Openforum Academy

White Paper

Trusted Cloud for the Enterprise –what are the key factors today?

Report

Trusted Cloud for the Enterprise –what are the key factors today?

10 October 2014, Silken Berlaymont, Brussels

Speakers

Jonathan Wisler - General Manager EMEA, SoftLayer
Carl-Christian Buhr - Member of Commissioner Kroes' cabinet
Georg Greve - CEO, Kolab Systems
Carlo Daffara - Founder and CTO, CloudWeavers

Moderator: Graham Taylor, CEO of OpenForum Europe
Rapporteur: Diana Cocoru, Policy Analyst at OpenForum Europe

Disclaimer:

This report was prepared by our rapporteur, Diana Cocoru, for OpenForum Academy (OFA). The summaries of the speakers' presentations and following discussions presented in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion.
The views expressed in the report do not necessarily reflect those of the rapporteur or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.

Executive Summary

In the current era of digital transformation and cloud computing solutions, the debates can often be spurred with fears and misconceptions, some of them unjustified. Those irrationalities need to be addressed, together with tackling the real security concerns and law enforcement issues, in order for people to gain trust in cloud computing. This will enable them to fully benefit of the opportunities that cloud solutions offer.

The event looked at the key factors that matter today which affect the level of trust when it comes to migrating to cloud platforms. The discussion covered three main points: first, what is the extent to which the fear surrounding cloud solutions is actually justified and how much is irrational and thus impedes customers to reap the full benefits of cloud solutions. Second, what are the factors which realistically ensure trust when it comes to cloud computing. And third, the degree to which cloud certification is the valid solution to ensure trust in cloud solutions and whether it is the only or the best one.

These points were analysed from different angles, with the participation of four speakers with varied backgrounds: one European Commission official, the CEO of a large company which offers cloud infrastructure as a service, the CEO of an SME which offers cloud solutions and a researcher of the real macroeconomic opportunities of SMEs when it comes to migrating to cloud platforms. The discussion which followed the introductory presentations was interactive, involving an audience of 30 participants, coming from the industry, public national and European institutions, SMEs, research and users' community, as well as media.

Table of Contents

Setting up the context

Mr Graham Taylor opened the round table by presenting OpenForum Europe (OFE), which is a non-profit and independent organisation, with the mission to support an open and competitive IT market. He then introduced the OpenForum Academy (OFA), which is an independent think tank, driven by a network of over 40 peer appointed Fellows, which work independently from OFE. OFA is the framework where innovative ideas are brought into the area of openness in the IT market.

Mr Taylor first presented the format of the Round Table: after short introductions by the panellists, a moderated discussion took place under Chatham House Rule.
Before giving the floor to the speakers, Mr Taylor introduced the topic of the event:
Cloud is the debate. No company small or large is able to ignore it anymore, every public sector organisation is considering it. The danger is that we talk about it as an "it", but it is not an “it”. It is a number of business models, old and new. It is a matter of balancing between the industry and the other stakeholders.

Although we see a coming together of views, between the industry, Commission representatives and politicians, in the framework of the Cloud Select Industry Groups (C-SIGs) set up by the Commission, two concerns still remain. First, there is the issue of timeliness: people are making purchasing decisions today. What are the elements, the principles that they should consider today, rather than in three-four years' time?
Second, the fact that the term "open" is one of the least defined terms in the IT jargon. It is a term used to give an easy fluffy positive feeling, but very rarely does one see it justified. Therefore the question remains what should be meant by openness in the IT market, but also specifically in the context of cloud: what do we mean by Open Cloud?

After underlining that the debate would not avoid any of the controversial areas, Mr Taylor introduced the four speakers, by describing the role they played in the debate of open cloud and the factors needed in order to gain trust.

Mr Jonathan Wisler is the European head of Softlayer, which was bought by IBM in 2013. He presented his view, from the perspective of a large company providing Infrastructure as a Service (IaaS). 75 million dollars are being invested in establishing the operation in Europe- a point which was picked up during the debate.

Mr Georg Greve is one of OFA's Fellows, who started with a not-for-profit organisation and now is an entrepreneur, working with around 200 people to provide collaboration technologies. He presented a different point of view, based on what it means to be on the other side of the equation.

Mr Carlo Daffara is also an OFA Fellow and also working in a small cloud based SME. He has substantial experience in working with the European Commission, representing SMEs' interests across Europe, but also looking at macroeconomic opportunities in different areas. He did a lot of work in open source and cloud. During the discussion, he focused on different perspectives of market opportunities.

