

**JOINT 'ICT SECURITY' – 'ICT FOR GOVERNMENT AND PUBLIC SERVICES'
WORKSHOP ON
“Identity Management in the Future Digital Society”**

14 October 2008 – 10:00 - 16:30

Venue: Brussels, Avenue de Beaulieu 25, Room 0/S9

Agenda

Rapporteur: Jim Clarke, Waterford Institute of Technology



Workshop Report

Executive Summary

On 14 October 2008, a workshop was held with the purpose of bringing together major European initiatives in the domain of Identity Management in the future digital society, specifically the STORK project, which aims at cross-border recognition of national electronic identities, and several activities of the IST/ICT Research Program focusing on identity (FIDIS, PRIME, PRIMELIFE, PICOS, SWIFT, SWEB). The rationale for this workshop was that the FP6 IST and FP7 ICT program provide substantial support for activities in the domain of user-centric identity for life in the digital age as well as in the field of security and trust in ID cards and tokens. With the start of STORK, a major pilot project of the Competitiveness and Innovation Program, DG INFSO supports all together a significant amount of work in the area of identity management. Therefore, bringing the major actors together would greatly benefit a coordinated and effective European approach to this area.

The specific objective of the workshop was to prepare the ground for a wider involvement of a larger and open community and investigate the scope for an all-encompassing e-IDM system in the longer term as the basis for trust in the digital society of the future. In this context, the positioning and reconciliation of public and private identity schemes are a key issue. It seems important to ensure coherence to this area to enable the development of a competitive market in trustworthy technology and services, ensuring consistent user experiences and creating opportunities for European industry. With this in mind, presentations and discussions were held on a number of approaches being taken by Member States.

A number of building blocks on various levels were presented and discussed by the participants. These included ICT Research, Policy Support and Government as shown on Figure 1 (the "Market" layer was less addressed, but needs further attention). It became clear that the individual activities presented can contribute quite effectively together to an overall ID Management Meta-layer.

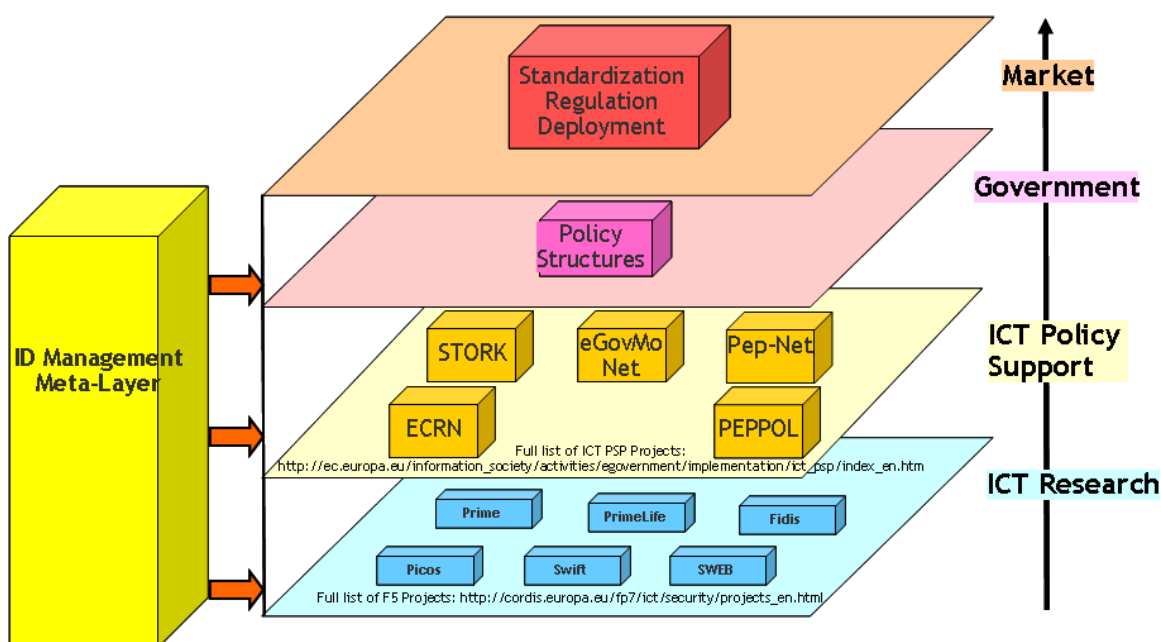


Figure 1. Layered approach to IDM communities

A number of concrete ideas were identified between the projects and participants for further actions. A full description of these can be found in the workshop report, but in summary, the main concepts identified for follow up included:

- It was agreed that all parties could work together on use cases to their mutual benefit. This could be done on a case by case or joint workshop levels. More concretely, further co-operation on the eGovernment use case was highlighted to be used for PrimeLife's privacy protection and data minimization technology.
- The participants from eGovernment domain can look further at the ID Metasystem paper to see how it fits within their environments: for example, if it is general enough to fit within their activities and provide useful feedback to the authors.
- STORK is a significant project driven by Member States for implementation of interoperable electronic identity across EU for eGovernment services. A common specification for interoperable electronic ID will be made publicly available. A number of use cases on interoperability will be tested and running for one year. Considerable potential exists for the ICT R&D projects that can give a good insight into the kinds of systems available or could be available in future.
- In the Belgian presentation, the need was discussed for the Member States administrations to agree on a minimum set of data to identify an EU citizen and coming to a common set of levels of trust. The links with the ICT projects could help with the definition of these aspects. For example, the projects could assist with a technical evaluation of the levels of trust.
- STORK will look at how to interact with the private sector (e.g. for financial services) – ICT projects could provide them initial links.
- The ICT projects could help assist with interoperability issues if encountered or provide lessons learned.
- It was discussed how it is vitally important for technologists to explain to the ones making the administrative systems and work flows and laws what technology can do to ensure privacy etc. The working together of these communities can enable this process to start taking off or at least defining the best way to do it.
- Some governments are already rolling out services and their feedback can be highlighted in future meetings (for example, Germany).
- Strategic and visionary approaches, including outside the scope of the current participants, should also be discussed together to plan for the future.

The workshop will be considered successful if these joint undertakings could lead to memorandums-of-understanding, mutually beneficial cooperative work, to scenario development for the projects involved and the ID meta-system paper and eventually to the activation of European stakeholders in the eID markets.

Table of Contents

Welcome and introduction.....	6
Introductory Keynote (setting the scene).....	6
Presentations of the Stork project.....	8
Presentations from the member states.....	10
Austria.....	10
Belgium.....	12
Spain	13
Questions/Discussions on morning session.....	15
Panel with project presentations focusing on research in digital identity management issues	16
PICOS: Kai Rannenber (Goethe University Frankfurt).....	17
SWEB: Petra Hoepner (Fraunhofer Institut Fokus).....	17
SWIFT: Amardeo Sarma (NEC Laboratories Europe).....	18
PRIME and PRIMELIFE: Jan Camenisch (IBM Zurich Research Laboratories).....	19
Recent work on user-centric identity meta system	20
Discussion	21
Wrapping up and next steps	22
Annex I. Agenda	24
Annex II. List of Attendees	25

Welcome and introduction

Jacques Bus (INFSO-F5), DG INFSO, Head of Unit for F5¹, Security, welcomed everyone to the Workshop and noted that it was very good to see so many constituencies involved in today's workshop. The objective of the workshop is to bring together the people from STORK project with the IST FP6 and ICT FP7 projects working on ID management to learn and benefit from each other. With this coordinated approach, it will be possible for the communities to bring ideas and work together with a strategic thinking approach to ensure we are going forward both in the short term and with a longer term vision on the future. In addition, in the afternoon, there would be a number of presentations on eID standardisation work for a longer term strategy as a result of the work of Reinhard Posch, Kai Rannenberg and Kim Cameron.

