirements that must be fulfilled by the cloud service provider. This list will be used afterwards (cf., activity GEN_1.1) to evaluate the different available cloud services. Particular attention must be paid to the rights that a PII principal may have relating to their PII data (e.g. right to examine the data which the customer holds about the principal).	AC, DI, HA, SD
GEN_1.1	Service assessment and comparison	Examining the cloud service offerings of (one or more) cloud service providers to determine if the service offered meets the business and technical and security requirements of the customer and comparing it with other offerings on the market. This typically involves the reading of a service catalogue and documentation for each service, which should include information about the service and its SLAs, plus business information including pricing, and security & privacy. With respect to the latter, the customer retrieves information about the service offering from the provider's product catalog, including: • service availability, including redundancy & disaster recovery • confidentiality & integrity of data flowing between the customer and the SaaS application • measures to ensure availability, confidentiality and integrity of customer data that is stored on the providers systems and used by the SaaS application • location(s) for storage of the customer data • acknowledgement by the provider that the SaaS service involves the storage and processing of PII and that the provider plays the role of PII Processor in relation to this PII. • logging and reporting capabilities, both of routine operations and also relating to security incidents. Examination of the cloud service provider's security & privacy may be supported by a recurrent certification process.	AC, DI, HA, SD
GEN_1.2a	Negotiation with one provider	Negotiation of the terms for the cloud service (if the cloud service provider permits variable terms for the service) or selection among market offerings. If the cloud service provider permits variable terms for the service, then the customer might need to specify additional security & privacy requirements for the provider to implement. Includes the definition of the termination process, metrics and related actions such as data migration in the SLA	AC, CB, DI, HA, SD
GEN_1.2b	Negotiation for multiple providers	Negotiation of the terms for the cloud service are similar to GEN_1.2a. In addition, determining the individual providers for deployment of the different applications and the data according to the requirements of the service consumers.	HA
GEN_1.3	Standards expression of SLA	Agreement on SLA/certificate data format, acceptance of the contract for the cloud service and registration with the cloud service provider	AC, DI, SD, HA
CB_1.1	Enabling Interopera-bility	Agreement on common interfaces between the provider and the customer, including management and administration interfaces	CB

Activity	Short Summary	Description	UC
CB_1.2	Enabling Data Portability	Agreement on common formats of the Data (e.g. VMs image)	CB
GEN_1.4	Integration of cloud solution with legacy systems	Integration with e.g. legacy OSS/BSS, security systems, etc.	DI, HA
HA_1.6	Data Provisioning in Multiple Clouds	Regular upload/import of VMs and latest data from one provider to the other cloud providers (e.g. to facilitate data recovery).	HA

The principal activities of the service provider in this phase are:

Activity	Short Summary	Description	UC
GEN_1.5	Determining SLA targets / thresholds	Setting up targets and thresholds in the SLA (based e.g. on its capabilities and feedback from its business)	AC, DI, HA
GEN_1.6	SLA publication	Drafting and publishing an SLA including compliance with regulatory norms	AC, DI, HA

3.4.3 Phase 2: Operation of Cloud Service

The principal activities of the cloud service customer and its end-users in this phase are:

Activity	Short Summary	Description	UC
HA_2.0	Deployment over multiple providers	Deployment of the different VMs with data and applications into the negotiated infrastructures of the different cloud providers.	HA
GEN_2.1	Independent monitoring of SLA	Independent monitoring of service levels, including application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service	AC, DI, HA
GEN_2.2	Receiving and processing SLA reports	Receiving and processing service level reports from the cloud service provider (or a trusted third party (auditor) as e.g. discussed in TMF) , comparing them with SLA objectives.	AC, DI, HA, SD
GEN_2.3	Reporting SLA infringements	Reporting service level agreement infringements detected by the cloud service customer or end-users	AC, DI, HA
GEN_2.4	Responding to SLA infringements	Responding to SLA infringements either as reports from the cloud service provider or detected by the cloud service customer (for example, informing their end-users of service interruptions, switching service to an alternate provider, raising a ticket, claiming service credits etc.)	AC, DI, HA, SD
GEN_2.5	Resolving SLA infringements disputes	Resolving disputes around SLA infringements	AC, DI, HA
GEN_2.6	Administration of users, identities and authorizations	Administration of users, identities and authorizations.	AC, DI, HA, SD

The principal activities of the cloud service provider in this phase are:

Activity	Short Summary	Description	UC
CB_2.1	Creation of a VM image for the public cloud	Creation of a VM image for the public cloud (B) corresponding to the exact functional objectives of the VM image running on the private cloud (A), for a coordinated use on A and B. This requires to know exactly what functional differences could exist between B and A (if any).	CB
CB_2.2	Provision of an infrastructure to allow the creation and management of (set of) VMs	Provision of an infrastructure to allow the creation and management of (set of) VMs - Upload the VM image onto the public cloud (B) - Start the technical process that will be able to start VM instances on B when required or start the VM instances on B · an overview about the running phase · monitoring of VMs (e.g. compliance with SLA) · possibility to reconfigure resources (e.g. re-scaling resources - add or remove VMs)	CB
GEN_2.7	Monitoring Service Levels	Monitoring service levels and reporting them to the cloud customer. The content of this activity depends strongly on the type of attributes/targets being monitored. Key examples are found in the sub-activities below. NB. the information contained in these reports may need to be sanitized to avoid disclosing sensitive data.	AC, DI, HA, SD
GEN_2.7a	Monitoring: Availability	Monitoring service levels: Availability	AC, DI, HA, SD
GEN_2.7b	Monitoring: Incident management	Monitoring service levels: Incident management (targets)	AC, DI, HA, SD
GEN_2.7c	Monitoring: Storage performance	Monitoring service levels: Storage performance	AC, DI, HA, SD
GEN_2.7d	Monitoring: Processing performance	Monitoring service levels: Processing performance	AC, DI, HA, SD
GEN_2.7e	Monitoring: Networking performance	Monitoring service levels: Networking performance	AC, DI, HA, SD
GEN_2.7f	Monitoring: Access security event information	Monitoring service levels: Access security event information	AC, DI, HA, SD
GEN_2.7g	Monitoring: uptime	Monitoring service levels: Uptime	AC, DI, HA, SD
GEN_2.8	Preventive response to SLA infringement	Responding (in particular preventively) to SLA infringement incidents: · Availability, Incident Management, Elasticity, etc.	AC, DI, HA

3.4.4 Phase 3: Termination of a cloud service

The principal activities of the cloud service customer and its end-users in this phase are:

Activity	Short Summary	Description	UC
GEN_3.1	Termination process initiation	Launching the termination process (as defined in Phase 1), which might include retrieval of image (IaaS) and data (SaaS, quick switch). Ensure both the return of all customer data (including PII) and its secure deletion.	AC, CB, DI, HA, SD
GEN_3.2	Termination: SLA evaluation	Evaluate whether the SLA was fulfilled, i.e. the outsourced application did run in the new environment and fulfilled all functional and non-functional requirements	DI, HA
GEN_3.3	Contract termination	Terminating the contract as defined by SLA or on demand	AC, DI, HA

The principal activities of the cloud service provider in this phase are:

Activity	Short Summary	Description	UC
GEN_3.4	Providing an evaluation report	Provide an evaluation report on closing, including confirmation of deleting customer data at a defined point of time as agreed in the SLA	AC, DI, HA
GEN_3.5	Resolving disputes	Resolve disputes around cloud service termination	AC, DI, HA
GEN_3.6	Transaction records retention	Keep a record of past transactions, under data retention obligations.	HA, SD

4. Map of Standards and Specifications

This section contains the mapping of activities defined in the above section to the list of documents defined in Annex 1 and Annex 2:

- Activity and short summary: refers to the activity name and short summary above
- Related Standards: see list in Annex 1
- Related Work: see list in Annex 2
- Remark: explains why a Specification or Standard has been included in the table.

4.1.1 All Phases

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
ALL_1.0	Terminology and Metrics		[TMF8] TR178 SLA management	Provides a good overview on terms, roles & responsibilities and Cloud SLA Metrics.
		[ISO12] ISO/IEC 19086		Still in draft.
			[ITU1], [ITU2], [ITU3]	Published.
			[NIST1], [NIST2], [NIST5] Metrics	Work in progress.
			[ODCA3], [ODCA9]	Proposed cloud commercial framework and standard units of measure for IaaS
			[TMF10] Business Metrics Solution Suite 2.0	Non cloud computing-specific document dealing with business relationships

4.1.2 Phase 1: Acquisition of Cloud Service

Cloud Service Customer activities

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
GEN_1.0	Requirements specification	None at this time. Standards needed.	This is on-going work at TMF, OGF, OASIS, ODCA, …	Such standards may help comparison of providers.
			SLA* [SLA1], SLAware [FIW1].	
			FP7 projects results [FP7-SLA]	
GEN_1.0a	Security & Privacy Requirements specification		[CSA2] Security Guidance	There is a number of non cloud computing-specific but widely used and very relevant security standards (e.g. OAuth 2.0, SAML 2.0, Kerberos)
			ISO/IEC 27001, ISO/IEC 27002	
			ITU X.1600	

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
			Certification created by the FP7 Europrise project.	Europrise specifications is a standard of privacy requirements compliant with DP legislation.
GEN_1.1	Service assessment and comparison	[OGF4] GFD.192 WS-Agreement		WS-Agreement (GFD.192) is a recommendation of the Open Grid Forum for creating electronic SLAs
			[CSCC4] SLA White Paper	CSCC is a high level guide for end-users what to pay attention to when accepting an SLA of a provider
			[TMF3] GB963	GB963 is intended for Enterprise Cloud Service Providers desiring to offer a commercially credible SLA based on ECLC “Enterprise-Grade External Compute IaaS v1.0”, and for an Enterprise Customer seeking enterprise-grade SLAs.
			[CSMIC1] SMI Framework	Initial standard specification for comparison of cloud services. This is monitored and progressed by CSMIC
		[CSA1] CCM	[CSA5] CAIQ	Contains answers about which security measures a provider has taken.
			SLA* [SLA1], SLAware [FIW1]	Specification of flexible SLA models
		[ISO5], [ISO6] 27001/2		If the provider is ISO 27001/2, it shows a certain level of security measures are in place (which fulfills part of the Data Protection legislation).
GEN_1.2a	Negotiation with one provider	[OGF5] GFD.193 WS-Agreement Negotiation		WS-Agreement Negotiation is a proposed recommendation of the Open Grid Forum for multi-round negotiations of SLAs on top of WS-Agreement.

