Think Cloud Services for Government,
Business & Research

D3.6 Security and Interoperability Standards Status Report

This deliverable reports on the status of the security and interoperability standards analysed in Task 3.1. It includes a list of standards in use in related FP7 and H2020 projects; identified standardisation gaps; and a list of recommended priorities for new standardisation efforts.

Furthermore, it describes the level of adoption of the used standards and the most common implementations. Identifies contributions to existing and developing standards from on-going FP7 and H2020 projects and provides evidence to the standardisation community of identified gaps by analysing input from ongoing FP7 and H2020 projects, as well as completed projects.

CloudWATCH Mission

CloudWATCH2 takes a pragmatic approach to market uptake and sustainable competitiveness for wider uptake and commercial exploitation. It provides a set of services to help European R&I initiatives capture the value proposition and business case as key to boosting the European economy.

CloudWATCH2 services include:

- A cloud market structure roadmap with transparent pricing to enable R&I projects to chart exploitation paths in ways they had not previously considered, or help them avoid approaches that would not have been successful
- Mapping the EU cloud ecosystem of products, services and solutions emerging from EU R&I projects. Identifying software champions and best practices in mitigating risks associated with open source projects, and ultimately, enable faster time-to-value and commercialisation
- Impact meetings for clustering and convergence on common themes and challenges. Re-use of technologies will also be of paramount importance
- Promoting trusted & secure services through roadshows and deep dive training sessions. Giving R&I initiatives a route to users at major conferences or in local ICT clusters
- A portfolio of standards for interoperability and security that can facilitate the realisation of an ecosystem of interoperable services for Europe
- Cloud interoperability testing in an international developer-oriented and hands-on environment. Findings will be transferred into guidance documents and standards
- Risk management and legal guides to the cloud for private and public organisations to lower barriers and ensure a trusted European cloud market

Disclaimer

CloudWATCH2 (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 Horizon 2020.

The information, views and suggestions set out in this publication are those of the CloudWATCH2 Consortium and of its pool of international experts and cannot be considered to reflect the views of the European Commission.

Document Information Summary

Document title:	D3.6 Security and Interoperability Standards Status Report
Main Author(s):	Marina Bregkou (CSA)
Contributing author(s):	Damir Savanovic (CSA)
Reviewer(s):	Nicola Franchetto (ICTLC), Nicholas Ferguson (Trust-IT)
Target audiences:	Public Administration, SMEs, Policy Makers, Standardisation Bodies
Keywords:	Cloud security, Interoperability, Privacy by Design, Security by Design, Gaps in Standards
Deliverable nature:	Report
Dissemination level: (Confidentiality)	Public
Contractual delivery date:	February 2017
Actual delivery date:	September 2017
Version:	vFinal
Reference to related publications	D3.3 Cloud Interoperability Plugfests Outcome Report D4.3 Roadmap to a cloud market structure encouraging transparent cloud pricing – Final iteration

Executive Summary

The benefits of cloud computing are clear: faster implementation of services, greater accessibility to computing resources, added functionality and more at cost savings. Yet these advantages can create incompatibility among vendors' services and internal applications requiring customer to lock-in with specific cloud services reducing the benefits of moving to the cloud. Standardization efforts and initiatives to prevent lock-in and security analyse and champion standards for interoperability and security.

Achieving this objective results in a better understanding of the fast-evolving standards landscape. Specifically, it uses data collected through project interaction to identify the most commonly implemented standards in the market and in the context of European projects on cloud, software and services. The focus being on interoperability and security. This helps identify which extensions, refinements, and gaps should be addressed. Testing is a key stage in the adoption and development of standards and therefore important in the vision of creating an ecosystem of interoperable services for Europe.

Table of Contents

1 Introduction

CloudWATCH2 focuses on the cloud ecosystem emerging from European research and innovation projects, where technology and pricing are both an equally important part of market equation. It takes a pragmatic approach to market uptake and sustainable competitiveness by clustering projects around common themes and challenges, with deep dive training for wider uptake and commercial exploitation. According to the CloudWATCH2 Cloud Market Roadmap (D4.3)[1], standards and interoperability is one of the areas in which the cloud computing market has not yet caught up with the more mature commodity markets such as the electricity market. Having a clear market structure is vital for any market to mature. Diversification of a market is a key step towards this and frictionless interoperability between different cloud providers is an important step forward, allowing competitors to enter the market. A key recommendation of the Cloud Market Roadmap is that the EC continue to fund interoperability projects, and that the uptake of standards should be encouraged where commonality brings economic advantage through increased sharing and competition.