Mechthild Rohen (INFSO-H2), DG INFSO, Head of Unit H2, ICT for Government & Public Services², welcomed everyone and explained the rationale for the Workshop. When the Directorates first discussed about holding a joint workshop, it was decided that the STORK (Secure idenTity acrOss boRders linKed) project would be the most appropriate project to meet with the IST/ICT Research projects. STORK is within the ICT-PSP (ICT Policy Support Programme³), under the CIP (Competitiveness and Innovation Programme). CIP is the first program where projects are deploying technologies and one of major instruments is a large scale pilot. Stork is a large scale pilot addressing cross border interoperability between existing standards in Member States. The goal is a cross border specification to enable businesses and citizens to securely use their national electronic identities and get help from public administrations in any Member State they live in or travel to. It is recognised that there are many areas where joint research needs to be carried out and that was the reason to bring these constituencies together starting with today's workshop. It is expected that this will not be a once off event and the desire is to continue the mutual work together following the workshop. It was noted that there are other large scale pilots that also include e-ID aspects and it is expected that the initial workshop will identify ideas for future collaboration in both programmes and that we can proactively work together.

Introductory Keynote (setting the scene)

Malcolm Crompton, Information Integrity Solutions, explained his background. From 1999 – 2004, he was the Privacy Commissioner of Australia. Mr. Crompton started by observing that there had been two attempts at ID mgmt in Australia, one in 1988 and one few years ago. Both failed for non technology reasons and he has been advocating that getting privacy right is essential when developing ID mgmt systems, especially where government is involved. There is a need to talk outside our specialist fields & the joint workshop was a particularly good example of seeking to achieve this.

An extraordinary debate has been going on about how to exchange data differently than we were before. After 9/11 there was a period when almost any data exchange could be justified as contributing to the war on terror, regardless of any new risks to which individuals might be exposed as a consequence. More recently, this has turned around as Data Breach Notification law has revealed how poor information handling practices are in both government and the private sector. First introduced in California, it is now applied in 40 different states in US. On the other hand, while the EU doesn't have too much in this area currently, it has the concept under active consideration. However some regulators, including in financial services, are now requiring notice to consumers if data about them is lost or stolen as part of the institution's duty of care.

By way of example, Mr. Crompton noted that while US lose data at a rate of 1/3 per annum, it is very possible (and likely) we are losing similar amounts in the EU. In Australia, they

¹ <http://cordis.europa.eu/fp7/ict/security/>

² http://ec.europa.eu/information_society/activities/egovernment/index_en.htm

³ http://ec.europa.eu/information_society/activities/egovernment/implementation/ict_psp/index_en.htm

have no idea about the quantity of data loss and there is no evidence whether better or worse, so can only assume it is likely the same or worse.

Mr. Crompton explained his view on the concept of where is the individual when we “manage” “identity”. A succinct definition of “Identity” is hard to find. Our “Identity” starts out as a child, we grow up live in a family context and behave differently in those contexts. We have parents and they do things that affect our identities and behaviors in context. We start to work and this is now part of our identity. Some of this may be obvious but we need to have conversations like this to understand what our users have in mind when talking about their identity.

Mr. Crompton presented a Case study on the Australia’s failed access card. This failed due to loss of community trust, hidden agendas – lack of transparency. Eg. It was presented as “voluntary” yet was going to be compulsory to use for all interactions with Government, including Australia’s universal health insurance scheme Medicare. Hence the only Australians in practice who might not “apply” for such a card was the tiny minority who were both very healthy and very wealthy. It also involved a strong, intrusive, time wasting registration process quite out of proportion with the services it was espoused to provide, inadequate governance and accountability. Old website – www.accesscard.gov.au

By way of further setting the scene, Mr. Crompton noted the pace of technological change & the growing question mark hanging over current process based laws protecting personal information based on the 1980 OECD Privacy Guidelines. Even the person who chaired the OECD committee that developed the 1980 OECD guidelines, Justice Kirby, has recognized this. Some quotes from him:

“... technology will outpace in its capacity, the imagination of even the most clever law makers. ...

“Of course that is not a reason to do nothing. To do nothing is to make a decision.”

