

Conference Report

The European e-Identity Conference and eema's 21st Annual Conference Managing Employee, Citizen and Private Identities The Hague, The Netherlands June 10–11 2008

This year's Annual Conference took place in the beautiful city of The Hague, where some 150 delegates from around the world convened to discuss and debate the latest issues in eID technologies and services. We would particularly like to thank the Municipality of The Hague, ENISA and the UK Department of Trade and Industry for their support. We also thank our numerous sponsors: Cyber-Ark, Novell, BlackBerry, CoreStreet, DigiNotar, Grabowsky, ING, Microsoft and PricewaterhouseCoopers. Below are just some of the highlights from the conference.

Day 1

Plenary session

David Goodman, eema chairman, opened the proceedings by welcoming delegates and providing a background on how the industry has evolved. eema has advanced with it, and is today focused on digital identity technologies and services. As David predicted, by 2020 digital identity will have a significant impact on everyone. The building blocks for the infrastructure are already in place but the current model is not scalable: we need an industry-wide strategy to make it so. The question remains, who should be the major players in terms of moving it forward? eema's role is to provide a place for them to come together and resolve these issues.

Welcome address

Frits Huffnagel, Vice Mayor of The Hague, was in buoyant mood following Holland's defeat of Italy in the UEFA cup the previous evening. He was clearly proud of the achievements the city has made. As he said, tens of thousands of people in The Hague are working to make the world a better place, and on May 28 a new campaign was launched: 'Be My Guest', to ensure that visitors feel at home and welcome. Mr Huffnagel is responsible for the marketing of the city, ICT and internal affairs, and he was proud to inform us that The Hague is host to three of the four Dutch Telecommunications companies, as well as being the headquarters of Siemens and a number of other international companies such as Royal Dutch Shell. Within the municipality, work is ongoing to provide excellent public service provision, which means making 100% of transactions available online. That in turn necessitates the implementation of secure identity access management systems, which is why this conference was so important to him.

Market overview: eidentity comes of age

Roger van Boxtel, CEO of Menzis and Chair of ECP.NL explained the development of ECP.NL and the issues of interoperability. The topic is high on the agenda for the European Commission, and it has recently launched an initiative to stimulate easy access to services using OpenID.

In the early days, ECP.NL was set up to resolve relatively easy issues within The Netherlands, but that was before electronic transactions became commonplace for governments, businesses and citizens alike. The traditional paper-based framework was no longer applicable to electronic transactions and ECP.NL developed an eBusiness Code of Conduct. What he termed the user-centric ICT revolution has now made deployment of OpenID of paramount importance; and the trend is now one of 'converge and merge', whereby technologies, markets, users, producers etc have developed growing interdependencies and vulnerabilities.

He stressed the need for users to be involved in the process of developing interoperable identity management solutions. In The Netherlands this is being addressed through the Authoritative Alliance, a body which brings together all stakeholders in a multidisciplinary forum to find solutions. The aim is to create a user-centric vision, and then a roadmap to achieve it.

The criminal justice perspective

Ian Blacker of the International Criminal Court (ICC) discussed the challenges of authentication in the context of criminal cases, by which he meant international crimes of so serious a nature that militia or governments could be involved, and the disclosure of a witness' ID could cause many deaths. Under such circumstances, witness protection is paramount.

The evidence collected by the ICC can run into millions of pages, and while it is quicker to move the data electronically, there is a risk of interception. As he said, as soon as a new technology comes out, there is someone trying to crack it. The main reasons he gave for using eID are: speed in the context of global participation; unreliability of local postage systems; and worldwide system availability for accelerating time to trial.

It took the ICC two years to develop their system, not least because the company they hired to encrypt their hard drives went bankrupt. Other challenges included: security versus convenience; intangibility of benefits; the integration of diverse technologies deployed throughout the ICC; and different identities and access rights. He saw the market for IT systems as being immature, fragmented, largely proprietary and unstable. In addition, the trend towards takeovers and mergers made it difficult to plan for long-term solutions.

Some of the main lessons learned through the implementation of the project included:

- Don't let the users say it is too technical!
- Ensure you have all the necessary skills on board before embarking on the project
- Understand that ICT sometimes knows better than the user
- Assess users' willingness to adopt new technology
- Create a strong business case.

The banking system perspective

Herco le Fevre of ING described the challenges of managing the bank's suite of 15 eChannels. The need for the highest degree of security possible is critical, and customers have a wide range of security devices. In addition, since 9/11 regulation has increased in terms of due diligence, money laundering and terrorism, which makes it even more necessary to know the customer and to be able to check transactions against business rules. In addition, initiatives such as SEPA (Single Euro Payments Area), which aim to create a level playing field for all parties necessitate a rethink of ID management in terms of what customers expect.