Mr Carl-Christian Buhr works in the cabinet of current Commissioner Neelie Kroes. He has been one of the people that we have seen central for the thinking and the practicality of cloud. He stressed that although he was in charge of the cloud computing portfolio in the cabinet, he could not speak in the name of the new Commission, therefore he expressed his own views on the issue.

Panellists' introductory speeches

The members of the panel presented short introductions each, in order to lay down their thoughts on the topic and to set up the framework for the following interactive debate.

Jonathan Wisler introduced himself as the General Manager for Softlayer for Europe. Before expressing how they view cloud and how they view transparency and openness in the cloud, he first took a step back and focused on why these are important. Looking back at Nokia, Kodak and then comparing those with the newly established companies like Whatsapp, Spotify and Netflix, he underlined that what we witness right now is a digital transformation, which is happening at a fast pace. This led him to the conclusion that the outcome of cloud is to drive innovation.

Questioning why transparency and openness are important, Mr Wisler referred to the children of our generation, who are growing up in the digital age and who are used to a high level of choice and transparency. However, he underlines the importance of making sure it is a secure place for them to be online.

Speaking about Softlayer's perspective, Mr Wisler informed the audience that the company opened the first European data center in Amsterdam 3 years ago. Recently, they have built a data center in London, which was opened this summer and are currently building one in Paris and Frankfurt, by the end of 2014. He underlined that the company needs to build a new data center very other month, to keep up with the pace of growth.

Mr Wisler focused on three main points which underline how they are open and transparent when it comes to cloud computing:

1. Full visibility on where the customers' data sits
As a IaaS provider, their market approach is to ensure that people have transparency and full control of their own data. They do this by building data centers in country and providing customers with access and detailed information down to the server level, which allows them to know exactly where their data sits.

2. Technology agnosticism
By contrast with other providers, Softlayer has developed an open standard cloud which equally supports open source and proprietary software. Therefore customers can build their own private cloud and use the software and the technology they like.

3. Accessibility for everyone, regardless the size of company
Softlayer has ensured that their services are easily accessible for everyone and the level of performance is independent of the size of the customer's company.

He concluded his speech by underlining that since, in cloud computing, customers only pay for the computing power that they use, they do not need high capital investments. Therefore this is the way to "democratise innovation".

Mr Georg Greve started by describing his background, which "is in the open, or in the free, but with clear reference to liberty". He has been working to build more liberty into the digital society, first during a non-profit phase and now turning this into a for-profit company, for the simple reason that someone has to and also because the economics behind it must work, otherwise the best ideas will not survive in today's world.

He is the CEO of Kolab Systems, a pure open source vendor, which provides collaboration solutions (email, calendar, address book, tasks, file cloud), similar to Microsoft Exchange & Outlook, with a bit of Sharepoint. They do this with 100% free software and 100% open standards.

Their solution was initially developed for the German office for IT security (BSI), in 2002, and the BSI is using it until today. In the past, Kolab Systems has mostly deployed its services on premise, meaning a solution which is installed on the customer's server at home or in his/her own data center. They continue to do this, currently deploying for the city of Munich, for 40.000 city employees on their own infrastructure.

He focused his speech on two main questions: **where is the right point to take control on the infrastructure** and **what is the real price of the customers' privacy data.**

Regarding the first question, he considers that the scalability that cloud services offer, as well as the gains, become much bigger when ones reaches a certain size. Once the customer can run infrastructure using cloud computing, the cost-effective benefit is much higher. It can be run fully virtualised in different scenarios and customers can maintain control down to the physical level if needed. This is the motivation for Kolab to have moved their services into a place where they can serve all these scenarios: besides deploying it on premises in Munich, they have also started, in January 2013, their own version of Software as a Service (SaaS), which is is a web-based email and groupware service, called “MyKolab”.

For the second question, Mr Greve voiced concerns that with big vendors, when people submit their data, they pay with their privacy. As a society, the level of this price remains yet unknown, because the negotiation process is lacking transparency and also because we lack real damage scenarios. Moreover, he emphasised that the price tag attached to our data is not small, but fairly large.

Currently, the questions of where the cloud goes and how it is going to look are so open, that Kolab Systems does not want to force people to make those decisions right now. They want their customers to be able to experiment and actually run a fully open stack that they can control themselves. To support this, Kolab has published everything down to the puppet scripts that manage the servers.

