D3.7 Cloud Interoperability Plugfests Final Outcome Report

CloudWatch

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.

This document constitutes an update of its predecessor document (D3.3) instead of an independent deliverable. Significant changes in comparison to the predecessor document are described appropriately.

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.

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-lived, 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
5. The cadence of innovation, particularly *disruptive* innovation, may have become too fast. *[New]*

CloudWATCH2 has address some of the conjectures during its second year, 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

1 Introduction

Over the course of its duration, the CloudWATCH2 project aimed to continue the cloud interoperability testing work started during the CloudWATCH project (2013-2015). In CloudWATCH2, three deliverables were envisaged and agreed upon to capture the strategy and structure of interoperability planning (D3.1), conduct three interoperability testing events (MS12, MS13, and MS14), and report on the outcomes of these events (D3.3, and D3.7) as follows:

- D3.1 - Structure and aspired outcomes of Cloud Interoperability Plugfests;
- D3.3 - Cloud Interoperability Plugfests Outcome Report;
- D3.7 - Cloud Interoperability Plugfests Final Outcome Report (this document).

D3.1 provided a brief review of the then cloud interoperability plugfest setup. Located in the area of expertise in the cloud ecosystem, assessed that setup against the cloud characteristics developed by NIST. Finally, the document proposed a new and innovative way of delivering cloud interoperability plugfests virtually.

This final outcome report will follow the model of *include and amend* for deliverables capturing outcomes[4]. This deliverable will include the content from D3.3 in its entirety, and amend and extend wherever necessary using appropriate indications. This is important as firstly, the observations and conjectures described in D3.3 still hold true, and by including the content of D3.3 in this deliverable, becomes the *final* outcome report. Secondly, conclusions are easier to understand as the full context and timeline of events are clearly provided.

1.1 What are cloud standards plugfests and why are they important?

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.

Interoperability testing 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".[5]

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.

[4] Typical sequential, back-referencing independent deliverables are more suited for progress reports linked to some sort of chronological periodity.

[5] http://www.bipm.org/en/CGPM/db/17/1/

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.
6. Standards emerge and establish within a defined context, or problem statement. *[New]*
7. There may be multiple standards within one defined context. *[New]*
8. The term "standard" itself bears different meaning in different communities. *[New]*

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.[6] 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 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?[7] 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 economic 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[8], CDMI 1.0, 1.0.1, 1.0.2, 1.1[9] to name but a few.
6. Within the context of API access to IaaS cloud computing resources, there are many different definitions competing with each other, even though they all address the same problem statement.

[6] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[7] 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.

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

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

To name a few, there exist OCCI, Amazon AWS EC2, CIMI, Google GCE, Azure, OpenNebula native, OpenStack native, and many, many more. *[New]*

7. The Oxford Dictionary defines[10] "standard" – selecting the most appropriate definition for the IT and tech industry – as *"Something used as a measure, norm, or model in comparative evaluations."*, and provides the example of *"the system had become an industry standard".* Thus, not only the context, but also the community pertaining to a standardised definition determines the scope and reach of this definition. One classification of types of standards differentiates between de facto, industry, community and de jure standards[11,12]. *[New]*

Predating the publication of NIST's definition of cloud computing, the Cloud Plugfest Initiative[13] (CPI) started its activities as early as April 2011 with the first instance of its Cloud Plugfests.[14] Meanwhile in its 25th event instance, Cloud Plugfests are a recurring and necessary event of harmonisation and standardisation.

1.2 How CloudWATCH has supported cloud plugfests

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 an object of the project was to organise three such events combining both physical and remote participation.

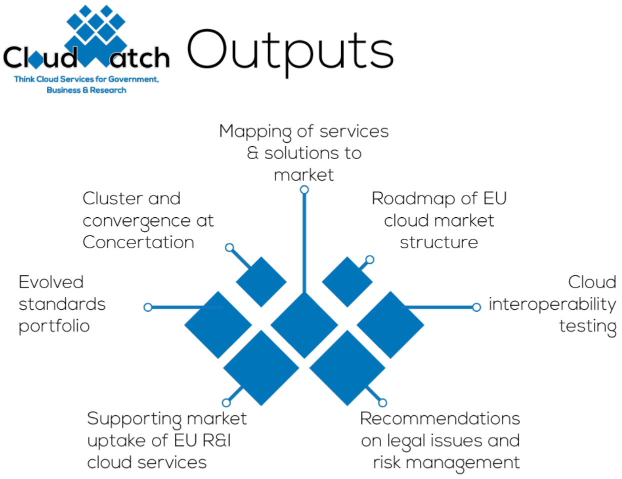
CloudWatch
Think Cloud Services for Government, Business & Research
Outputs
Mapping of services & solutions to market
Cluster and convergence at Concertation
Roadmap of EU cloud market structure
Evolved standards portfolio
Cloud interoperability testing
Supporting market uptake of EU R&I cloud services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

