SYMPOSIUM 10-13 OCTOBER 2011

DITTON MANOR, SLOUGH, UK

REPORT

Prepared by:

John Borras
Chair eGov Member Section

John Sabo
Chair IDtrust Member Section

OASIS
Advancing open standards for the information society

Introduction

The International Cloud Symposium focused on the unique attributes of Cloud computing and the important business and policy considerations that it raises. It examined the ways individuals and organizations are handling information and interacting with Cloud providers. The effectiveness of current international Roadmapping projects and standardization efforts was also explored. Together delegates and presenters charted the progress and helped to define a possible path to enable robust and trusted public sector Cloud deployments.

The interactive format of the Symposium allowed professionals from all around the world responsible for developing, influencing and managing policy from public, private and academic sectors to converge in a single location to share experiences on Cloud adoption challenges and barriers, as well as the latest developments in successful Cloud computing implementations. Also the evolutionary progression of understanding the implications of Cloud computing was addressed with respect to security, privacy and trust, and the significant contribution being made by OASIS and other international standards development organizations to addressing these major issues.

The specific topics covered during the Symposium included:

- Governance
- Legal impediments
- Security & Identity
- Privacy & Trust
- Interoperability & Data Portability
- Data Management
- Standards Roadmapping

This Report is an attempt to capture key ideas discussed and offers a general summary of the discussions. In some instances it presents the consensus of conclusions about the issues and barriers to full adoption of the Cloud by public sector bodies. It also sets out the plans OASIS has to take forward the issues raised and to continue its leadership role in this very important new aspect of public sector ICT.

As a caveat the editors recognize that this report presents only a flavour of the arguments, analysis and viewpoints offered by a stellar group of international experts. We do not wish to over-represent our content: this is truly a case where “you had to be there.” Having said that, we fully subscribe to the adage, perfection is the enemy of the good. And so on that basis we have put together this summary report using the notes taken by session moderators and the tweets posted on the Twitter account.

Full details of the Symposium, the presentation slides and a copy of this report are available at http://events.oasis-open.org/home/cloud/2011 . The list of all those involved in putting on the Symposium is contained in the Annex – Acknowledgements.

Observations

The following attempts to summarise the presentations and discussions from the various Symposium panels, which were organized thematically. It is clearly not possible to document every discussion point from a three day event like the Symposium but we have tried to capture major highlights. It should also be recognised that many of the issues cut across more than one theme, and that the expert panellists again and again addressed cross-cutting issues and presented overlapping solutions.

Governance

Many of the challenges related to the delivery of Cloud based services are not new ones. The need to address changes to business and operational processes, legal impediments and other non-technical interoperability issues are just as relevant for the Cloud as they are for existing e-Government programmes and other e-business initiatives. The technical challenges are also not new but they are of a lower order of importance in so far as information itself (and finding workable information governance and risk management policies) is more important than underlying Cloud computing technologies. To this point, it was observed at the Symposium that technologies are a commodity and that it is information that has value.

A key to ensuring a workable governance structure necessitates understanding and managing effective Cloud computing contracts and SLAs, and having standards-based metrics and instrumentation in place to ensure compliance. Gaining and utilising the experience of the evolving future of the Cloud will determine the success or otherwise.

It was suggested that the work of the OASIS Transformational Government Technical Committee (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tgf) was very relevant to this whole area as it is delivering a new governance framework for the delivery of government services.

Legal impediments

The legal challenges to widespread adoption of Cloud based services are seen by many as a real barrier. However many existing laws, case laws and risk allocation practices are today in place to inform cloud service providers, government policymakers and developers. Therefore this challenge needs to be kept in perspective.

There are new areas in which Cloud computing is impacting current legal structures and compliance practices, including:

- Cloud computing security
- Virtualization and hypervisor interactions
- Reliable messaging and transactional patterns
- Federated identity (of humans and organizations)
- Remote data storage access

The following are aspects that are not currently being addressed to any great extent and are seen as priorities for future legal guidance:

- Comparable Quality of Service measures
- Vocabularies for SLAs & “dashboardability”
- Data ownership and access
- Jurisdiction
- Identifier rigor
- Contract issues - scope, SLAs, liability cover, risk and governance.

The whole issue of Data Protection and inconsistent legal and regulatory regimes is seen by many as a significant barrier, and it was suggested that some attempt should be made to set out a set of basic criteria that all jurisdictions could include in their respective legislation. This would make it easier to harmonise regulatory frameworks and reduce data sovereignty problems.

It was also noted that there are extreme negative consequences for entrepreneurial activity in Cloud computing because of the fragmented legal and regulatory environment with respect to moving data across international borders, even within Europe.