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
			[TMF3] GB963 [TMF1] GB917 [TMF14]	GB917 is a handbook that provides a full set of definitions, rules and methodology for the specification and development of SLA’s.
			[TMF8] TR178	
GEN_1.2b	Negotiation for multiple providers		[CSA5] CSA/CAIQ	
GEN_1.3	Standards expression of SLA	ISO SC38 SLA Framework & Terminology (in process)		
CB_1.1	Enabling Interoperability	[OGF1], [OGF2], [OGF3] OGF/OCCI		
		[DMTF1] CIMI		
		[ISO4] CDMI	[SNIA1] CDMI	Same specifications
		[OASIS1] CAMP		
		[OASIS5] TOSCA		
CB_1.2	Enabling Data Portability	[DMTF3] OVF		
		[OASIS5] TOSCA		
GEN_1.4	Integration of cloud solution with legacy systems	None at this time. Standards needed.	[CSA7] SECaaS	
HA_1.6	Data Provisioning in Multiple Clouds	Same as CB_1.1 and 1.2 above		

Cloud Service Provider activities

Activity	Short Summary	Related Standards	Related work	Remark
GEN_1.5	Determining SLA targets / thresholds	[OGF4] WS-Agreement		Identical to Customer view
			[ENISA1] Procure Secure	
GEN_1.6	SLA publication	[OGF4] WS-Agreement		

Activity	Short Summary	Related Standards	Related work	Remark
		[CSA1] CCM 3.0	[CSA5] CAIQ	

4.1.3 Phase 2: Operation of Cloud Service

Cloud Service Customer activities

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
HA_2.0	Deployment over multiple providers	[OGF3] OCCI		
		[DMTF1] CIMI		
		[OASIS5] TOSCA		
GEN_2.6	Administration of users, identities and authorizations.		[CSA7] SECaaS	There is a number of non cloud computing-specific but widely used and very relevant security standards (e.g. OAuth 2.0, SAML 2.0, Kerberos)
			[OASIS2] ID in the Cloud use cases	
GEN_2.1	Independent monitoring of SLA	[CSA3] CTP		
		[CSA4] A6		
		DMTF CADF		
GEN_2.2	Receiving and processing SLA reports	[CSA3] CTP		
		[CSA4] A6		
		DMTF CADF		
		[QuEST1] TL 9000 Measurement		
GEN_2.3	Reporting SLA infringements	[OGF4] WS-Agreement	IETF Abuse Reporting Format	Challenge is some degree of trust and automatization.
GEN_2.4	Responding to SLA infringements	None at this time. Standards needed.		Challenge is some degree of trust and automatization.
			[FP7 projects results: see [FP7-SLA].	

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
GEN_2.5	Resolving SLA infringements disputes	Not sure standards are needed.	[TMF2] GB960	Consider progress in Cloud SIG.

Cloud Service Provider activities

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
CB_2.1	Creation of a VM image for the public cloud	[DMTF3] OVF		
CB_2.2	Provision of an infrastructure to allow the creation and management of (set of) VMs	[DMTF1] CIMI		
		[OGF1], [OGF2], [OGF3] OCCI		
		[DMTF3] OVF		
GEN_2.7	Monitoring Service Levels	[CSA3] CTP		
		[CSA4] A6		
			DMTF/CADF	
		[OGF4] WS-Agreement		
			[ODCA9] Standard Units of Measure	
GEN_2.7a	Monitoring: Availability	[QuEST2] TL9000 Requirements		
			[ETSI12], [ETSI19] Resiliency Requirements	
GEN_2.7b	Monitoring: Incident management	Not at this time. Standards welcome.	IETF/ARF, X-ARF, M-ARF	
GEN_2.7c	Monitoring: Storage performance	Not at this time. Standards welcome.	SNIA/Storage Performance Benchmarking Guidelines	Really applicable at run time ?
GEN_2.7d	Monitoring: Processing	Not at this time. Standards welcome.	SPEC benchmark	Really applicable at run time ?

Activity	Short Summary	Related Standards & Specifications	Related work	Remark
	performance			
GEN_2.7e	Monitoring: Networking performance	Not at this time. Standards welcome.	[IETF4] ALTO, [IETF9] IPPM	
GEN_2.7f	Monitoring: Access security event information	Not at this time. Standards welcome.		
GEN_2.7g	Monitoring: uptime	Not at this time. Standards welcome.		
GEN_2.8	Preventive response to SLA infringement			

4.1.4 Phase 3: Termination of Cloud service

Cloud Service Customer activities

Activity	Short Summary	Related Standards & Specifications	Related work	Remarks
GEN_3.1	Termination process initiation		[TMF1] SLA Mgmt Handbook	May be resolved through certification.
			[CSA2] Security Guidance	Difficult to standardize
			Europrise	
GEN_3.2	Termination: SLA evaluation	[OGF4] WS-Agreement		
			[TMF1] SLA Mgmt Handbook	
			[TMF8] Enabling E2E SLA Mgmt	
GEN_3.3	Contract termination	[OGF4] WS-Agreement		
			[TMF1] SLA Mgmt Handbook	

Cloud Service Provider activities

Activity	Short Summary	Related Standards & Specifications	Related work	Remarks
GEN_3.4	Providing an evaluation report	None at this time. Standards needed.		Such standards may help comparison of providers.
			[TMF1] SLA Mgmt Handbook	
			[TMF8] Enabling E2E SLA Mgmt	
GEN_3.5	Resolving disputes	Not sure standards are needed.		Consider progress in Cloud SIG.
GEN_3.6	Transaction records retention			Consider progress in Cloud SIG.

5. Global cloud standardization landscape

The following organizations have been considered for the elaboration of the list of Standards and Specifications and the list of Reports and White Papers relevant to the cloud (as outlined in section 2):

ATIS	Alliance for Telecommunications Industry Solutions
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique
CSMIC	Cloud Services Measurement Initiative Consortium
CSA	Cloud Security Alliance
CSCC	Cloud Standards Customer Council
DMTF	Distributed Management Task Force
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GICTF	Global Inter-Cloud Technology Forum
IEC	International Electrical Commission
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
ODCA	Open Data Center Alliance
OGF	Open Grid Forum
OSS/BSS	Operations Support System/Business Support System
QuEST	Quality Excellence for Suppliers of Telecommunications
SNIA	Storage Networking Industry Association
TIA	Telecommunications Industry Association
TMF	TeleManagement Forum
TOG	The Open Group

These organizations have developed or are in the process of developing Standards, Specifications, Reports and White Papers that are listed in Annex 1 and Annex 2.

6. Conclusions / Recommendations

Introduction

Cloud computing has started with the activities of multiple organizations and industry players that have offered new services, based on a variety of technologies and platforms. It has gained momentum and credibility, thus generating new offers and demands for more complex use cases and services.

In this perspective, standardization is seen as a strong enabler, potentially bringing more confidence to investors as well as to customers – in particular SMEs, Municipalities, Governments, etc. Regulators and policy makers are in turn willing to understand how they can help solidify the industry without disrupting innovation.

Therefore, it is important to understand the actual status of standardization. CSC was asked to provide an accurate answer to a number of questions – even if this assessment is only as a snapshot of a very fluid situation. Early conclusions of its work are summarized here.

6.1 Lessons learned

A Dynamic Landscape

Cloud is a very dynamic industry segment where a large number of actors are delivering new technologies, products, solutions. In support of this, cloud computing standards groups are producing a large number of documents, circulating and referenced at some degree. This is reflecting strong innovation, and presenting significant choice for customers, perhaps too much choice. In order to get a clearer picture of the relevance of all this information, it is important to understand in a standardization perspective, which actors and which elements of their production are most relevant.

It is important to keep in mind that cloud computing is not completely new and that many standards used for cloud computing are not cloud specific. In the future, these standards may continue to evolve to better reflect cloud computing scenarios.

Regarding standards that are more specific to cloud computing, CSC has identified around 20 organizations whose results are largely significant for those who want to deal with cloud services: both Standards Development Organizations that have created standards and industry initiatives that have produced standards and other related materials (and probably more of the latter). The global number of documents that CSC is referencing in this document is around 150 in two categories: 'Standards & Specifications' and 'Reports & White Papers'. From this standpoint, it is not possible to consider cloud standardization as a 'jungle'.

Moreover, the analysis of typical Use Cases has lead to the identification of a relatively small number of generic (i.e. common to many such use cases) or specific activities that are undertaken across the whole 'life-cycle' of the associated cloud services. Once the group of around 150 documents mentioned above has been associated to these activities, it is easy to observe that the number of relevant standards in a given activity is rarely above 2. This gives an indication that cloud standardization is focused.

In short: the Cloud Standards landscape is large but not chaotic and by no means a 'jungle'.

Maturity and adoption

Given its dynamism, Cloud Standardization will likely mature as new standards for technology elements are needed. We will see this starting to happen within the next 12-18 months.

Emerging Cloud specific standards are not seeing widespread adoption by cloud providers to date. Cloud standards need to be flexible enough to allow each providers unique selling points to be advertised and consumed.

For example, adoption may be encouraged if mechanisms are found for domain-specific stakeholders to agree on shared vocabularies and formal definitions that are machine readable. Further research is required in this area. Some cloud specifications are being matured and adopted by the community – additional, appropriate support or investment could accelerate their maturity into official standards that meet the needs of cloud providers and consumers alike.

Another aspect of the cloud computing environment that is worthy of consideration is the role of the various open source projects which are addressing many of the topics discussed in this report. While not formal standards, the open source projects are creating tried-and-tested APIs, protocols and environments which address aspects of interoperability, portability and security relating to cloud computing. It is possible that future specifications and standards may derive from one or more of the open source projects. Some examples of positive interaction have already been seen between standards bodies and open source projects that should be encouraged. The role of open source projects was not addressed in this report.

- Interoperability

Interoperability in the cloud requires standardization in APIs, data models, vocabularies. Cloud interoperability standards are being actively developed with significant progress already made in standardizing compute and storage APIs, IaaS data models and high level cloud vocabularies.

There is however a fundamental challenge for interoperability standards in the cloud: for maximum adoption, flexibility and automation it is important for arbitrary terms (including service monitoring requirements and service level agreement concerns) to be unambiguously defined. However, the rapid evolution of cloud technologies means that such details cannot be quickly incorporated into traditional standards.

Further effort is required to explore how best to meet this challenge. Interoperability standards need to be formal and complete enough that cloud computing workflows can be automated, but flexible enough that new concepts in the underlying technology or in a particular domain (e.g. public cloud procurement) can be quickly introduced and accommodated.

- Security

There are many good and widely adopted existing standards which relate to security that can be used by cloud computing. A number of new security and privacy standards, best/good practises and recommendations have been developed or are under development, which address some of the challenges associated with the cloud.

One problem that exists for security specifications in particular is that security is a dynamic topic - so, for example, an encryption algorithm that works well at one point in time could be broken or found to have exploitable flaws at some later date. Meanwhile, there is a flow of newer technologies from researchers and security technologists who aim to improve the security of systems. So some security standards dealing with specific technologies are likely to become obsolete over time and newer technologies need to be adopted, once they are proven and agreed. Any approach to cloud computing security needs to deal with this dynamic aspect of the technologies required to provide secure cloud services over time.

Our analysis has shown that cloud computing governance and assurance standards specifically developed for and aimed at the cloud already exist (e.g., cloud controls framework, security cloud architectures, continuous monitoring of cloud service provider's) and some of them are considered as sufficiently mature to be adopted.

Further standardization work may be helpful as a supplement to best practices in areas such as incident management, cloud forensics, and cloud supply chain accountability management.

Potential users of this report, should clearly identify their security and privacy requirements (including legal and regulatory compliance), in order to assess if in their *particular context* (e.g., organization, business driven, …) the identified standards are also relevant and applicable.

➢ Service Level Agreement

There are relatively few existing standards that apply to service level agreements for cloud services.

The main requirement for standardization in relation to Service Level Agreements is the creation of an agreed set of terminology and definitions for Service Level Objectives, and an associated set of Metrics for each service level objective. This will enable cloud service customers to have a clear understanding of the service levels which apply to a particular cloud service and how they will be measured. For cloud service providers, such standard definitions would make it easier to create SLAs that describe their services and would make it easier to differentiate cloud services which offer different service levels.