One of the primary objectives of the CloudWATCH2 project is to analyse and champion standards for interoperability and security, by monitoring the fast-evolving standards landscape, new implementations, extensions and protocols with a focus on the value creation of interoperable and secure services, identifying gaps and making recommendations to address them. This report identifies the most commonly implemented interoperability and security standards in the market in the context of European projects on cloud, software and services. The objective is to understand the value created from standards implementation for interoperability and security.

According to the ETSI Cloud Standards Coordination (CSC) Final Report, the standards landscape is a lot less fragmented than previously described and that it allows for extensions and emerging standards to fill gaps identified.

CloudWATCH2 analyses the status of this landscape post 2015. This assessment can be linked back to consumers' concerns and the level of choice and freedom afforded to them.

The **updated standards portfolio** in the "**Standards Hub**"[2] serves as a reference point on the standards implementation status, the level of adoption, offering a detailed account of the most commonly used standards and the unique selling points for projects adopting them, highlighting gaps and recommendations. This deliverable can be used as a reference for the existing standardization efforts and also analysis of research projects.

[1] D4.3 Roadmap to a cloud market structure encouraging transparent cloud pricing – Final iteration. Available: http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Roadmap-to-a-cloud-market-structure-encouraging-transparent-cloud-pricing_vFinal.pdf

[2] http://www.cloudwatchhub.eu/standards-hub

To further support the interoperability and security standards findings, this deliverable refers to three **Cloud Interoperability Plugfests Report (cf. D3.3) CloudWATCH2** organized and which enabled research and innovation projects to identify and compare the implementation of standards.

1.1 Scope of the document

This document provides a monitoring of the standards landscape, identifying necessary extensions and profiles, and identifying relevant standards groups for future engagement of the EU projects.

Through this deliverable CloudWATCH2 is able to:

- Leverage input provided by finalized and on-going FP7 and H2020 projects to prepare and maintain a list of standards used by the different consortia. The list describes the level of adoption of each standard and the most common implementations.
- Identify contributions to existing and developing standards from the FP7 and H2020 projects.
- Provide evidence to the standardization community of identified gaps by analysing input from the above mentioned FP7 and H2020 projects.

1.2 Objectives and Target Audience

This document provides an insight on the current use of standards for interoperability and security, and provides an updated portfolio of standards, implementations, extensions and recommendations of how gaps identified can be addressed.

The audience for this deliverable on Security and Interoperability Standards Status Report includes:

- Standard development organizations which can refer to the document and help improve Quality of Service.
- Cloud service customers, in particular European research and innovation projects who report on whether they use standards appropriately or even bring their own contributions to address specific challenges.
- All sizes of cloud service providers who can use the document to promote standards for interoperability and security, including potential for market expansion and business opportunities for both consumers and providers.
- Policy makers who should be able to use it to understand and identify the areas that lack in standardization and specifications and that they may wish to extend policies in order to better satisfy the cloud customers' needs.

1.3 Structure of this document

The rest of this document is structured in the following manner:

- Section 2 focuses on the status of the Security and Interoperability standards by presenting an analysis of the gaps identified by the EU projects but also of the areas that lack yet in standards for the work that is required.
- Section 3 provides a list of recommended priorities for new standardization efforts.
- Section 4 concludes this report.

2 Status of the Security and Interoperability Standards

Focusing on an essential element of the European cloud marketplace development and its long-term sustainability which is the interoperability of services, as well as recognising the emphasis given on how interoperable services and open source help creating value in the marketplace, D3.6 aims to monitor the standards landscape and to identify necessary extensions and profiles.

Following the work done by the Cloud Standards Coordination initiative led by ETSI, on the mapping of the standards required to support a series of policy objectives defined by the European Commission, CloudWATCH2 aims to report on what the status and maturity of these standards is in 2017. Furthermore, we want to identify the existing gaps if any, and what is the adoption range by the European projects of the security and interoperability standards presented in the ETSI CSC-1 and CSC-2 reports in 2015.

For this purpose, we created a questionnaire that was disseminated to FP7 and H2020 projects. In section 2.1 we describe the approach followed and then present the results from the questionnaire findings, along with the identified gaps. Validation of the identified gaps and lacks in standardization, are presented in section 2.4 as a next step to the analysis of the data gathered.

