D3.3 Cloud Interoperability Plugfests Outcome Report

Think Cloud Services for Government, Business & Research

www.cloudwatchhub.eu|info@cloudwatchhub.eu |@cloudwatchhub

This deliverable accounts for the results and impact of Cloud Interoperability Plugfests conducted under the auspices of the CloudWATCH2 project. Based on the results of the plugfests, the report outlines a series of considerations and actions regarding the future of plugfests.

CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

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

Document Information Summary

Document title:	D3.1 Cloud Interoperability Plugfests Outcome Report
Main Author(s):	Michel Drescher (UOXF)
Contributing author(s):	
Reviewer(s):	Nicholas Ferguson, Trust-IT Services, Damir Savanovic, Cloud Security Alliance
Target audiences:	CloudWATCH2 consortium, The Cloud Interoperability Plugfest project, standards development organisations
Keywords:	Cloud interoperability plugfests, interoperability testing, cloud, standards, interoperability, testing, virtual plugfests
Deliverable nature:	Report
Dissemination level: (Confidentiality)	Public
Contractual delivery date:	M16 (31 December 2016)
Actual delivery date:	M16 (31 December 2016)
Version:	vFinal
Reference to related publications	D2.2 Mapping of EU cloud services, solutions technological readiness D3.1 Structure and aspired outcomes of Cloud Interoperability Plugfests D3.2 Structure and Interoperability Status

Executive Summary

Since human interaction has been harmonised more formally in semantics and terminology, adherence to standards as a form of formal harmonisation has been the subject of validation. More recently, this form of validation has been conducted in formal testing including formal recording of outputs and results. The rise of agile and lean service development and operation, has meant that these tests have been developed to be run as less formal events, being called "plugfests", which allow for rapid testing against published standards in an easier manner than previous events of this name.

Similar to software services, standards experience a lifecycle from inception/ideation to obsolescence – for example W3C RFC 2616 defining the HTTP/1.1 protocol[1] formally obsoletes RFC 2068 defining the very same protocol but two years earlier[2] – as well as receiving updates throughout their lifetime.

Although often seen as long-living, if not static, standards live in a dynamic environment driven by needs that are often considered detrimental even to each other: Standards are frequently reported as stifling or even "killing" the scoped market[3]. Operating within this environment, CloudWATCH2 organised and conducted a number of Cloud Interoperability Plugfests with varying outcomes.

This deliverable summarises the outcomes of all organised Cloud Interoperability Plugfests, and derives conclusions on their respective results in form of specific and concrete conjectures regarding current plugfest sustainability as listed below;

1. Active development vs. software maintenance may lead to lower participation.
2. EC project funding inflated event participation
3. Lack of incentives for service providers to implement standards
4. EC projects have an intrinsically different perception of security, or customer requirements in general

CloudWATCH2 will further address some of the conjectures during its remaining lifetime, while leaning on the wider community to take up and address the remaining issues.

[1] https://www.ietf.org/rfc/rfc2616.txt
[2] https://www.ietf.org/rfc/rfc2068.txt
[3] Simply searching the Internet for something similar to "are standards killing the cloud" will provide enough sources for this claim.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

Cloud Plugfests are a long-running activity and are typically events where technology providers mutually test their implementations of standardised specifications for conformance and interoperability in an arena where the test results are private, allowing the testing of upcoming or pre-production products/services.

Plugfests as a concept have existed since the emergence of more formalised standardisation of any type of information that is exchanged within or even across domains: For example, while historic definitions and units of distance are still actively used today – for example, yards, feet and inches – some have gone out of "fashion" and are no longer or rarely used, such as leagues and fathoms. Other definitions are overloaded, and are further qualified, such as a mile, and a nautical mile, which denote different distances.