Figure 1 CloudWATCH2 Outputs

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, and describes the change of strategy as a consequence of the experiences it faced: Section 2 accounts for how the project managed the manifestation of the risk of lack of participation to traditional

[10] https://en.oxforddictionaries.com/definition/standard
[11] https://www.slideshare.net/MichelDrescher/a-tale-of-ice-and-fire-or-the-cloud-and-the-standards, slide 15
[12] http://www.cloudwatchhub.eu/sites/default/files/05_Why%20standardise%3F_A%20Tale%20of%20Ice%20and%20Fire%20v6.pdf
[13] http://www.cloudplugfest.org/
[14] http://www.cloudplugfest.org/events/past-plugfest-agendas

interoperability plugfests, and how and which remedy it applied. Section 0 recounts the plugfests and interoperability workshops the project organised; the accounts of the plugfests and workshops reflect the change of strategy in the project. In particular section 3.5 describes supplemental and ancillary standards related activities, including the virtual plugfests, to underpin the new project strategy. Section 4 analyses the outcomes of the plugfests in an attempt to find common patterns of success (or failure). Section 5 concludes the document with a set of recommendations for future projects and policy makers that take the project experiences into account.

2 Managing project risks and a new direction for plugfest activities *[New]*

During preparation for plugfest activies, the CloudWATCH2 consortium identified a risk pertaining to plugfest attendance[15]:

> **Risk:** Lack of a minimum significant number of participants and organization represented at the Plugfests.
> **Mitigation:** The consortium will build on the experience of the organizers of the previous edition of the Plugfest, leverage their community and eventually co-host the events with other relevant technical workshop and events. Members of the consortium are regular co-organisers to these events & have co-located their events around them in the past.

Additionally, the project reviewers gave the following comments and recommendations in their Interim project review[16]:

> *"The consortium proposes to organise virtual plugfests, but does not explore further an interesting road involving more intensely the educational institutions into the activity and organise plugfests in this setting. The consortium should keep a very close tab on the event in Madrid and analyse in detail what has worked and what not, and include lessons learned in the report on the event to ensure these are taken up in future plugfests."*
>
> **Recommendation 1:** The Consortium is recommended to work intensively on the task related to promoting standardization during the next period as this is an important objective of the CloudWATCH2 project and little progress was achieved on this task during the first reporting period.
>
> **Recommendation 1:** Plugfests on cloud service compatibility are interesting and valuable outputs of CloudWATCH2 as well. More careful planning and intensive promotion is essential over the next period to ensure higher attendance.

The project took pro-active steps to address the risk, and the reviewers' recommendations for further action. The project therefore decided to run virtual plugfests *as well as* F2F plugfests and review performance in case further action was necessary.
Using the results of the cloud security deep dive event[19], CloudWATCH2 decided to test the concept of a plugfest at the policy level rather the traditional approach of focussing on the technical interoperability at the interface level: The third cloud interoperability plugfest in Madrid (see section 3.3).

[15] CloudWATCH2 DoA, Risk 7
[16] CloudWATCH2 Result of the 1st interim review

However, facing the poor outcome of the first virtual plugfest and the second virtual plugfest having to be cancelled due to lack of interest, the project was faced with the dilemma of continuing to drive standards plugfest events in the European ICT landscape despite low attendance and considering appropriate and effective use of resources. In light of the results and attendance of previous plugfest, would it make sense to further pursue the concept of virtual plugfests? What impact would alternate activities yield in comparison? Did we even perhaps address the wrong issue?