Security

There are three main aspects to security (writ large) that need to be addressed; risk management, data classification and the use of open standards. There are different attitudes to risk management in the Cloud and security in different geographies. Industry and Government do not view risk in the same way:

- industry manages and accepts risks, manages it day by day and balances security spending against other business costs; in essence, risk issues are monetized and choices made about the cost/benefit of appropriate risk management controls and the management of residual risk;
- government for a variety of reasons does not monetize risk, and in practice treats risk management as the elimination of all risks.

There is a need to develop and leverage a common understanding of risk management in Cloud based services, and adopt sound risk mitigation practices.

Data classification is the second major issue. Granularity is required in classifying data beyond broad brush descriptions, such that appropriate risk management strategies can be applied. Clear principles must be applied to the use of public/shared infrastructure and services so that data may be protected as appropriate to their classification. This includes the use of encryption. These principles should include the fact that end devices may be compromised and that data which persists in the Cloud must be robustly maintained against failure of service or access. There are relevant laws (e.g. Data Protection Act) and information management standards (e.g. ISO 27001) which apply to these concerns.

The importance of open standards was stressed. For security experts, standards are NOT optional. The migration of applications to the Cloud should actually lead to the greater adoption of standards.

Identity

Identity management is clearly seen as one of the biggest challenges of Cloud Computing although the issues are very much the same as in other e-Government services. The main issues are seen to be:

- Identity - when services are offered via the Internet how can you trust the identity of the user? Identity providers need to be trustworthy to both the users and the service providers. A particular challenge is confirming a user's attributes while protecting privacy.
- Authentication - using the Cloud changes the risk profile and demands a more flexible approach to authentication. The risk may vary depending upon the location of the user, the device they are using, the nature and size of the transaction. Stronger technologies (like PKI) need to be deployed to support versatile authentication where proof is dependent upon the context.
- Administration - organizations should avoid duplication of identity administration by using existing standards (like SAML) and technologies like identity federation.
- Authorization - there is no common standard authorization model adopted by Cloud service providers and yet granular access control is a key requirement. The XACML standard provides a good match to the requirement and should be more widely promoted and adopted.

- Auditing - a major missing component is auditing. There is work taking place within OASIS to develop standards for this area.

It was noted that in Europe the STORK project is focussing on the interoperability of national eID infrastructures and is based on traditional Member State to Member State trust arrangements.

Privacy & Trust

There is no agreed definition of privacy and there are many varied perspectives of what it encompasses. But as with other aspects there are very few new privacy issues that are specific to the implementation of Cloud based services. Some key aspects of different interests were identified:

- User interests
  - Authorized access – can third parties access my data?
  - Unauthorized access – is my data protected against intrusion and loss?
  - User access – when can I not obtain my data?
  - Availability – on the sale of the Cloud supplier to another provider, can I still retrieve my data?
  - Government access – can governments obtain my data?
  - Law Enforcement – what is the standard for national security?
- Authorized Access
  - There is the need for the adoption of frameworks that put service providers and users in control and then extending beyond the framework level principles into business practices
  - Outside audit – there is the need to verify that data flows and privacy controls are what they claim to be
  - Harmonization of privacy laws – there is a need to harmonise laws across jurisdictions
  - There is the need to promote the strong rule of law
- Government Access and Policies
  - There is currently no treaty or convention in place addressing government rights/practices for access to information
  - It is unlikely that a single set of rules can resolve these issues
  - There are three possible approaches to improving things: harmonizing standards across countries; defining “reasonable” demands; defining “exorbitant” demand
  - the promotion of strong standards for government access is seen as key
  - there is a need to resist demands for jurisdiction-specific storage

Interoperability & Data Portability

These two themes are seen by many as perhaps the major barriers to Cloud adoption. Without guarantees of the ability to transfer data from one Cloud service provider to another, public sector organisations may under-utilise public clouds and possibly private clouds. Also interoperability between services in different Clouds is essential and again the lack of this facility may prohibit the take-up by the public sector. The solution to these concerns is not necessarily a technical one but more one to be handled by Contracts and SLAs. It is also imperative to utilise open standards to enable the easy transfer between providers.

Data Management

There are two major areas of concern under this heading. The first is the variation in Data Protection regulations across the globe which gives rise to the significant issues around data sovereignty. Most governments have very strict rules about data sovereignty and not allowing data outside of their jurisdictions, but this is primarily because of the lack of trust in the Data Protection regimes of other countries. A common approach to the basic rules of Data Protection would help obviate the data sovereignty problem. Secondly and allied to this is the question of data classification. Again there are

wide variations on how data and information are classified. Data is mostly classified at the record level rather than at the element level. Having a common approach to classification and applying that at the data element level within Cloud based services would significantly help the whole data management and data handling issues.