Other definitions have been harmonised in terminology and semantics, and organised into an interchangeable framework of units. For example, the metric system is based on the definition of "one metre". While many harmonisations are directly based on a natural frame of reference (such as one foot, one stone), the metre represents a synthetic harmonisation (i.e. standardisation); yet the exact length is defined using the laws of physics as, currently, "the length of the path travelled by light in vacuum during a time interval of 1/299 792 458 of a second.[4]

The essence of standardisation is thus:

1. Harmonisation of units is an intrinsic element of human interaction, and happens inevitably.
2. Standardisation can thus be seen as harmonisation across cultural borders, or across historic semantic barriers.
3. Standardised units are frequently synthetic, yet based on natural frames of reference.
4. Standardised units have a lifetime,
5. Standardised units undergo amendments as required by advances in their underlying frame of reference.

If one accepts this as the "axioms of standardisation", then these should be relevant and still impact in modern life, specifically in this context in cloud computing.

In fact, examining the current cloud computing landscape, these observations are still in force:

1. Some semantics of cloud computing have been harmonised into a common understanding – yet some areas are still in flux. The definition of IaaS, PaaS, and SaaS clearly has its roots – its frame of reference – in the classic three-tier architecture of enterprise applications (data/storage, business logic, and user access). Yet, somewhat similar to varying definitions of the length of a foot, or the volume of a pint, diverging "schools of architecture" differently scope infrastructure – dogmas of definition of infrastructure emerge: While many define infrastructure as the trinity of (bit) storage, compute and network, others include databases and other low-level components in the infrastructure.
2. One of the earliest, and to date most cited definition of cloud computing, is the definition published by NIST in September 2011.[5] Still relevant today, this definition aimed at harmonising the terminology across the different "schools of architecture" that existed at that time within a single country. This definition resonated worldwide, and is nowadays almost commonplace.
3. NIST's definition was received as very intuitive and acceptable since its frame of reference bore from the then very actively deployed three-tier enterprise architecture model as described above. Although born and based on physics, ICT itself is not natural, it is entirely artificial. Yet, within this

[4] http://www.bipm.org/en/CGPM/db/17/1/
[5] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

frame of reference or domain, was perceived as a law of nature within that domain – and served itself as a frame of reference for the definition of cloud as published by NIST.

4. Taking NIST's definition of cloud computing as an example, some of its definitions have gained traction in the community, some have not at all, and some are on the rise (only possibly to in future loose traction again). For example, while IaaS and SaaS have gained traction and common understanding early on, the semantics of PaaS are still unclear: Does PaaS include DB services, messaging services, etc. or are these part of the IaaS model, and does PaaS hence describe only application service models similar to the J2EE definition?[6] Likewise, NIST defines "community clouds", but this term has not gained traction at all (at least not in the industry sector), and "hybrid cloud" is only gaining traction and understanding in the last couple of years.
5. Cloud computing is a fast-paced domain of technology, and as such requirements will constantly change, until a universally accepted equilibrium has been achieved – in economical terms, the state of utility (services) or commodity (products) has been reached. Until then, standardised definitions will have to be updated, which is reflected in the versioning identifiers of many published documents such as OCCI 1.1 and 1.2[7], CDMI 1.0, 1.0.1, 1.0.2, 1.1[8] to name but a few.

Predating the publication of NIST's definition of cloud computing, the Cloud Plugfest Initiative[9] (CPI) started its activities as early as April 2011 with the first instance of its Cloud Plugfests.[10] Meanwhile in its 25th event instance, Cloud Plugfests are a recurring and necessary event of harmonisation and standardisation.

CloudWATCH, and also CloudWATCH2, have been longstanding partners of the CPI in the organisation of Cloud Plugfests (see Figure **1**). The community focussing on technical interoperability, particularly the cloud software landscape as is the focus of this report, needs to address the impact these identified factors have on its business. Even though these may not be disruptive, they are certainly exerting significant impact that we as a community must address. CloudWATCH2 supports such testing and will organise three such events combining both physical and remote participation, as outlined in this document.