If conjectures 1, 2 and particularly 3 (see section 4) were true (specifically when factoring in open source), then windows of opportunity should be observed for convergence in how APIs and domain specific languages are addressed and developed. In other words, otherwise uncoordinated and unrelated organisations and groups happen to work on solving the same problem with increasingly similar solutions, until this movement (for the lack of a better word) gained sufficient momentum to prevail. In that sense, standardisation may be comparable to self-igniting fuel combustion (i.e. diesel engines) as opposed to spark-ignite fuel combustion (i.e. petrol engines). Did we try to apply spark-combustion to something that might be inherently self-ignited?

As the CloudWATCH2 Cloud Market Roadmap reports (D3.3), the cloud IaaS market is dominated by three maybe even four service providers: These are in no particular order; Amazon, Microsoft, Google, and IBM. Smaller service providers tend to serve niche markets, mostly packaging and embedding OpenStack deployments – and they all are exposing OpenStack's implementation of the EC2 and S3 protocols and interfaces, which are controlled by Amazon.

The market situation as seen by the CloudWATCH2 project exposes the following mechanics:

- There exists a dominating set of IaaS cloud interfaces, controlled by one company.
- Service availability zones, and multiple datacentre locations – a feature available across all service providers – make it very attractive for consumers to integrate with one service provider when implementing their own service scalability, availability, and reliability; especially in the absence of interoperability.
- There are no indications for interoperability across the largest IaaS service providers any time soon.
- The sheer hyperscale of the dominating IaaS providers make it very attractive to disregard spreading services across competing providers (very much unlike data centre operators spreading connectivity risks across ISPs)
- There are open source tools available addressing the lack of interoperability across IaaS service providers. These implement an additional software architecture abstraction layer on top of IaaS services, exposing an *internal* common interface[17].

Generally, albeit not the ideal situation, this nonetheless provides a solution that is apparently sufficiently efficient and effective, providing a path of far less resistance (in terms of efforts and money spent) towards achieving the market participants' goal of short(est) time to market, in order to earn money.

Quite apparently therefore, there is *no need* for commercial operators, in their vast majority SMEs, to insist on interoperability or wait for truly interoperable services.

With these considerations very much in mind, the CloudWATCH2 project decided to change its strategy for standardisation support in WP3 to discontinue the virtual plugfests series. Moreover, the project decided to repurpose the envisioned F2F Cloud Interoperability Plugfests as interoperability policy events. To

[17] For example, Apache jClouds, https://jclouds.apache.org/

maintain consistency with the DoA, this deliverable will still refer to these events as Cloud Interoperability Plugfests. But in practice, these became interoperability policy events.

3 Cloud Interoperability Plugfests

As stated in section 2, only those events in year one were actual Cloud Interoperability Plugfests. In year two, the plugfest event series became interoperability policy events. These events are summarised in this section.

3.1 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 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.

3.2 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.

3.3 Cloud Security Interoperability Policy workshop

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.[18]

In continuation of the conversations with stakeholders at events such as the Cloud Security deep dive event held at Cloudscape 2016 in Brussels[19] 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 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.

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

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 of the 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 [20]Open Certification Framework	X	X
ISO 27000[21] (Information Security)	X	X
NIST SP 500-292[22] (Cloud Reference Architecture)	X	X
NIST SP 800-144[23] (Guidelines on Security and Privacy in Public Cloud Computing)	X	X
EC Regulation (EU) 216/679 (GDPR, General Data Protection Regulation)[24]	X	X
ISO 29000[25] (System of International Certification)	X	X
CIS SYS-20[26] (security controls)		X
ASD ISM[27] (information security manual)		X
PCI-DSS[28] (payment industry data security)	-	-

Table 1: Cross-checking security standards expertise

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

3.3.1 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 as follows:

[20] https://downloads.cloudsecurityalliance.org/initiatives/ocf/OCF_Vision_Statement_Final.pdf
[21] http://www.iso.org/iso/iso27001
[22] http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505
[23] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[24] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG
[25] http://www.register-sic.com/iso-29000
[26] https://www.cisecurity.org/critical-controls.cfm
[27] http://www.asd.gov.au/infosec/index.htm
[28] https://www.pcisecuritystandards.org/pci_security/

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 does indeed exist competition between SDOs even though this may be unexpected by those outside the community. For 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 reduces the possibility of 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.

3.3.2 “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 demand for standards is too much. Standards therefore should be consolidated. The question remains how to do this?

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 more often than not still binary decisions.