In today's cloud computing business, there is interest in dynamically negotiated electronic SLAs.

State-of-the-art is one standard for creating agreements and one specification for multi-round negotiations. Moreover, there exist a number of activities aiming to develop recommendations and standards around Service Level Agreements as they apply to cloud services.

Coverage And Gaps

Important gaps in the Cloud standards landscape have been identified. New cloud computing standards, or cloud computing specific extensions to existing standards that fill these gaps should be encouraged.

➢ Interoperability

Coverage of management protocols and interfaces is maturing, particularly regarding IaaS. Management specifications for PaaS and SaaS require more effort. There are many proprietary and open source solutions, but very few, if any standards. This is potentially an issue since vendor lock-in is a significant concern in relation to cloud computing services.

Other domains where there is a lack of specifications and standards include:

- Standards to describe cloud computing service metrics
- Standards to provide monitoring information.

➢ Security and Privacy

From a security and privacy perspective, suitable standards are important for the uptake of cloud computing. Our analysis shows a need for a common vocabulary to enable the cloud service customer to express their requirements and understand the capabilities offered by a cloud service provider. Some existing security and privacy standards exist which are helpful in this area but further development of common vocabularies and metrics specific to cloud computing is needed.

Finally, our security and privacy analysis also shows the need for further standardization efforts in the area of accountability and cloud incident management (e.g., related with a SLA infringements). Such work would greatly benefit the whole cloud supply chain, although once again the main challenge is trust/security assurance among the involved stakeholders

- Service Level Agreement

The main requirement for standardization in relation to Service Level Agreements is the creation of an agreed set of terminology and definitions for Service Level Objectives, and an associated set of metrics for each service level objective. Some work is on-going in this area, but it requires completion and adoption by public cloud service providers.

Our analysis of the state-of-the-art in Service Level Agreements shows encouraging progress in domain-independent standards for negotiation and creation of Service Level Agreements involving multiple cooperating SDOs. In some cases, this work has already demonstrated practical field-proven mechanisms for electronic expression and negotiation of Service Level Agreements, but needs to be extended to cover end-to-end multi-party agreements typical of cloud computing usage.

- Regulation, Legal and Governance aspects

The legal environment for cloud computing is highly challenging and a key barrier for adoption. Solutions need to accommodate national and multinational (e.g. EU) and international legal requirements.

Given the global nature of the cloud and its potential to transcend international borders, there is a need for international Framework and Governance, underpinned via global standards.

6.2 Audience perspective

Cloud standardization has achieved significant results though areas for improvement still exist. Its current status has some implications on the action plans of the various intended audiences of this report.

- Cloud Service Providers

The CSC analysis provides the picture of a cloud computing industry that has already developed a set of standards offering important possibilities. It also shows that standardization is facing a number of challenges regarding maturation (e.g. vocabularies, SLA or security), gaps (e.g. federation, cross-border collaboration, verification of legal obligations), support to regulators and policy makers, etc.

- Cloud Service Customers

The Acquisition phase of the Cloud Service Life-cycle is key for the establishment of a contract between the customer and the provider. At this point in time, providers are not using standards to publish their capabilities to allow the customer to retrieve this information in a standardised way and to compare providers. Moreover, no standards exist yet for describing providers' capabilities. Only some written guidance and recommendations exist for customers on how to manage this phase, but one project is under development.

Regarding the Operation phase, the support of standards differs depending on the delivery model: our analysis has shown a maturing support for IaaS whereas more work is required for PaaS and SaaS. Consequently, the global level of trust may vary depending on the services offered.

In addition to the above considerations, additional points can be made regarding the following categories of customers.

- SMEs
  The lack of standards support for SLA definitions and vocabularies is likely to make it harder for SMEs to choose appropriate cloud services and may slow adoption of cloud services by SMEs. From the perspective of cloud service providers, adopting clear standards for the description of cloud services and their SLAs could become a selling point once standards for SLA definitions and vocabularies become available.

- Administrations
  Unlike SMEs, administrations have more resources available for the expression of their requirements and the activities of the Acquisition phase. This may allow them to better prepare the negotiation phase. However, some limitations remains, e.g. when it comes to multi-provider support.

- Governmental Authorities
  As outlined above, the legal environment for cloud computing is highly challenging and a key barrier to adoption. Solutions are need at national and multinational (e.g. EU) and international levels. Governmental authorities support and guidance is expected.

6.3 Way Forward

This report provides a broad overview on the cloud computing standardisation landscape. This accommodates the need as expressed in the European Cloud Strategy of the European Commission. The Commission should take its conclusions out of this report and bring them in as suggestions into the EU Rolling Plan for ICT Standardisation. On the basis of the Rolling Plan all stakeholders shall analyse and coordinate on required actions regarding standards developments.

Moreover, the current report provides a snapshot at a given point in time only. Given the dynamics of the IT market and of cloud computing standardisation, the latter will progress fast and develop further. Therefore, the Commission should provide for CSC to work on an updated report, a new snapshot, in 12 to 18 months from now, considering that the maturation of standardization will be significant in this time frame and new conclusions could help the cloud community to better address its standardization longer-term challenges.

For such an update lessons learned from the first 12 months of work of the CSC should also be considered. A "lessons learned" session leading to a list of improvements to the process and to the document should be held by CSC jointly with the European Commission.

In addition, greater coordination and collaboration between standards bodies should be encouraged, and the European Commission may wish to consider promoting such a dialogue through groups like the ICT Multi-Stakeholder Platform and any 'follow on' activities of the CSC.

7. References and Acronyms

7.1 Acronyms

CDMI	Cloud Data Management Interface
CIMI	Cloud Infrastructure Management Interface
CSC	Cloud Standards Coordination
CSP	Cloud Service Provider
ETSI	European Telecommunications Standards Institute
HLUC	High-Level Use Case
IaaS	Infrastructure as a Service
IOP	Interoperability
OCCI	Open Cloud Computing Interface
OSS/BSS	Operational Support System / Business Support System
PaaS	Platform as a Service
SaaS	Software as a Service
SDO	Standards Development Organization
SLA	Service Level Agreement
TGx	Task Group 1 to 3 of CSC
UC	Use Case
UC AC	Use Case: App on a Cloud (analysed in section 5.3)
UC CB	Use Case: Cloud Bursting (idem)
UC DI	Use Case: Data Integrity (idem)
UC HA	Use Case: General Availability (idem)
UC SD	Use Case: Protecting Sensitive Data (idem)
VM	Virtual Machine
VPN	Virtual Private Network

7.2 References

These are documents that are referred to in the text of this report.

[DA] URL: http://europa.eu/rapid/press-release_SPEECH-12-38_en.htm

[DC1] URL: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[DC2] URL: https://cloudsecurityalliance.org/research/top-threats/

[DC3] URL: http://www.cloudstandardscustomercouncil.org/Security_for_Cloud_Computing-Final_080912.pdf

[FP7-SLA] URL: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2496

[ODCA] Web site: http://www.opendatacenteralliance.org/

[SLA1] Practical Guide to Cloud Service Level Agreements Version 1.0. pages 1-44, May 2012. URL: http://www.cloudstandardscustomercouncil.org/webSLA-download.htm

[SLA2] The Open Cloud Manifesto. Website: http://opencloudmanifesto.org/

Annex 1 List of Standards and Specifications

The list below contains **Standards**, and **Specifications** collected by CSC.

The new European Standards Regulation has been the reference regarding the selection of Standards & Specifications. It refers to "standards" in two ways: a Standard is an output from a formally recognized SDO (such as ETSI or ITU-T), a Specification is a standard from any other form of SDO.

This list is also available in a document that includes additional metadata (columns) and the documents of Annex 2 that can be found on-line at:

http://csc.etsi.org/Application/documentapp/downloadLatestRevision/?docId=180

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[ATIS1]	ATIS	ATIS-0200003	CDN Interconnection Use Case Specification and High Level Requirements	Specification	Published
[ATIS2]	ATIS	ATIS-0200004	CDN Interconnection Use Cases and Requirements for Multicast-Based Content Distribution	Specification	Published
[ATIS3]	ATIS	ATIS-0200005	Cloud Framework for Telepresence Service	Specification	Published
[ATIS4]	ATIS	ATIS-0200006	Virtual Desktop Requirements	Specification	Published
[ATIS5]	ATIS	ATIS-0200008	Trusted Information Exchange (TIE)	Specification	Published
[ATIS6]	ATIS	ATIS-0200009	Cloud Service Lifecycle Checklist	Specification	Published
[ATIS7]	ATIS	ATIS-0200010	CDN Interconnection Use Cases and Requirements in a Multi-Party Federation Environment	Specification	Published
[ATIS8]	ATIS	ATIS-I-0000001	Format of ATIS Namespace	Specification	Published
[ATIS9]	ATIS	ATIS-I-0000002	ATIS XML Schema Development Guidelines	Specification	Published
[CSA1]	CSA	CCM 3.0	Cloud Control Matrix	Specification	Published
[CSA3]	CSA	CTP	Cloud Trust Protocol	Specification	Published
[CSA4]	CSA	A6	Cloud Audit	Specification	Published
[CSA6]	CSA	PLA	Privacy Level Agreement	Specification	Published
[CSA8]	CSA	TCI	Reference Architecture - Trusted Cloud Initiative	Specification	Published
[CSA9]	CSA	OCF	Open Certification Framework	Specification	Published
[CSMIC1]	*CSMIC*	*SMI Framework 2*	*Service Measurement Index - measures for Cloud Services*	*Specification*	*Draft*

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[DMTF1]	DMTF	DSP0263	Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP Specification	Standards	Published
[DMTF2]	DMTF	DSP0264	Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM)	Standards	Published
[DMTF3]	DMTF	DSP0243	Open Virtualization Format Specification V2	Standards	Published
[ETSI29]	ETSI / TC CLOUD	TS 103 142	Test Descriptions for Cloud Interoperability	Specification	Published
[EuroCloud1]	EuroCloud	Star Audit	EuroCloud Star Audit	Specification	Published
[FIW1]	*FI-WARE*	*n/a*	*SLAware: Service Level Agreements Specification*	*Specification*	*Draft*
[ISO1]	ISO/IEC	17203	OVF	Standards	Published
[ISO2]	*ISO/IEC*	*17788*	*Cloud Computing Overview and Vocabulary*	*Standards*	*Draft*
[ISO3]	*ISO/IEC*	*17789*	*Cloud Computing Reference Architecture*	*Standards*	*Draft*
[ISO4]	ISO/IEC	17826	Cloud Data Management Interface (same as SNIA CDMI)	Standards	Published
[ISO5]	ISO/IEC	27001	Information security management systems – Requirements	Standards	Published
[ISO6]	ISO/IEC	27002	Code of practice for information security controls	Standards	Published
[ISO7]	*ISO/IEC*	*27017*	*Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002*	*Standards*	*Draft*
[ISO8]	*ISO/IEC*	*27018*	*Code of practice for data protection controls for public cloud computing services*	*Standards*	*Draft*
[ISO9]	ISO/IEC	20000-1	Service management system requirements	Standards	Published
[ISO11]	*ISO/IEC*	*27036-4*	*Information security for supplier relationships — Part 4: Guidelines for security of cloud services*	*Standards*	*Draft*
[ISO12]	*ISO/IEC*	*19086*	*Cloud computing --SLA framework and terminology*	*Standards*	*Draft*
[ITU8]	ITU-T	X.1600	Security framework for cloud computing	Standards	Published
[ITU9]	*ITU-T*	*X.idmcc*	*Requirements of IdM in cloud computing*	*Standards*	*Draft*
[ITU10]	ITU-T	Y.3501	Cloud Comp Framework & High-level Requirements	Standards	Published
[ITU11]	ITU-T	Y.3510	Cloud Computing Infrastructure requirements	Standards	Published
[ITU12]	ITU-T	Y.3520	resource management framework for e2e cloud	Standards	Published
[ITU13]	*ITU-T*	*Y.ccdef*	*Cloud Computing overview and vocabulary*	*Standards*	*Draft*
[ITU14]	*ITU-T*	*Y.ccic*	*Framework of Inter-cloud*	*Standards*	*Draft*
[ITU15]	*ITU-T*	*Y.ccra*	*Cloud Computing Reference Architecture*	*Standards*	*Draft*
[ITU16]	*ITU-T*	*Y.daas*	*Requirements Reference Architecture of DaaS*	*Standards*	*Draft*
[OASIS1]	*OASIS/CAMP*	*CAMP*	*Cloud Application Management for Platforms (CAMP)*	*Specification*	*Draft*