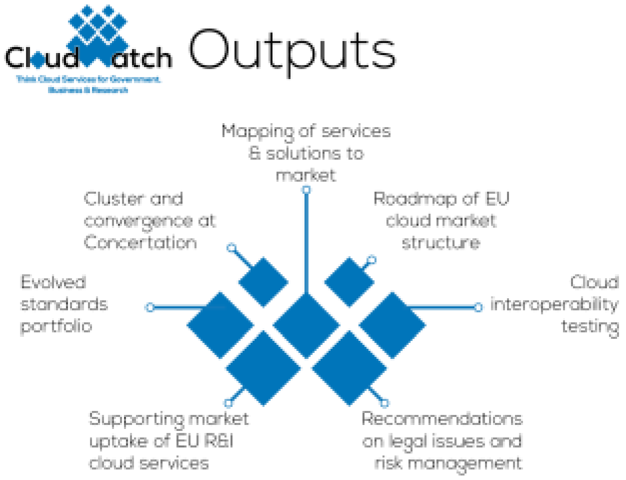
CloudWatch
Think Cloud Services for Government, Business & Research
Outputs
Mapping of services & solutions to market
Cluster and convergence at Concertation
Roadmap of EU cloud market structure
Evolved standards portfolio
Cloud interoperability testing
Supporting market uptake of EU R&I cloud services
Recommendations on legal issues and risk management

Figure 1 CloudWATCH2 Outputs

[6] While there is a widespread presumption in the technical community on hardware virtualisation being the main driver of cloud computing, there is however no indication or requirement to implement virtualisation to achieve cloud computing. Hence, the corollary notion of "VMs for compute, and bit buckets for storage" is an obvious first choice, but nonetheless the only or exclusive architecture of cloud computing.

[7] http://occi-wg.org/about/specification/

[8] http://www.snia.org/cdmi

[9] http://www.cloudplugfest.org/

[10] http://www.cloudplugfest.org/events/past-plugfest-agendas

However, as described in D3.1 ‘Structure and aspired outcomes of Cloud Interoperability Plugfests’ the participation at and frequency of traditional face-to-face plugfests are declining.

This deliverable underpins this observation with the results of face-to-face Cloud Plugfests organised by CloudWATCH2: Section 2 provides formal accounts of the plugfests conducted by CloudWATCH2. Section 3 analyses the outcomes of the plugfests in an attempt to find common patterns of success (or failure). The document concludes with an outline of the next actions for the remainder of the CloudWATCH2 project.

2 Cloud Interoperability Plugfests

2.1 Plugfest 1: Cloud Interoperability Initiative Plugfest

The first plugfest organised within the CloudWATCH2 project was collocated with the Cloudscape 2016 conference on 8-9 March 2016 in Brussels.

This plugfest instance, however, had to be cancelled due to lack of interest and participation. This instance has already been subject to discussion and analysis in conjunction with the Y1 review of the CLoudWATCH2 project and will not be further discussed in this deliverable.

2.2 Plugfest 2: Cloud Interoperability Initiative Plugfest 24

This plugfest was organised and conducted in collaboration with SNIA and their annual Storage Developer Conference 19-21 September 2016 in Santa Clara, CA, US. Due to demand this plugfest featured F2F as well as remote access and testing.

With five organisations represented by six participants across local and remote participation, attendance at this plugfest was small.

Implementations of CDMI and OCCI were tested. However, participants were mostly novices in interoperability testing, which led to significant time in the event being spent mostly on education and introduction to the concept of plugfests and coordinated testing. Therefore, although technical testing did occur, results were not formally recorded due to lack of time.