6) **Standardisation process and timing.**
This problem is as old as standards are. This leads many market participants to believe that standardisation is at best irrelevant, market stifling or at worst killing the market. 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.

3.3.3 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.
There is a dire need for reference implementations for technical standards which 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 should be freely accessible at no cost, just as reference implementations should 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, academic 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.

3.4 “Why standardise? The business case for the adoption of cloud standards” – Policy workshop *[New]*

Returning to the model of conducting F2F meetings, CloudWATCH2 organised a panel-driven conversation about the business case for the adoption of cloud standards (and standards at large) at the CloudWATCH2 summit 2017[29], which at the same time marked the project’s final event on 19/20 September 2017.

Setting the scene with a shortened version[12] of the original presentation given at the EIT-Ditigal “International Industry-Academia Workshop on Cloud Reliability and Resilience”[30], the panel featured renown experts in the field of standardisation crossing the areas of academia, public authorities, and open source:

- Wolfgang Ziegler, SCAI, OGF and StandICT.eu
- Cedric Thomas, OW2
- Arthur van der Wees, Arthur’s Legal
- Bruno Chenard, CEN/CENELEC

The experts provided the following input regarding the standardisation process:

1. **Balancing standards & the freedom to innovate** - How do we find the right balance between standardisation and the freedom to innovate?
    a. Innovation comes first. This normally only occurs where there is no open source tool or service already available. The innovation then becomes widespread (or dies out) and becomes a product(s) or service(s). It is at this point that standardisation tends to emerge together with Open Source solutions.
    b. This cycle closely resonates with the business innovation cycle (see slides for final event, slide 24), and Simon Wardley’s “Climatic pattern: Peace, War and Wonder”[31]

2. **Standardisation process & timing** – What is the right process to follow in developing standards? And when is it time to begin the standardisation process?
    a. There is no single one right process; it entirely depends on the context (public domain/international, or commercial).
    b. Standardise as soon as possible vs. standardise late in the market: Fast-moving markets mean that industry pushes ahead with new deployments that are not interoperable (i.e. the freedom to innovate). Building a strong network is key for consensus, which is prerequisite for successful standardisation to cake place, but this takes a long time. Consensus building – through influencers – early in the market as a means to build the foundations for formal standardisation means that we can help accelerate the process and drive the market.

3. **SMEs vs. Corporates** – What are the advantages and disadvantages of having standards in cloud computing? Are those advantages and disadvantages different for a large company compared to a startup? If so, whose interests should be prioritised?
    a. Standards penetration rates in industry are appallingly low but there is no clear reason why. Do we need to re-fit the way how standards are developed, published, and defined? Or is this linked to the inertia of change often seen in organisations large and small?

[29] http://www.cloudwatchhub.eu/summit17
[30] https://www.eitdigital.eu/news-events/events/article/international-industry-academia-workshop-on-cloud-reliability-and-resilience/
[31] Wardley Mapping, https://medium.com/wardleymaps/, chapter 9

b. Is there a correlation between the cost of switching in non-standardised ecosystems and the cost of implementation (or, for policy/process standards, compliance) that governs whether and at which rate standards are adopted?

Recommendations:

A. Standards are useful, but cannot be seen as the broker for progress. They are closely related to innovation, and together form a perpetuating cycle of innovation and standardisation that follow in each other's footsteps.

B. We are also facing new challenges as the landscape becomes more complex with the digitisation of industry, bringing in different cultures and different speeds. Early roundtables can facilitate consensus building as part of the long-term, voluntary efforts, which encourage collaboration for standardisation.

C. There is no single correct way of how standards develop or emerge. Standards cover both the technical domain, and the policy domain being closely related to regulation and law – highly similar in process how both types of standards emerge and then initially develop.

D. From emergence though, technical standards and policy standards will then take different routes as they are generally trying to attain slightly different goals: Technical standards aim to simplify and allow higher level functionality to become the differentiator, whereas policy standards are aiming for simple unification.

3.5 Supplementary cloud interoperability events and activities *[New]*

The CloudWATCH2 also engaged above and beyond that in a number of other interoperability related activities as follows.

3.5.1 Virtual plugfest 1: Trying alternative interoperability event models

The CloudWatch2 project planned the first virtual interoperability plugfest for February 2017[32].

