D4.2 Best practices for Cloud standards profile development

www.cloudwatchhub.eu|info@cloudwatchhub.eu
@CloudWatchHub | @CnectCloud

Standard profiles provide a clarification and constriction of a set of standards for a given application domain. The purpose of this report to provide a summary of the specific cloud standards profile activities undertaken, based on that present a best practices methodology for initiating and overseeing the development of cloud standards profiles that should be implemented.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

CloudWATCH Mission

The CloudWATCH mission is to accelerate the adoption of cloud computing across European private and public organisations. CloudWATCH offers independent, practical tips on why, when and how to move to the cloud, showcasing success stories that demonstrate real world benefits of cloud computing. CloudWATCH fosters interoperable services and solutions to broaden choice for consumers. CloudWATCH provides tips on legal and contractual issues. CloudWATCH offers insights on real issues like security, trust and data protection. CloudWATCH is driving focused work on common standards profiles with practical guidance on relevant standards and certification Schemes for trusted cloud services across the European Union.

The CloudWATCH partnership brings together experts on cloud computing; certification schemes; security; interoperability; standards implementation and roadmapping as well as legal professionals. The partners have a collective network spanning 24 European member states and 4 associate countries. This network includes: 80 corporate members representing 10,000 companies that employ 2 million citizens and generate 1 trillion in revenue; 100s of partnerships with SMEs and 60 global chapters pushing for standardisation, and a scientific user base of over 22,000.

Disclaimer

CloudWATCH (A European Cloud Observatory supporting cloud policies, standard profiles and services) is funded by the European Commission's Unit on Software and Services, Cloud Computing within DG Connect under the 7th Framework Programme.

The information, views and tips set out in this publication are those of the CloudWATCH Consortium and its pool of international experts and cannot be considered to reflect the views of the European Commission.

Executive Summary

Standard profiles provide a clarification and constriction of a set of standards for a given application domain. The purpose of this report to provide a summary of the specific cloud standards profile activities undertaken, based on that present a best practices methodology for initiating and overseeing the development of Cloud standards profiles that should be implemented.

Hence, this report addressed the following topics:

- It provides a methodology (best practice) that is supposed to be suitable for defining standards profiles and shows how to approach the relevant Standard Development Organizations.
- It provides an extensive documentation of outreach activities that have guided the work presented in this report.
- It provides an in-depth analysis of the current landscape of standardization in the area of cloud computing, including a gap analysis of issues not yet addressed by any standard.

Table of Contents

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

Figures

1 Introduction

Standard profiles provide a clarification and constriction of a set of standards for a given application domain. As defined in the CloudWATCH description work, the purpose of this report to provide a summary of the specific cloud standards profile activities undertaken, based on that present a best practices methodology for initiating and overseeing the development of Cloud standards profiles that should be implemented.

Hence, this report addressed the following topics:

- It provides a methodology (best practice) that is supposed to be suitable (validation will take place in the second half of the CloudWATCH project) for defining standards profiles and shows how to approach the relevant Standard Development Organizations (SDOs). The approach is based heavily on the achievements of the use case work of the project that is documented in [D2.1] and [D2.2], respectively.
- It provides an extensive documentation of outreach activities that have guided the work presented in this report.
- Moreover, it provides – as background information – an in-depth analysis of the current landscape of standardization in the area of cloud computing, including a gap analysis of issues not yet addressed by any standard.

The report is structured as follows:

- Section 2 explains the term “standards profile”.
- Section 3 provides a process for the definition of a standards profile based on four steps: Application domain analysis (Section 3.1), standards analysis (Section 3.2), definition (Section 3.3). Section 3.4 provides a reduced educational example that illustrates (some of) these steps.
- Section 4 provides an extensive analysis of existing standards based (a) on the final report of the Cloud Standards Coordination group of the European Telecommunication Standardization Institute [ETSI13] and the Cloud Computing Standards Roadmap of the National Institute for Standards and Technology [NIST13].

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- A documentation of dissemination activities that has contributed to this work is provided in Section 5.
- The final Section 6 gives an overview on next steps that are planned.

2 Standard profile definition

Standard specifications establish normative behaviour and interaction between a number of interacting computer systems, including at least one cloud bases system. In many cases, standard specifications are written modelling a previously collected set of use cases in mind. Hence, standards may allow for a certain degree of variability in the normative behaviour, particularly if the selected use cases are diverse in nature. Also, standards may also leave certain elements intentionally undefined to *foster* extensions and uptake.

Variability in encoded normative behaviour (not the implementation!), as well as ambiguous language use in the documents itself can lead to incompatible and non-interoperable implementations of the same specification. Specification profiles therefore aim at *reducing* the complexity and variability of normative behaviour for implementations, intending to remove any variability. Standards profiles may normatively reference more than one standard specifications (i.e. any implementation for the profile specification must also implement the referenced standard specifications in the defined way. The set of standards that are relevant for a given profile are usually determined by an application domain. For instance, governmental institutions concerned with information technology security usually define standards profiles for networking protocols and networked applications that clarify how standards related to the Internet protocol family have to be constricted for the use in the public sector application domain.

Technically, profiles refer to specific sections and terms defined in the referenced standard(s), and make normative statements, such as to reduce ambiguity and variability. For instance, where a standard uses the term “MAY”, the profile may reduce variability by tightening the original statement into a “MUST” In general, a profile tightens the scope of a standard specification so that any software accurately implementing the profile will always be implementing the underlying standard (but not necessarily vice versa)

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

3 Best practices

More and more, consumers are expressing concerns about the lack of control, interoperability and portability. Why? Because they are central to avoiding vendor lock-in, whether at the technical, service delivery or business level, thus ensuring broader choice. As a user, open standard interfaces protect you from vendor lock-in, so you avoid significant migration costs you would face when open interfaces are not provided. Standardization has become a best practice and a reference to the EU Cloud Computing Strategy as part of the drive towards trusted, secure and reliable cloud services. The ETSI Cloud Standards Coordination report also recognizes that compliance can be a competitive advantage for a cloud service provider.

"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." (ETSI CSC 2013: pg29)

With regard to research and innovation initiatives, standardization is also important for taking new products and services to market.

Best practices for standards profile definition is provided by the following three-step process:

- Practices to explore the application domain;
- Practices to understand the current landscape of available and missing standards for the application domain in question
- Practices to involve relevant SDOs and to trigger standardization processes needed to fill the gaps.

3.1 Application domain description

3.1.1 Stakeholder Analysis

A first step for exploring the application domain is to identify the parties that define interests in the interoperability of systems that belong to this application domain, and thus in associated interoperability standards. Stakeholder analysis is usually described as part of project management activities and aims on understanding the interests and influence of the various stakeholders to a particular project, and provides guidelines how to manage them in the context of the project, hence, it assumes a 1-to-many relationship between project management and stakeholders.