Mr Greve concluded his speech with a reference to the law enforcement and the Snowden revelations. He made it clear that no one knows the right answers yet and that those answers probably do not yet exist.

Mr Carlo Daffara introduced himself by explaining that he currently designs ways to help and facilitate the participation of small enterprises in IT processes to adopt new technology in open source. He has extensive experience in finding and designing ways to understand how to help not only the big companies (which are good enough by themselves to create technology and adopt it), but especially the companies that do not have the initial competences, who face knowledge gaps in adopting technology, budget gaps and infrastructure gaps. Those economic problems are easy to find in Europe and one of the biggest problems is the knowledge gap, which is quite common, according to his statement.

Mr Daffara set up the context of his speech by questioning the actual size of the market for Cloud outside the US, pointing to the fact that the share of Amazon revenues outside the US is estimated to be only around 5%, although the precise figure cannot be ascertained. Being a 2.5 billion dollar business, Amazon has only 4.83% in revenue shares outside of the US, out of which he estimates

roughly 2 % in Europe.

He then moved on to the Gartner report, which mentions that Amazon is bigger than all the other five biggest cloud players combined. Based on that, Mr Daffara stated that we can safely say that **the take-up of cloud computing in Europe is slightly different than what has been presented in most research papers** and relayed by the press.

Mr Daffara asserts that cloud adoption in Europe has a very high penetration rate: 70% of companies would say that they are nowadays using cloud in one way or another. However, he also pointed out that the level of IT spending raises only to 1-2%. He moved on to explain the economic reasons for this situation:

1. Less evidenced advantage for SMEs to migrate to cloud

Mr Daffara spoke about the forklift approach to the cloud. How this works in practice: the customer picks up the existing IT infrastructure and moves it to the cloud. For the SMEs in Europe, Mr Daffara argues that this approach has very little economic advantage: 70% of those interviewed reported less than 10% of savings due to migrating to cloud through this approach.

2. For scalability purposes, the software needs to be changed

There is a lot of potential in the cloud that is very easy to see in our world today. Speakers mentioned beforehand Spotify, Facebook, Twitter, Netflix. All these new companies have one thing in common: the software they develop is totally different in structure and scale from what was developed before. Unless the software is changed, it is simply impossible for companies that existed before, to take their existing IT solution, migrate to cloud and scale from 1 to 1000 servers. They first need to change their software.

Moving on to discuss about the Trusted Cloud Europe, Mr Daffara covered the lack of interest of small companies to get any cloud certification, referring to it as a simple "rubber stamp". He went on underlining that there are already certifications and most of them are nearly equivalent. Therefore one company that acquired one of those, can perform one slight adjustment and can get all the others. However, it is nearly impossible for a small company to get such certifications, for two different reasons:

a. the barrier for getting such a stamp is very high;
b. they do not get an economic advantage from doing so: all the large companies already have the stamp, thus having it would not make any difference;

Speaking about the process to develop standards and create an open market, Mr Daffara focused on the need to take an economic approach: **if we are able to create an economic network of companies that can sell products to each other and that can cross-pollinate with each other, they will find the natural incentives to collaborate and thus standards will inherently be open.**

Mr Daffara moved on to speak about the **real incentives for companies to participate in such an open market.** He criticised the **wrong assumptions** that can be read in most research papers, which present the incredible economic potential of the cloud, but do not provide realistic estimates. Those papers point out to an incredible number of new jobs, an incredible rate of growth, based on the assumption that in maximum 4 years, 100% of the companies would move 100% of their IT to the cloud. Mr Daffara pointed out that this would be totally impossible, because we do have data that shows that for the next 2 years, nearly half of the new server capacity in Europe would still be delivered on physical servers, not even virtualised.

Mr Daffara concluded his speech by emphasising that before talking about an open cloud and a trusted cloud, we need to talk about a cloud that satisfies the needs of European companies, especially those of SMEs, which account for 99.9% of all European businesses.

Mr Carl-Christian Buhr spoke about where the Commission stood and stands in the policy of cloud computing. He underlined that the point is to satisfy needs that are there, instead of creating needs which are not real, for the sake of marketing. The reason for adopting cloud should be supported by the economic and societal aspects behind it, in order for it to be interesting.

Mr Buhr underlined that since 2010, there has been an increase in the public debate and also in the public interest. What the Commission has done, was to **put cloud computing on a map in terms of policy**. It consulted with companies, as well as with the demand side and led a process in order to reach an agreement of what the needs really were. Identifying the needs also means that the providers would adapt to those, in order to satisfy the demand.