While event registrations (25 participants) indicated a busy and productive meeting, actual attendance was disappointingly low: Only four participants joined the event, which was open for participation all day (to accommodate international attendance across a wide span of time zones). Out of these, three participants did in fact join the plugfest event to *learn* about the indicated topic, not to actually *test* their existing implementations against those of other participants.

3.5.2 Virtual plugfest 2: Trying again

CludWATCH 2 scheduled a second virtual plugfest conjoined with a physical co-location at the Cluj Innovation Days 2017 event in Cluj, Romania in March 2017[33]. However, this second virtual plugfest was cancelled due to lack of participation. Instead attendance at this event was used to promote the standards and policy work within CloudWATCH2.

This disappointing result led to the fundamental assessment of the situation and subsequent adjustment of the project strategy with regards to technical interoperability testing as described in detail in section 2 above.

[32] http://www.cloudwatchhub.eu/cloudwatch2-virtual-interoperability-plugfest

[33] http://www.cloudwatchhub.eu/register-now-our-virtual-interoperability-plugfest-march-17-2017

3.5.3 Cloud standards dissemination and education at externally organised events

As decided, the CloudWATCH2 project engaged in a number of events to promote, and educate on standards and standardisation in the cloud service sector in Europe:

3.5.3.1 International Industry-Academia Workshop on Cloud Reliability and Resilience

7-8 November 2017, Berlin, Germany

EIT-Digital, together with Huawei Germany, organised this event to bring together leadership in industry and academia to discuss how cloud reliability and resilience can be implemented to address the still eminent problem of service outages.

CloudWATCH2's presentation focussed on the raising awareness of the key role that standards play in cloud computing. Since standards can help avoiding vendor lock-in, and support application portability across vendors, customers of standards supporting cloud vendors would be empowered to implement their own application's resilience and reliability – through actively including standards in their service architecture. Arguably a somewhat exotic stance among the contributors an audience, the presentation[11] nonetheless was received with interest, and sparked an engaged discussion afterwards.

3.5.3.2 EC workshop to promote practical collaboration between the Cloud Open Source and Standardisation

17 January 2017, EC, Brussels, Belgium

Interoperability between the different commercial Cloud platforms and also the interoperability with open source based approaches is lacking in several dimensions, e.g., portability of Cloud services, VM formats, access control, data protection and rights management, hindering moving between different providers and making multi-Cloud environments difficult to realise. The workshop[34] focussed on identifying similarities and differences in standardisation and open source processes and ways to bring the two communities together. It also tried to identify which Open Source technologies in the area of Cloud could be standardised. Finally, a set of practical steps the Commission could take -as customer, facilitator, incubator for R&D and policymaker- to promote further collaboration and integration between Cloud open source and standardisation were proposed.

How OSS communities & SDOs have been collaborating has evolved with both communities often made up of the same people, but different cultures existing with SSOs following strict guidelines in establishing standards and OS community a lot freer from this. As the OS community grows though, there is a need for more standards in OS and a greater highlighting of the benefits of standards in the OS community. Future collaboration is key in terms of increasing trust in cloud computing which standards bring and also to support procurement of cloud computing.

The role of the European Commission is significant as customer, facilitator, R&D incubator and policy maker. CloudWATCH reported to the workshop the challenges it had faced in encouraging EC projects to participate to standards testing activities and the difficulty that projects have in terms of contributing to standardisation development once funding for their project has ceased.

3.5.3.3 1st Meeting of C-SIG's Working Group on Cloud Standards

18 January 2017, EC, Brussels, Belgium

This forward-looking event[35] focused on the role the C-SIG may play in the future in addressing the EC's communication on "ICT Standardisation Priorities for the Digital Single Market" (April 2016). For

[34] http://www.cloudwatchhub.eu/workshop-promote-practical-collaboration-between-cloud-open-source-and-standardisation-17th-january

[35] http://www.cloudwatchhub.eu/1st-meeting-c-sig%E2%80%99s-working-group-cloud-standards-18th-january-2017-brussels

CLoudWATCH, CSA and UOXF participated as panellists further disseminating the results of its work in standards and interoperability (both technical conformance and policy compliance).[36]
At this meeting, through the panel discussions, the first thoughts on taking a different approach to the process of standardisation of IT emerged, which eventually led to the recommendation of considering "standardisation as code" (see section 5, recommendation IV).