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[OASIS5]	OASIS/TOSCA	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA)	Specification	Published
[OASIS6]	OASIS/OData		Open Data Protocol	Specification	Published
[ODCA1]	ODCA	n/a	Master Usage Model: Compute Infrastructure as a Service	Specification	Published
[ODCA2]	ODCA	n/a	Master Usage Model: Service Orchestration	Specification	Published
[ODCA3]	ODCA	n/a	Master Usage Model: Commercial Framework	Specification	Published
[ODCA4]	ODCA	n/a	Usage: Data Security Framework	Specification	Published
[ODCA5]	ODCA	n/a	Virtual Machine (VM) Interoperability in a Hybrid Cloud Environment	Specification	Published
[ODCA6]	ODCA	n/a	Master Usage Model: Software-Defined Networking	Specification	Published
[ODCA7]	ODCA	n/a	Master Usage Model: Scale out Storage	Specification	Published
[ODCA8]	ODCA	n/a	Master Usage Model: Information as a Service	Specification	Published
[ODCA9]	ODCA	n/a	Usage: Standard Units of Measure for IaaS	Specification	Published
[OG1]	*The Open Group*		*Cloud Computing Reference Architecture*	*Specification*	*Draft*
[OGF1]	OGF	GFD.183	Open Cloud Computing Interface - Core	Specification	Published
[OGF2]	OGF	GFD.184	Open Cloud Computing Interface - Infrastructure	Specification	Published
[OGF3]	OGF	GFD.185	Open Cloud Computing Interface - RESTful HTTP Rendering	Specification	Published
[OGF4]	OGF	GFD.192	Web Services Agreement (WS-Agreement)	Standards	Published
[OGF5]	OGF	GFD.193	WS-Agreement Negotiation	Specification	Published
[QuEST1]	QuEST Forum	TL9000	TL 9000 Measurements Handbook	Standards	Published
[QuEST2]	QuEST Forum	TL9000	TL 9000 Requirements Handbook	Standards	Published
[SLA1]	SLA@SOI	D.A5a	SLA: An abstract syntax for Service Level Agreements	Specification	Published
[SNIA1]	SNIA	CDMI	Cloud Data Management Interface - ISO 17826:2012	Standards	Published
[TIA1]	TIA	ANSI/TIA-942-A	Telecommunications Infrastructure Standards for Data Centers	Standards	Published

Annex 2 List of Related Work (reports, White Papers, …)

The list below contains **Reports**, **White Papers** , and **other** type of related work collected by CSC.

This list is also available in a document that includes additional metadata (columns) and the documents of Annex 1 that can be found on-line at:

http://csc.etsi.org/Application/documentapp/downloadLatestRevision/?docId=180

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[CSA2]	CSA	Securiry Guidance	Security Guidance for Critical Areas of Focus in Cloud Computing	report/white paper	Published
[CSA5]	CSA	CAIQ	Consensus Assessments Initiative Questionnaire	Other	Published
[CSA7]	CSA	SecaaS	Security as a Service	report/white paper	Published
[CSCC1]	CSCC	n/a	Practical Guide to Cloud Computing	report/white paper	Published
[CSCC2]	CSCC	n/a	Public Cloud Service Agreements: What to Expect and What to Negotiate	report/white paper	Published
[CSCC3]	CSCC	n/a	Security for Cloud Computing: 10 Steps to Ensure Success	report/white paper	Published
[CSCC4]	CSCC	n/a	Practical Guide to Cloud Service Level Agreements	report/white paper	Published
[CSCC5]	CSCC	n/a	Cloud Security Standards: What to Expect & What to Negotiate	report/white paper	Published
[ENISA1]	ENISA	ProcureSecure	Procure Secure - A guide to monitoring of security service levels in cloud contracts	report/white paper	Published
[ETSI1]	*ETSI / ISG NFV*	*DGS/NFV-INF001*	*NFV Infrastructure Overview*	*report/white paper*	*Draft*
[ETSI2]	*ETSI / ISG NFV*	*DGS/NFV-INF002*	*NFV - Infrastructure; Illustrative Use Cases*	*report/white paper*	*Draft*
[ETSI3]	*ETSI / ISG NFV*	*DGS/NFV-INF003*	*NFV - Infrastructure Compute Domain*	*report/white paper*	*Draft*
[ETSI4]	*ETSI / ISG NFV*	*DGS/NFV-INF004*	*NFV - Infrastructure Hypervisor Domain*	*report/white paper*	*Draft*

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[ETSI5]	*ETSI / ISG NFV*	*DGS/NFV-INF005*	*NFV - Infrastructure Network Domain*	*report/white paper*	*Draft*
[ETSI6]	*ETSI / ISG NFV*	*DGS/NFV-INF006*	*NFV - Infrastructure Scalability*	*report/white paper*	*Draft*
[ETSI7]	*ETSI / ISG NFV*	*DGS/NFV-INF007*	*NFV - Infrastructure; Interfaces and Abstractions*	*report/white paper*	*Draft*
[ETSI8]	*ETSI / ISG NFV*	*DGS/NFV-INF008*	*NFV - Infrastructure; Portability and Replicability*	*report/white paper*	*Draft*
[ETSI9]	*ETSI / ISG NFV*	*DGS/NFV-INF009*	*NFV - Infrastructure; Test Access*	*report/white paper*	*Draft*
[ETSI10]	*ETSI / ISG NFV*	*DGS/NFV-MAN001*	*NFV - Management and Orchestration*	*report/white paper*	*Draft*
[ETSI11]	*ETSI / ISG NFV*	*DGS/NFV-PER001*	*NFV Performance & Portability Best Practises*	*report/white paper*	*Draft*
[ETSI12]	*ETSI / ISG NFV*	*DGS/NFV-REL001*	*NFV Resiliency Requirements*	*report/white paper*	*Draft*
[ETSI13]	*ETSI / ISG NFV*	*DGS/NFV-SEC001*	*NFV Security Problem Statement*	*report/white paper*	*Draft*
[ETSI14]	*ETSI / ISG NFV*	*DGS/NFV-SWA001*	*NFV Network Function Classification*	*report/white paper*	*Draft*
[ETSI15]	*ETSI / ISG NFV*	*DGS/NFV-SWA002*	*NFV Network Evolution Towards an NFV-enabled Environment*	*report/white paper*	*Draft*
[ETSI16]	ETSI / ISG NFV	GS NFV 001	NFV Use Cases	report/white paper	Published
[ETSI17]	ETSI / ISG NFV	GS NFV 002	NFV Architectural Framework	report/white paper	Published
[ETSI18]	ETSI / ISG NFV	GS NFV 003	Terminology for Main Concepts in NFV Terminology for Main Conceptional Entities in NFV Terminology for Main Conceptional Entities in NFV Terminology for Main Conceptional Entities in NFV Terminology for Main Conceptional Entities in NFV	report/white paper	Published
[ETSI19]	ETSI / ISG NFV	GS NFV 004	NFV Virtualisation Requirements	report/white paper	Published
[ETSI20]	ETSI / ISG NFV	GS NFV-PER 002	NFV Proof of Concepts; Framework	report/white paper	Published

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[ETSI21]	*ETSI / TC CLOUD*	*DTR/CLOUD-0013-GHGmitigation*	*Cloud as a mitigating technology to reduce emissions in other sectors*	*report/white paper*	*Draft*
[ETSI22]	ETSI / TC CLOUD	TR 102 659-1	Study of ICT Grid interoperability gaps;Part 1: Inventory of ICT Stakeholders	report/white paper	Published
[ETSI23]	ETSI / TC CLOUD	TR 102 659-2	Study of ICT Grid interoperability gaps;Part 2: Interoperability Gaps and proposed solutions	report/white paper	Published
[ETSI24]	ETSI / TC CLOUD	TR 102 766	ICT Grid Interoperability Testing Framework and survey of existing ICT Grid interoperability solutions	report/white paper	Published
[ETSI25]	ETSI / TC CLOUD	TR 102 767	Grid Services and Telecom Networks;Architectural Options	report/white paper	Published
[ETSI26]	ETSI / TC CLOUD	TR 102 997	Initial analysis of standardization requirements for Cloud services	report/white paper	Published
[ETSI27]	ETSI / TC CLOUD	TR 103 125	SLAs for Cloud services	report/white paper	Published
[ETSI28]	ETSI / TC CLOUD	TR 103 126	Cloud private-sector user recommendations	report/white paper	Published
[ETSI30]	*ETSI / TC LI*	*DTR/LI-00083*	*Lawful Interception (LI); Retained Data; Virtual Services (CRD)*	*report/white paper*	*Draft*
[ETSI31]	*ETSI / TC LI*	*DTR/LI-00084*	*Lawful Interception (LI); Cloud/Virtual Services (CLI)*	*report/white paper*	*Draft*
[ETSI32]	ETSI / TC USER	EG 202 009-1	Quality of telecom services; Part 1: Methodology for identification of parameters relevant to the Users	report/white paper	Published
[ETSI33]	ETSI / TC USER	EG 202 009-2	Quality of telecom services;Part 2: User related parameters on a service specific basis	report/white paper	Published
[ETSI34]	ETSI / TC USER	EG 202 009-3	Quality of telecom services; Part 3: Template for Service Level Agreements (SLA)	report/white paper	Published
[GICTF1]	GICTF	n/a	Use Cases and Functional Requirements for Inter-Cloud Computing	report/white paper	Published
[GICTF2]	GICTF	n/a	Technical requirements for inter cloud networking	report/white paper	Published
[GICTF3]	GICTF	n/a	Intercloud Interface Specification Data model	report/white paper	Published