ING revamped its strategy two years ago, taking as its motto 'Easy *and* secure'. As Herco explained, customers expect their treatment online to be the same as that they receive face to face: they don't want to be just a number on the internet and they don't want to have to fill in forms to go from one application to another.

An example he gave was ING Online, an application in Central Europe spanning seven countries and seven user management systems. It was piloted in 2003 with software certificates, but the pilot demonstrated that the security was insufficient. The bank therefore switched to true PKI and smartcards. Following the introduction of SEPA a new, umbrella portal site was rolled out for all seven.

The business perspective

Dr Stefan Brands of Microsoft gave a view of how large technical companies view security on the internet. He saw the main online challenges as:

- Secure and convenient authentication
- Data sharing across services.

As he said, we do not have good authentication mechanisms on an online scale: we are still 'stuck on passwords', which tend to be reused and written down. PKI certificates are only used by advanced organisations, and then only on a discretionary basis. In the meantime, threats become more and more advanced. Emerging authentication mechanisms tend to be one-off solutions and lack the necessary framework. In addition, there is an issue with data portability.

He cited the main ingredients of any successful online scale authentication system as identity selectors and protection technology for claims. The identity selectors are claims-agnostic ways of retrieving claims from claims providers. The individual sits between the transfer of claims being made about him/her and thus retains control. The protection technology is complex, guarding against threats that can come from anywhere within the authentication chain, for example:

- Preventing the interception of claims
- Preserving the integrity of the contents of the claims
- Preserving the integrity of the source of authentication of the claims
- Preventing replay attack
- Preventing attacks by a claims issuer.

Microsoft is working on minimal disclosure tokens to issue claims securely and avoid unwanted traceability – a topic that was further discussed in an afternoon session.

Roundtable discussions

The afternoon of the first day consisted of a number of simultaneous round table sessions which proved very popular, and at times extremely lively, with some very different viewpoints being expressed by large numbers of participants.

Getting to grips with eID interoperability

Chaired by Danny Frietman of Marquit Analysts with panellists Jon Shamah of CoreStreet and Martin Linda of Siemens.

One of the questions that this group debated was whether or not there was a killer application to drive interoperability. There were a number of different views, for example:

- In Germany a workshop was held to bring together application service providers and present plans for interoperable eID, but no one killer application emerged.
- We cannot predict what the killer application will be. It will simply arrive and catch the public's attention. It will then be the role of government to put an eID strategy in place and enable the infrastructure. The government should do it because it is there to invest in the future. Companies will not do it without ROI.
- Governments are wrong to think that government services constitute the killer application. People interact with the government only three to four times per year.
- The US is doing for identity what the EU did with GSM: create a common technology. Once the GSM standards were in place a healthy and competitive environment developed. In the US FIPS 2021 has enabled the same environment for identity.
- eInvoicing could be the killer application for eID interoperability.

This was a fast moving debate and here are just some of the issues that were raised regarding progress in the EU and the role of industry *vis a vis* that of government.

- There is no real privacy interoperability model in the EU, we need a stronger umbrella framework. The lower the level of abstract the easier it is to standardise so there is a need to assess the right level.
- Users are reluctant to hand authority to governments.
- Government-issued documents are regarded as more trustworthy than, say, a document issued by an insurance company.
- Applications should not be rolled out before the complete eID infrastructure is in place, because until then there will be a need to keep all other systems running.
- The 1999 Digital Signature Directive was a flop and there is no adequate supervising authority to monitor CAs. The Directive envisaged the proliferation of a single identifier for electronic purposes and that is a broken model (a hotly debated view).
- National ID is not the same as eID. The National ID card should be the generator of the eID card, which could contain multiple identities and should be untraceable back to the National ID.
- How China develops will influence the EU. There are still huge issues of interoperability within the EU.
- Germany, Austria and Switzerland have some degree of regionality and rely on trust rather than Advanced Signatures.

Advanced privacy techniques for data minimisation

Chaired by Dr Stefan Brands and Caspar Bowden of Microsoft

Caspar and Stefan provided an overview of data minimisation principles and technologies for identity management. Topics included the identity meta-system, data protection legislation, identity policy, minimal disclosure tokens and identity selectors. Caspar started by explaining Kim Cameron's 7 Laws of Identity (www.identityblog.com), highlighting issues such as:

- Justifiable parties: users don't want the identity service to be aware of all their internet activities as with Microsoft Passport.
- Directed identity: the security token has technical identifiers which can be logged and consolidated with other logs to create a user profile.
- Pluralism of operators and technologies.