This observation implies that classical approaches of stakeholder management are not directly applicable to analyze an application domain for cloud computing, because this domain is not defined by a simple 1-to-many relationship but by possibly complex eco-system (i.e., a network) of various interested parties. For instance, even a simple contractual relation between a cloud service customer and a cloud service provider involves various stakeholders beyond the two primary ones, with various interests and concerns:[1]

- The cloud service customer is interested in a service with appropriate quality, has concerns about data security and service availability. This includes interoperability both on technical level, and on organizational level.
- The cloud service provider is interested in satisfying the needs of its customer, while providing services at the highest possible profit margin. Therefore, interoperability with its customer's systems and processes is important.
- The cloud service provider may additionally use cloud services of a secondary provider. Therefore, they adopt the interests and concerns of the cloud service customer indicated above.
- The cloud service user (i.e., the person in the customer's organization that actually uses a cloud service) is interested in working with an ergonomic service, and is concerned about the protection of personal data that refer to them.
- The cloud service provider may utilize a single sign on (SSO), which includes a 3rd party identity provider. The identity provider is interested in supporting as many SSO standards as possible, to widen their customer base.
- An auditor needs access to all relevant data to perform a financial audit of the cloud service provider. Therefore, they are interested in interoperability of their data base and analysis software with the cloud service provider's data management systems.

This example provides just a small snapshot of the relationships between the various stakeholders of a basic, very general application of cloud computing (service provisioning with SSO). It illustrates that an understanding of a cloud computing application domain requires an analysis of the network of its stakeholders. We therefore took inspiration from a stakeholder analysis methodology presented in [CSC10]. The authors of this article were interested in quantitative analyses of stakeholder networks

[1] The lists of interests and concerns given in this example are not intended to be complete or of general validity, but to illustrate the complexity of a cloud service eco-system.

that are not applicable within the context of this report and thus have not been considered. Moreover, we adapted the method to be in alignment with previous work (in particular [D2.1]).

For each stakeholder, we therefore define the following attributes:

- Its interests to participate in the cloud computing eco-system;
- Its concerns on interoperating with other stakeholders;
- Regulatory requirements and restrictions that are applied;

The analysis is however not yet complete, as we do not aim to provide technical solutions to establish these relationship. Our goal is rather to trigger standardization activities for this domain wherever they are needed. Therefore, a subsequent step has to map the stakeholders to their involvement in the various SDOs of relevance, and to identify their influence and the concrete relationship to other stakeholders (e.g., are they competitors, cooperators, or do they target different market sectors?).

3.1.2 Use case collection

The next step in the domain analysis comprises the collection and analysis of use cases illustrating the interaction of the various stakeholders of a cloud service eco-system. Use cases are important to understand the concrete interactions between the various stakeholders identified in the previous step, and to validate the assumptions made on their interests and concerns.

3.1.2.1 Methodology

A methodology for the presentation of use cases has been already provided in the CloudWATCH Deliverable D2.1: Reference Model Framework Report. D2.1 introduces the notion of a usage scenario for cloud computing as a concrete (real life, or fictitious but realistic) usage context of a cloud-based system or service: a business case or the usage of a set of cloud services for a particular purpose; hence usage scenarios are high-level descriptions of cloud service application domains that needs to be processed by further analyses as described in this section.

Moreover, D2.1 classifies use cases into several types:

- Legal use cases show how certain interactions between actors by regulatory restrictions. For instance, use cases showing how data deletion is done across various cloud service provider illustrates rights on the deletion of personal identifiable data (“right to be forgotten”) that is granted to natural persons by many regulatory systems.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- Organisational use cases show how operational and business processes of various stakeholders can interoperate. For instance, operational procedures on software updates requires the interworking between the cloud service provider (who updates certain services), and the cloud service customer (who needs to understand how and when updates of its in-house system are necessary in reaction to the service update).
- Technical use cases describe the interoperation of system components on the level of interfaces, protocols, and data formats. For instance, the steps necessary to deploy and to start a virtual machine on a cloud infrastructure constitute a use case of this category.

D2.1 provides a rich framework for the description of cloud systems and related organisational processes based on a cloud reference architecture identifying:

- Roles and sub-roles regarding the cloud service customer and the cloud service provider as primary stakeholders of the cloud service eco-system;
- examples of secondary stakeholders summarized under the cloud service partner category;
- the technical components of a cloud system structured into layers, multi-layers, and cross-cutting aspects.

Clearly, the description provided in D2.1 is "context-free" in the sense that it applied to any application domain. Concrete domains need to refine and to extend the framework introduced in D2.1.

3.1.2.2 Use case acquisition

This section gives an outline of the methodology used to acquire use cases and summarizes the experiences gained so far in the ongoing work of the CloudWATCH project. For details please refer to the intermediate CloudWATCH Deliverable [D2.2].

Desktop research on relevant aspect of the application domain and potential use cases is an important pre-requisite to the subsequent methods.

Using online surveys. An online survey was developed (see [D2.1] for details) and presented during the EC Concertation Meeting, *Towards an interoperable European Ecosystem of Services* (Brussels, 12/13 March 2014). Interest and engagement of the audience at the workshop was good, however, uptake of the online survey was not as high as expected, both during the workshop and in subsequent weeks. Gathering use cases by motivating community engagement in this way stalled

completely and expectations that this approach could be successful in the future should be carefully reconsidered.

As a contingency action, CloudWATCH requested the intervention of the EC Project officer who distributed an email message to the projects requesting enagagement.

Interviews. A series of one-to-one interviews, via telephone or online, with the key representatives from each of the projects, has been initiated. Initial one-to-one interviews were conducted at agreed times, by Skype or telephone. These interviews took the form of relatively informal discussions where the respondent had the opportunity to describe their project in their own words. To achieve a higher level of accuracy in the representation, and provide a solid basis for further analyses, subsequent iterations of the interview process is needed and will be performed in the future work of the CloudWATCH project.

3.1.2.3 Outcomes, conclusions and recommendations

Again, we refer to D2.2 for a complete discussion of the outcomes achieved so far, and provide a summary related to best practices for standards profile definition.

Self-submission of use case information. While self-promotion of projects, that has been approaches for the acquisition of use cases, within the community is high, engagement with self-submission of information pertaining to use cases was low.

Perception of usefulness. Interviewees displayed a great willingness to discuss projects and clearly with a high degree of knowledge, though in general respondents felt they were less able to make a useful contribution on legal, organisational and technical aspects pertaining specifically to use cases.