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[GICTF4]	GICTF	n/a	Intercloud Interface Specification Protocol	report/white paper	Published
[IEEE1]	*IEEE*	*IEEEP2302*	*Standard for Intercloud Interoperability and Federation (SIIF)*	*Other*	*Draft*
[IETF1]	*IETF*	*draft-stein-cloud-access*	*Accessing Cloud Services*	*Other*	*Draft*
[IETF2]	*IETF*	*draft-khasnabish-cloud-reference-framework*	*Cloud Reference Framework*	*Other*	*Draft*
[IETF3]	*IETF*	*/draft-hoff-cloudaudit*	*CloudAudit*	*Other*	*Draft*
[IETF4]	IETF / alto	ALTO Working Group	Application-Layer Traffic Optimization (alto)	Other	
[IETF5]	IETF / l3vpn	L3VPN Working Group	Layer 3 Virtual Private Networks (l3vpn)	Other	
[IETF6]	IETF / nvo3	NVO3 Working Group	Network Virtualization Overlays (nvo3)	Other	
[IETF7]	IETF / oauth	OAUTH Working Group	Web Authorization Protocol (OAuth).	Other	
[IETF8]	IETF / scim	SCIM Working Group	System for Cross-domain Identity Management (scim)	Other	
[IETF9]	IETF / ippm	ippm Working Group	IP Performance Metrics	Other	
[ISO10]	*ISO/IEC*	*20000-7*	*Guidance on the application of ISO/IEC 20000-1 to the cloud*	*report/white paper*	*Draft*
[ITU1]	ITU-T	FG Cloud Part1	Introduction to the cloud ecosystem	report/white paper	Published
[ITU2]	ITU-T	FG Cloud Part2	Functional requirements and reference architecture	report/white paper	Published
[ITU3]	ITU-T	FG Cloud Part3	Requirements framework architecture of cloud infrastructure	report/white paper	Published
[ITU4]	ITU-T	FG Cloud Part4	Cloud Resource Management Gap analysis	report/white paper	Published

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[ITU5]	ITU-T	FG Cloud Part5	Cloud security	report/white paper	Published
[ITU6]	ITU-T	FG Cloud Part6	Overview of SDOs involved in cloud computing	report/white paper	Published
[ITU7]	ITU-T	FG Cloud Part7	Cloud benefits from telecommunication & ICT perspectives	report/white paper	Published
[NIST1]	NIST	SP 80-145	The NIST Definition of Cloud Computing (NIST Special Publication 800-145).	Other	Published
[NIST2]	*NIST*	*SP 500-292*	*NIST Cloud Computing reference Architecture*	*Other*	*Draft*
[NIST3]	*NIST*	*SP 500-293*	*US Government Technology Roramap Vol 1 Release 1 (Draf)*	*Other*	*Draft*
[NIST4]	*NIST*	*SP 500-293*	*US Government Technology Roramap Vol 2 Release 1 (Draf)*	*Other*	*Draft*
[NIST5]	NIST	800-53 Rev. 4	Security Controls	report/white paper	
[OASIS2]	OASIS/Id in the Cloud		Identity in the Cloud Use Cases	report/white paper	Published
[OASIS3]	*OASIS/Id in the Cloud*		*Identity in the Cloud PaaS Profile*	*report/white paper*	*Draft*
[OASIS4]	*OASIS/Id in the Cloud*		*Identity in the Cloud Outsourcing Profile*	*report/white paper*	*Draft*
[TMF1]	TMF	GB917	SLA Management Handbook	report/white paper	Published
[TMF2]	TMF	GB960	Quick Start Pack for Cloud: Trouble to Resolve	report/white paper	Published
[TMF3]	TMF	GB963	Cloud SLA Application Note	report/white paper	Published
[TMF4]	TMF	TR174	Enterprise-Grade IaaS Requirements	report/white paper	Published
[TMF5]	TMF	TR174-A	Cloud Business Models	report/white paper	Published
[TMF6]	TMF	TR174-B	TM Forum Enterprise-Grade External Compute IaaS Requirements	report/white paper	Published
[TMF7]	TMF	TR174-C	Reference Implementation	report/white paper	Published

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[TMF8]	TMF	TR178	Enabling End-to-End Cloud SLA Management	report/white paper	Published
[TMF9]	TMF	TR194	Multi-Cloud Service Management Pack – Introduction	report/white paper	Published
[TMF10]	TMF	GB935	Multi-Cloud Service Management Pack – Business Guide	report/white paper	Published
[TMF11]	TMF	GB981	Partnership and B2B2X Best Practices Overview	report/white paper	Published
[TMF12]	TMF	TR211	Partnership and B2B2X Best Practices Partnering Guidebook – Concepts and examples	report/white paper	Published
[TMF13]	TMF	TR218	Parterning Guidebook -- A Step by step Guide	report/white paper	Published
[TMF14]	TMF	GB982	B2B2X Partnering Developer Pack	report/white paper	Published
[TMF15]	TMF	GitHub and APIgee	REST (Management) API Zone http://www.tmforum.org/APIZone/15739/home.html These cover product ordering, catalog management. Simple Management, Agreement, Trouble Ticket.	Specifications, open source code, API console APIgee / Github	Published
[TMF16]	TMF	TR218	Multi-Cloud Service Management Pack – Business Guide	report/white paper	Published

Annex 3 List of Use cases

The list below contains **the list of Use Cases** collected by CSC.

The full list is available in a spread sheet that include additional metadata (columns).
This sheet can be found on-line at: http://csc.etsi.org/Application/documentapp/downloadLatestRevision/?docId=185
The UC highlighted in yellow are those at the basis of UC analysis in section 3.3.

High Level Use Cases	ID	UC Title	UC Short Description
Prepare & Procure Service	**1**	**End User to Cloud**	Applications running on the cloud and accessed by end users
Prepare & Procure Service	**2**	**Enterprise to customer and employee**	Applications running in the public cloud and accessed by employees and customers
Prepare & Procure Service	**3**	**Enterprise to Cloud**	Cloud applications integrated with internal IT capabilities
Prepare & Procure Service	**4**	**Enterprise to Cloud to Enterprise**	Cloud applications running in the public cloud and interoperating with partner applications (supply chain)
Prepare & Procure Service	**5**	**Private Cloud**	A cloud hosted by an organization inside that organization's firewall.
Operate Service - Migrate	**6**	**Changing Cloud Vendors**	An organization using cloud services decides to switch cloud providers or work with additional providers.
Prepare & Procure Service	**7**	**Broker coordinated Hybrid Cloud**	Multiple clouds work together, coordinated by a cloud broker that federates data, applications, user identity, security and other details.
Prepare & Procure Service	**8a**		Between a **consume**r and a **CSP**: an authenticated consumer accesses and uses data or applications in a CSP, choosing dynamically virtual hardware specification and environment (i.e. operating system).
Prepare & Procure Service	**8b**		Between an **enterprise** and a **CSP**: an enterprise using a virtual desktop service from a CSP for its internal processes selecting applications or OS in the DaaS service for certain enterprise functions. It normally uses storage for backups and can overcome peak loads and save energy by requesting the CSP to increase or decrease the number of virtual desktops dynamically.
Prepare & Procure Service	**8c**		Among an **enterprise**, a **consumer**, and a **CSP (tele-work)** the enterprise makes the consumer do works with its internal processes from outside of the enterprise by transferring virtual desktops and related data through the CSP. The consumer cannot select applications freely and more limitations to access data in the enterprise exist. CSP interacts with the Enterprise to send feedback data to the consumer by accessing the enterprise to handle or bypass corresponding data.

High Level Use Cases	ID	UC Title	UC Short Description
Prepare & Procure Service	**9**		End users access the enterprise applications and data hosted in virtual desktops which are created within a DaaS server. The sales staff also can view customer information and marketing records on the enterprise website. The DaaS server interacts with traditional enterprise IT facilities to achieve many control tasks, for instance, authentication via AD enterprise server.
Prepare & Procure Service	**10**	**Virtual desktop pool**	Virtual desktop pool supports the distributed deployment model with the dynamic stretching of resources to consolidate queuing resource and desktop resources. Unified phone call dispatching and delivery and maintenance of the desktop can be achieved in an intensive way.
Prepare & Procure Service	**11**		Provide a SDPs able to support multi-domain service convergence, or an environment where application developers can fully collaborate and share services, through a number of interconnected, distributed service nodes which may support redundancy, different service profiles for different business and market sectors, and full support for application developers. Through the exposure of “SDP as a service” (SDPaaS) by a cloud service provider via open SDPaaS APIs, cloud service users can easily access new converged ICT services (e.g. IMS applications, IPTV applications, M2M/IoT applications) through multiple kinds of terminal devices e.g. PC, thin client, pad computer, mobile phone, smart phone, virtual desktop client.
Prepare & Procure Service	**12**	**Mobile Cloud Apps development & deployment**	A mobile cloud application can be developed by service partners, or by the cloud provider, or by third-party service provider and can be stored in a marketplace. The mobile cloud application sends processing tasks to the cloud and stores data in the cloud, and receives results generated by the resources from the cloud, including computing resources and storage sources.
Operate Service - Migrate	**13**	**Move three-tier application from on-premises to cloud**	An organization moves a three-tier application (front-end web server, back-end database, and middle-tier business logic) from an on-premises data center to a cloud infrastructure provider that will run the application off-premises. Platform services for data, identity and access are considered available for source and target clouds but not addressed in this case. This use case represents the most common type of web-based application deployed both in enterprises and mid-sized companies
Operate Service - Migrate	**14**	**Move three-tier cloud application to another cloud**	An organization moves a three-tier application from one cloud infrastructure provider to another.
Operate Service - Migrate	**15**	**Move part of on-premises application to cloud to create “hybrid” application**	An organization moves one or more parts – or tiers – of an on-premises application to the cloud, in order to separate data storage from processing, for example. This creates a cloud that is a hybrid of both public (off-premises) and private (on-premises) clouds.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Migrate	16	**Hybrid cloud application that uses platform services**	An organization moves one or more parts – or tiers – of an on-premises application to the cloud and chooses to implement cloud components of a hybrid application using platform services available from the cloud platform provider, such as structured or unstructured cloud storage or identity and access control services.
Operate Service - Migrate	17	**Port cloud application that uses platform services to another cloud**	Porting an application that uses services provided by the cloud platform to another cloud platform implies these requirements: 1) bulk import/export of customer data, and 2) Semantic cloud application management protocol.
Prepare & Procure Service	18	**Telco uses Cloud for data analytics**	Large-scale telecom operators generate a lot of information in the normal course of running their communication networks. Typical data comprises Call Data Records (CDR) and Internet-surfing data records (IDR). In addition the network also generates various signalling data between switches and nodes. We need all the data to complete the telecom services and bill customers. At the same time, we also need them to analyze and predict user behaviour, optimize network QoS, filter spam messages, and so forth. Because of the limitations of the current system, the parallel data inquiry and mining tool, set on the cloud distributed parallel processing systems could be a better solution and achieve massive scalability and high-speed processing .
Prepare & Procure Service	19	**SLA mapping between ISB (inter-cloud service broker) and CSP**	CSP-ISB is the contact point for CSU, and there is SLA (SLA0) between them. CSP-ISB integrates services from multiple CSPs, for instance, storage service from CSP-1 and computing service from CSP-2. There are B2B level SLA between CSP-ISB and CSP-1, CSP-2 respectively (SLA1, SLA2). For CSP-ISB, in order to guarantee SLA0 for CSU, it needs to map SLA0 to SLA1 and SLA2, because SLA0 is actually implemented by SLA1 and SLA2.
Operate Service - Manage	20	**guaranteeing performance against an abrupt increase of the load**	• A CSP guarantees its service performance, even when an unexpected surge of access to the service arises, by using cloud resources provided by other CSPs on a temporary basis. • Network connections among interworking CSPs are instantaneously established or reconfigured. Then service-related data including user ID, user data, and application data are transferred from the original CSP to the CSP that is leasing the resources. • Access from CSUs is appropriately changed to the interworking CSPs so as to achieve load distribution, and thus mitigate the overload of the original CSP.
Prepare & Procure Service	21	**Contracting guaranteed performance regarding delay**	CSP-ISB is the contact point for Cloud Service User (CSU), and there is SLA (SLA0) between them. CSP-ISB integrates services from multiple CSPs, for instance, storage service from CSP-1 and computing service from CSP-2. There are B2B level SLA between CSP-ISB and CSP-1, CSP-2