Justice Michael Kirby, High Court of Australia

IIA Dinner speech, 21 February 2008

http://iia.net.au/index.php?option=com_content&task=view&id=617&Itemid=32

The UK Information Commissioner has clearly reached a similar conclusion. Earlier in 2008, his office called for tenders on a review of privacy frameworks, remarking that:

“... the Commissioner believes that the time has now come to start a new debate. This recognises the pace of technological change ... [and] .. a growing feeling that the [EU] Directive is becoming increasingly out-dated ...”

Information Commissioner UK

Invitation to Tender – Review of EU Data Protection Law, 14 April 2008

www.ico.gov.uk/upload/documents/pressreleases/2008/invitation_to_tender_1404081.pdf

Mr. Crompton also emphasised the impact of cultural and history aspects on attitudes towards IDM. For example, in Scandinavia, citizens appear more willing to trust government with their identity, possibly through higher levels of trust through history of openness – FOI & stronger accountability.

He provided a link to relevant work on this thinking: “Use Cases for Identity Management in E-Government”, Robin McKenzie, Malcolm Crompton, Colin Wallis, *IEEE Security and Privacy*, vol. 6, no. 2, pp. 51-57, Mar/Apr, 2008

<http://doi.ieeecomputersociety.org/10.1109/MSP.2008.51>

Mr. Crompton presented a number of questions for governments including:

- How will you gain citizen trust where choice not an option?
- What is your agenda for stronger identity management?
- Are you willing to be transparent about your agendas?
- If you cannot be fully transparent are you prepared to be highly accountable?

- Are you willing to take responsibility for fixing failures?

Mr. Crompton concluded by quoting a senior specialist at Microsoft who had observed that “Identity isn’t a revenue situation. It’s an infrastructure situation”. In a nutshell, Mr. Crompton concluded that “User Centric Identity Management: It’s not an oxymoron, It’s inevitable”.

A paper that provides further background on user centric IDM can be found at “User centric identity management: an oxymoron or the key to getting identity management right”, which is online at http://www.iispartners.com/NZ_background_paper_29.04.08.pdf.

Mr. Crompton provided links to a number of other relevant papers that his company has written on the subject of user centric identity management and privacy, and they can be found on the publications page of the company website, <http://www.iispartners.com/publications.html>.

Presentations of the Stork project

Antonio Paradell (Project Manager), Atos Origin, SAE presented an Introduction to Stork⁴ (**Secure Identity across borders linked**). STORK is a Type A project on eID interoperability and it’s goal is the provision of Interoperable services with e-ID across borders. The project includes 13 member states from most of western EU + Iceland. It is currently lacking Eastern EU states. To account for this, there will probably be an extension in the future. The project started 1st June 2008 and will run for 3 years.

Frank Leyman (member of the project Executive Board), Manager International Relations, FEDICT, presented more details on the project.

The project vision is

“To simplify administrative formalities by providing secure online access to public services across borders when it comes to e-ID”.

The project mission is

“To develop and test common specifications for secure and mutual recognition of national e-ID”.

The project objectives are:

1. **Define** common rules and specifications to assist mutual recognition of eIDs across national borders;
2. **Test** in real life environments, secure and easy-to-use eID solutions for citizens and businesses;
3. **Interact** with other EU initiatives to maximize the usefulness of eID services.

The overall project approach is to develop a cross border architecture, build in a lab environment, build in real life environment and validate in real life pilots. This will enable conclusions for the Member States will a follow on project to implement in all the countries.

The Work packages were presented in the project phases

WP1-Project Mgmt

“**Definition phase**”

WP2 – eID inventory, trust and application groups

WP3 – eID and upcoming technologies

“**Architecture phase**”

WP4- eID process flows

⁴ <http://www.eid-stork.eu>

WP5 – eID and common specifications (Note: the idea is not to change what is in the MS already but to build on top of this.)

“Implementation phase”

WP6- Pilots (specification – definition – implementation – evaluation). It is the intention to keep up and running for at least 12 months for testing e.g. process flows.

WP7 – Communication and Sustainability.

The project is using open standards and an example would be a citizen from country A can access applications in a local environment in country B – “any to any” is possible for the citizen. The project will also work on helping the enterprise level. Security and privacy are serious concerns in the project and all efforts will be made to ensure that mutual recognition of e-ID is secure.