3.5.3.4 First plenary meeting of Cloud Select Industry Group

15 Feb 2017, Brussels, Belgium
CloudWATCH2 led a session on mapping cloud standards and user guides, and participated in a discussion panel[37]. Also, CloudWATCH was prominently featured in the talk given by Mr. Luis C. Busquets Pérez regarding new and follow-up work streams regarding cloud computing policy work[38]
This session saw a presentation by CloudWATCH2 on standards mapping (T3.1), standards plugfest testing (T3.2) and the importance of user guidelines for supporting the adoption of cloud standards. The main findings of the survey on the take-up of cloud interoperability & security standards were that there is a lack of standards related to containers (OCP), in too many cases unfortunately, privacy and security is an afterthought in the design process and the R&I projects they have analysed were mainly focussed on interoperability standards with few of them contributing to standardisation process such as OASIS' TOSCA. CloudWATCH2 also presented an overview of the existing cloud standards in every layer and project's future plan to provide a status report on Security and Interoperability standards and disseminating cloud standards related information through www.cloudwatchhub.eu.

Cluj Innovation Days 2017

30-31 March 2017, Cluj, Romania
Our participation in this event[39] was in two parts. Firstly Prof David Wallom gave a keynote presentation on the importance of security in the cloud and how new developments ongoing to bring an intersection of cloud computing and trusted computing. This will enable cloud computing consumers to no longer have to have total trust in the cloud providers security model, staff vetting procedures and technical cybersecurity measures. Following this we then led a workshop as a deep dive event on European ICT regulation and cloud computing entitled "What can be the impact of European scale regulation on cloud computing security?" with panellists;

- Marius-Leonard Motofei-Radu, UPC Romania
- Tudor Damian, Avaelgo
- Gelu Vac, Crossover,
- Radu Stefan, Microsoft Romania

Following brief presentations from the panelists a recap was given over either soon to be introduced or new regulations of importance. These include GPDR, NIS and eIDAS.
The questions asked of panelists during the event were;

1. Best Practice: Risk Management of cloud computing services
   - *What is the role of eIdentification, authentication and trust services under the eIDAS Regulation for accessing and provisioning cloud services?*
   - *How do cloud service customers decide between Public vs Private Cloud services?*
2. Transparency: Incident Notification and Information Sharing for cloud computing services
   - How can suppliers demonstrate compliance throughout the supply chain?

[36] http://www.cloudwatchhub.eu/sites/default/files/CloudWatch2_C-SIG_vFinal.pdf
[37] http://www.cloudwatchhub.eu/first-plenary-meeting-cloud-select-industry-group-15-feb-2017
[38] http://ec.europa.eu/newsroom/document.cfm?doc_id=42968
[39] http://www.cloudwatchhub.eu/looking-forward-cluj-innovation-days-2017

    - How could we strengthen cooperation between industry and the public sector to build trust in cloud-based services?"
3. Recognition: Cloud Certification Schemes & Assurance Levels
    - How could we raise awareness of cloud security that already meets the highest requirements in terms of cyber security?
    - How can certification be made accessible for all cloud service providers, including SMEs?
    - What could be the most effective method to enable standardisation agreements or mutual recognition of distinct or national cloud certification schemes across the Digital Single Market?
4. Impact Factors: Service Authentication, Law Enforcement Access, and Export Controls on cloud services
    - What approaches are necessary for cloud computing services to support the Digital Single Market in relation to service authentication, encryption, law enforcement access, or export controls?
    - What service authentication possibilities are made available and recognised across borders by cloud service providers to ensure a secure way of processing data?

The providers and 'resellers of cloud services are obviously well versed in both the new regulations and the need to ensure that they fully understand how these will affect customers that are using services they provide. Of the consumers they all suggest that there must be great scope for support to ensure that compliance is seen as a good thing rather than just something that consumers will be punished for. The chair also questions how the panel saw the scope for who would be the actor interacting with the regulatory bodies to which it was clear that overall it was felt that though cloud providers are engaged and committed to supporting these regulations they are currently not working closely with their customers to ensure that they will be compliant.

From the point of view of compliance it was felt by the panel though that there would need to be public visibility of certification and compliance with these schemes otherwise there is always the problem of possible lip service being paid to regulation without the work done in spirit which is also required.