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Manage	**22**	**guaranteeing availability in the event of a disaster or a large-scale failure**	• CSPs continue their service offering by the resources leased from each other, even when systems in one CSP are damaged due to natural disasters or large-scale failures. • Available resources in other CSPs are autonomously discovered and reserved through the inter-cloud federation. • The services with a high priority are only recovered if available resources are not enough to recover all services. In examining the availability of the resources given from other CSPs, the guaranteed level of quality of the resources is taken into account. • The services requiring early recovery are recovered using available resources on a best-effort basis even if their quality requirements are partly satisfied. • Network connections among interworking CSPs are instantaneously established or reconfigured. The lead CSP, which is preconfigured and governs the recovery procedure, manages the roles of available CSPs and instructs service continuation based on the original CSP data. • Access from CSUs is appropriately distributed to the interworking CSPs so as to achieve the disaster recovery, and thus mitigate the service discontinuity.
Operate Service - Manage	**23**	**service continuity**	• A CSP continues its service offering by the collaboration with other CSPs, even when the original CSP terminates its business. • Available resources in CSPs other than the service-terminating CSP are discovered and reserved in advance. • Network connections among interworking CSPs are established or reconfigured. Then service-related data including user ID, user data and, application data are transferred from the original CSP to new CSPs. • Access from CSUs is appropriately changed to the interworking CSPs so that the same service is continuously offered. • If the capabilities (VM and applications) at the original CSP migrate to other CSPs, the CSU, who keeps the same user ID, can continuously access the service at the same level of performances as before.
Operate Service - Manage	**24**	**market transactions via brokers**	• The CSP with an ISB role (CSP-ISB) mediates between CSPs meeting the CSU's quality requirements and provides the list of selected CSPs to the CSU. • The CSP-ISB coordinates multiple services offered by other CSPs
Operate Service - Manage	**25**	**Guaranteed end-to-end quality of service Guaranteed performance**	Use case of guaranteeing performance against a abrupt increase of the load
Operate Service - Manage	**26** [HA]	**Guaranteed end-to-end quality of service Guaranteed availability**	Use case of guaranteeing availability in the event of a disaster or a large-scale failure

High Level Use Cases	ID	UC Title	UC Short Description
Prepare & Procure Service	27	**Citizen centric one-stop service**	The e-application service provided by City A has been pre-arranged to allow interaction with other provider's services (e.g., family registry management service in a municipality cloud, passport management service of the national government, etc.) by negotiating the methods for coordinating ID information and security measures. A citizen in City A applies for his or her passport using the relevant e-application service provided by the municipality A. When he or she has entered required information, such as his or her identity information, the input data is transferred to other cloud system's services (e.g., family registry management service, passport management service, etc.) to authenticate, sharing user ID information entered for application, then information acquisition and inquiry take place. The results of the interacted services are provided to the consumer. Thus, the consumer can receive a one-stop service, which enhances his/her convenience.
Operate Service - Manage	28	**Service continuity by pre-configuration of alternative services**	Normally, if the business of Provider A is suspended, the consumers need to re-register with similar services that are provided by different providers. To avoid a situation above, resources, applications, and consumer's ID data for the services provided by Provider A are transferred to the cloud systems of Providers B and C in advance. Then, in the situation of the business suspension of Provider A, its consumers can continue to use similar services provided by Providers B and C. This arrangement can also be applied when a service consumer requests a transfer of his or her service to another provider.
Prepare & Procure Service	29	**Market transactions via brokers**	When a consumer wants to uses services provided by cloud systems, he or she needs to compare his or her quality requirements for the services with the SLAs of multiple providers, and to select the most appropriate provider. For this purpose, the consumer provides Broker A with information about his or her quality requirements for services. By receiving information provided by Broker A, that Provider B provides an SLA that best meets the quality requirements of consumer, consumer can use services with best fit to his or her quality requirement. The consumer selects a cloud provider included in the provider list provided by broker, and contracts with Provider B.
Prepare & Procure Service	30	**Establish Relationship**	A potential consumer of a cloud-based service establishes their identity with a cloud service provider for use in future transactions.
Prepare & Procure Service	31	**Administer Relationship**	A potential consumer of a cloud-based service requests administration of a contract. Administration is distinguished from changing a service because administration does not affect the technical delivery of a service. Usually, contract administration involves actions like adding new users or changing user passwords that are associated with an umbrella contract (usually called the "relationship"), not a contract for a specific service.
Prepare & Procure Service	32	**Establish Service Contract**	A potential consumer of a cloud-based service requests a service contract for a cloud-based service.
Prepare & Procure Service	33	**Update Service Contract**	A consumer of a cloud service contract and a provider of a cloud service contract agree to update the contract.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Monitor	**34**	**SLA ~~Contract~~ Reporting**	A cloud service consumer requests and receives a report about an established service contract.
Operate Service - Manage	**35**	**Contract Billing**	A cloud service provider issues an invoice for contracted or consumed services.
Operate Service - Terminate	**36**	**Terminate Service Contract**	A consumer of a cloud service contract and a provider of a cloud service contract agree to terminate a cloud service contract.
Operate Service - Provision/Configure/Administer	**37**	**Provision Resources (from a contracted pool)**	Within the context of an existing contract, an administrator allocates resources from the contracted pool. The resources could be of a wide variety, such as virtual system platforms or a preconfigured mini data center that contains virtual systems and virtual storage, connected via a virtual network.
Operate Service - Provision/Configure/Administer	**38**	**Deploy Service Template**	A cloud service consumer deploys a parameterized service template in the context of a service offering.
Operate Service - Manage	**39**	**Change Resource Capacity**	A cloud service consumer adds or changes the capacity or resources associated with a service instance, which is an instance of a service template. This can include adding or removing whole resources, or expanding or contracting resource limits associated with the service.
Operate Service - Monitor	**40**	**Monitor Service Resources**	A cloud consumer configures a monitor for a deployed service instance and resources that support the service instance. A monitor may collect data (for example, resource consumption, throughput, response times, or availability) or establish an exception threshold.
Setup Cloud Service	**41**	**Create Service Template**	A cloud service developer creates a template of a service that may later be used to create an instance of a service.
Setup Cloud Service	**42**	**Create Service Offering**	The lifecycle of a new service offering is initiated and publicized for potential subsequent: • Advertisement • Contract assignment • Provisioning • Monitoring • Update • Consumption • Deletion
Operate Service - Monitor	**43**	**Notification of Service Condition or Event**	A service has been configured and is in operation. Certain conditions or runtime operational events have been identified or detected that are significant enough to demand immediate notification of the condition or event to the service customer. An example is the detection of an intrusion or an unexpected configuration change.
Prepare & Procure Service	**44**	**Add Subscriber**	The **consumer** enters into a business relationship with the **provider** to enable it to use an agreed to set a cloud service.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Provision/Configure/Administer	45	**Provision New Administration Domain (or Provision New Tenant)**	Subscriber administrator is provisioned with a new administration domain.
Operate Service - Provision/Configure/Administer	46	**Add/Change/Delete User**	A cloud **consumer administrator** adds or removed user, or changes their privileges.
Setup Cloud Service	47	**Build Application and Package**	Developer builds an application and package it for deployment on a cloud
Setup Cloud Service	48	**Build Application in Cloud and Optionally Package**	Develop an application and optionally package it using an application development environment on the Cloud.
Operate Service - Provision/Configure/Administer	49	**Install Application Component**	A new application component is uploaded and installed to the cloud.
Operate Service - Provision/Configure/Administer	50	**Deploy Application (also Undeploy)**	To deploy a package comprising all the required application components to an execution domain.
Operate Service - Provision/Configure/Administer	51	**Start an application**	To start executing an application such that **end-user** may start interacting with the hosted applications.
Operate Service - Manage	52	**Hibernate/Resume**	Puts a running application into hibernation. Resume a hibernating application.
Operate Service - Manage	53	**Stop/Restart**	Stop a running application and create a “snapshot”. Resume from a snapshot.
Operate Service - Manage	54	**Patch**	Patch (update) one or more components in an application template.
Operate Service - Provision/Configure/Administer	55	**Upload Machine Image**	The cloud user or third party software provider has a local copy of a “machine image” (a snapshot of a stack of software which may include operating systems, virtual machine runtimes, database servers, application servers, applications, etc.) that they wish to make available for deployment on an IaaS cloud.
Operate Service - Provision/Configure/Administer	56	**Deploy Machine Image**	The cloud consumer wishes to create a new instance of a “machine” (a logical instance of one or more CPUs connected to local memory and, optionally, local data storage) with software loaded from a machine image.
Operate Service - Provision/Configure/Administer	57	**Capture Existing Machine Instance**	The cloud consumer wishes to create a new machine image that captures the state of an existing virtual machine instance.
Operate Service - Provision/Configure/Administer	58	**Create Persistent Storage Volume**	The cloud consumer wishes to create a new storage volume image that captures the information stored on an existing volume instance.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Provision/Configure/Administer	**59**	**Load Image onto Storage Volume**	The cloud consumer wishes to load a “volume image” (e.g. an ISO image) onto an existing persistent storage volume.
Operate Service - Provision/Configure/Administer	**60**	**Attach Storage Volume to Machine**	The cloud consumer wishes to attach a persistent storage volume to a machine instance. Once attached, the volume is accessible by processes resident on that machine instance, usually as a local device (e.g. /dev/sd2).
Operate Service - Provision/Configure/Administer	**61**	**Capture Storage Image**	The cloud consumer wishes to create a new storage image that captures the information stored on an existing storage image.
Operate Service - Provision/Configure/Administer	**62**	**Detach Storage Volume from Machine**	The Cloud User wishes to detach a persistent storage volume from a machine instance. Once detached, the volume is no longer accessible by the processes resident on that machine.
Operate Service - Manage	**63**	**Create Network**	The cloud consumer wishes to create a new instance of a “network”. A network is an abstraction of a layer 2 broadcast domain. Any two nodes (machines, volumes, etc.) attached to the same network can connect to one another. To connect to a node on another network a route must be created between the source network and the destination network. A common reason for creating networks is to isolate machines and volumes into protected sub-domains for security and administration purposes.
Operate Service - Provision/Configure/Administer	**64**	**Attach Machine to Network**	The cloud consumer wishes to attach a machine to a network. The higher level goal is to allow this machine to connect to one or more of the other machines or volumes on the target network and/or to allow one or more machines on the target network to connect to this machine.
Operate Service - Provision/Configure/Administer	**65**	**Detach Machine from Network**	The Cloud User wishes to detach a machine from a network. This is usually a step in a higher-level network management process such as “attach this machine to the back-end, database network and detach it from the default network”.
Operate Service - Provision/Configure/Administer	**66**	**Attach Storage Volume to Network**	The Cloud User wishes to attach a volume to a network. The higher level goal is to allow this volume to be attached to one or more of the machines on the target network (see Attach Storage Volume to Machine).
Operate Service - Provision/Configure/Administer	**67**	**Detach Storage Volume from Network**	The cloud consumer wishes to detach a volume from a network. This is usually a step in a higher-level network management process such as “attach this volume to the back-end, database network and detach it from the default network”.
Operate Service - Migrate	**68**	**Capture Aggregate Assembly**	The cloud consumer wishes to capture an aggregate assembly consisting of zero or more machine instances, zero or more volume instances, zero or more network instances, and the attachments/connections between these entities. The artifacts generated by this capture operation (the “assembly package”) can be used to deploy “a copy” of the assembly onto this or some other cloud.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Migrate	69	**Upload Aggregate Assembly**	The cloud consumer or third party software provider has a local copy of an assembly package which includes zero or more machine images along with metadata that describes the machines on which these images must be deployed, zero or more volume images along with metadata that describes the volumes on which these images must be deployed, zero or more descriptions of network instances, and a map of the attachments/connections between these entities. The Cloud consumer or third party software provider wishes to make this assembly available for deployment on an IaaS cloud.
Operate Service - Migrate	70	**Deploy Aggregate Assembly**	The cloud consumer wishes to deploy an aggregate assembly consisting of zero or more machine instances, zero or more volume instances, zero or more network instances, and the attachments/connections between these entities for the purposes of re-creating the system that was captured in IR01.25 (Capture Aggregate Assembly).
Operate Service - Migrate	71 [SD] [DI]	**Move three-tier application from on-premises to cloud**	An organization (customer) moves a three-tier application from an on-premises datacenter to a cloud infrastructure provider that will run the application off-premises. The data associated with the application is sensitive and confidential and it is necessary to assure its integrity. Issues to be considered include: • suitable SLA/certificate, • responsibility for the provision and application of encryption, • key management processes • data validation • etc…
Operate Service - Migrate	72	**Move three-tier cloud application to another cloud**	An organization (customer) moves a three-tier application from one cloud infrastructure provider 1 to another provider 2.
Operate Service - Migrate	73	**Move part of on-premises application to cloud to create "hybrid" application**	An organization (customer) moves one or more parts – or tiers – of an on-premises application to the cloud, in order to separate data storage from processing, for example. This creates a cloud that is a hybrid of both public (off-premises) and private (on-premises) clouds.
Operate Service - Migrate	74	**Hybrid application with shared user ID and access services**	This use case is the same as the use case "Move part of on-premises application to cloud to create 'hybrid' application" with the added condition that user ID and access are shared between on-premises and cloud components. This requires a common user ID and access control methodology between components based on either on-premises directory access or identity federation.
Operate Service - Migrate	75	**Move hybrid application to another cloud with common infrastructures**	An organization (customer) moves the cloud portions of a hybrid application from cloud A to cloud B, both of which support common infrastructures and VM packages.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Migrate	**76**	**Hybrid cloud application that uses platform services**	This use case is similar to the use case "Move part of on-premises application to cloud to create 'hybrid' application" except the cloud application developer in this case chooses to implement cloud components of a hybrid application using platform services available from the cloud platform provider, such as structured or unstructured cloud storage or identity and access control services.
Operate Service - Migrate	**77**	**Port cloud application that uses platform services to another cloud**	Porting an application that uses services provided by the cloud platform to another cloud platform implies the same requirements as for the use case "Hybrid cloud application that uses platform services".
Prepare & Procure Service	**78 [AC]**	**Create cloud application with components that run on multiple clouds**	An organization chooses to develop a cloud application with components that run on multiple clouds simultaneously.
Operate Service - Manage	**79**	**Cloud application workload requires use of multiple clouds (cloudburst)**	Sometimes referred to as a cloudburst scenario, the application normally running onpremises or in a private cloud needs to elastically run on other clouds in the cases of short-term, significant increase in user demand load. Cloud tenants can use both their own private clouds as well as hosted/public clouds as the workload may require. VMs and applications can migrate between private cloud and public/hosted clouds and can seamlessly be managed from either side regardless of their location.
Prepare & Procure Service	**80**	**Customers can “shop around” for cloud services**	Customers and developers shop across hosted or public cloud searching for services offering adequate price and the desired level of non-functional properties like performance, security, availability, expressed via Service Level Agreements (SLAs)/certificates.
Operate Service - Manage	**81**	**Document release towards an administration**	An Electronic Document Storage (EDS) is a secure storage for official documents provided as SaaS. Governmental institutions or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedures. The use case describes how a public administration requests a document from a citizen in the course of an administrative process.
Operate Service - Migrate	**82**	**Cloud Burst**	An Electronic Document Storage (EDS) is a secure storage for official documents provided as SaaS. Governmental institutions or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedures. To reduce its own operational costs, the EDS provider decides to accept an IaaS offer from another Cloud provider and use its virtualized resourced to provide the EDS service.