3.2 Understanding the current standardization landscape

3.2.1 Resources

A number of resources are available to obtain information on standards related to cloud computing:

- An account of standards relevant for cloud computing is provided by CloudStandards[2].
- The European Telecommunication Standardization Institute (ETSI) has recently published standards analysis document [ETSI13]. Section 4.1 of this deliverable contains a summary of the ETSI report.

[2] http://cloud-standards.org

- The National Institute for Standards and Technology has published a Cloud Computing Standardization roadmap that contains an a discussion on current standard development activities [NIST13]. This document is discussed in Section 4.2.

The following SDOs are actively contributing to standardization in the area of cloud computing:

- Cloud Standards Customer Council[3]
- Distributed Management Task Force (DMTF)[4]
- The European Telecommunications Standards Institute (ETSI)[5]
- International Standardization Organization / International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1)[6]
- International Telecommunications Union (ITU)[7]
- National Institute of Standards and Technology (NIST)[8]
- Open Grid Forum (OGF)[9]
- Object Management Group (OMG)[10]
- Open Cloud Consortium (OCC)[11]
- Organization for the Advancement of Structured Information Standards (OASIS)[12]
- Storage Networking Industry Association (SNIA)[13]
- The Open Group[14]
- Association for Retail Technology Standards (ARTS)[15]
- TeleManagement Forum (TM Forum)[16]
- IEEE Cloud Computing Initiative[17]

[3] http://www.cloud-council.org/.
[4] http://www.dmtf.org/.
[5] http://www.etsi.org/.
[6] http://www.iso.org/iso/jtc1_home.html.
[7] http://www.itu.int/.
[8] http://www.nist.gov./
[9] http://www.ogf.org/.
[10] http://www.omg.org/.
[11] http://www.opencloudconsortium.org/.
[12] https://www.oasis-open.org/.
[13] http://www.snia.org/.
[14] www.opengroup.org/.
[15] https://nrf.com/membership/committees/arts-board-of-directors.
[16] http://www.tmforum.org/.
[17] http://cloudcomputing.ieee.org/.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- Cloud Security Alliance (CSA)[18]
- Cloud Computing Interoperability Forum (CCIF)[19]

3.2.2 Gap analysis

A gap analysis based on the use cases collected in the step described in Section 3.1.2 can be done using the following approach:

(a) **Identify standards** that are relevant for each use case. For this, explain what aspect that is described in the use case is covered by which standard, and for which aspect currently no standard is available.

(b) **Constriction and clarification**: From this collection of standards, determine which clarification or constriction is required to apply the standard for a given aspect

(c) **Aggregation**: Then, a table of the following format can be used to summarize available standards and aspects that are not covered by the available collection of standards on the level of usage scenarios (the last two columns are exclusive):

Scenario	**<Scenario identifier and title>**		
Use case	**Aspect**	**Covered by**	**Not covered**
<use case #1 identifier and title>	Specific aspect described in use case #1 defines standardization requirements	List of standard available for this aspect; description of clarifications and constrictions needed	Standards that can be possibly extended to capture this aspect
<use case #2 identifier and title>	Specific aspect described in use case #2 defines standardization requirements	List of standard available for this aspect; description of clarifications and constrictions needed	Standards that can be possibly extended to capture this aspect
. . .	. . .	. . .	. . .

Aggregation and summarizing the “aspect”/”covered by”/”not covered” columns than leads to a precise definition of

- How to apply a certain standard within a usage scenario or application domain.
- Aspects that are not covered by any standard.

[18] http://www.cloudsecurityalliance.org/.
[19] http://www.ccif.org/.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

(d) **Leaderboard**: The assignment of priorities might be a useful supplementary step: Standardization requirements not covered by any standard receive a very high priority, followed by those standards which need most constriction or clarification.

3.3 Profile definition

Now it is time to start the marketing process.

3.3.1 Roadmap

The following checklist is provides a possible roadmap for approaching relevant SDOs:

- **Develop a strawman profile document** that illustrates the incorporated standards, profiling statements and use cases as "marketing" material.
- Collect the SDO that once hosted the process of defining the collected standards, and retain stewardship of them.
- **Network, network, network**! Find other communities that utilize the same or a similar set of standards as your use case, and keep working on your strawman profile document. In other words, find collaborators that would back your effort in developing a profile
- Approach each of these SDOs, perhaps according to the ranking in your leaderboard, enquiring whether they see the proposed proposal in scope for their organization. Some may actually decline! In general though SDO's enjoy witnessing activities and popularity around "their" standards. SDOs will generally disseminate the idea of new standardization activities through their own community building channels, which you can use to build your own community around the profile.

3.3.2 Stakeholder analysis, again

The activity described in the roadmap outlined above should be underlined by an extended stakeholder analysis. The network of potential stakeholders relevant for an application domain captured by a usage scenario has been already addressed in Section 3.1.1. Evidently, many of these stakeholders such as cloud service providers, customers, public sector authorities, or research organizations, are actively involved in standardization processes, and their business interests

naturally influence their standardization activities. Therefore, an analysis should be performed that classifies the stakeholders as follows:[20]

- **Primary stakeholders** are those ultimately affected, either positively or negatively, by the standards profile under consideration.
- **Secondary stakeholders** are the 'intermediaries', that is, organizations who are indirectly affected by the profile.
- **Key stakeholders** (who can also belong to the first two groups) have significant influence upon or importance within the SDO.

Once key stakeholders are identified, they can be mapped on the following grid in order to determine the best strategy to approach and collaborate with them:

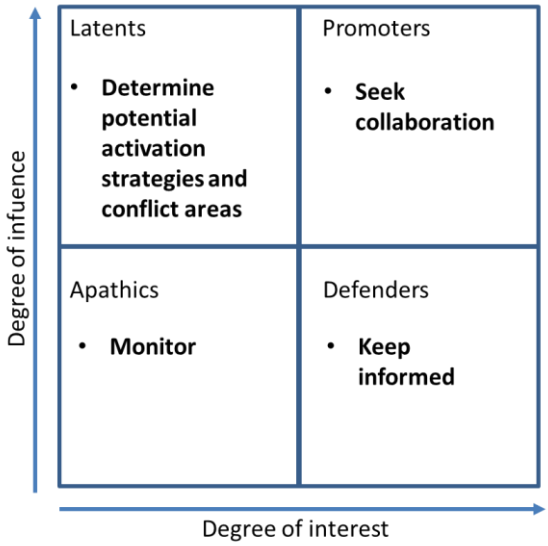

Figure 1. Stakeholder management matrix ([ICL], modified).

3.3.3 Approaching and collaborating with relevant SDOs

Once relevant SDOs have been identified that are willing to host the profile definition activity, the following gives a general guideline on how such a process will often go. Note: The actual process **will** vary from SDO to SDO!