Within this event we were able to showcase some of the outputs of CloudWATCH2 and disseminated material created on the legal guidance for cloud computing to all delegated through the event documentation packs.

3.5.3.5 Data Protection, Security and Privacy (DPSP) Cluster meeting at Net Futures 2017

29 June 2017,

Organised back to back with the NetFutures 2017 conference and the Concertation meeting (organised by Task 2.2; see also deliverable D2.3) this meeting mainly focused on the proceedings of projects within the cluster.

CloudWATCH partners CSA and UOXF presented the progress the project made in their work on mapping cloud security standards (CSA, Task 3.1; deliverable 3.6) and cloud standards interoperability work (Task 3.2, UOXF). The project summarised the results and outcomes of the Cloud Security Standards Interoperability workshop (see section 3.3). While the first call to action (mandatory breach notification) was discussed with some contention, the remaining three calls to action were unanimously agreed upon:

- **Reference implementations & white papers** (close relationship with academia and OSS)
- **Free [and open] standards** (to reduce access and participation barriers for SMEs)
- **Involve academia** (e.g. as the long-term steward of a standard and/or reference implementations)

4 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 the success of the meetings, let alone measuring the impact of plugfests as such, even though CloudWATCH2 did collect participation information for the three testing 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[40] featured three days of workshops and actual testing packed with attendees between 30 and 50 on any of the three days, 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

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.

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

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[41] – 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[42], GRNET's Okeanos project[43], 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[44] 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 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.

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

In this context, an almost 30 years old court ruling regarding policy level standards implementation from 1988[45] 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.[46] However, EC projects seem to be considered an incubator of technical innovation and therefore focus on technical maturity of their outputs.[47] 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.

Conjecture 5: The cadence of innovation, particularly *disruptive* innovation, may have become too fast.
Referring back to the Wardley Mapping methodology, especially the cycle of "Peace, War, and Wonder" (see above), in intrinsic property of this cycle – and the cycle of innovation and standardisation – is *time*: It requires time to let innovations settle in and turn into products (or services), and finally commodities (or utilities).

But what if the frequency of innovation, especially disruptive innovation becomes too high, cutting deeply into the time necessary for innovations to mature and set the scene for standardisation to occur?
Signals that that might be the case are there, for example:

- The business models and business strategies of Uber, AirBnB, Facebook and Google are under serious scrutiny or threat, with the latest example of Uber's license to operate in London being revoked[48]
- These companies are increasingly considered not as tech companies but as companies with a classic business model that just happens to aggressively use technology – but "dodging" the pertaining sector's regulations: Uber in the sector of hail riding services, AirBnB in the sector of hospitality, Google and Facebook in the news & media publishing sector.

Large-scale IT tech firm leaders begin to at least think about the pace of change, the pace of innovation and its impact on society[49].

[45] 45/87 Commission vs Ireland ('Dundalk') [1988] ECR 4929
[46] https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf
[47] As further described in CloudWATCH2 deliverable D2.2 Mapping of EU cloud services, solutions technological readiness
[48] https://www.theguardian.com/technology/2017/sep/22/uber-licence-transport-for-london-tfl
[49] https://www.theguardian.com/technology/2017/oct/07/google-boss-sundar-pichai-tax-gender-equality-data-protection-jemima-kiss

5 Final recommendations

This deliverable, D3.7 concludes the work performed in the CloudWatch2 project relating to supporting standards in the European ICT landscape.

Within WP3 the project experienced a situation where the proposal (with all its intentions and commitments) faces reality more than half a year later. While this situation is usually not much of a problem, the ICT sector and especially the cloud computing segment are faced with an unprecedented level and frequency of disruption and change: a 6-month period is considered a very, very long time span in which anything can happen.

While standards interoperability testing was a successful activity in the first CloudWATCH project, it seemed prudent to build on that success and continue with this activity – only to realise that all of a sudden attendance at these events plummeted. CloudWATCH2 was forced to react, so we decided to take a different approach as outlined in this document.

We believe that the decision we took was the right one, given the outcomes of the activities highlighted in this document.

Given what we experienced, we feel we are in the position to summarise and recommend the following actions for future projects and policy makers alike:

I. **Address different value propositions of standards in different sectors**
Looking at the commercial, public, and academic sectors, we believe that while standards are beneficial for any sector, the reasons are actually different, because of different needs, different obstacles and different sector mechanics. We think that in the past, the value proposition for standards in ICT were not sufficiently differentiated. As a result, market stakeholders and influencers became disenfranchised, and even adverse to the idea of standardisation.