2.1 Approach

The objective of this activity is to focus on monitoring in order to produce an updated version of the standards maturity level of the Cloud Computing standardization landscape in 2017.

The scope is to identify the most commonly used standards in the market in the context of EC funded projects (with a main focus on interoperability and security). In order to achieve its objective, CloudWATCH2 developed a questionnaire (cf. Appendix A.) in order to map the use of standards by European FP7 and H2020.

We contacted FP7 and H2020 projects in DG Connect’s Unit E2 Cloud and Software Services and requested them to complete the questionnaire. The questionnaire was accompanied by a document including all relevant standards from the ETSI CSC1 and CSC2 report[3], which respondents could consult in order to identify extensions, refinement and gaps that need addressing, supporting relevant activities of the EC on standards as a follow-up of the ETSI Cloud Standards Coordination Task Force.

Based on the answers collected from 30 different FP7 and H2020 projects, we describe below the findings and all identified gaps where standards are lacking.

2.2 Use of standards and implementation use cases

The main objectives of the activity undertaken were to identify:

- gaps in existing standards;
- the most commonly leveraged standards by the projects' use cases/pilots/demonstrators;
- additional needs in the existing standards landscape;
- Which standards the projects are contributing to;
- Which standards projects would like to contribute to;
- the areas that are lacking in standardization;
- standards that the projects are refraining from implementing;

30 European projects (see Appendix B.) responded to the questionnaire distributed and from the data gathered the main result is that projects, finished and on-going, mainly focus on interoperability standards while security and privacy is still an afterthought. The projects were asked to describe their use cases, pilots or demonstrators that leverage standards and these cases mainly worked on interoperability of services with a focus of security, mainly on user authentication level in the service front end. Few projects reported that they intended to work on designing and developing security and privacy-preserving protocols for their projects' needs.

Such use cases involve monitoring the SLAs of their cloud based services, scalable hosting, testing and automation for other organizations, high availability in eHealth, telco infrastructures, transport and media, network functions virtualization (NFV) use cases, IoT, eLearning, etc.

The most used standards projects report using during their lifecycle are:

- OASIS TOSCA
- OAUTH2
- ITU-T standards
- DMTF standards
- ISO 19941, 19944,
- ETSI13

[3] ETSI CSC1 and CSC2 available: http://csc.etsi.org/

- OGF1,2 and C-SIG code of conduct

It appears that the majority of the European projects whose data was collected mainly work with standards on how to move data or applications from one service to another and mainly make use of the standards or specifications that support portability for cross-Cloud scenarios in general.

Regarding security, the standards that are usually consulted were reported to be:

- ISO 27001, 27002, 27018, 19086
- NIST 800-144
- EC Directive 95/46/EC and GDPR
- Advanced Encryption Standards (AES), IEEE

From the above, the most commonly leveraged standards by the projects' use cases, pilots or demonstrators are: OASIS TOSCA, IETF OAUTH2, ISO12, TMF standards and OCCI standards.

The European projects require functionalities that are not yet covered in any of the existing standards. When asked about ongoing work on standards, European projects revealed that through their work and use cases, they are contributing and leveraging standards that they can extend to their needs. Such standards are reported to be:

- OCP and Docker environment
- OASIS TOSCA, CAMP, XACML
- ISO 19086 1 and 2
- OGF standards
- ETSI SR 003 931, CAMEL
- ITU-T Y.CCTIC, Y.CCICTM, Y.CCICDM
- GS NFV-MAN 001, NFV-SWA 00, NFV-SEC 002, NFV-TST002
- IETF WG SFC Draft
- OCCI standards

The most common way of contributing to standards is through a partner with a liaison e.g. SLA-Ready. Although less common, there are also projects which have requested a liaison (e.g. SLALOM) or made a direct individual contribution. The SLA-Ready project used the liaison that CSA had with ISO. Contributions from SLA-Ready to ISO 19086 were therefore made by CSA on behalf of the project. This reduced the bureaucratic burden of setting up a liaison through the project, thus saving valuable effort. In addition, CSA was able to follow up these contributions beyond the project lifetime.

