



The European e-Identity Management Conference
eema's 22nd Annual Conference
June 25-26 2009, London, UK

Conference Report

eema's European e-Identity Management Conference and the association's 22nd Annual Conference was held in the heart of London, UK. For those of you unable to attend, here are just a few of the topics discussed.

Day 1

Welcome and keynote sessions

eema chairman David Goodman welcomed delegates and thanked the sponsors, without whom the conference would not have been possible. After explaining the work that eema undertakes on behalf of its members and the broader IT community, he voiced some thoughts on the future role and importance of e-ID. He described a key theme going forward as that of convergence, and from the point of view of a Telco, that represents huge potential: some 5 billion people are likely to be 'connected' by 2015, Web 2.0 is a massive opportunity, and the Telcos are poised to influence the market with appliances, infrastructure etc. The challenge is how to ensure connectivity 'anytime, anyplace'.

In his view, the future lies in subscriber-centric networks catering for cellular customers, domestic broadband customers, teleworkers etc. However, at the moment Telcos are only beginning to realise that silo networks and silo data do not work in the new model. There is a need for a subscriber-centric data layer. Telco 2.0 is the opportunity to bring the internet and Telco worlds together. The IdM framework going forward will be another pillar of convergence, and in his view the Telcos are in a strong position to influence the eID debate.

June Leung, OASIS

June Leung outlined the evolution of OASIS, explaining how the organisation had moved away from the 'PKI' word because no-one wanted to be associated with it. OASIS today focuses on four themes:

- Identity and the trust infrastructure
- Trust policies and enforcement
- Emerging issues
- Education and outreach.

Kim Cameron, Microsoft

Kim started by outlining claims-based access and how it works, stating that the goal is to be able to move identities from one context to another. At the moment, there are commonly accepted standards, although others are likely to appear; interoperability has been proven; platforms are being built with claims inherent in them; and there are many proofs of concept. However, there are also many non-technical hurdles to overcome such as business models, legal framework, governance, the lack of understanding of claims and how to benefit from them on the part of developers, and the problem of multilateral security. In terms of multilateral security he made the following observations:

- There is a need to pessimistically evaluate threats (insider, social engineering, organised crime etc)
- Systems must fundamentally distrust each other: sharing vulnerabilities is bad
- Minimal disclosure is fundamental in a federated world.

In conclusion he asserted that privacy is not opposed to security but is a precondition for multilateral security. For example, we can prove we are not on a list without revealing who we are; and identifying the masses is not likely to identify the criminals.

Howard Schmidt, Information Security Forum, R & H Security Consulting LLC

Howard started by outlining some different visions of what eID actually means. For example, for the UK Government it means an easy way for people to prove who they are; in Germany the view is that it should be a safe tool for proving identity within the context of the internet; in

Italy it is seen as an electronic authentication mechanism; ENISA views it as a gateway to personal information; and Wikipedia defines it as electronic proof of identity.

He cited what he saw as some of the main impediments to eID as:

- Trust
- Culture
- Cost/benefits
- Competing solutions
- Cross-border compatibility
- Aggregation and mapping of data
- Biometric maturity (now getting there)
- Usage for the disabled (no one-size-fits-all solution)
- Conspiracy theories (the Government will know all about me).

In summary he said that eID is not a perfect countermeasure against cyber threats but can go a long way; eID cards can help to secure identity, but may also provide a target for criminals; and that the debate surrounding national security vs privacy is not yet concluded.

Tim Brown, CA, Inc.

Tim looked at identity in the context of cloud computing. While there has been some success in terms of collaboration, federation and authentication services; and in managed security services (providing customised identity services), adoption is not yet widespread. Today, however, we are on the verge of new opportunities for identity services in the cloud.

For example, at the moment, most enterprises simply add new people into their directory and give them privileges. This creates administrative problems and risk in terms of trying to understand who has access to what; and provisioning and deprovisioning becomes an impossible task. This model may not work well into the future. Possible cloud services include collaboration, user provisioning, authentication, authorisation, federation, data loss prevention, role management and log management, enabling enterprises to:

- Delegate administration to partners rather than adding individuals themselves
- Recertify access automatically
- Audit and create reports automatically
- Add other services such as role management and log management.

The end result would be decreased cost, decreased risk and improved compliance. In Tim's view the path to eID must be phased, requiring the use of old and new models, a combination of on-premise, off-premise and managed offerings and 'smart administration'. The catalyst for change will be collaboration and data sharing.

Mary Ellen Callahan, US Department of Homeland Security

Mary outlined the DHS's 'Fair Information' concepts involving:

- Limitation of collection
- Data quality
- Specific purpose
- Specific use
- Security safeguards
- Openness
- Individual participation
- Accountability.

She then described how the US-VISIT programme has been implemented to enhance the security of visitors and citizens; to facilitate legitimate travel; to ensure the integrity of immigration procedures; and to protect privacy. The programme was inaugurated following 9/11 and involves the collection of biometric data. As Mary said, with some 110 million biometric records, the need for integrity is vital, and privacy has to be 'operationalised'.