2.3 Plugfest 3: CloudWATCH2 Cloud Security Plugfest

With traditional cloud plugfests focussing on technical interoperability in machine-to-machine communication use cases, process-level interoperability – or compliance – is often not considered. Particularly, privacy and security are more often 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.[11]

In continuation of the conversations with stakeholders at events such as the Cloud Security deep dive event held at Cloudscape 2016 in Brussels[12] one question naturally emerges: How interoperable – that is, equivalent – are cloud services regarding process-level standards? While technical interoperability on the service integration level allows smooth transition from one provider to another, from a service consumer’s point of view both providers (the former and the current) ideally need to provide the same, or at least an

[11] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192; strategy item 3.4)
[12] http://www.cloudscapeseries.eu/

equivalent level of service. In other words, the same service provision across service providers may be ensured by compliance to the same process-level standards. Equivalent service, on the other hand may be achieved by compliance to different yet equivalent process-level standards.

On this background CloudWATCH2 organised a Cloud Interoperability Plugfest on the topic of cloud security. The Plugfest was organised at the Cloud Security Alliance EMEA event, Madrid, 14 November. The venue was selected specifically to attract participation from cloud security experts.

Five EC cloud projects were represented by six participants: CloudWATCH2 (also as contributor), Witdom, MUSA, Credential and PrismCloud. One participant was an independent consultant primarily visiting the CSA EMEA event, and not affiliated with any of the EC funded cloud projects.

The scope of the cloud security business cases represented by the projects were manifold:

- e-Wallet systems and e-payment infrastructures
- Advanced cryptography
- Cloud governance
- ISO and NIST standards

In order to obtain a grasp on the level of overlap between expertise between participants and CloudWATCH2's survey conducted for Deliverable 3.2 'Structure and Interoperability Status' we briefly listed a number of cloud security standards and their presence in the CloudWATCH2 survey, and participant's expertise:

Name	CloudWATCH2 survey	Workshop participants
CSA OCF [13]Open Certification Framework	X	X
ISO 27000[14] (Information Security)	X	X
NIST SP 500-292[15] (Cloud Reference Architecture)	X	X
NIST SP 800-144[16] (Guidelines on Security and Privacy in Public Cloud Computing)	X	X
EC Regulation (EU) 216/679 (GDPR, General Data Protection Regulation)[17]	X	X
ISO 29000[18] (System of International Certification)	X	X
CIS SYS-20[19] (security controls)		X
ASD ISM[20] (information security manual)		X
PCI-DSS[21] (payment industry data security)	-	-

[13] https://downloads.cloudsecurityalliance.org/initiatives/ocf/OCF_Vision_Statement_Final.pdf
[14] http://www.iso.org/iso/iso27001
[15] http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505
[16] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[17] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG
[18] http://www.register-sic.com/iso-29000
[19] https://www.cisecurity.org/critical-controls.cfm
[20] http://www.asd.gov.au/infosec/index.htm

Table 1: Cross-checking security standards expertise

It was immediately clear to the workshop participants that this list is neither complete, nor does it sufficiently cover the number of security standards that exist. Participants were able to add further to this list, proving the importance of such security standards events in terms of pooling together collective knowledge on this important topic. It also became very quickly apparent that not all participants knew of all the standards which were listed, demonstrating the complex and dispersive nature of security standards in the cloud.

2.3.1 Reducing the complexity: How are standards chosen?

However, in reality the problem is less complex as there are a number of aspects to be considered when choosing a set of standards to implement:

National standards.
Examples of national security standards selection are the NIST series of standards in the US, GCHQ Top 10, BSI (German government institute for security in information technology) and other national bodies. These are the prime source of security standards and best practices industry is tapping for guidance.

International standards.
Although not explicitly mentioned, the differentiation between national and international standards selection seem to follow the lifelines of differentiation between national and international business and trade relationships.

Technical maturity.
Of course, standards need to be technically mature before one even considers implementing it so as to lower the cost of implementation and adjustment over draft publication versions.