The desired Impact of the project will be smooth cross – border operation of several key public services interconnecting the countries.

There are three “buttons” to get involved:

1. Member state reference group – EC and consortium members, representatives of all EU MS not already in the project, will conduct 3 focus group meetings over a 3 year period.
2. Industry – open forum for industry
3. Community of Interest – e.g. press

For more information, please email info@eid-stork.eu

Jim Purves (member of the project Executive Board), UK Government Dept. of work and pensions, presented an overview of the pilots in WP6. There are a number of pilots including:

1. Cross-border authentication platform for electronic services, building a demonstrator showing that cross-border electronic services can operate in a number of Member States.
2. Safer Chat, to promote safe use of the Internet by children and young people.
3. Student Mobility, to help people who want to study in different Member States.
4. Electronic Delivery, to develop cross-border mechanisms for secure online delivery of documents.
5. Change of Address, to assist people moving across EU borders.

The initial deliverable for each Member State is to provide their use cases and within their use case to define the follow items:

- whether they are service provider identity provider;
- credentials to be used in the pilots;
- attributes to be transferred between Member States;
- initial view of architecture approach, proxy model vs. middleware.

An example Use case was presented of an Estonian resident who wants to work in Belgium.

The entire business process was defined and is summarized here (more detail in the presentation)

- The Estonian resident is required to enroll in the Limosa service on the portal.
- User clicks on the portal and redirected to the Limosa portal.
- The Limosa portal asks the resident where they are from. The resident selects Estonia.
- The resident is redirected back to the Estonian citizen portal
- The resident selects how they want to authenticate. The citizen selects their ID card.
- Resident authenticates with ID card
- Resident is redirected back to the Limosa portal. Limosa can now create a secure session with the citizen.

Note: all the actions with the Estonia portal are the business of the Estonia portal.

Another use case was presented on an Austrian resident authenticates to the German service-bw Portal. For the business process, the Austrian resident authenticates to the German Service-bw portal with their Austrian ID Card. The steps to follow are:

1. Austrian resident navigates the German portal, clicks on link
2. Austrian resident redirected to the German service – bw portal
3. The Austrian resident selects to logon and places their card in a reader. The portal via client side middleware detects the card and requests the user to Authenticate (without having to go back to the Austrian side.
4. The Austrian resident is authenticated on the German portal.

Summary of pilots:

- Implementation and demonstration of interoperability – starting June 2010
- Starting with services that exist
- The pilots will enable Evaluation to take place over a period of 12 months
- to re-inform/feedback to the common specification

There were a number of questions and discussions following the three presentations.

Q. From the presentations, authentication is generally provided by the government. Is the project looking at any other aspects? eg. Authenticating for financial services?

A. Yes, the project will look at how the Member States interact with the private sector.

Q. It is important for the citizen to know what kind of checking is going on e.g. going back to the Estonian web site. When there is an authentication happening, how much calling back takes place? Is there a middleware that holds the amount and definition of callback(s) that will happen. It might give the user more control of what they will have to go through.

A. It is something the project will look at. User consent is very important but the project will not be responsible for the back office processes but they will have to learn the systems.

Comment: We can have some further discussions during the Primelife presentations.

Presentations from the member states

Austria

Prof. Dr, Reinhard Posch (Federal Chief Information Officer Austria) presented the eID government approach in Austria (AT), explaining how it must be a holistic approach to meet the take-up and inclusion demands. With this it differs from the „conventional approach“ where the different phases of an eGovernment process are arranged fully independently. Only this next step of integration responding to the needs of the various steps of an eGovernment process offers the potential of both saving and enhancing comfort as viewed by the citizen.

As such, we need to closely view together the application and the result – which is the fully valid electronic document – and the delivery of the result. In all these phases, we also have to make sure that the customer is free to switch back and forth from electronic to paper. Professor Posch explained this fact makes the electronic process much more complex and asks for robust basic elements of eGovernment.