Standards Roadmapping

The work of the two Roadmapping projects, i.e. Siena and NIST, is seen as extremely important and all participants should continue to support and monitor their work. Both projects will be posting their final reports for public comment in the near future and everyone is encouraged to provide responses.
The benefits of these projects are seen as:

- Identifying priorities for resources
- Limiting the replication of work
- Identifying and limiting overlap
- Encouraging unification and liaison
- Encouraging appropriate representation and key requirements into existing efforts
- Promoting user input as essential to focus on requirements – especially "higher up the stack"

It was noted that interoperability is of prime importance to the European Commission and is the second pillar of the Digital Agenda for Europe. The EC is working on a guideline to allow for competition and avoiding lock-in as part of a new standardisation framework package, which will be presented to the European Parliament later this year.

It was also noted that NIST is building a *USG Cloud Computing Technology Roadmap* focused on the highest priority security, interoperability and portability requirements and gaps, as well as leading efforts on developing standards and guidelines in close consultation and collaboration with standards bodies, the private sector and other stakeholders.

SDOs Responses

Authoritative representatives of bodies generating standards and best practices regarding Cloud computing responded to the challenges and concerns raised earlier in the Symposium. The contributions generally focused on the private sector but emphasized their relevance to the challenges confronting the public sector too. The speakers demonstrated the many different approaches to building standards and creating best practice models, also indicating that the "Cloud" is currently a very broad concept permitting different and to some extent divergent models. The relevance of experience regarding SOA was frequently stressed. The core desiderata were seen as open approaches and recognition that interoperability is essential. It was also emphasized that standards bodies should be as responsive as possible to industry needs, and that the latter are themselves evolving very rapidly.

International Initiatives

There were several presentations from international Cloud leaders from Europe, USA, UK, Singapore, India, and China. In each case it was clearly evident that there are extensive public sector Cloud activities underway. In the Western countries, the focus was mainly on improving government ICT. In the Asian countries, public sector Clouds are generally seen as more broadly targeted at supporting government services, research, and enterprise computing.

China has the largest initiatives underway. Singapore is planning to use public sector Clouds as regional resources. In India, the potential for international Cloud outsourcing is being discussed. In Europe the EC is working on issues such as e-ID in cross border Clouds. The UK is developing a coordinated government Cloud strategy. In the USA, there is a decentralized government Cloud initiative driven by Federal CIO mandates, procurement guidelines, and NIST Cloud Technology Roadmaps.

Continuing information exchanges and coordination across international public sector Cloud activities is seen as a very valuable exercise and one that this community should continue to undertake.

Twitter and the Symposium

A Twitter account (#intcloudsym) was set up for use during the Symposium to capture questions and comments during the sessions and the following are a selection of the "tweets" posted by those present and their network contacts. They give a good summary of the diverse opinions of those responding to the presentations and discussions amongst the panel speakers.

"Security needs standards; you can't do security without standards"

"Cloud is not all or nothing. Management and orchestration of cloud services for consistent security and governance are key"

"Ultimately how different are public sector issues over cloud solutions compared to the levels of outsourcing in central Government?"

"Most of the Cloud is not new - virtualization, network accessible, distributed, hosted... these are the foundations of cloud computing"

"Defining the standards around data & securing the data should be the priority rather than defining standards for securing the devices"

"Reusable components and open standards are critical for information assurance"

"We don't need to go and develop lots of new standards because we have something called Cloud"

"Industry and Government do not approach risk in the same way, industry accepts and manages risk whereas Government tries to eliminate risk"

"Ability to extend existing enterprise Information Assurance Management to the Cloud is a key challenge"

"Widespread Cloud identity is impossible without stable open standards"

"Auditability is an absolute requirement"

"There is a need to strike a balance between price & security for Cloud to become a reasonable place in which to do business"

"The number one driver for moving to Cloud computing is flexibility, not cost savings"

"The lack of open standards for Quality of Service and heterogeneous service management are real obstacles to cloud contracting"

"Between the Patriot Act and EU-related FUD there is better protection from government interception in the US than in the EU"

Conclusions

Flowing from the diversity of views, the overlaps, and the commonalities, there are a number of usable conclusions from the three-day Symposium:

1. There is a very compelling need to continue the dialogue between public sector officials, industry and SDOs over the deployment of Cloud based services by the public sector. The participants in this Symposium form a very useful nucleus for this need and efforts should be made to maintain and grow the community.
2. Many of the issues and barriers to the adoption of the Cloud are not new, and there is a need to focus on the fundamental business, operational, legal and semantic issues before worrying about the technical issues.
3. With the scale that the Cloud can deliver, there are strong economic motivations for open interfaces because they will drive truly broad adoption to take advantage of that scale. But governments need to be clear on what they aim to achieve from adopting Cloud computing, which might include enhanced applications for civil servants, save money, reduce the burden on the taxpayer, and/or provide better services for citizens.
4. The development and deployment of Cloud based services is still in its infancy and an evolutionary approach to implementation should be taken until much more maturity comes through in the market delivering the real needs of end users.
5. Standards are essential for Cloud deployments and are beneficial for the economy as a whole because they broaden choice, foster the emergence of new markets and provide a tool to speed up the time for innovation to reach consumers. There is a great deal of cloud-related work underway within the various standards bodies. This work, as well as the applicability of existing e-business standards, should be examined very closely before there's any attempt to establish new standards specifically for the Cloud.
6. The legal and compliance issues around Contracts and SLAs require a new skill set for public sector bodies to fully understand what is possible with purchasing and maintaining effective and efficient Cloud based services. One part of this is to fully understand who the supplier is and what their supply chain is.
7. Governments seldom know the true cost of their current services and hence cannot judge the cost benefits of new Cloud based services. This area of costs and benefits over time needs greater attention.
8. Attempts should be made to align data protection and privacy regulations across the world to enable robust, trusted cloud deployments.
9. There is a need for shared forums to discuss risk management and to determine how to develop and standardize improved risk management metrics.
10. More guidance to architects and engineers is needed, especially on interoperability. A certification and accreditation system to reduce the burden on industry and government with a conformity assessment system is required. Testing needs to verify that the specified functions are actually in place.
11. Clarity is required in classifying data beyond broad brush descriptions, such that appropriate risk management strategies can be applied.
12. The Roadmapping efforts by Siena and NIST are extremely important and alignment between the two projects is essential. Involvement of the Asian community in this work is to be encouraged.

Way Forward for Further Action by OASIS and Other SDO's

The following actions may advance the various issues and recommendations identified in the Symposium and can go a long way towards helping the delivery of robust, trusted cloud deployments. As OASIS was the principal organizer of the Symposium, they have an OASIS focus. However, collaboration across the policy, technical and SDO communities is essential if we are to address barriers to Cloud adoption in the public sector.

1. OASIS to maintain and attempt to grow this Symposium community with a view to a continuing dialogue on Cloud related issues.
2. OASIS to appoint a Single Point of Contact for all Cloud related work to co-ordinate the promotion of the various strands of OASIS work and also deal with enquiries from the outside world.
3. OASIS to host a follow-up Symposium in Autumn 2012 in USA to review progress on the various issues raised in this event. A further follow-up in 2013 in Asia could be a possibility.
4. OASIS will liaise very closely with ETSI and the European Commission's DG INFSO on future work programmes arising from their recent "Standards in the Cloud" event.
5. OASIS to attend the planned workshop outside Washington D.C on March 20/21 hosted by the Cloud Standards Customer Council.
6. OASIS will coordinate with SDOs and other forums involved in Cloud standards work to clarify their focus and identify which aspects of Cloud they are addressing. This will benefit standards development efforts and help reduce confusion in the market place and with end-users.
7. OASIS to continue its participation in the Siena and NIST projects.
8. All participants are to be encouraged not to re-invent wheels and to utilise and build on current efforts to resolve the various issues highlighted in the Symposium.

Annex - Acknowledgements

OASIS would like to acknowledge and thank all the following organisations and individuals for their help and support in putting on the Symposium.

Partners

Cloud Best Practices Network
SIENA Initiative

Sponsors

CA Technologies
IBM
Microsoft

Organising Committee

Peter Alterman, U.S. National Institutes of Health (NIH)
John Borras, eGov Steering Committee
Peter Brown, official of the European Parliament (on leave)
Daniel Caprio, McKenna Long & Aldridge LLP
Carol Cosgrove-Sacks, OASIS
Roger Dean, eema.org
Jane Harnad, OASIS
Bob Marcus, G-Cloud Group
Neil McEvoy, Cloud Best Practices Network
Silvana Muscella, Siena Initiative
Steve Mutkoski, Microsoft
Ian Osborne, Intellect UK
Bruce Rich, IBM Software Group
John Sabo, CA Technologies & IDtrust Steering Committee
Anil Saldhana, Red Hat and IDCloud Technical Committee

Supporting Organizations and Media Outlets:

NIST
ENISA
World Economic Forum
Object Management Group
Open Data Center Alliance
Cloud Security Alliance
eema.org
Cloud Times
ECM Plus
Kantara