Industry support vs. consumer demand.
The dynamics and mechanics of industry support and consumer demand are frequently reciprocal, and confusingly, also corollary: While usually strong industry support is a driver for further uptake in a positively self-enforcing manner, it can also be reciprocal, depending on consumer demand: If consumer demand is satisfied by current supply, it may be *adverse* to also implement a standard. On the other hand, if consumer demand out-paces supply, or if supply is yet low, it may be a very attractive opportunity to implement a standard as a competitive advantage over other supply-side market participants.

Reputation of the SDO and SSO.
Standards Development Organisations (such as OASIS, DMTF, SNIA, OGF, and many others) and Standards Setting Organisations both need to maintain their reputation for quality of delivery: In that sense, there indeed does exist competition between SDOs even though this may be unexpected by those outside the community. As an example, the very controversial process of ECMA standardising MS Office's XML document format (in the OOSXML structure) was perceived as very damaging to its reputation.

Complexity & re-use.
Complexity of standards plays an important role in selection and eventually in adoption. Increasing scope of a specification intrinsically adds to its complexity, if not complicatedness, which is very adverse to its re-use in other domains.

Policy declaration & regulation.
Particularly in dysfunctional markets or segments, or where sovereign topics are at hand (e.g. data protection, and privacy), national and international policy and regulation replaces selection.

[21] https://www.pcisecuritystandards.org/pci_security/

2.3.2 “implementers' dreamland"

It is clear that the cloud security landscape is staggeringly complicated and ridden with obstacles and hindrances. To get a grasp of the most pressing needs we compiled a list of the top 10 issues developers have with the current cloud (security) landscape:

1) **Equivalence of policy-level standards**
There are many standards out there which try to address the same issue. However, it is unclear whether at all these are equivalent, or at least partially equivalent (and with which overlap?). Do they overlap in their formal requirements? Or do they diverge in terminology, and semantics?

2) **Too many standards.**
Clearly, the sheer amount of standards needs is too much, they need to be consolidated - but how?

3) **Cost of implementation.**
The cost of implementation must not be underestimated, and the ROI on this is a key differentiator of the success of one standard over the other.

4) **Limit the scope!**
Naturally, a tightly scoped standard will cause a lower cost of implementation, and vice versa, hence software frequently includes only partial implementations of standards.

5) **Modularity and levels of conformance/compliance.**
Frequently, standard specifications are designed and written as large monolithic behemoths. Instead, the "architecture" of standards should change into small cores and optional modules that may or may not be implemented based on the actual need at hand.
Such an approach, however, has a direct impact on traditional assessment and certification of conformance to a standard which are often enough still binary decisions.

6) **Standardisation process and timing.**
This problem is as old as standards are, which leads many market participants to believe that standardisation is irrelevant at best, market stifling or killing at worst. Timing is an issue, in that one must find the right point in time, not too early, not too late, when to begin formal standardisation - and then it needs to finish in time to be still relevant. The exact mechanisms are still unclear. Yet, the overwhelming perception is that of standardisation from start to finish, takes too long.

7) **Stability and backwards compatibility.**
There are clearly antagonist forces at play in the lifecycle of standards. From the viewpoint of implementers, stable standards have a zero cost of update. Yet, standards need amendments to stay relevant and reflect market conditions. The worst possible scenario for implementers are entirely new standards that have nothing to do with the previous version, maximising cost of update to the cost of a completely new implementation. Therefore, backwards compatibility between intermediate versions of standards are a necessity so as to not invalidate conformance or compliance of existing implementations without reason.

8) **Reference implementations and case studies/white papers.**
Often, standards specifications are difficult to read and understand; they frequently use a specific language and taxonomy alien to the "uninitiated". Also, the intellectual leapfrog from formal language on paper to live code producing data, or procedures implementing policy level standards, represents a steep learning curve. Reference implementations and primers/guidelines for technical

standards, and white papers and case studies for policy-level standards lower the barrier of implementation significantly.