While having the impression that some of the current debates still reflect the level of maturity specific for 2010, it is clear that more effort is needed in order for real opportunities not to be missed: SMEs can gain openness, they can gain access to network, an ecosystem that they would not have had in the past. Mr Buhr admits that perhaps things are not easy to be tackled, but he believes there is a lot of **unused potential** there and it would be important for the overall economy to take advantage of it. This is why the Commission invested a lot of efforts and attention to drafting the EU cloud strategy.

Referring to Mr Taylor's remark about Oettinger's announcement of no new regulation for the cloud, Mr Buhr drew the attention on the fact that in July the Commission published a report on the implementation of the cloud strategy and mentioned that, for the future, **co-regulation would continue to play an important role**. He spoke about the 'Communication on a data driven economy', also known as the 'Big Data Communication', which touches on cloud computing. The Commission considers that these things belong together. Through those 6 pages, the Commission placed a reference for possible future work in the area of cloud computing, just to keep the opportunity open politically, for the new Commission.

Mr Buhr underlined that the paper that came out of the European Cloud Partnership was a **collective document** delivered by the European Cloud Partnership, not the Commission, and that it was created in a work stream made up of industry and public sector. The idea of grouping senior representatives from industry together with the public sector was motivated by the aim to encourage the latter to become clear about its needs when it comes to cloud and its opportunities. Once this is achieved, SMEs, which traditionally are less conservative and cautious than the public sector, would also make better use of cloud solutions.

Mr Buhr emphasised the level of irrationality in simply considering cloud dangerous and pointed to the lack of proper understanding that even with a server in your own basement, secret services can get your data. While irrational, this worry cannot be ignored, because the Commission wants the people to take the opportunities available to them.

Mr Buhr concluded his speech with an encouragement to **keep occupying the space, and to make sure that all new ideas and initiatives come in the existent trajectory: "We need to ensure coherence".** To support this, he also called on his colleagues not to fall into artificially defined areas, because a real European Single Market cannot function if they focus on their respective silos.

Discussion

Disclaimer: These comments were taken from the general part of the meeting and do not necessarily represent any of the speakers' views or those of their organizations. The discussion took place under Chatham House Rule and therefore names and affiliations of participants are not reported.

A list of three cross-cutting issues emerged from the discussion.

1. What is the degree of irrationality and wrong assumptions?

There was a consensus in the audience that the Snowden revelations and the debates that followed had a positive outcome overall. That is because it forced people to think about those issues much more than before. However, there were also some opinions considering that Snowden created some fear that is at times irrational. It was pointed out that part of the public perception is unfortunately directly influenced by some of the press reports, which argue that 'there is danger out there, so let's not go'.

The existing level of irrationality in the cloud debate leads to people doing things that are actively harming their own security and making them less secure, out of a feeling of insecurity. This is not helpful objectively, but everyone agreed that security is a very difficult topic and that some of the issues related to cloud computing are applicable in IT, across the board.

It is understandable that people feel insecure to a certain extent, but this also leads to them overreacting in some ways. There was a shared feeling that this irrationality does not end with security, because there is no way in which an SME can deal with this threat in a cost effective manner. One participant said: "From a technical point of view, we do not know how to make it 100% secure. It is an open technical problem, because we can safely say that no IT system is secure against an attack with enough resources."

It was also put forward that certification has its elements of irrationality too, when it comes to what people think it provides. The experience has shown that in the security realm, certification provides extremely little value, often at high cost. Hard evidence shows that even fully certified companies, like Amazon and Google, are not fully secure. Moreover, there is a significant gap between the certification process and what happens on the operational level. If one wants security, one has to also look at the operational level.

The discussion continued with underlining the wrong perception of believing that because the server is in one's own basement and because one has a European cloud provider, it is safe. That might not be the case, because the machine is connected to the Internet. This is why the best recommendation someone can make is to encrypt your data, both in traffic and at rest, because that is the only way to secure your data. Thinking that only because the physical data sits in a country, then it is secure, it is a misconception.

Some Member States' politicians and public officials still take a conservative approach: they prefer to have the cloud very close to home. This is not necessarily to be criticised, but there was a strong encouragement to actually take a closer look at the details, because a proper analysis might lead to

the conclusion that by migrating to cloud, while offering the same protection as keeping it close to home, it also makes it less expensive. This is not an advise to the companies about what to do, but a way of saying “let's not be scared by something diffuse. If we are to be scared, let's be scared of something concrete”.