High Level Use Cases	ID	UC Title	UC Short Description
Operate Service - Migrate	**83**	**Document Migration**	An Electronic Document Storage (EDS) is a secure storage for official documents provided as SaaS. Governmental institutions or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedures. The use case describes how a public administration requests a document from a citizen in the course of an administrative process. The use case describes the migration process of documents from one EDS (EDS 1) hosted by EDS space provider A into another one (EDS 2) (hosted by provider B):
Prepare & Procure Service	**84**	**Material Distribution to Agents**	A global insurance company named “ABC” uses manuals and videos to teach the company’s agents and affiliates about their new life insurance product. The company distributes the educational materials through the company’s PDAs assigned to every agent considering mobile characteristics of their work. The use case describes technical processes and considerations to distribute company’s educational material for new product to their agents. A correct version of the material among three different versions should be delivered to agents in a qualified VO group with an auditable access control mechanism that enforces the company’s security policies.
Operate Service - Manage	**85** [CB]	**Burst Capacity**	A system or service runs in a defined “source” location, and bursts into an alternate location or cloud environment such as a shared or public cloud (target) to obtain additional resources to accommodate business peak processing requirements. Requires license flexibility, and sufficient network and security controls.
Operate Service - Migrate	**86**	**Project Capacity**	Temporary capacity from an alternate cloud (public or shared private) to support short term initiatives
Operate Service - Provision/Configure/Administer	**87**	**Onboarding for VEM**	Onboarding of a customers applications to IaaS service
Operate Service - Monitor	**88**	**Monitoring & management of deployed software**	Monitor the health of infrastructure & perform capacity planning for future needs
Operate Service - Manage	**89**	**Integration of on-premise resources with public cloud resources**	Cloud service customer makes use of public cloud IaaS resources for some workloads but still has other workloads retained on-premise, with the need to link the on-premise workloads and the public cloud workloads
Prepare & Procure Service	**90**	**cloud storage as a service**	Customer uses public cloud storage as a service offering to store ever-increasing volumes of data as an alternative to adding to on-premise storage infrastructure
Setup Cloud Service	**91**	**Cloud developer makes application available from cloud infrastructure**	ISV or application developer makes their application available as a service, by deploying the application on IaaS infrastructure of a cloud service provider
Setup Cloud Service	**92**	**Deploy application to a PaaS cloud service**	Application developer must prepare the application components and associated metadata and enable deployment to the PaaS platform offered by the cloud service provider

High Level Use Cases	ID	UC Title	UC Short Description
Setup Cloud Service	93	**Automate deployment of test environments for applications**	Application developer requires to test an application to determine the cause of a problem - requires the deployment of the application in an environment that matches the environment in which the problem was experienced
Prepare & Procure Service	94	**Provision of Database capabilities as a cloud service**	Customer wants to use a Database as a Service capabilities with ability to upload database images containing data and configuration information.
Prepare & Procure Service	95	**Provision of big data analytics platform**	Cloud service provider provides a dedicated Hadoop cluster as a service platform for big data analytics
Prepare & Procure Service	96	**Cloud Brokerage**	The Cloud broker offers *cloud service intermediation* for services to add value-addition and *cloud service aggregation* bringing two or more cloud based services. The Cloud Brokerage use case brings out the following innovations/value to the Cloud ecosystem. A) provide support for multi-cloud deployment B) provide standards-based SLA negotiation and agreement mechanisms to allow the broker to perform a match between the requirements of the C) Allows the broker to make SP-IP matches based on the Trust, risk, eco-efficiency and cost. D) The service deployment takes into account the legal bounderies as contraints in the service manifest. E) The cloud broker provides a framework to provide variety of value added services to the SP. Some the existing valued added sevices implemented as a supoort for the service includes, VPN overlay, Intelligent Protection system and Secure data storage. F) The cloud broker allows deployment of service in the non-optimis IP, providing interoperability support.
Setup Cloud Service	97	**IDE driven cloud development, deployment and operation**	The IDE driven cloud development, deployment and operation Use Case is based on the creation of new value-added services and how business processes are implemented and adapted to be deployed on the cloud. New services by SMEs have to be easily implemented and adapted for benefiting from the advantages of the Cloud. For developing the Value-Added Service, the Service Developer uses the OPTIMIS Programming Model and IDE for assisting him/her to make an efficient implementation for the Cloud. During this process, the Service Developer implements the service, focusing on the business logic of the service without worrying about the Cloud issues, and as result of this implementation, he/she obtain the Service Manifest and Service Images required for deploying the service in the Cloud. This information is provided to the Service Provider which uses the OPTIMIS toolkit to select the most appropriate Infrastructure Provider to deploy the service. Once the Value-added Service is deployed, the final users of the service can invoke the service, accessing directly to the deployed service VMs as another standard web service.

High Level Use Cases	ID	UC Title	UC Short Description
Prepare & Procure Service	**98**	**goBerlin**	The focus of goBerlin is the provisioning of a service marketplace combining commercial services and public governmental services to state-of-the-art applications with personalised SaaS for administrative matters (e.g. birth, marriage, children). The architecture is a loosely coupled combination of functional and security related aspects, e.g. access control, privacy, multi-tenancy. It can be applied to other cloud services running in similar cloud infrastructures, operated by public data centres.
Prepare & Procure Service	**99**	**Bioinformatics - BLAST and BLAT tools for sequence mapping**	Provide a framework for the seamless execution of widely used bioinformatics tools in the VENUS-C cloud (IaaS, PaaS), easing migration across target platforms (commercial and non-commercial providers). The aim of the VENUS-C user scenari on on bioinformatics (Technical University of Valencia) was to address the challenges faced by biomedical researchers in coping with the exponential growth of annotated databases and increases in the throughput of sequencing. The overall objective was to wrap different processing tools (e.g. for alignment and phylogeny) in a user-friendly framework running in the cloud. Migration across target platforms is ensured by implementation of standards, e.g. OGF-BES, OCCI, OVF, CDMI. Cost-effectiveness, flexibility and scalability over grid infrastructures have been demonstrated.
Prepare & Procure Service	**100**	**Wildfire: Fire Risk Estimation and Fire Propagation**	Provide a framework to execute fire risk estimations and fire propagation models, enabling end-user actors (e.g. fire-fighters, emergency crews and civil protection authorities) to run the models in the cloud using a user-friendly web-based graphical user interface. The aim of the VENUS-C user scenario, Wildfire (University of the Aegean) was to provide a tool for calculating fire risk indexes (hourly and over 5 days) and the expected propagation, using weather forecasts (including the direction of the wind), topography, vegetation and socio-economic parameters. It uses a hybrid cloud approach (MS Azure and OpenNebula via the Engineering Group) and has been tested and used by fire-fighting crews in Greece, who can respond to different workload situations; e.g. unpredictable and/or predictable bursting of CPU needs during the summer period.
Prepare & Procure Service	**101**	**Radiotherapy planning (CloudERT pilot deployment in Spain)**	Provide an eIMRT platform with remote tools to facilitate physicians in defining cancer treatment plans and verification using Monte Carlo simulations. Generate a single virtual cluster for each request to move the computing back-end to the cloud, which ensures independent processing for each request. The VENUS-C pilot, CloudERT, is led by the Centre of Supercomputing of Galicia (CESGA). It is aimed at improving hospital planning for cancer treatment with a pilot deployment in Spain, which currently involves 65 users from 47 hospitals. The eIRMT platform has been analysed from the point of view of SaaS, which must scale to thousands of users and service requests every day. It leverages the cloud to overcome the limitations of local clusters, which increase time-to-solution and decrease QoS, and of the grid, due to task grouping and the movement of large files.