[20] Our approach Is based on [IPL], other stakeholder analysis approaches are available.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- Identify the relevant technical representative within the SDO who can give you advice on the process and necessary steps within the SDO.
- Typically, SDOs use a formalize process of how the profile that involves chartering a new group, or an existing group, to undertake this endeavor. These groups can have different names, such as "Working Group" (OGF), "Technical Committee" (ITU), or any other name, but the intention is always the same: To provide a platform where collaborators can work together. SDOs have a process by which such a group is formed, to ensure uptake and assure sufficient contributions to drive the work forward.
- Once the SDO has formally decided to charter a group to take on defining the work, the actual technical work begins within the SDO
- People can join and leave a Working Group at any time, but typically there is a core team of members driving the specification forward.
- A profile is almost always a very technical document that makes specific references to statements in existing standards, and applies further constraints to such statements, removing variance and ambiguity. These statements can be of various nature:
  - Linguistic clarifications of normative text
  - Tightening normative constraints of the referenced Standards, e.g. turning a "MAY" into a "MUST", etc.
  - Tightening the cardinality of sequences or sets of elements, e.g. turning a "zero or one" into a "exactly one" statement
  - Referencing extension points in a base specification, and defining the allowed set of extensions (or defining these on the fly)
- Profiles incorporate by reference specific standards specifications into one document. This depends on the actual use case, and at times this may comprise of only one base specification, or several. Incorporation by reference means that provisions made in the base specifications must be considered integral and unconditional elements of the defined profile. In other words, if implementing the profile in software (or as a process), the base specifications must also be implemented.
- Once complete, the profile document undergoes a public review process that may vary from SDO to SDO in details. The result is a final specification that is often tagged as "proposed recommendation".

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- Profiles may undergo public implementations' interoperability testing, similar to standards. Once a threshold of interoperable implementations has been reached, Profiles may be tagged as "recommendation" and further published as final and in use.
- From this point on, the formal and technical profile definition work is completed, and uptake and popularity determine whether a given standard or profile will prevail or not.

3.4 Example: Provisioning management

Section 3.1.1 emphasizes the complexity of the cloud service eco-systems as motivation for a thorough stakeholder analysis phase. Complexity, however, is inappropriate in educational examples. We therefore provide an extremely simplified "eco-system" comprising only two stakeholders with very specific interests. Moreover, only a single use case is provided.

The following example is bases on a "true story": The EGI Federated Cloud community has identified the need for a mechanism to pass context information to virtual machine images before starting them up. Additional information can be found on the FedCloud WIKI[21].

3.4.1 Domain analysis

3.4.1.1 Stakeholders

- Cloud service customer: Service Administrator. Service administrators are interested to have convenient ways to configure instances of virtual machines according to their in-house environment.
- Cloud service provider. In order to make their cloud service offers as attractive as possible to their customers, a cloud service provider aim on simplifying the configuration efforts needed to set-up virtual machines.

3.4.1.2 Use case

We explicitly list just one use case there, using the simplified use case presentation format defined in D2.1. Another, obvious use case (referred to as "Startup of a non-contextualized virtual machine") describes the basic actions required to startup a virtual machine.

[21] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Contextualisation.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

Use Case		
Contextualization		
Description		Contextualization is the process of installing, configuring and preparing software upon boot time on a pre-defined virtual machine image (e.g. setting the hostname, IP addresses, SSH authorized keys, starting services, installing applications, etc.).
Goals and aspirations for the use case		The EGI Federated Cloud VM Management interface utilizes the OCCI family of specifications
Technical aspects	Preconditions	NONE
	Criteria for success	▶ Make use of transient images (i.e. not persisting any VM state after it has been stopped) as much as possible ▶ Configure/contextualize a base image during its runtime ▶ Apply any local configurations that might be necessary before making the VM instance available for use ▶ Stop the VM, losing all transient data accumulated during runtime. ▶ This pattern needs to be employed across the entire federated Cloud infrastructure, in a consistent way.
	Failure conditions and responses	NONE
Existing specifications to rely on		▶ OCCI 1.1, which does not define any mechanisms for delivering contextualization information to VM instances
New specifications required		Conveyance mechanism for contextualization information
Additional comments		**NONE**

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

3.4.2 Profile requirements matrix

Hence, the following profile requirements matrix can be constructed on the basis of these two use cases. Aggregation emphasizes the need of a contextualization mechanism that receives position one (in our example, the only position) of a leaderboard.

Scenario	**Provisioning management**		
Use case	**Aspect**	**Covered by**	**Not covered**
UC1: Startup virtual machine	Startup of a non-contextualized virtual machine	OCCI 1.1	
UC2: Contextualization	Passing context information to virtual machine images before start-up		Contextualization mechanism
. . .	. . .	. . .	. . .

3.4.3 Subsequent technical work and standardization activities

The EGI Federated Cloud has incorporated contextualisation capabilities in its VM Management interface. For this, EGI has developed a system employing "cloud-init" as conveyance mechanism, and a set of golden images that have cloud-init pre-installed.

To allow users make use of this system, EGI also defined two specific extensions for OCCI and declared their support in EGI mandatory.

- Passing arbitrary user-provided data to the virtual machines on instantiation
- Passing ssh public keys for given user accounts into the machine.

These extensions are defined as OCCI Mixins, an extension mechanism built into OCCI without changing the core specification

These extensions have not been formalised, nor referenced in any profile document – but this *could* have been the case had this not been depreciated by the OGF OCCI-WG accepting these extensions as input material to a future OCCI 1.2 version including contextualisation capabilities

4 Gaps in the current landscape of cloud computing standards

The brief analysis and description of the *status quo* proposed in this paragraph is largely based on the Final Report of the ETSI Cloud Standards Coordination (CSC) activity [ETSI13] and on the NIST Special Publication "NIST Cloud Computing Standards Roadmap" [NIST13] and supported by non-exhaustive desktop research and informal consultation with key industry stakeholders as well as based on Cloud Security Alliance (CSA) interaction and collaboration with key SDOs.

Since the two baseline documents were published respectively on July and November 2013, the purpose of the desktop research, the consultation with stakeholder and the work of CSA has been to verify any possible change in the cloud standards landscape as described in the ETSI and NIST document.

4.1 ETSI Cloud Standard Coordination Report

The report [ETSI13] is the result of an exercise of collection and analysis of cloud relevant standard performed by a group of subject matter experts coordinated by ETSI, on behalf of the European Commission (EC). The purpose of the CSC was to bring some clarity in what is defined in the European Cloud Strategy as a "jungle of standards" and to help cloud customers and provider in their approach to cloud computing. The project was kicked off in October 2012 and finalized in November 2013, and it is one of main actions defined in the EC European Cloud Strategy.