There are five steps in the conventional applications:

1. Application in paper (mail or in person)
2. Officer **taking decision** about ID and process. He is making the key decision
3. Process back office
4. Document processing and authentication
5. Delivery

Step 2 is key to this process where the receiving offices judges content, identity, signatures/ authentication etc. At this point, we see several degrees of freedom which make an electronic process complex and shows the need for a strict and formalized regime.

For the fully electronic system, the steps are instead:

- form fill in – with eID where needed
- government portal
- automated back office
- official signature
- electronic delivery.

Performing the same elements fully electronic – i.e. with the potential to avoid human intervention at step 2 for the conventional applications above – will lead us to:

- a system that is capable to electronically identify as needed;
- a system that allows the expression of explicit consent/authentication;
- a system that produces electronic originals with the value of rubber stamped documents;
- a system that can deliver and prove the delivery.

As seen, there are major changes – only the core process at the back office remains untouched and could even remain manual in some cases depending on efficiency.

What is the change associated with the changing from conventional to eID process?

- No human reading of application → web forms (automatic analysis)
- No human decision → machine providable ID (eID and mandates)
- No human intervention → Formalised process
- No rubber stamp and signature → Official signature
- Need for a proof → Electronic delivery

There are a number of legal assumptions that must be considered. These are:

1. We have to be sufficiently assured of the identity of the person making the application.

- not depending on the application type
- ie. Legally no basis for security classes for citizens
- AT: IDENTIFIED or NO ID CHECK (very simple situation used in Austria)

2. Data protection is the major issue

- eg. Cancer registers, tax, education,...
- Austria: eID everywhere usable – including private sector – but sector specific not cross sector traceable.

With regard to access security, the Austrian approach has three cases, 1 – 2 without the need for ID and 3 with the need for ID.

1. Open Access – no specific security provided/needed. Typically general information.
2. Pay and Get service - Business oriented service delivered by administration eg. Parking, garbage, gas,...
3. eID to get access - whenever identity related, relevant data held by the administration or delivered with previous applications us used for processing or delivery with this service.

The eID implementation – Austrian approach can be characterized with:

eID

- crypto, sector specific mapping of unique identifier
- qualified signatures to authenticate – inheriting security
- standard XML-records – SAML based

Mandates

- to enable businesses – contribute to eInclusion
- to comply with existing legal regulations

Middleware online

- lessons learned: installation a major hurdle

- moving to browser based situation

data protection and mandates are key elements for eGovernment

there is an urgent need for an “installation free interoperable system”

Cutting red tape: no prior registration to applications

- get there and do it!
- **instant eGOV everywhere with single eID**
- **over 2500 communities i.e. several thousand autonomous government agencies**
- **eID needs a data protection aware infrastructure**

The Austrian approach uses **middleware online „BÜRGERKARTENSTRATEGIE 08“**

- **cope with the need of the service directive**
 - giving full and legally recognized access
 - enabling and enforcing legal constraints (e.g. delivery and deadlines)
- **having regard to practical issues**
 - very rare use with high demand on security
 - including electronic signature for applications where appropriate

With regard to eID implementation in EU, there are a number of constraints:

- **legal**
 - governments are bound to their legal framework when it comes to eID
 - interoperability is often not part of this framework
 - laws usually focus compatibility and exchangeability with paper processes
 - generally data protection and avoiding divides are major legal concerns
- **organisation**
 - applications are implemented making additional „de facto assumptions“
 - these assumptions like „security classes“ often lack legal background
 - organisational constraints usually are not well specified
- **technical**
 - as the lowest layer this inherits the constraints from ORG and LEGAL
 - standards available :: SAML etc.

Belgium

Frank Leyman (Manager International Relations, FEDICT), described the approach of Belgium which uses a building blocks approach. There are the different Ministry: Ministry A, Ministry B,, Ministry Z. The Ministry's are responsible for their unique databases. FEDMAN stands above these databases without changing the lower layers. The Federal Service Bus is an intelligent machine that knows where the data resides and rules of the game e.g. Who is entitled to know which data and where it can be used. Above this there is a National Portal Website, ie. the front door to the outside world.