Participants to the discussion pointed to the fact that there still are inappropriate barriers to an increased adoption of cloud computing, like countries still having unadapted laws, dating back to the pre-digital technology years. In those cases, the need for the data to sit in a certain location has no other grounds than the lack of legal adaptation to the digital era. Some people suggested that important for the digital market, is that from a legal perspective, there should be no difference where the data is stored, because that is the interest in having a cross border, bigger, competitive market.

During the debates, one participant raised the point that when we look at how US treats data versus EU laws, there is actually a rather strong case to be made that EU companies may have to limit themselves to EU cloud providers, until the concerns over privacy / surveillance are better addressed. There currently are concerns that a US company cannot adequately protect its clients' information and prevent it from getting accessed by the authorities without due judicial process. Nowadays, there are debates at Europol about the tensions between law enforcement and the requirements for privacy. It was raised the point that currently European cloud providers may stand in a better position to ensure privacy, following the EU law, than American providers might do. And American providers have to solve it, because it has an impact on citizens.

In reply to the point presented above, a counter argument was presented, in order to clarify the current controversy regarding a company having its headquarters in Europe, which would arguably not be subject to US laws. The point made was that if you are a European cloud service provider like Deutsche Telekom, Telefonica or Telecom Italia and you have any market operations in the US (i.e. marketing, sales) or some sort of representation that links you to the US market, you fall equally under the US law as well. So if you want to be totally protected, you need to avoid any presence in the US. This aspect is considered to be insufficiently reflected upon.

When it comes to the public administration, the irrationality presents itself differently: they might be aware of the value of the data, but they have different ways of thinking about the impact of their decisions. For example, some public authorities might be reserved about adopting cloud solutions, considering that the advantage of doing so is so little, that it is not worth it. Their officials are afraid that if something bad happens with the data stored on cloud platforms, the public service itself might immediately be pointed to as the culprit, even when the problem might originate somewhere else. This approach is irrational because they are discarding the potential advantages of migrating some of their infrastructure to cloud.

A gain which is often overlooked when migration is considered, is the procedural advantage of using cloud solutions. Once the decision to migrate is made, there is the real and imminent necessity of understanding what one uses internally: more than half of the companies which participated in a survey had no inventory in place, they did not know what software they have, which server they have, or whether they had backups in place. When the company decides to start using cloud services, it has to first look at what it has and decide what it actually needs to move. This process is healthy because it allows them to question whether they really need to have those servers which manage everything locally or it would be more efficient to have them in the cloud.

There was a general understanding that we need to change our thinking about adopting cloud solutions and also that instead of focusing only on government and law enforcement, we need to

take into account that there are lots of issues that may arise in voluntary disclosure as well.

The conclusion was that we should rationalise the debate to a certain extent and that education is very important. Rationalising the debate goes through first defining what trust means as far as cloud is concerned, and then questioning certification as the valid solution for granting trust in the cloud.

2. What defines trust, as far as cloud is concerned?

Throughout the debate, the notion of trust was invariably linked to **three indispensable requirements**:

- transparency;
- ownership;
- control/avoid lock-in.

When it comes to transparency, it was agreed that the whole Snowden debate raised the need for transparency, both in the management of one's data and in the law enforcement.

As exemplified earlier, in order to guarantee the needed transparency and control, a supplier needs to ensure that their customers have full transparency of the system. They should be able to see not only who the network providers are and where their data resides, but also have full rights on that location. This can be a major differentiator from other cloud providers and can be ensured by granting the end customer root access to the server, together with the keys and the passwords.

There is high demand of being able to trust, extended to being able to control. Regarding the point of controlling how data is managed, two points were underlined. First, there is a problem of understanding, especially by SMEs, of the value of the data they have. Second, the variety of existing business models depends on the level of *protectable data* that has to be managed. When the data is not sensitive (e.g. gaming companies, online entertainment companies), the business model is to drive high performance at low cost. When the data is sensitive (e.g. healthcare companies), **it is important to strike the right balance of the protection level,** in order to ensure enough sharing, so that there is mutual benefit, but enough privacy, so that individual healthcare data is not exposed.

Another participant asked whether the **potential (legal) fragmentation across Europe** is a blocker of market opportunities. The reply inclined to consider it as a blocker: if one builds too much of a silo, it leads to fragmentation, which leads to a loss of the collective intelligence, because the different silos do not intercommunicate. And that is a real danger of the Snowden revelations, namely the fact that currently people are storing their data “under the mattress”. By avoiding to open up and use that data, they miss on the opportunities to grow and improve their companies.