Microsoft uses CardSpace to supply to a Service Provider only those identifying data necessary to access the service. There is a difference between self-issued and managed cards. Self-issued cards consist of self-asserted claims; are stored locally; are an effective replacement for userid/passwords, as well as being easier to use; and eliminate shared secrets. Managed cards are provided by banks, stores, governments etc; are stored at the Identifying Party; only contain metadata; and can optionally be subject to audit.

Stefan Brands discussed federated identity solutions, highlighting the problem with identity silos. For example: user Alice is known in Service Provider (SP) A as Alice S; in SP B as Alice Doe and in SP C as A Smith. When we use an Identifying Party (IP) using Federated Identity SSO (Single Sign On) then the user Alice will be connected to the IP and the IP sends a generated number to the SP, in which proprietary system this number is linked to the identity the user has there. For example, 12345 = Alice S in Service A; 98765 = A Smith in Service C etc. In the IP the user Alice Smith is listed for Service A with number 12345 and for Service C with number 98765. The IP doesn't reveal to the SP the full names of the subject, so there will be no data privacy issue. However, now there is a concentration of profiles at the IP level which will increase the power of the IP to impersonate a user's identity: the IP insiders become all powerful. It will also be hard to find out that it was not the real user in case of disputes.

With minimal disclosure these problems are circumvented because the user is in control and can limit claims to what is minimally necessary to access a service.

Dinner at the Madurodam and the Patricia Doward Awards

In the evening delegates enjoyed dinner at the famous Madurodam miniature village, courtesy of the Department of Trade & Industry. For further details about the Madurodam visit:

http://www.travelpod.com/travel-blog-entries/teickhoff/holland/1191766440/tpod.html#ENTRY_LIST.

During the dinner **eema** Chairman David Goodman announced two winners of the Patricia Doward Award, which is presented to **eema** members who have made an outstanding contribution to the association. The first was to Robert Garskamp, whose sterling efforts were in no small measure responsible for making the conference a success, and the second was awarded posthumously to Henk Tobias, former **eema** chairman, in acknowledgement of his outstanding work in positioning the association to the forefront of our industry.

Day Two: General Assembly

The June Conference is also the venue for **eema's** General Assembly. David Goodman reported that 2007 had been a better year financially, and that the association's new structure and focus had proved to be the right move. He also announced the imminent launch of

eema's Fast Response Forum. Jon Shamah of CoreStreet, who has been heavily involved in **eema's** new strategy, was elected to serve on the Board of Directors.

Whodunit? The favourite game of your compliance officer

Henk Marsman of Deloitte said that compliance is about 'not having to do it in real life'. There are numerous models and standards around this ongoing process and the smallest atom within compliance is identity: identity ties a specific transaction to a specific time and to a specific user. The elements of identity include:

- The creation of the ID – not just a technical issue, but one which must involve, for example, HR.
- The symbolic representation of the ID and its properties
- The ongoing proof that the digital and physical entities are linked
- The process of destroying the symbolic representation when the physical entity is no longer there.

He then turned to corporate governance and described some of the challenges: account collisions due to conflicting IT processes, speed of being able to access an account, deleting entitlements, single identities for segregation of duties and log review. As he said, it's good to have a comprehensive log in order to detect when something goes wrong, and also to be able to prevent such issues arising. For example, you may be able to spot some strange activity and put an alert in the system, such as a person logging on repeatedly late in the evening and accessing Finance for no apparent reason.

Physical and logical convergence in identity management environments

Hans Krogull of Novell described convergence as the interface between systems involving the following:

- Interfacing of mission critical systems
- One card solutions for physical security and IT
- Software controlled processes.

From a business perspective convergence automatically reduces error, and increases performance and speed. With relation to identity it reduces costs and risks. However, because people's behaviour is difficult to change with regard to, for example, common passwords, there is a need to think differently about identity. The Novell vision encompasses five trust assurances:

- My identity is not compromised
- Resources are secure and available
- Data and communications are private
- Roles and accountability are clearly defined
- There is a timely response to risks and threats.

Hans then described a project that Novell had worked on for the US Government following 9/11, which was to deliver an access control system for government buildings. The company worked in partnership with others to provide physical access control using biometrics. The scan used was the back of the hand, as that recognises attributes such as pattern of veins, blood pressure etc without being intrusive. Having delivered the logic to combine systems and ensure control, the next move is to extend it into the area of green IT in terms of automatically turning off lights, servers etc.