2.3 Gaps in standards

As mentioned before, many standards are not fit to be used by the requirements for ongoing European projects. Previous work done in CloudWATCH2, Deliverable 3.3 [4] (Cloud

[4] D3.3 Cloud Interoperability Plugfests Outcome Report, available at: http://www.cloudwatchhub.eu/cloudwatch2-cloud-interoperability-plugfests-outcome-report

Interoperability Plugfest Report), produced an Outcome Report on Cloud Interoperability Plugfests, also identified issues related to the gaps in the clouds standards landscape. In particular, data protection and security appear to be more of an afterthought in service design and implementation, despite security being an essential element of a sustainable European cloud marketplace in the wider context of the Digital Single Market. [1]

When asked about any functionalities that the European projects require in their work they reported that the following are not yet covered by the existing standards in scope:

- Standards related to containers (e.g. OCP)
- Specific node types for OASIS TOSCA (e.g. one project reported thinking about extending TOSCA in order to be able to support containers)
- Extensions of ETSI CAMEL
- Lack of standard requirements for inter-cloud data management, architecture and components.
- Harmonization among the ETSI NFV standards and the OASIS TOSCA NFV-related activities
- Automatic deployment and configuration of the secure federated infrastructure require trust bootstrapping protocol as application of IETF ABFAB architecture and Trusted Computing Group Architecture.
- Extending TMF ZOOM (Zero Touch Operation, Orchestration and Management) architecture and model to ZTPOM (Zero Touch Provisioning, Operation and Management)
- OASIS Virtual I/O Device (VIRTIO) TC to extend to the standard of HPC interconnect and virtualization for the Cloud.
- ISO 19086, has taken a step forward in the definition of SLA metrics, but they are still defined differently (in terms of formulas) by the CSPs, which makes the comparison difficult.

In addition, projects identified that their contributions to standards would be facilitated if there were:

- Simple international rules for ethics and data protection that are understandable by engineers
- Better efficiency especially in cloud computing scenarios (IETF)

As referenced earlier, D3.3 also makes a call to action for the existing need of the continuous improvement of standards. This is further developed below in the Section 3, Recommendations.

2.3.1 Lack of standards related to the work of projects

It is worth noting that, apart from specific functionalities that were found not to be covered by the standards in scope, European projects have also identified a lack of standardisation in different areas that are relevant to their work. Such areas would be:

- Payment and rewarding mechanisms (incl. international law).
- Intercloud/Multi-cloud, data portability
- Cloud Automation
- Data Protection and Security by design
- Context-aware access control modelling and enforcement
- Security of trusted inter-cloud environments
- Reputation in inter-cloud environments.
- SLA languages
- Ability to capture simultaneously the energy, cost and performance goals of applications.

The survey findings demonstrate that there is still a lack of standards or specifications in support of portability for cross-Cloud scenarios in general as there are unclear capabilities of individual cloud service offerings ability to move data or applications from one service to another [2]. Furthermore, results show that key areas which are often cited as barriers to cloud adoption, such as security and data protection, are still significantly lacking in standardisation.

2.3.2 Additional Standards not included in ETSI report:

It is interesting to note that EU projects are considering additional standards which were not included in the ETSI CSC 1 and CSC2 report. Such would be:

- OCP / Docker, OpenStack
- OMG Marte
- OASIS SAML2.0, VIRTIO, XACML
- DIN SPEC 91337
- ISO/IEC 15480, 25010:2011
- IETF ABFAB standards/RFCs
- ETSI VNF Draft, ES 203 237
- Open Service Broker
- OWASP ASVS
- Several legal requirements:
    - Council of Europe 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (‘Convention 108’)
    - Directive 2013/40/EU on attacks against information systems
    - Directive 2014/41/EC on the European Investigation Order in criminal matters
    - Privacy Shield Agreement
    - ePrivacy Directive 2002/58/EC

2.3.3 Standards that refrain projects from use

When considering the use of standards (after the definition of the project’s requirement and the analysis of the existing standards) many European projects, not only identified gaps and lacks in standardisation, but they also reported that they refrain from using some of them.

One of the main reasons for this would be the lack of dynamism from certain standards and the effort needed to work on their extension. Projects consider it to be a risk that they are not ready to take because of the time and money required.

For instance, several projects considered implementing several ISO standards such as 27001, 27002 and 27017 but decided against it as these standards primarily deal with processes. The reason for this could be either because the nature of the project makes the process based standards unfit for use, or the maturity of projects is too low to have a process based Plan-Do-Check-Act (PDCA) approach to security. Other examples include not implementing OASIS TOSCA, CAMP due to the effort required.