Based on the customer demand and out of a need to ensure **data sovereignty**, suppliers like Softlayer choose to build data centers in several European countries. From a strictly cost perspective, the providers could be better off building more data centers in the same European country, because they could get more scale at a lower cost per unit. But from a **data sovereignty perspective**, if they want to give their customers full control and ownership, suppliers need to ensure that their customers' data sits in their respective countries.

Referring to how the hardware is directly linked to the software which runs on it, a challenging remark came from the audience, namely: why did Brazilian public authorities decide, two years ago, not to use cloud services for governmental data, justifying this decision on security reasons, if everyone agrees that any machine can potentially be reached and accessed from anywhere, once it is

connected to the Internet?

A detailed reply was provided: Brazil as a country, is so large that they can virtually get all the scalability benefits out of running things from their own data centers. From the trust point of view, confidence can be gained not only by being able to access the data, but also by ensuring that the software can be trusted. That is why Brazil has been following a strategy encouraging the use of open source software for a long time and why they are currently rolling out updates of their collaboration platform. This is because the president of the country feels strongly about the intrusion of privacy.

This is a clear explanation why, if one wants to enjoy control, one needs to look at the whole stack, from the bottom to the top and to approach the issue from a holistic perspective. When trying to foresee whether Brazil would be able to succeed, one can look at several details: they have the benefit of being the 4th largest country in world, they have done fairly well at developing their industrial sector, they have the needed determination at the moment and they have a pretty big budget. Therefore they certainly are in a position to pull it off.

Coming back to the EU, not every country is Brazil. Theoretically, the EU has the necessary size to tackle this as well, but then there is also the question of the divergence of views at the political level, that exists between different Member States. The question of more EU integration is not necessarily popular to everyone. Therefore in Europe, we are facing not only a technical dilemma, but also a political one.

Another angle to look at trust is the possibility of the customer to take the data it owns and move it to another cloud provider. Or, differently put, **one can trust in the cloud if there are available ways to avoid lock-in**.

The danger of being trapped into a certain IT solution is exactly the problem that the IT industry has been suffering from, for a number of years. OFE pushes open standards very strongly, but standards take time to emerge, so the two main questions which were raised during the discussion were:

1. What to do at the moment, until those standards are developed and
2. What other factors, besides the technical interfaces, can cause lock-in?

It is a known fact that there are very few standards in the current state of the market for cloud computing, apart from a few de facto standards. Lots of companies are targeting Amazon APIs, but there was only one company that actually claimed to have built their product on the Amazon API, with their support, and that is Eucalyptus. Other companies replicated Google APIs.
Some of the companies have started using those pieces despite knowing that no other company is re-implementing them. And this is because they feel that the advantage of using that software is higher than the cost of moving somewhere else. In this context, the best question to ask is: "**Is there a way to re-implement somewhere else the software infrastructure that I am using with this cloud provider?**" Unless your setup allows you to reimplement your solution somewhere else, you should take into account that locking yourself in comes with the risk of being forced to accept any change and condition of your cloud provider. The example of Netflix, who implemented most of their own infrastructure on top of Amazon, simply by changing small things, shows this is possible, even for complex architectures.

One can also look at **lock-in from a market perspective**, based on ensuring the required performance. Knowing that usually, by definition, the customer can easily get out of the contract quickly (most often the longest contract is 30 days), by nature there is no lock-in. However, the

provider can add more features, more value and high performance, thus providing its customers with the needed set of tools to control their own data. This would give them the needed applications, together with the right resources to compute it for the right level of security and the right level of performance, so the companies and large enterprises remain with the same cloud provider, because they have the level of control and performance that they are looking for. Perceived from this angle, cloud fundamentally moves the industry away from lock-in.

Naturally, when speaking about how to avoid lock-in, the issue of standards emerged. Standards are considered to be innovation-following, by nature. And so, if one standardises too early, this can stop innovation, and if one standardises too late, the entire development process might be over and the market might have already moved to a problematic monopoly situation. Therefore, the standardization must happen between these two points in time.