4.1.1 Approach

The analysis took stock of approximately 150 technical standards, best practices and white papers relevant to cloud computing and identified 20 key players in the cloud computing standards landscape.

The CSC's work focused on three (3) main areas:

- Security and privacy
- Interoperability and portability
- Service level agreements

The work of the CSC group identified the standards available in these areas for each of the phases of a simple cloud service lifecycle composed of the steps:

- Acquisition
- Operation
- Termination.

4.1.2 Conclusions

The conclusions of the ETSI CSC task force were the following:

- The cloud standard landscape appears to be less fragmented than expected, it's "complex but not chaotic and by no means a 'jungle'".
- Most of considered standards have still a low level of adoption (quoting the CSC report: "*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*" [ETSI13, Executive Summary]).
- The cloud market and community would benefit from a definition and widespread adoption of a "shared vocabulary" and "formal definitions that are machine readable." In particular in the Service Level Agreement, which is a fast maturing area, where gaps are still to be filled, there a clear need for an agreed terminology for Service Level Objectives and associated metrics
- From the security perspective the work done by the CSC showed that there are many available standards in the areas of visibility and transparency, assurance and trust, certification, audit and testing, identity and access management, virtualization and multi-tenancy risks, data location control, secure data deletion and the exit process, but either they are in most of cases not 100% fit for purpose for cloud computing since they were created before the raise of cloud computing or they are cloud-specific but not quite mature of sufficiently adopted yet. Few exceptions can be found in the area of cloud computing governance and assurance standards. Moreover the security and privacy analysis showed that gaps exists in the area of accountability and cloud incident management (e.g., related with a SLA infringements).
- The Interoperability and Portability analysis showed the existence of mature standards especially at IaaS level while effort is required for supporting a true interoperability and portability at PaaS and SaaS level.
- Other areas where gaps exist are in the area of "federation", cross border collaboration and verification of legal obligations, management interfaces and protocols (especially at PaaS and SaaS level), service metrics and service performance monitoring.

- In the cloud service "Acquisition phase" there's need to have more sophisticated tools for comparing cloud providers' capabilities.
- The analysis of the "Operation phase", showed that standards for IaaS are available and are sufficiently mature and adopted while still more work is required for PaaS and SaaS.

4.2 NIST Cloud Computing Standards Roadmap

The NST Cloud Computing Standards Roadmap Version 2 [NIST13] it's a follow up activity of the first version of the Standard Roadmap, which has been published in August 2011. The Standards Roadmap is part of the NIST Cloud Computing Program that is one of the mechanisms in support of United States Government secure and effective adoption of the Cloud Computing model to reduce costs and improve services.

4.2.1 Approach

The NIST Cloud Computing Standards Roadmap has been elaborated by a Working Group, which has collected and analyzed the standards landscape, looking in particular at the areas of:

- Interoperability
- Performance
- Portability
- Security
- Accessibility

Similarly to the ETSI CSC's effort, the NIST's work based the assessment of standards and identification of gaps on the analysis of uses cases.

The Roadmap identifies gaps and suggests possible candidate organizations to pursue the task of developing new standards and / or enhancing existing ones.

4.2.2 Conclusions

The conclusions identified in the [NIST13] are the following:

- Standards to support cloud interoperability and portability exist, but gaps remain in standardization, specifically in the PaaS area. Moreover, some of the current standards need to mature in order to describe how services interoperate and how data can be readily ported between cloud offerings.

- At the same time, according to NIST we'll see an increase focus on standard to support cloud governance and orchestration. At this regards a definition of suitable standards to describe SLAs will be required.
- In the area of standards for Portability NIST suggests: "*A future direction of workloads data and metadata standardization is to help improve the automation of inter-cloud system workload deployment. Concepts such as standardized SLAs, sophisticated inter-virtual machine network configuration and switching information, and software license information regarding all of the various components that make up the workload are possibilities.*" [NIST13, p. 42].
- In the area of standards for SaaS interoperability NIST' cloud standard roadmap suggests that "[…] *it is more likely that data formats and metadata-based interchange methods will be standardized in cloud system products rather than having SaaS interfaces themselves converge. Examples of such data format description standardization include the* ***Data Format Description Language (DFDL)*** *from OGF and the* ***Cloud Data Management Interface (CDMI)*** *data-container metadata model of the Storage Networking Industry Association (SNIA). As the cloud computing landscape is currently heavily populated by vendor-specific formats, such general-purpose standardization efforts may be crucial to achieving interoperability at the SaaS level*" [NIST13, pp. 41-42].
- The NIST Roadmap suggests five areas of focus for cloud computing standards:
  - Management APIs
  - Data exchange formats
  - Federated identity and security policy APIs
  - Resource descriptions
  - Data storage APIs
- In more detail, NIST highlights the need for standards in the areas of:
  - Standard interfaces to metadata and data objects: results in this area can be reached by supporting the further development of CDMI from SNIA
  - Common VM description format, common service and application description format to facilitate cloud migration, the development of hybrid clouds, disaster recovery capabilities and cloud-bursting: results in this area can be reached by supporting the further development of OVF from DMTF, TOSCA from OASIS, OpenID, Oauth

- Resource and performance requirements description languages to facilitate a cost-effective deployment: results in this area can be reached by supporting the further development of DMTF CIM and OGF GLUE. For Master Service Agreements and Service Level Agreements, WS-Agreement and WS-Agreement-Negotiation (WS-AG, WS-AN) from OGF; for cloud application and service level description of attributes, relationships, requirements, and capabilities, TOSCA from OASIS.
- Standard metadata/data formats for movement between cloud systems: standards to be considered for further development are AS4, OAGIS, NoSQL, GridFTP, DFDL, CDMI
- Federated identity, authorization, and virtual organizations: standards to be considered for further development are OpenID, OAuth, SAML, WS-Federation and WS-Trust, CSA outputs; Virtual Organization Management System (VOMS) from OGF.
- SLA description language to support selection of appropriate cloud service: possible standards to be considered are WS-Agreement (GFD.107) and WS-Agreement Negotiation (OGF).
- Auditing standards and verification check lists: results in this area can be reached by supporting the further development of CSA Cloud Audit.

4.3 Examples of existing standards identified by ETSI and NIST

Following a no-nexhaustive list of available standards in the areas of interoperability, portability, security and privacy and service level agreement.

4.3.1 Standards for interoperability

At IaaS level:

- Open Cloud Computing Interface (OCCI) specification from Open Grid Forum
- Cloud Infrastructure Management Interface (CIMI) from the Distributed Management Task Force (DMTF).

At PaaS level:

- Cloud Application Management Protocol (CAMP) technical committee by the OASIS

At SaaS level:

- Most of the standards are neither new nor cloud specific: IP (v4, v6), TCP, HTTP, SSL/TLS, HTML, XML, REST, Atom, AtomPub, RSS, and JavaScript/JSON, OpenID, Odata, CDMI, AMQP, and XMPP, XML.