9) **Certification**

The world of certification for conformance/compliance is endlessly fragmented. In an attempt to make sense of it, participants identified for archetypical modes of certification/adherence to standards on a whole spectrum of variations:

a) Voluntary adherence / code of conduct (weakest)
b) Self certification / self assessment
c) 3rd party external certification
d) Legislative regulation (strongest)

Particularly (c) rises and falls with the certification auditor's qualification and conduct of the actual audit - after all, external certification presents a significant cost for businesses, and thus should be reputable, fair, independent, comparable and repeatable.

2.3.3 A call to action

In conclusion of the workshop, participants assembled a succinct list of actions that should be tackled in the short term. While some of these are already well-known, others are quite novel and almost guarantee a controversial discussion:

a) Align mandatory breach notification with SDO/SSO for continuous improvements of standards

This action aims at opening up, or improving, the communication channel between Standards Development Organisation and implementing bodies. While it is fairly obvious that no organisation likes to admit to having experienced security breaches, outputs and results from post mortems need to be fed back to SDOs for further improvement of the relevant existing standards. Such a feedback channel would require a secure, save and trusting foundation (likely including NDAs). On the other hand, similar structures already exist for technical aspects of services (covered by Problem Management, Configuration Management, Release Management and other service management procedures), which might be adopted and adapted according to the needs.

b) Reference implementations & White Papers.

Reference implementations for technical standards are in dire need, and should:

- Come free of capital expenditure,
- Be available in source code format (however, which language?)
- Carry an industry-friendly open source license (e.g. Apache 2, BSD style)

Transposed to process-level standards, white papers and case studies can provide implementers with the necessary jumpstart in their strategy on how to implement process-level standards.

c) Free standards.

Standards are frequently developed with the support of government expenditure. Aligned with the EC's new Open Data policy for the H2020 programme, standards developed with the financial support of governments shall be freely accessible at no cost, just as reference implementations shall be (see above)

d) **Involve academia.**

Academia has been long underestimated in their value and drive of standards. In order to maintain relevant education of future capacities and leaders in the IT industry, academia needs a constant influx of requirements, ideas and technologies that it can transform into education of future generations. As such, academia involvement in the standardisation process needs to be re-evaluated and adjusted as the prime candidate for development and maintenance of reference implementations as a means and vehicle for higher education on various topics of computer science.

3 Conclusions

In their current state, Cloud Interoperability Plugfests are facing serious challenges for relevance.

The Cloud Plugfest Initiative, with whom CloudWATCH2 collaborates, does not collect user interaction statistics beyond Mailchimp's free subscription options, particularly regular event registration and participation is not cohesively collected. Hence a historic analysis and trajectory extrapolation for the future is not possible.

This makes it difficult to measure success of the meetings, let alone measuring the impact of plugfests as such, even though CloudWATCH2 did collect participation information for the three events it organised (of which the first had to be cancelled, see above). It is questionable whether the current plugfest format is still relevant. While participation levels between the second and the third plugfest are negligible, the stark difference of the respective outcomes is very sobering in terms of assessing the success of the traditional plugfest with high participation in its heydays compared to contemporary events.

While, for example, Cloud Plugfest 10, co-located with the EGI Technical Conference 2013 in Madrid[22] featured three days of workshops and actual testing packed with attendees between 30 and 50 on any of the three days (the figures are available only because the author organised the event in his past capacity as Technical Manager at EGI.eu), recent plugfests faced participation levels of less than 10 at each event.

The reasons behind this observation are not conclusive, yet several conjectures serve as plausible explanations.

Conjecture 1: Active development vs. maintenance.

Looking at the mere chronology of events, Cloud Plugfest 10 took place in autumn 2013, and more recent plugfests over the course of 2016. Standards such as OCCI and CDMI, representing technical cloud interfaces, were relatively new (OCCI 1.1 was published in 2011), and implementations were rare and in an immature state.

Fast-forward three years, and presuming continuous interest and demand in standards-based implementations, one would expect implementations to mature in that time, alongside with maturing and near-perfect standard implementation and interoperability. Naturally, the need of interoperability testing and implementation guidance of developers in 2013 will have subsided in 2016, explaining the decline in participation to events.