II. **Different meanings of the term “standard” mean different approaches**
There are different semantics attached to the term “standard”. While in essence addressing the same topic of repeatability, internal standardisation (i.e within a company, or organisation) is much easier to address than inter-organisational standardisation. While the former is typically a passive, emerging activity (an evolutionary process), the latter tends to be seen and experienced as a managed/controlled or top-down activity – perceived as in conflict with the freedom of choice and decision in the commercial market.

III. **Offer help and support for the “unloved” elements of standardisation**
As repeatedly pointed out in this document, standardisation on the technical level across organisations tends to emerge as a successful contender in a somewhat evolutionary process. The outputs of this process are, in the ICT world, pieces of code, that manifest interoperability. This is what provides value to commercial organisations – as opposed to the formal documentation of the standard, which is perceived as “dead wood” effort companies see as unnecessary expense without value.
One approach to that solution may be to either financially support experts to be present in the formal standardisation process. The StandICT[50] projects is a good example for such an approach providing a continuous open call to support European standards experts in contributing to the standards process in the five pillars of the Digital Single Market: cloud computing, 5G, data science, cyber security and IoT.

[50] http://standict.eu/ funded under H2020: 01/01/2018 – 31/12/2020

IV. Consider a "standards as code" approach

With the recent emergence of DevOps and "infrastructure as code" concepts to literally subject as much as possible not only software source code, but also infrastructure configuration, and even deployment information to automation and version control; it is viable to apply the same to technical standards in the ICT industry. Instead of forcing software developers to break the barrier of their medium and to learn the formal language of standardisation (this is from experience literally an education task!), take the technical standards to the software developers in their own language: Encode and express standards not in human language and semantics, but in SW engineering languages and tools that are used in SW engineering tooling chains.

V. Do not engage in formal standardisation too early – or too late – in the market.

Markets inevitably mature: They mature in terms of size, number of participants, number of services provided, and operational best practices. Some markets become so widespread and ubiquitous, that the products and services provided are increasingly perceived as utilities or commodities, respectively.

Markets in that stage typically expose a reduced level of innovation, are highly automated and exchange large volumes with small margins. Mature markets are stable.

However, a high degree in automation and small profit margins both represent obstacles for standards to penetrate such markets: the cost of change is too high.

Instead, carefully analyse which markets (or which if its segments) are on the verge of becoming utilities/commodities, and engage in standardisation at that point in time.

In our opinion, the cloud computing market at large is far from being commoditised, with the exception of parts of the IaaS market related to compute and storage resources. While the cloud compute and storage segment is indeed at the verge of becoming commoditised (some stakeholders consider it already commoditised), we see the market at the brink of being dysfunctional with too much influence concentrated on few large hyper-scale providers.

7 Appendix 1: Questions for the final Plugfest panel

The following questions were made available to the panel for discussion:

1. **Balancing standards & innovation** – How do we find the right balance between standardisation and freedom to innovate?

2. **Standardisation process & timing –** What is the right process to follow in developing standards? And when is it time to begin the standardisation process?

3. **Standards: SMEs vs. Corporates** – What are the advantages and disadvantages of having standards in cloud computing? Are those advantages and disadvantages different for a large company compared to a startup? If so, whose interests should be prioritised?

4. **Standards for cloud, IoT, 5G** – Comparing IoT, 5G and cloud, what are the differences in the segments, and how do they impact standardisation?

5. **Security standards & certification** – How do you see security standards and certifications building confidence from the point of view of consumers? Do you see certification as a way that trust can be built in providers? What requirement is there on a third party verification activity?

6. **Open Source & (Open) Standards** – How do you see the relation between Open Source and Standards, mutually contradictory or mutually beneficial? Do you consider openness of standards relevant for broader adoption and increased impact?

7. **Benefits of cloud standards** – What do you see as the biggest benefits of having standards for cloud computing?

8. **Cloud standards topics** – When we talk about standards in cloud computing, what sort of things are we talking about standardising?

9. **Standards vs. certification** – Can you describe how you see the difference between standards and certification?

10. **Standards in procurements** – At what point in the procurement lifecycle would you consider it important to think about standards?