4.3.2 Standards for portability

- **Open Virtualization Format (OVF)** from the Distributed Management Task Force (DMTF): addresses portability concerns between various virtualization platforms. It consists of metadata about a virtual machine image or groups of images that can be deployed as a unit. It provides a mechanism to package and deploy services as either a virtual appliance or used within an enterprise to pre-package known configurations of a virtual machine image or
- **Topology and Orchestration Services for Applications (TOSCA**) from OASIS: provides a machine-readable language to describe the relationships between components, requirements, and capabilities.

4.3.3 Standards for Service Level Agreement

- WS-Agreement Negotiation from OGF
- Web Services Agreement (WS-Agreement) from OGF
- SLA: An abstract syntax for Service Level Agreements from SLA@SOI
- GB917 SLA Management Handbook, Release 3.1 from TM Forum
- TR178 Enabling End-to-End Cloud SLA Management, Version 0.4 from TM Forum

4.3.4 Standards for security

- ISO / EIC 27018 Code of practice for data protection controls for public cloud computing services
- NIST 800-53 Rev.4 Security Controls
- NIST Security Reference Architecture
- Cloud Controls Matrix (CCM), Cloud Security Alliance
- Open Certification Framework (OCF), Cloud Security Alliance
- Cloud Trust Protocol (CTP), Cloud Security Alliance
- CloudAudit, Cloud Security Alliance
- Privacy Level Agreement, Cloud Security Alliance
- Star Audit, Euro Cloud
- Data Security Framework, Open Data Center Alliance

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

4.4 Recent advancement

As mentioned in the beginning of the section, this analysis of standards is largely based on the information available at the time of writing of the ETSI CSC report and NIST Cloud Standards Roadmap.

In the timeframe from November till the present time (June 2014) the following new elements in the standards landscape have emerged:

- The publication of the ISO / IEC 17788**,** Information technology — Cloud computing – Overview and vocabulary
- The publication of the ISO / IEC 17789, Information Technology, - Cloud Computing – Reference Architecture
- The finalization (not published yet) of the ISO / EIC 27018 Code of practice for data protection controls for public cloud computing services
- The publication of the CSA STARS Attestation, the joint attestation developed by the Cloud Security Alliance and AIPCA, based on CCM and SOC2.
- The TOSCA Simple Profile in YAML

It should also be noted that the following guidance and standards are due for finalization in the next three months:

- EC Selected Industry Group: Certification Schemes
- EC Selected Industry Group: Code of Conduct
- EC Selected Industry Group: Cloud Service Level Agreement Standardization Guidelines
- CSA Cloud Control Matrix v3.01
- CSA Control Assessment Initiative Questionnaire (CAIQ) v3.01

Moreover very encouraging steps forward have been done by the International community on the definition of SLA and current effort of the ISO/IEC JTC 1/SC 38/WG 3 on “Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology” is very promising.

In terms of standards adoption, it appears that since the end of 2013, there been an increased in use of new standards in the area of certification, compliance and security controls.

4.5 Gaps

Based on the conclusions and recommendation included in ETSI and NIST and other information collected and assessed with regard to the standards for cloud computing, we have drawn the following conclusion on potential gaps:

- Development and adoption of a common vocabulary: this gap has been partially addressed with the recent publication of the ISO / IEC 17788**,** (Cloud computing – Overview and vocabulary) and of the ISO / IEC 17789 (Cloud Computing – Reference Architecture), and further improvement should be expected once other ongoing effort, such as the ISO/IEC 19086 project on Cloud SLA, will be completed.
- Governance, Risk and Compliance (GRC): there are several ongoing efforts in the area of GRC, which include development of mechanisms for assessing cloud service before their acquisition, for measuring the service performance, for SLA monitoring, for service orchestration, but it appears from the reluctance of portion of potential cloud customers to embrace cloud service and from their remarks on the confusion around accountability, liability, compliance and security in the cloud, that those ongoing efforts to simplify the provider selection process and the governance and control of cloud programmes are not yet mature enough or at least the level of awareness about them is not satisfactory.

  A typical example of this gap in area of GRC tools is “cloud certification”. In the CloudWATCH deliverable D4.1 – Cloud certification guidelines and recommendations we analysed a number of certification schemes. Some of them are definitely mature and solid enough to satisfy the need of assurance of most of potential cloud computing customers, but the level of the adoption of those certification is not yet satisfactory.

  In the specific case of certification it appears that the reason for this low-level of adoption is linked to: 1) low awareness around the schemes. 2) knowledge gap around the technical standard underlying the certification process.
- Application-specific data and metadata standards: According to the NIST Cloud Standards Roadmap, confirmed by a consolation of the members of the CSA ISC: “application-specific data and metadata standards remain standardization gaps in portability and interoperability. For example, email and office productivity application data format standards and interfaces are required to achieve interoperability and portability for migrating from existing systems to cloud systems.

Another important area for standardization is the metadata format and interfaces, in particular, to support compliance needs. For example, standard metadata format and APIs to describe and to generate e-discovery metadata for emails, document management systems, financial account systems, etc., will help government consumers to leverage commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software products to meet e-discovery requirements."

- Management interfaces: gaps are noticeable also in the area of space management interfaces to administer application functionalities. Despite the lack of interfaces to satisfy very diverse and sometime complex needs, it appears that some management functionalities are becoming common (e.g. user account and credential management). According to NIST report: "…these common management functionalities represent candidates for interoperability standardization." Data format for backup and migration of application workload, including database serialization/de-serialization, need further standardization to support portability.

5 Outreach report

A number of communication and outreach activities have yielded additional information and contacts for the further development of the cloud standards profile. CloudWATCH has worked closely with partners to help define messaging around the benefits of standards, standards profiling and interoperability.

In line with the Commission's drive towards a trusted cloud, where compliance to relevant standards can give European service providers a competitive advantage, CloudWATCH has assessed the identified standards for implementation by initiatives that have received funding under FP7 Software, Services and Cloud. With regard to research and innovation actions, the standards are one of the most important means to bring new technologies to the market[22].

With the launch of the European Cloud Scout online service on 10 July 2014, the CloudWATCH communication specialists will increase the emphasis on the benefits of interoperability and

[22] Standards and Standardization Handbook, European Commission. 2013, http://ec.europa.eu/research/industrial_technologies/pdf/handbook-standardisation_en.pdf.

standards for European businesses. This approach is aligned with increasing consumer concerns over lack of openness and interoperability[23].

Awareness and communication

The text below is an example of current messaging on the key role of standards for Europe.

Turning interoperability from a best practice to a common practice

Why does Europe need interoperability and portability of data?