Instead of spending time and money they might have in standards that are partially helpful to the design of the project's needs, projects preferred using other industry standards that are more appropriate.

2.4 Validation of results

2.4.1 Methodology

Once the data gathered had been analysed, we then carried out a validation exercise of the results with representatives from EU projects and from industry. This was done in order to see how these projects that had identified the gaps and lacks in standards were coping with them. Furthermore, our intention was to identify any potential steps the projects or the industry have been taking to mitigate these obstacles.

This validation exercise was carried out in two steps. Firstly, through a cluster workshop for the Data Protection Security and Privacy cluster (DPSP) at NetFutures 2017 in Brussels (attended by representatives of new European projects and a European-Brazilian partnership). Secondly, through an email validation exercise to 10 more industry experts.

In both cases, we presented the findings of the survey. Namely, the most used standards, the gaps identified, and the lacking standardization. Based on the findings, we then posed a set of questions to find out whether:

- The respondents had identified any additional gaps or another group of gaps in the existing standards;
- these gaps are being addressed in any way by their projects;
- they have been undertaking any activity to address the gaps in standards from the identified areas and if not, what would they do to address them;
- their projects have been contributing in any way in the creation of standards in the identified areas regarding lack of standards;
- the respondents were contributing to the standards area in general;
- they would refrain from using a standard.

2.4.2 Results

All respondents agreed on the identified gaps and stated that they had not been taking any actions to address the gaps in any way in the context of their respective projects. The main reason cited for this was a lack of time, effort and money, and that it is not part of the scope of their respective project's focus. In the case of few European projects, they are seeking for their own solution to overcome the gaps.

Regarding contributing to the standards landscape in general, their primary focus is on the adoption of current standards that fully serve their projects in order to facilitate the uptake of their project's results by the software industry. Any possible contribution to standards is left to take place near or after the project's finalization. One respondent stated that their project however is voting in the standardization committees (e.g. TOSCA) and are trying to influence them for the aspects concerning their projects, namely the deployment of big data frameworks.

Indeed, all respondents agreed that the timeframe of standards is not compatible with that of a typical European project which has a limited lifetime with an established start and end date. This contrasts with the longer timeline of the typical standardization process which is much longer. By the time a European project has finalised its work and is in position to contribute to a new standard, there are no more funds or effort left to continue with this procedure.

In order to allow European projects to have an impact on standards, both the cluster projects and the contacted experts agree that the most probable way for doing so, could be to offer to mature/terminated projects some funding exclusively dedicated to standardization. That would actively contribute to standardization initiatives and help leveraging the level of adoption.

Indeed, in January 2018, a new project will commence to address this very point. StandICT.eu (Supporting European Experts Presence in International Standardisation Activities in ICT). Coordinated by Trust-IT, StandICT.eu defines a pragmatic approach to reinforcing EU expert presence in international ICT standardisation. By setting up, managing & monitoring a continuous open call, StandICT.eu will provide a streamlined process supporting the participation & contribution of European specialists in SDOs & SSOs in the 5 essential building blocks of the Digital Single Market (DSM), viz.: cloud computing, 5G communications, IoT, cybersecurity & data technologies.

Through a Standards Watch, StandICT.eu will map and monitor the international ICT standards landscape and then liaise with SDOs, SSOs & industry-led groups, in order to identify gaps & priorities which match EU DSM objectives: These will become topics for the continuous open call over a two-year period.

Findings from this report (i.e. D3.6), in particular regarding standardisation gaps will feed into the StandICT.eu mapping exercise. In addition, findings regarding the timing of project contributions to SDOs will also be of value in identifying experts who can apply for the open calls. Finally, UOXF will also be represented on the Expert Advisory Group on the topic of cloud computing. This will ensure impact of CloudWATCH2 results beyond the project's lifetime.

3 Recommendations

In section 2 we identified the most commonly used standards in the market in the context of EC funded projects (with a main focus on interoperability and security).

We also identified extensions, refinement and gaps that need addressing, which can be used to support relevant activities of the EC on standards as a follow-up of the ETSI Cloud Standards Coordination Task Force.

Gaps identified in the present document (cf. Section 2.3) may need further analysis to identify the relevance of each gap, e.g. which gaps are blocking the adoption and use of standards, and need to be addressed with priority.

The main takeaway from the survey conducted and the 30 European projects consulted is that European projects still mainly focus on interoperability standards which are supported by the Pilots/demonstrators/use cases they are developing too, while in too many cases unfortunately, data protection and security are an afterthought in the design process of the project.