Conjecture 2: Correlation of event participation with project funding

From a European perspective, the heydays of cloud plugfests correlated with the funding of three major projects as part of the EC FP7 programme lasting from 2007 to 2013, with projects running well into 2016.

These three major projects were:

EGI-Inspire,	May 10 – Dec 14,	70M €,	25M € EC PF7 contribution
EMI,	May 10 – Apr 13,	24.9M €	12M € EC FP7 contribution
IGE,	Oct 10 – Apr 13,	3.6M €	2.3M € EC PF7 contribution

[22] https://sites.google.com/a/cloudplugfest.org/welcome/events/past-plugfest-agendas/cloud-interoperability-week

All three projects together comprised involvement of nearly all EU member countries, including Norway and Switzerland, in particular the EGI-InSPIRE project covered almost all member countries.

All three projects received significant funding from the EC (35%, 48% and 63% finding for EGI-InSPIRE, EMI and IGE, respectively) continuing the EGEE series of projects funded by the EC in the years before. With EGI-InSPIRE initiating the cloud-related activities in this ecosystem in September 2011 as a federation of cloud infrastructure – the EGI Federated Cloud[23] – based on standardised interfaces such as OCCI, CDMI, OVF, GLUE, Usage Records and others, activities in standards conformance and interoperability testing in the academic cloud landscape in Europe sharply increased, impacting ancillary projects such as OpenNebula[24], GRNET's Okeanos project[25], and many more with connections and collaborations in the EGI community.

Correlating available sparse historic information with the runtime and funding of the projects mentioned above, the second half of the EGI-InSPIRE project seeing the EGI Federated Cloud initiative ramping up, particularly correlates with the most successful and most visited Cloud Plugfests.

This leads to a possible conjecture: Participants attended Cloud Interoperability Plugfests simply because EC project funding was available to cover the costs. Without funding, attendance might have been considered of lower importance.

Conjecture 3: Lack of incentives for service providers to implement standards

Industry operates on a fairly simple condition: Spend as little money for as much revenue as possible. Although simplified, this serves well in explaining some of the underlying mechanisms of this conjecture. If existing services generate revenue over and above the cost of sales (cost of supply in case of products) then this represents an appropriate response to an existing demand, in a relatively stable equilibrium.

In such a scenario, deciding to sign off an expense to implement a particular standard without the demand side expressing this need represents a highly speculative cost that is difficult to justify, unless it is a standard being implemented internally in order to improve cost of supply and therefore increase the organisation's profit margin. This scenario can be observed time and again, and industry standards and best practices for service operations and implementation emerge as a direct corollary of this. As expressed by Sebastian Kirsch of Google Zurich, at the International Industry-Academia Workshop on Cloud Reliability and Resilience[26] hosted by EITDigital and Huawei Europe, as a recollection from memory, "Standardise, standardise, standardise!". What Sebastian meant, however, was not the aim to standardise on the public interface level, but internally, to improve reliability and resilience, and thus lower the cost of service in terms of service incidents, outages, and software errors.

Alternatively, a scenario including a rising demand of standardisation at the service interface level may support service providers in justifying the expenses of implementing previously disregarded standards in two ways, (a) through direct sponsoring of implementation in a project funding manner, or (b) as a threat and weakness of their own offer compared to others in the competition.

While alternative (a) is quite straight-forward in terms of cost-benefit analysis (vulgo: "Pay me to implement the standard!") in a customised software services business model, alternative (b) activates competition mechanics in that an organisation may consider rising demand of standards implementations in a SWOT analysis as a weakness ("Demand requires support of standards, which our products do not

[23] https://wiki.egi.eu/wiki/EGI_Federated_Cloud
[24] https://opennebula.org/
[25] https://okeanos.grnet.gr/home/
[26] http://www.eitdigital.eu/news-events/events/article/international-industry-academia-workshop-on-cloud-reliability-and-resilience/

provide") on the technical level, and as a threat to business sustainability ("Our services would be outcompeted, therefore our revenue of the services may diminish.") on the financial level.