Day 1 Afternoon

In the afternoon of the first day delegates chose from two breakout tracks, one organised by **eema** and the other by OASIS. The **eema** sessions focused on national eID interoperability and mobile eID.

Theo Hooghieemstra, ICTU, The Netherlands

For example, Theo outlined the Dutch eRecognition Agreements Scheme for business-to-government transactions. The project was initiated to provide a safe, reliable and easy means of interaction between business and government; and that requires identification, authentication, authorisation and digital signatures. The problem was that there were no universally applicable solutions available: whilst many major providers had their own scheme, they were for their own services only and small providers had no means available to them. Furthermore, because of the need to use a different means for each service provider companies were confronted with a digital key bunch.

There were three main preconditions for the project:

- **Functional:** capable of supporting several reliability levels; and able to distinguish different users within one company from each other
- **Legal:** principle of privacy by design, complying with Dutch and European regulations
- **Technical:** open standards, internet technology.

Theo said that eRecognition is a two-sided network, meeting the needs and desires of business and government regarding easy, safe and reliable electronic interaction. Already, following market consultation, customers are creating an agreements scheme, working groups are in place, and a large-scale rollout should start early 2010.

Dave Birch, Consult Hyperion

In the mobile eID session Dave described how contactless technologies will change the eID landscape, first outlining a few problems that we face:

1. We need eID for eBorders and eBay for the 21st century and not for something discontinued in the 18th century; and what people may think of as common sense is not always right. For example, an eBorder application may need to know who you are, but for eBay, which is based on reputation, you may need only to know something about the seller, such as how many stars he/she has.
2. Legacy solutions may cause a problem. For example, chip and pin cost millions to implement but fraud has escalated. In this case the technology has been subverted by legacy systems and the chips can be copied.
3. Many try to use eID to solve paradoxical problems. For example, a mother wants her son to be safe in a chat room so she wants all the details of who else is in it but will not disclose her own details: full disclosure for you but not for me.
4. Proof without disclosure. If you wish to report a wrongdoing, you need to identify yourself, but if you have to do that, you lose anonymity and are likely to withdraw any complaint.

In Dave's view we need to implement utilities that are regulated, convenient for users, without the need for special gadgets, extensible and symmetrical. However, while we have many technologies at our disposal, we lack vision, having 'cardboard age concepts and computer age systems in communication age contexts'.

eema Fellowship Award

After the conference sessions on Day 1, a drinks reception was held in the exhibition area, during which the **eema** Fellowship Award was presented to Jon Shamah of EJ Consultants for his outstanding contribution to **eema's** work. Jon is a highly active member and board director of the association, as well newly appointed vice chairman. Congratulations Jon!

Day 2

On the morning of Day 2 the **eema** sessions focused on IAM securing identity.

Stuart Hodkinson, Courion UK

Stuart discussed how to deliver IAM projects on time and within budget. Many IAM projects fail to deliver because:

- They are too big and take too long to implement
- Flexibility is sacrificed in the pursuit of security
- Products rather than solutions are acquired
- There is no consultation with business.

To implement a project successfully it is necessary to:

- Select a solution rather than a product
- Make sure that the price is fixed for both product and services
- Consult with the business at all stages
- Prioritise activities based on strategic needs (access control, compliance, efficiency)
- Deliver quickly and incrementally.

Stuart then described a customer implementation within the financial services sector.

Florin Lupescu, DG INFSO, European Commission

Mr Lupescu's talk, entitled European Large Scale Action (ELSA) on Future eID infrastructure – A new EU initiative, described the Commission's initiatives and vision for the future of eID. Under the social contract of today the state owns your identity, but the digital contract will put it back in the hands of the user. Within the EU framework for digital identity, the STORK project will demonstrate cross country interoperability. However, while technical progress may be fast, political and legal challenges will take longer. For example, governments throughout Europe will wish to preserve their sovereignty, and will not want to relinquish any part of that for the digital contract. ELSA therefore goes beyond technical, local issues and focuses on co-operation between Member States.

STORK workshop

On the afternoon of the last day a packed session discussed the latest developments in the STORK (Secure Identity Across Borders Linked) project. The purpose of the meeting was two-fold:

- to provide general information to those interested in the progress of the STORK project and to give them the opportunity to raise questions
- to continue the process by which industry can contribute to the evolving STORK project. A previous meeting had thrown up several themes worthy of further exploration with industry.

An introductory presentation was made by the project team; and this was followed by a 20 minute presentation of the latest strategy document produced by the EU in response to the economic crisis: 'A Strategy for ICT R&D and Innovation in Europe: Raising the Game' by Aniyar Varghese.

There followed further presentations from the project team, to keep industry abreast of progress and to introduce added pilots. A specific call for assistance was made for support in reviewing documents, with previous valuable input acknowledged. It was announced that there was an intention to hold workshops with specific themes and new policy statements. All were urged to follow progress on the STORK website and to offer help where sought. Also, a request was made concerning scrutiny of how new and emerging technologies might fit into the scenario.

The floor was then opened to questioning from the industry representatives, and a lively debate ensued.

***The presentations can be downloaded from:
<http://www.eema.org/index.cfm?fuseaction=events.content&cmid=394>
Remember that you will need your logon and password to access them.***