In order to have a better adoption of Cloud standards, the identified gaps and lack in standardization need to be addressed by outstanding standards and specifications that should address current concerns.

Therefore, the CloudWATCH2 has the following recommendations to make:

- **Further analysis is needed to decide whether intervention by the EC is needed to organize the effort to close the gaps identified** or the respective communities/projects will take care of and/or the market will drive the effort for closing the gaps. Although, let it be noted that many projects admitted to not be undertaking any additional acts to report or contribute in any way to these gaps. They admitted that their solution in these cases, if they do not already have a partner with a liaison to SDOs, is often to not engage any further in the matter and refrain from implementing those standards.
- **Addressing the lack of standardization in specific above mentioned areas of the cloud landscape** (i.e. Inter-Cloud). This appears to be critical as clouds could not interact without exploiting some specific standard. This could be carried out by the EC cluster on Inter-cloud Challenges, Expectations and Issues.
- **Allowing and increasing the impact of European projects on standards.** Support mature/finalized research projects with additional exclusive time and funds, when they have identified and are able to contribute to extensions of existing standards and/or the creation of new standards. Another solution would be to suggest a standardisation task in future projects, that would be responsible for developing the strategy to orchestrate the project's contributions to relevant standards and best practices from its very beginning.

- **The EC needs to** support such activities to address these gaps, and **help projects working with standards groups** to establish new standards or further developing the already existing ones. Through initiatives such as StandICT.eu European experts do now have the opportunity to contribute to the standardisation process through continuous open calls and dedicated funding.
- **The EC needs to promote and encourage all cloud market participants for optimal standardization.** As argued in CloudWATCH2 Roadmap to a Cloud Market Structure (D4.3), if there is a flaw/gap in a standard that has been adopted, then it presents a single point of failure. In order to avoid this and have standards that also facilitate innovation there need to exist at least 2 standards that are available for adoption, in order to diversify this risk.[3]

4 Conclusions

As presented in section 2.3, the findings from the survey to 30 European projects show that they are still focusing in interoperability more rather than privacy and security which remain an afterthought. The main gaps show lack of standards related to containers (OCP), standards for Intercloud/Multi-cloud environments and security and privacy by design.

This demonstrates that there is still work to be done to fully address the cloud users' main concerns and those of the EC which in previous tender has asked European projects to consider the security by design principle from the early stages of the projects[5].

Not just interoperability but security and data protection by design would increase the maturity level of organizations and leverage their work. Security by design would increase the maturity of the output and not only the technical aspects of the projects.

There already exist some widely-recognized security frameworks which are mentioned in the survey's results also such as CSA's Open Certification Framework (OCF), the Cloud Controls Matrix (CCM), ENISA's Cloud Certification Scheme Metaframework (CCSM)[6], and NIS directive (if relevant to EU projects), ISO27001/2, ISO 27017 and ISO 27018. This deliverable can serve also as a call upon experts in SDOs & SSOs to address the gaps identified by 30 European projects.

While gaps exist in many standards, work is progressing to address these gaps. One particular gap regarding data protection, could be addressed by using CSA's PLA v3. Code of Conduct.

CSA recognizes that no single certification, regulation or other compliance regime will supplant all others in governing the future of IT as well as the risk of adding more cost and complexity

[5] https://etendering.ted.europa.eu/document/document-file-download.html?docFileId=7469

[6] https://www.enisa.europa.eu/news/enisa-news/enisa-cloud-certification-schemes-metaframework/

to the already overloaded compliance landscape. While ISO standards have potential for being globally accepted, there are significant questions as to the future of 27017/8 versus 27001/2.

With the aim to harmonize and simplify provider certifications, CSA has developed the CSA OCF as an industry initiative to allow global, accredited, trusted certification of cloud providers that provides:

- A path to address compliance concerns with trusted, global best practices regardless of the region. For example, CSA expects governments to be heavy adopters of the CSA OCF to layer their own unique requirements on top of the franewirj and provide agile certification of public sector cloud usage.
- An explicit guidance for providers on how to use the framework for multiple certification efforts. For example, scoping documentation will articulate the means by which a provider may follow an ISO/IEC 27001 certification path that incorporates the CSA CCM.
- A "recognition scheme" that would allow CSA to support ISO, AICPA and potentially others that incorporate CSA IP inside of their certifications/framework.