In this context, an almost 30 years old court ruling regarding policy level standards implementation from 1988[27] illustrates the problem quite well: In essence, the court ruled that a procurer cannot exclude a tenderer from the selection process towards an invitation to negotiate, if they offer a solution or a service based on a standard that provides an equivalent output compared to a competing standard. While this document does not provide a legal analysis, the impact has widely impacted procuring processes, since this ruling effectively opens a door for organisations to demand compensation for being not selected in a procurement process where they can provide evidence that the selection process favoured one standard over the other. A probably unwanted corollary to this ruling is the effectively non-existence of clauses mandating the support for a certain standard (or a set thereof), and their replacement of clauses such as "or equivalent"), where equivalence is left undefined or to "common understanding".

The overall impact is that with the absence of demand of standards in procurement procedures, we see little incentive for organisations to implement and roll out standards-based services and products.

Conjecture 4: EC projects have an intrinsically different perception of security.

ISO 27001 etc. are considered an industry baseline set of standards.[28] However, EC projects seem to be considered an incubator of technical innovation and therefore focus on technical maturity of their outputs.[29] Perhaps correlating with conjecture 3 above, EC projects thus seem to operate on the presumption of not having to integrate customer demand and customer orientation – i.e. market readiness – into their project plans and activities: While H2020 Research and Innovation type project proposals are written with customer demand and need in mind, these seem being insufficiently subjected to project outputs and results as such.

4 Next steps

The outcomes of the Cloud Security Interoperability Plugfest warrant further validation in the wider community. CloudWATCH2 will circulate these findings not only among the clusters of EC project on cloud[30] but also at relevant community meetings such as:

- EC workshop to promote practical collaboration between the Cloud Open Source and Standardisation communities, 17 January 2017
- 1st Meeting of C-SIG's Working Group on Cloud Standards, 18 January 2017
- EU Catalogue of ICT Procurement Standards workshop (24 January 2017

The results of that validation will feed into CloudWATCH2's further strategy on Cloud Interoperability Plugfests.

While conjecture 4 will be further explored through the collaboration of WP2 and WP4 regarding market readiness of EC projects, WP3 will continue to conduct Cloud Interoperability Plugfests. In alignment with the strategy and infrastructure outlined in CloudWATCH2 Deliverable D3.3 on the structure of Cloud Interoperability Plugfests, CloudWATCH2 will also run entirely virtual plugfests (i.e. with exclusively remote participation).

[27] 45/87 Commission vs Ireland ('Dundalk') [1988] ECR 4929
[28] https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf
[29] As further described in CloudWATCH2 deliverable D2.2 Mapping of EU cloud services, solutions technological readiness
[30] https://eucloudclusters.wordpress.com/

These virtual plugfests are planned to take place on a quarterly frequency, in February, May, and August 2017, planned and conducted using tools and strategies outlined in Deliverable 3.1 “Structure and aspired outcomes of Cloud Interoperability Plugfests” for virtual plugfests. The strategy here will be to run plugfests for one day at most, with a few short introductory talks on technical advancements such as new editions and errata on standards specifications, new language renderings, etc. These then will be followed with technical testing, concluding with a brief collection and retrospection on the results gathered that day, including publication. Confidentiality of participants’ information will be maintained through anonymisation of the published content.

6 Log Table

DOCUMENT ITERATIONS		
v1	Defining structure & Introduction	Michel Drescher, OeRC
v2	Complete draft available, some references missing	Michel Drescher, OeRC
v3	Internal review	Nicholas Ferguson, Trust-IT Damir Savanovic, CSA David Wallom, OeRC
vFinal	Michel Drescher	Incorporating reviewer suggetions.