Effectively, it is easy to lock yourself into a cloud platform, if you approach it wrongly. Anyone who tries to be part of that innovation gain offered by the cloud, needs to be very careful to properly architect a solution which does not lock them into whatever cloud they might have chosen for the first deployment. Therefore this is an architectural issue, it is about whether you have a proper software architecture. Therefore, the advice for anyone who wants to have the innovation gain was to make sure to have a good architect on board to oversee that process. To reflect how this can happen, participants gave the example of many of existing customers who still have very traditional set-ups, in order to point out that **there is no certainty that cloud is always necessarily lock-in averse,** as previously stated. What can be seen is that some individual customers might say they want to use a certain product, but they have tied themselves into an online cloud identity with one provider, in a way which does not allow them to shift. The overhead of switching becomes too big for them at that particular moment, therefore they have to wait and do this when they have time to sort it all out. For large companies, that lock-in would be much stronger. So people need to avoid creating another level of lock-in, which is no longer on the traditional server, but in the cloud identity sphere. Moreover, the entire realm of data lock-in in terms of what formats and software are being used, are questions that still remain. So, if anything, **we currently have more options for lock-in and not fewer**.

When speaking about data lock-in, a point was made that there are some cloud providers, where for their platform to work, from an enterprise level, they need the data to sit on their servers. But they are getting value from the customers' data. Therefore, another big concern is to make sure there that you can get your data back at any time.

All this being laid down, it was then enquired whether certification is the best solution to ensure trust.

3. Is certification a valid answer to the lack of trust in the cloud?

The security concern is still perceived as the number one issue in terms of adoption of the cloud. Therefore, it was asserted that more security needs to be ensured, in order to gain trust.

In the context of Trusted Cloud Europe, certification comes strongly as a means to increase trust in the cloud. This is why the discussion focused on the value of certification, the degree to which it is an enabler or blocker for SMEs and whether certification is more than “just another rubber stamp”.

The focus was put on the work of the C-SIGs and their aim to ensure that the voluntary certification offers an added value not only to users, but also to cloud providers. When talking about

certification, an important point which was raised was the degree to which something is imposed or required and who requires it. What is aimed for at the EU level is to look at certifications and see what works best. Based on this analysis, the Commission tries to bring best practices at EU level and make it possible to exchange them between countries.

It was agreed that **certification is not a fixed thing**. It is something that evolves, and we can get better at certification, by getting closer to fulfilling the relevant requirements, in a satisfactory way. In order to reflect on this, the example of cars was put forward. It was underlined that those systems currently work very well, because there was a lot of time spent on understanding how to do it properly and a lot of effort has been invested in forcing producers to accept changes even when these impacted their business models (e.g. seat belts). When looking at certification for cloud computing, we are still at the beginning of this. Those who do not ask about certification, in reality say that the certification that interests them does not yet exist or they did not hear of it. This suggests that we need to take the opportunity to go deeper into what matters in the end, so that the right questions about certification are actually answered. The point of certification is to allow the needs for customers to get a service, without painfully checking whether what they are interested in, is really provided for, and who has the liability if something goes wrong.

From the perspective of an SME, the point was raised that for a lot of the security sensitive customers (e.g. law firms, legal professionals, journalists, private hospitals), who have a legitimate interest to protect their data, when it comes to trust and security, certification is the last question they ask. And these are the competent ones, who have someone who knows what questions to ask. Those who do not know, go for the certification.

For SMEs, certification is a costly process. If a customer asks for it and if that is the cost of doing business, SMEs would do it, but the customer ultimately has to pay for it. If the customers do not ask for it, SMEs do not necessarily do it, because it does not add an actual value to what they have to offer. It was also added that most of the certifications they asked for, as an SME, are totally useless today, unfortunately.

The discussion pointed out that the **certification risks to be a rubber stamp.** It was agreed that this danger exists, because people want to just get some boxes ticked and get the certification, but if people fail to look at the entire thinking process behind the certification, then it just becomes an additional cost, with no added value. Therefore, more thinking needs to go behind the certification, which also relies on the procurer and the supplier having the same level of understanding.

For some SMEs, it appears that other ways are more reliable and interesting in order to ensure that they invest in the right level of security needed for their enterprise. Knowing that security is always a matter of cost, which might be disproportionate to what companies want to protect, there is an available open source security testing methodology manual (OSSTMM), which helps companies quantify the level of security, by comparing the value of the asset against the likelihood of the threat. If the test result comes above 100, it means the company spends too much for its security in proportion to the estimated threat level. If it is below, they may want to invest a bit more in security. This seems to be an appropriate tool for bridging the gap between ISO certification and the operational level.