Although compliance with privacy and data protection law could be a challenge for organizations as GDPR imposes a high legal standard for privacy and data protection, the Cloud Security Alliance is developing the Privacy Level Agreement (PLA) V3, a compliance tool that reflects the new obligations set forth by the GDPR. Current PLA [V2] was based on actual, mandatory EU personal data protection legal requirements (Directive 95/46/EC and its implementations in the EU Member States), and could be used as an EU compliance tool. The upcoming version of PLA [V3] will be updated as required on the basis of the development of relevant legislation, opinions, guidelines and recommendations from competent authorities.

PLA [V3] will thus be designed to meet both actual, mandatory EU legal personal data protection requirements (i.e., Directive 95/46/EC and its implementations in the EU Member States), by leveraging the PLA [V2] structure, and the forthcoming requirements of the GDPR. This specific feature will make PLA [V3] a unique tool that helps CSPs, cloud customers and potential customers manage the transition from the old to the new EU data protection regime, and contribute to the proper application of the GDPR into the cloud sector.

Finally, the lengthy procedure of contributing or developing new standards, unfortunately doesn’t follow the timeframe of a European project or the fast birth of new needs for standardization. There is the need for additional time and funding that would accelerate the process of contributing and developing to the certification schemes that would significantly increase the adoption of standards in cloud computing and that would address and mitigate the concerns related to data protection and security by design. The STANDICT.eu project will address this challenge by providing open calls and the opportunity for European standards experts to contribute to standardisation in not only cloud computing but also, cybersecurity, 5G, Big Data and IoT.

Appendix A.

This appendix presents the questionnaire distributed to the various FP7 and H2020 projects for the purposes of monitoring the standards landscape in Europe.

CloudWATCH2 is a complementary and lean Consortium of experts from TRUST-IT, Cloud Security Alliance, Oxford eResearch Centre, University of Oxford, Strategic Blue and ICT Legal Consulting.

CloudWATCH2 aims to analyse the status of standardisation efforts post 2015, leveraging the conclusions from ETSI Cloud Standards Coordination Phase 1 and Phase 2 reports. The project will assess the extent to which cloud standards ensure greater flexibility, offer cloud providers a unique selling point and impact on wider implementation within both EU research and a more general context. The results of this survey will be used to create the "Standards Hub" on www.cloudwatchhub.eu and will serve as a reference point on standards implementation status, their level of adoption, a detailed account of the most commonly used standards and the unique selling points for projects adopting them.

CloudWATCH2 focuses to report on status of the Security and Interoperability Standards which will include:

list of standards in use in surveyed FP7 and H2020 projects

most common standard implementation use cases

gaps in standards

list of recommended priorities for new standardization efforts

We have prepared a list of relevant standards, and in order to achieve our goals we are kindly asking you to answer the following questions on behalf of the EU project you represent:

1-Up to this point, which standards are being leveraged within your project (please consult the attached list of standards)?

1a-Based on your answer to (1), which are the pilots/demonstrators/use cases that leverage those standards in your project?

2-Are there any functionalities that are not yet covered by these standards but you do require in your project?

3a- Based on your answer to (2), to which standards have you/would you like to contribute some of the advances identified in your research?

3b-Based on your answer to (2), have you/would you contribute to standards:

Through a partner with a liaison

Through a liaison requested by the project

Other (Please specify):

4-Have you identified a lack of standards in an area relevant to your work?

Yes (Please specify):

No

5-Were there any standards you considered implementing but refrained from doing so? If yes, please specify why.

6-Which standards not included in the list (cf., attachment) are being considered?

Demographic information

Name of the respondent:

Project being represented (name, funding scheme, FP7/H2020, start/end dates, URL):

Contact e-mail of the respondent:

References

[1] CloudWATCH2. (2017). D3.3 Cloud Interoperability Plugfests Outcome Report. Available: http://www.cloudwatchhub.eu/sites/default/files/CloudWATYCH2 Cloud Interoperability Plugfests Outcome Report_vFinal.pdf

[2] ETSI SR 003 392 V2.1.1 (2016-02). Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards

[3] CloudWATCH2. (2017). D4.3 Roadmap to a cloud market structure encouraging transparent cloud pricing – Final iteration. Available: http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Roadmap-to-a-cloud-market-structure-encouraging-transparent-cloud-pricing_vFinal.pdf