More and more, consumers are expressing concerns about the lack of control, interoperability and portability. Why? They are central to avoiding vendor lock-in, whether at the technical, service delivery or business level, thus ensuring broader choice.

As a user, open standard interfaces protect you from vendor lock-in, so you avoid significant migration costs you would face when open interfaces are not provided.

From a European research provider perspective, interoperability means more efficient resource utilisation. The EGI federated cloud is a pioneering examples of this.

CloudWATCH can offer practical guides to relevant standards and their level of maturity. This is important because the implementation of a core set of internationally recognised standards is key to avoiding multiple, inconsistent guidelines and bespoke solutions.

How we are making a difference with CloudWATCH

Over the past decade, peer collaborative work in Europe and beyond has built considerable expertise in standards development and implementation, laying the foundation for interoperability testing and fairer competition.

CloudWATCH will provide a portfolio of European and international use cases. The use cases will cover technical requirements, policy and legal requirements, such as service level agreement management. This will lead to the development of common standards profiles and testing around the federation of cloud services.

[23] See, for example, GigaOM, The Future of Cloud Computing, 3rd Annual survey, 2013, http://ow.ly/uq0tM.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

CloudWATCH will make an active contribution to standards and certification, driving interoperability as critical to boosting innovation in Europe.

CloudWATCH has made an analysis of existing certification schemes in Europe and across the globe. We have defined an initial set of recommendations for policy makers, public procurers, procurers of cloud services at the business level, and compliance managers.

So what's a standard profile anyway?

A Standard very often supports multiple use cases in its specification text which can lead to ambiguity and a lack of real interoperability across different interfaces.

A profile on a standard clarifies in an unambiguous way how a standard has to be interpreted, explaining how to implement it based on your specific use case.

5.1 ICT2013 - 4-5 November 2013

Information stand - The CloudWATCH EU Innovation Cloud Hub - 6-8 November 2013 in Vilnius. The CloudWATCH Information Stand - EU Innovation Cloud Hub - shone the spotlight on European investments in interoperable clouds contributing to an internal market of services in the European Union. The event was an important opportunity to engage with 22 EC-funded projects including other CSAs (Call 5, 8, 10 & CIP) who participated on the stand: ARTIST, BETaaS, CELAR, CitizenGrid, CloudCatalyst, CloudingSMEs CloudSpaces, Compose, HARNESS, KC Class, MIDAS, MobiCloud, Mobizz, MODAClouds, OCEAN, OPENi, PaaSage, PROSE, Riscoss, SUCRE, U-QASAR, VISIONCloud An A-Z directory of these projects was created providing an overview of all 22 projects.[24]

The event was also an opportunity to inform stakeholders of CloudWATCH objectives and in particular the development of cloud standards profiles. Over 150 contacts were made at the event.

5.2 Software and Services, Cloud Computing Concertation Meeting - 12-13 March 2014.

This Concertation meeting took stock of the latest activities of all active projects that have received funding through Unit E2 (including projects funded under Calls 5, 8 & 10, CIP as well as EU-Japan representation), including selected success stories, present and discuss new ideas. Position papers

[24] http://www.cloudwatchhub.eu/sites/default/files/A-Z_CloudWATCH%20Stand_ICT2013.pdf

were collected from participating projects. With the EC Cloud Computing Strategy stressing the importance of encouraging standards which are internationally coordinated with open specifications projects were requested to provide information relating to relevant standards for interoperability and portability. This included information on the key areas in the Cloud landscape identified in the project that requires re-use or active contribution to standards and information on the standards-related groups the project is working with. The collection of position papers gives an overview of standards adoption both actual and planned by Call 8 and 10 projects. Information also included project contributions to standards development including engagement with SDOs.

A snapshot of this information can be seen from the table below which shows some of the most used standards: OGF-OCCI, OASIS-TOSCA, SNIA-CDMI and DMTF-OVF. Other standards are also used by projects but are not cited here.

Standard	Usage in Call 8 & 10 projects
OCCI - Open Cloud Computing Interface (OGF)	Call 8: BETaaS, OCEAN (Interoperability testing) RISCOSS (Risk Analysis) Call 10: ASCETiC, CloudWave, ENVISAGE, ORBIT, PANACEA
CDMI - Cloud Data Management Interface (SNIA)	Call 8: OCEAN (Interoperability testing), RISCOSS (Risk Analysis) Call 10: ASCETiC, ClouT
OVF - Open Virtualization Format (DMTF)	Call 8: OCEAN (Interoperability testing), RISCOSS (Risk Analysis) Call 10: ENVISAGE, ORBIT, PANACEA
TOSCA - Topology and Orchestration Specification for Cloud Applications (OASIS)	Call 8: ARTIST, CELAR, MODAClouds, Call 10: SeaClouds

Table 1 Most used standards by Call 8 & 10 projects

Furthermore, projects are addressing issues requiring further focus above and beyond the current iteration of ETSI Cloud Standards Coordination report. It is clear that though the focus of these activities has been on the management interfaces that there are a number of different services that need to utilize standardized interfaces, for example accounting, monitoring and service description. The tables below provide the information on the standards used and contributions to the standards landscape.

5.3 Future Internet Assembly 2014

CloudWATCH played an active role in communicating the importance of standards at the Future Internet Assembly 2014 (FIA2014), 17-20 March 2014 in Athens:

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- A presentation and panel discussion as part of a pre-FIA workshop, "From data services to cloud services: concepts, applications and visions', 17 March 2014. This workshop was organised by Broker@Cloud, GloNet, Cloud4SOA, PaaSage, PaaSPort[25].
- CloudWATCH stand with live demos on the EGI Federated Cloud and role of interoperable standards, 18-20 March 2014.

5.3.1 Pre-FIA workshop: CloudWATCH contributions

Presentation by Stephanie Parker, *Trust-IT* on behalf of CloudWATCH, *Why interoperability and standards matter*

- **User story**: Just Eat, a large corporation headquartered in the UK. Drivers for moving to the cloud include: peaky weekend online orders and large global operations with flexibility and agility are top IT priorities, also enabling its engineering team focus on strategic & value-added IT projects (not software patching, fixing servers & IT performance). The company has taken a stepwise approach to the adoption of cloud computing, from basic services (Google) to beta production for smaller, non-critical applications and finally roll-out of its UK operations (its most lucrative) (AWS). In order to overcome concerns about the lack of standards and interoperability, the company has built the architecture in such a way as to enable it to change its current provider if a new and better solution is found any time in the future. This use case shows that moving to the cloud is ultimately a business decision so thinking strategically is important.
- **Important consumer needs** (Source: GigaOM Consumer survey 2013). The survey results highlight increasing consumer needs which need to become best practices on the part of cloud service providers.
  - Consumers concerns that might hurt the vendor include lack of control, lack of standards, lack of integration, and lack of return on investment (RoI) on total cost of ownership (TCO).
  - Consumers want "pain relief" and freedom in the cloud. They are increasingly demanding monitoring, management and transparency; interoperability and portability; integration, open APIs and open source; business cases and proof.
  - The Cloud Industry Forum has highlighted the following issues that might prevent or slow down adoption: provider language is complex and/or misleading. Hybrid IT environments which are forming organically are making interoperability and portability more important.
- **Standards and innovation**
  - The Standardisation Handbook says «*Standards are one of the most important means to bring new technologies to market. Standards provide a bridge connecting research to industry*».