High Level Use Cases	ID	UC Title	UC Short Description
Prepare & Procure Service	**102**	**Drug Discovery service by Molplex (SME)**	Provide a framework to calculate molecular virtual profiles that include shape/docking characteristics and QSAR biological activity predictions. The shape/docking calculation offers an embarrassingly parallel execution model, and has been parallelised with the use of OpenMP threads. Molplex requires regular access to computer resources to calculate the virtual profiles of molecules. The aim of the Molplex pilot (Cloud Against Diseases) in VENUS-C is to boost the performance of the comany's systems and reduce costs by allocating computing resources as needed. The virtual profiles are calculated using two techniques: shape/docking profile and QSAR profile. The deployment of former is supported by the Barcelona Supercomputing Center via the COMPSS interface, while part of the QSAR application is deployed on Azure using a legacy system from Newcastle University. Being able to solve a higher number of scientific problems (virtual profiling) gives the SME better market exposure and opportunities, as well as increase staff productivity.
Prepare & Procure Service	**103**	**Cloud4SOA (FP7 project)**	Interconnect public and private platform vendors for developers to help compare, manage and migrate between vendors by offering an open-source added value feature set for PaaS customers (developers and SaaS providers). Cloud4SOA interconnects platforms for added-value capabilities such as multi-platform management, comparative monitoring and application portability across collaborating or competing offerings. It prepares for the wider potential as the PaaS segment of cloud computing evolves, pointing towards concepts such as federation of multiple platforms and management between hybrid use cases of public and private PaaS. It leverages existing PaaS APIs and brings a harmonised layer and adapters to support its advanced features. Standardisation focuses on basic management protocols to enable platforms to focus on innovative concepts and ecosystem-empowered capabilities.
Setup Cloud Service	**104**	**Okeanos (GRNET)**	Okeanos is an open-source IaaS cloud software for the deployment of cloud services. The software is modular, comprising a number of components that can be deployed and exploited independently. Access to the services is through an intuitive user-friendly web interface and command line tools. It is currently being tested with beta release expected in spring 2013. Programmatically, it offers a set of dcoumented proprietary REST APIs and standard APIs like OpenStack Compute (Nova) and OpenStack Object Storage (swift compliant).
Setup Cloud Service	**105**	**Finnish Cloud Software Programme (national cloud strategy)**	It creates a new ecosystem that focuses on the most profitable cloud services for sustainable development while ensuring information security. The programme has applied the agile development methods of the software industry in collaboration with companies and research institutions. Client-centered approaches enable the rapid creation of added value services and flexible models of operation . The programme also proposes a set of "standard contract clauses", which can be offered for voluntary adoption for cloud service providers and customers and completed after risk analysis.

High Level Use Cases	ID	UC Title	UC Short Description
Setup Cloud Service	**106**	**EGI Federated Cloud Task Force**	Develop a 'blueprint' for EGI resource centres wishing to securely federate and share their local virtualised environments externally with collaborators as part of the production infrastructure. Ongoing efforts are centred around nine core capabilities required of a future EGI federated cloud. Implement interoperability across different cloud platforms. The core capabilities are virtual machine management, storage/data management, information discovery, accounting, monitoring, notification, federated authentication & authorisation infrastructure, virtual machine image sharing, brokering. The capabilities are currently implemented or being tested through resource provider test cases to cover all the necessary functionalities. EGI's Cloud Infrastructure Platform is based on the use of technical standards defining the interfaces and echange points between the services exposed to the public. The following cloud related standards are of key importance: OCCI as the universal and extensible interface description for the provisioning of virtualised computing resources; CDMI for describing the access interface to generic cloud storage resources (both block and object storage resources) and OVF as a declarative language for pre-packaged virtual server images and necessary contextualisation information. Several complementary standards are used to integrate with EGI's Core Infrastructure Platform: X.509v3-based federated authentication is used for safe and secure identification for services and end users; the Usage Resource is extensively used to account for resource usage (virtualised compute resources). The emerging TOSCA language is of interest for extending OVF with a richer deployment language across all cloud deployment levels (IaaS, PaaS, SaaS).
Operate Service - Terminate	**107**	Terminating cloud contract	An organization (cloud service customer) obtaining a cloud service from a cloud service provider directly or via a cloud service partner (a broker) would like to terminate its contract. There can be many reasons for doing so, for example the organization would like to changing cloud service provider of partner or wants exiting the cloud and move to a non-cloud environment. The use case is focusing on the terms and conditions that should be in a SLA, and the enforceability of those terms and conditions to do so.
Assure Quality - Audit Service	**108**	Independent third party assurance	Establishing an independent third party assurance (a regulator) to build trust whereby European SME's and other organizations (cloud service customers) will use cloud computing services more An independent third party assurance can contribute to building trust whereby European SME's and other organizations will use cloud computing services more. The idea is to establish a kind of active and pro active escrow service (a regulator role) by a third party in such a way that this party can assure a seamless takeover of the cloud operations that provider A executes for a user to cloud provider B. This should therefore include the (functionality of the) software, the users' data and the current state of transactions.

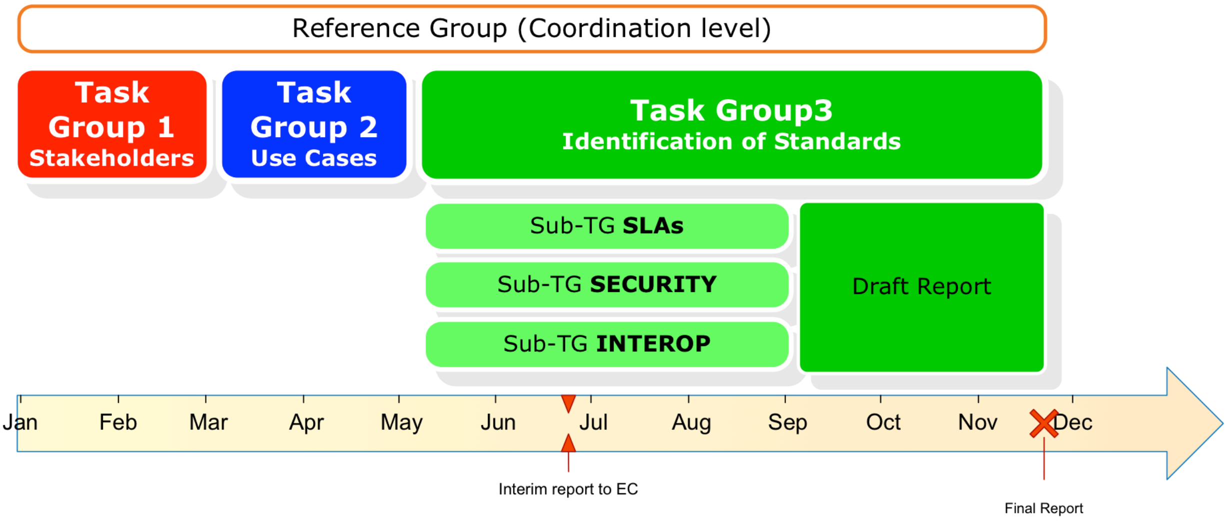
Annex 4 CSC Organization and Work Method

During the kick-off workshop in December 2012, three Task Groups (TGs) have been created:

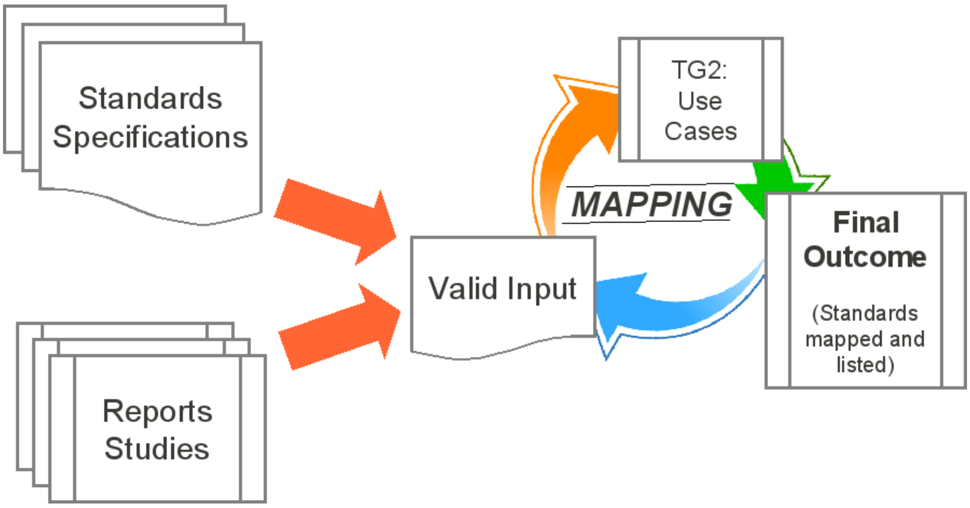
- TG 1 is in charge of the definition of roles and parties
- TG 2 is in charge of the collection and classification of the Use Cases
- TG 3 is in charge of analysing the Use Cases and identifying the Cloud-Computing relevant Standards and Specifications, possibly identifying the gaps and drawing conclusions. TG3 also highlights where no standards can be identified but are considered necessary or desirable.

  The work has been divided in three sub-groups in order to focus the scope of the analysis:
  - IOP Interoperability, Data Portability, and Reversibility
  - SEC Security and Privacy
  - SLA Service Level Agreements

The organization of the TGs is the following:



The figure below illustrates the working methodology for Task Group 3.



According to this methodology:

- use cases have been derived from the results achieved in Task Group 2 and form the basis for the mapping of standards. By taking this approach, i.e. by putting use cases in the focus of the activity, a high degree of real-life relevance is achieved. Users of the cloud standards mapping are able to work on the use case basis too, and thus have a realistic reference point that is based on actual business needs;
- the analysis of a small number of relevant use cases has provided a table of generic or specific activities across the 3 phases of the Cloud Services Life-Cycle (Acquisition, Operation, Termination);
- this decomposition into activities has been mapped with the two lists of documents from Annexes 1 (Standards & Specifications) and Annex 2 (Reports and White Papers). As a result, for each activity, the relevant Standards & Specifications (possibly none) or other documents (Reports and White Papers) have been identified. This gives an indication regarding the maturity of standardization regarding each activity and the possible existence of gaps.

To address the detailed map of the standards, the new European Standards Regulation has been the reference regarding the selection of Standards & Specifications. It refers to "standards" in two ways: a Standard is an output from a formally recognized SDO (such as ETSI or ITU-T), a Specification is a standard from any other form of SDO.

Once the methodology has been applied consistently, some conclusions have been drawn.

The completed report is now provided by the end of November 2013. It is worth mentioning that any complete report is, by nature, only a snapshot at the given point in time.