It was pointed out that **another danger of certification** is the fact that several different certifications are asking the exactly same question: secured access. Therefore, it appears it would be very useful for companies and procurement officers alike, to have **standards between certifications**, in order to avoid duplication and to also ensure meaningful criteria in the call for tenders, which would avoid direct references to brand names.

There was a consensus throughout the discussion on the fact that, besides transparency, certification and increased security, what is also needed in order to ensure trust is **more education and ethical statements and compliances**, in order for people to feel more comfortable. The information is there, the rest depends on peoples' ability and willingness to seek the information that would be useful for them to do a better job.

Most companies currently need to adapt their business models, in order to make their businesses sustainable on the web. The new business models have to take into account all types of competitive differentiators: ensuring transparency, full liability and the possibility to move data any time and avoid lock in.

Leaving aside the advantages or drawbacks of certification, and the need for more education, a valid point was raised about the lack of discussions between the legal and technical perspectives. When standards are becoming too technical, it appears to be difficult to ensure the communication between the lawyers and the technical experts. When this happens, the risk is that the legal recommendations that are developed in the framework of e.g. the Article 29 Working Party might not be useful and thus disregarded, because they cannot be implemented at the technical level. The suggestion was to ensure more communication between the two sides, in order to become better at understanding each other.

Concluding remarks

Although we are talking about "**the cloud**", this is not a thing, it is **a living entity,** which is developing under our eyes and it is largely not understood. When we talk about a cloud provider, we talk about a complex ecosystem, with networking equipment and servers, on top of which software is run and that has a set of procedures providing security.

In order to reduce the fear related to the adoption of cloud solutions and rationalise the debate, it is recommended to experiment this living entity with an open cloud in house, before choosing a public cloud. This way, people can learn about what the cloud really is, its strengths and weaknesses. Trying it for yourself substantially reduces the misunderstandings and enables you to identify the kind of lock-in you may encounter when you go to an external provider.

Although still nascent, the cloud industry is growing and shifting quickly. Trust can indeed be gained by the use of certification, only if this is not limited to a mere "rubber stamp". Attention needs to paid to the process behind certification, and to also link it to the operational level. Trust can further be built by using open standards and open source. Using these allows users to look at the technical aspects at each and every level.

Note
OpenForum Academy gratefully acknowledges the support of IBM in this Round Table. OFA welcomes financial support for its events, but always maintains independence of the discussion itself and the follow up White Paper.

Speakers' Bios

Jonathan Wisler, General Manager EMEA, SoftLayer

Wisler is a technology veteran who has been driving innovation, profitability and international expansion in technology companies for close to 15 years. Prior to SoftLayer he was a principal at Magnify Consulting, where he helped technology startups with international expansion and develop scalable operations. He has also spent 8 years at Kodak Gallery, growing the business unit from an idea to an international market leader; there he was responsible for hosting and developing a global web to print infrastructure on a limited capital budget. He graduated from the University of California at Santa Cruz with a major in economics.

Carl-Christian Buhr, Member of Commissioner Kroes' cabinet

Buhr, an economist and computer scientist by training, is a member of the cabinet of Digital Agenda Commissioner and EU Commission Vice-President Neelie Kroes. Among others, he advises her on the developing European Cloud Computing Strategy, Data protection, Standardisation and interoperability policies as well as ICT research policy. He previously dealt with antitrust and merger control investigations by the Commission, such as the Microsoft antitrust case and the Oracle/Sun Microsystems merger.

Georg Greve, CEO, Kolab Systems

Greve is CEO and managing director of Kolab Systems. Previous commitments include: responsible for managing the Free Software Foundation Europe (FSFE) as its founding president; consulting Google on standardisation issues around OOXML; and playing a key role in the Microsoft antitrust trial in Europe. Greve is considered one of the world's first and foremost experts on Free Software and Open Standards issues, consulting among others the European Commission in its research and development programmes. In 2009 he was awarded the Cross of Merit on Ribbon by the Federal Republic of Germany for his achievements in the area.

Carlo Daffara, Founder and CTO, CloudWeavers

Daffara is Technical director of Cloudweavers and co-coordinator of the working group on SMEs of the EU ICT task force on competitiveness. He is also co-chair of the SIENA EU cloud initiative roadmap editorial board. He has researched on collaborative development and open source business models; recently he worked with public authorities like UK JISC and CENATIC on estimating the economic impact of cloud computing and the adoption of open source development models. He has developed the first Europe-wide macroeconomic analysis of the economic value introduced by the adoption of open source software, and is currently researching the strategies for increasing adoption of cloud services by SMEs.