Lessons learnt from real life experiences

Marc Sel of PricewaterhouseCoopers explained some of the challenges of implementing IAM and some lessons learned from three implementation models: in-house, implementation suite and best of breed integration.

The first case study involved the in-house use of Roquette/COBOL. It was expensive to maintain and inflexible. The company decided to implement an IAM solution, but while they are now on their third vendor, the original in-house developed solution is still being used.

The second case study involved a bank. They initially went for an in-house solution, then turned to a vendor. However, the users weren't happy with it so they chose another vendor...who stepped down. They have since returned to their in-house solution, and the exercise has cost them a great deal of wasted time and money.

The third case study involved an EU telecoms company. They developed an in-house system but focused on the technology rather than user requirements. They ended up with a system no-one could use, and are now implementing a best of breed solution from multiple vendors.

As Marc pointed out:

- The first scenario reinforces the message 'if it ain't broke don't fix it'
- The second scenario tells you to choose your vendor carefully
- The third scenario tells you to fix your organisational problems first.

The three necessary steps are: requirements, design and implementation.

What if your daughter brought him home?

Calum Macleod of Cyber-Ark Software started with some challenges. For example:

- Many companies are so concerned about ID that they neglect the very real threat from inside the company – within the IT department. To counter such a threat companies should monitor behaviour so as to try to prevent it. The majority of attacks occur after a disgruntled employee has left the company, so it is very important to ensure adequate deprovisioning.
- Another challenge is outsourcing. Since it is generally done to improve profitability, much is performed in countries where the workforce comes cheaply and background checks are inadequate. In such a situation, hundreds of people could be looking after a system, all with privileged access.
- In most companies there are more shared accounts than private accounts, which entails passwords. While password policies may exist, enforcing them is another issue. In addition, passwords are often duplicated or written down which decreases their security. Just to make things worse, 42% of private passwords are never changed from the manufacturer's default.

He went on to describe some of the specific attributes of Cyber-Ark Vault which solve the problems associated with managing passwords.

Holistic approach to secure your mobile information

Sanisha Patkovic of RIM started by describing the modern work paradigm and enterprise mobility. The handheld evolution has moved through connect, communicate, interact, transact and transform: all of which equates to business process reengineering, which is where the handheld's real value lies.

The security challenges, however, are increasing: while most PC LAN issues have now been resolved, the wireless world has a completely new set of challenges; and increasing complexity only multiplies them:

- Confidentiality: Does the system keep data secret?
- Integrity: Can data be changed or tampered with in any way?
- Authentication: Does the system know who is performing operations?
- Authorisation: Is the person allowed to perform the operation?
- Availability: Can it perform services when called upon?
- Reliability: Can it cope with sub-system failures?

These have to be balanced against corporate governance in an increasingly legislative environment while remembering what users want:

- Always-on, always-connected mobility
- Open, extensible platforms
- Downloadable applications

- Access to calendar, email, contacts, intranet/extranet

In addition, there are a growing number of external threats including, for example, 300 variants of mobile malware, all waiting to pounce on an insecure system. As Sanisha said, these new realities demand new approaches to security, requiring an end-to-end approach that focuses on the entire platform rather than the device.

Credential validation – critical for secure and usable citizen ID infrastructure

Jon Shamah of CoreStreet started by outlining the reasons for using PKI. However, as he said, it can take time to validate a certificate in a large organisation, and if multiple certificates are used, there will be even more delay. He went on to explain three models of credential validation, CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol) and distributed OCSP.

- CRL: He likened CRL to a phone book. It requires downloading, becomes large and unwieldy, and can use both time and bandwidth. Jon saw CRLs as an impediment to the adoption of PKI.
- OCSP: This is a better means, because it is more akin to 'dialling the operator' so that you only get what you need to know, and it is always the same size. However, it requires online access to the validation authority all the time, so needs to sit within the firewall: there are issues with security and resilience, especially with cross-border transactions.
- Distributed OCSP: This was the model put forward as the best, as it addresses some of the issues above such as security, speed and resilience. In this model all OCSP responses are pregenerated and presigned, and pushed out to responders, which can be located locally. Relying parties can go directly to the local responder. Another advantage is that the model is easily scalable.

In conclusion, Jon said that this model provides fast, local validation while maintaining centralised trust – which equates to high security; it is resilient, and provides simple and low cost scalability at low bandwidths.

Our next main conference is ISSE, which will be held in Madrid, October 7–9 2008. Visit the website: www.isse.eu.com and if security is your remit, come and join the debate.