[25] http://www.fi-athens.eu/program/workshops/data-services-cloud-services-concepts-applications-and-visions.

- The SIENA Roadmap (June 2012), where Neelie Kroes, Vice President of the European Commission, underscores the importance of standards and interoperability for the Digital Agenda for Europe: "*I invite all stakeholders to use it as a reference*". Mario Campolargo, Director of Net Futures, DG CONNECT, *"The SIENA Roadmap demonstrates that Europe has a huge potential for innovation".*

- **CloudWATCH on interoperability and standards**:
  - *Europe* has over a decade of standards development and implementation through R&D for distributed computing infrastructures.
  - CloudWATCH is leveraging considerable expertise in standards development, implementation and testing over the past decade. It is also playing a key role in shaping standards roadmaps for cloud computing.
  - CloudWATCH will provide a portfolio of European and international use cases covering technical requirements, policy and legal requirements, including Service Level Agreement (SLA) management.
  - CloudWATCH will develop common standard profiles and testing around federation of cloud services. This is important because a profile on a standard clarifies in an autonomous way how a standard has to be integrated and implemented based on a specific use case. This overcomes ambiguities in specifications and the lack of real interoperability across different interfaces.
  - Promotion of the online survey and provide information on use cases
- **CloudWATCH standards profiles and compliance:**
  - Cloud profile portfolio strategy: technical interfaces; procedural practices; compliance and assessment and business relationships.
  - Working with standards groups to charter a Working Group and get traction with implementers and users.
  - Deploy implementations in test beds.

5.3.2 The CloudWATCH stand and demos

Provided by Stephanie Parker (Trust-IT), Salvatore Pinto (EGI), and Guiseppe La Rocca (INFN).

- **Standards-based Interoperable Cloud Using the EGI Federated Cloud – HelixNebula Use Case, Salvatore Pinto, EGI.eu.**

  Target audiences: Anyone interested in cloud federation, open standards and innovative technologies for IT service deployment.

  The EGI Federated Cloud is based on open standards, which enables interoperability not only between the cloud providers of the federation, but also with external providers. This demo showed how it is possible to leverage the adoption of standards to interoperate academic and

commercial cloud resources. One of the aims is to ensure availability even if providers change over time.

The demo repeated the European Space Agency Proof of Concept of the Helix Nebula initiative, using SlipStream, showing how users are able to see all the EGI Federated Cloud resources under the same hood, enabling them to provision reliably across them all, improving resource sharing and utilisation. The demo also showed how you can easily start a complex deployment on the cloud using broker capabilities.

Another demo feature was the EGI Federated Cloud appliances marketplace and other EGI cloud services, all based on open standards and open source implementation.

- **Exploiting the EGI Fed Cloud and the CHAIN-REDS Cloud Testbed with the Catania Science Gateway Framework – Use Case, Guiseppe La Rocca, INFN.**

  This demo, jointly presented by the CHAIN-REDS[26] and EGI-InSpire[27] projects, focused on demonstrating interoperability across different distributed computing infrastructures, including Clouds, using OCCI and SAGA as standard interfaces and the CHAIN-REDS Science Gateway[28] as a virtual research environment.

  This work builds on the experiences of the EGI Federated Cloud Task Force, with the aim of extending the vision to other regions of the world through the CHAIN-REDS project.

  The demo showed how:

  - A researcher can seamlessly run applications on HPC machines, Grids and Clouds.
  - The cloud-tenant of a real or virtual organisation can seamlessly and easily manage Cloud resources pledged by providers owning/operating infrastructures based on different middleware stacks.

Two use cases address these goals.:

1. How a user can sign in on the CHAIN-REDS Science Gateway using his/her federated credentials, select an application from a menu and transparently execute it on HPC machines,

[26] www.chain-project.eu.
[27] www.egi.eu/about/egi-inspire/index.html.
[28] http://science-gateway.chain-project.eu.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

Grids or Clouds. The fractions of executions on the three different platforms can be adjusted to simulate the need to "boost" resources during temporary peaks of activity.

2. Cloud-tenant: how the cloud-tenant of a real or virtual organisation can sign in on the CHAIN-REDS Science Gateway using his/her federated credentials, select virtual machine(s) from a geographically shared repository and deploy/move/copy it/them across the multi-Cloud he/she is entitled to use. The graphic user interface will be very intuitive including "point & click" and "drag & drop functionalities". The virtual machine(s) belong to the same domain name (chain-project.eu in the particular case) independently of the site where it/they are instantiated and of the underlying Cloud middleware stack.

6 Next steps

- As already explained, the identification of application domains where standard profiles are needed critically depends on the analysis of these application domains. Therefore, strong interworking with WP2 is needed.
- WP2 concentrates on the collection of use cases from three different sectors, namely, the academic, public, and industry sector. Due to the support target group of the CloudWATCH project, namely EC funded projects from FP7, most of these use cases are from the academic sector. Additional efforts have been initiated to collect use cases from the other two sectors too.
- Application domain analysis and use cases analysis are – contrary to the "water fall approach" used for presentation purposes in this report – interleaving activities. Hence, application domain analysis has to be performed in cooperation with WP2 (WP2 and WP4 overlap with regard to key partners).
- The next step will therefore be the selection and analysis of one or several suitable application areas with subsequent activities towards the definition of standards profiles.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

References

IPL Imperial College London. (September, 2007). "Project Stakeholder Analysis." from www3.imperial.ac.uk.

ETSI13 Cloud Standards Coordination, Final Report, November 2013, avail at http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

D2.1 CloudWATCH Deliverable D2.1: Reference Model Framework Report

D2.2 CloudWATCH Deliverable D2.2: Use Case Report

CSC10 Cameron, B.G., T. Seher, E.F. Crawley (2010). "Goals for space exploration based on stakeholder network value considerations." in: Acta Astronautica, doi:10.1016/j.actaastro.2010.11.003.

NIST13 NIST; “NIST-SP 500-291, Version 2, NIST Cloud Computing Standards Roadmap”, National Institute for Standards and Technology (NIST), July 2013