The security layer encompasses everything and a smart card is the key that opens the door into the system.

eID is only an electronic key to open doors and is built for those who need a proof of identity: national and international and public and/or private sector.

eID is one of the building blocks. There are three databases – one for Belgian citizens (broken into > 12 years and Children <12 years), one for foreign residents and one seeking citizenship. However, cards are treated in the same way and not differentiated.

Card has protected data (PKI) and flat data for identity purposes ID, Address, ...

Therefore, there is a requirement for the Member States to agree on a minimum set of data to identify an EU citizen.

There are 5 Levels of Trust (L.o.T) in Belgium that are applied even though no law behind them: There is a table in the slides describing the levels.

Therefore, there are two requirements

1. MS to agree a common set of levels of trust.

2. The owner of the application decides on the required L.o.T.

The link with the Stork process was discussed and it has 6 steps:

1. Citizen connects to Service provider
2. request connection to originating country authentication provider
3. authentication (eID card)
4. additional attributes gathering
5. identity transmission to service provider
6. service open to citizen.

With regard to International eIDM:

- Layered model also at international level
- Only CA of origin can validate its eID's
- Preferably only one C.A. per country or one national C.A. gateway per country
- PEPS model
- National eID's only guaranteed by national (public sector) CA's
- Bilateral agreements in the mean time
- Need for an EU legal framework
- Back-to-back liability to be defined

Question: Seeing Austria and Belgium is very revealing about what has to be overcome. From the security perspective, is there anyone in STORK looking at distributed Federal databases of identity data.

Answer: No. The approach being taken is centralized access (eg. XML) but the data is not centralised.

Spain

Miguel Alvarez Rodriguez (Ministerio de Administraciones Públicas) presented the current national scenario for Spain with eID:

- PKI digital certificate is the most common solution for eID as well as for digital signatures
- Lively market for CAs: 12 recognised CSPs by the Ministry of Industry's QC issuers
- Important uptake in the usage of QC in recent years more than 7 million QC already issued
- Since 2006, issuing of national eID card
- Killer application since 2000 is the Tax Declaration. **Early return of payments if submitted over the internet (10 days)**

An insight into accredited CSPs in Spain:

- Public CAs
 - Royal Mint: More than 2M certificates issued
 - Police Directorate: National eID card: More than 4M cards issued and expected to reach the whole population over the next few years
 - Regional PKIs: Set-up by the Governments of Catalonia, the Basque Country and Valencia
 - Issuance fee is mostly free for the holder
- Private CAs
 - Mainly focused on Professional Bodies: Lawyers, Chambers of Commerce, Public Notaries, Enterprise Certificates, Civil Servant Bodies...
 - The issuance cost is supported either by the holder of the certificate or by the Professional Body

The National eID card is the main PKI in the country

- National eID (DNle) is the way forward from the traditional paper-based National Identity Card.
- Universal and mandatory Spanish identification card since 1937 and Schengen Territory Travel Document. There is no social rejection to its use

- 97% of the Spanish electronic records with personal data include the ID number of the DNI as the primary citizen identifier.
- Two digital certificates inside the chip:
 - One for authentication
 - One for electronic signature
- The roll-out phase has recently finished and reached more than 240 Police offices. In fact, 500K cards monthly issued in the country

The National eID (DNle) is the way forward from the traditional paper based National ID card. The CA is the Police Directorate, dependant on the Ministry of Interior Affairs. By end of year, it is expected that 6 million will have them, 12 million next year... and by 2014, the eID will reach the whole population of people over 14 years.

The main challenge in Spain is to connect the public administrations that are going to accept the certificates from the National CAs for access.

There are technical challenges

- accept certificates from many CAs
- install and maintain software for
 - validation of the authenticity and integrity of the certificate
 - interpretation of the content of the certificate
 - verification of digital signatures
- technical complexity increases with scale.
- The number of integration software components needed to process the certificates increases accordingly.

Launch of the national Multiple-PKI Platform:interconnection scheme

- Since eID and digital signatures are key enablers to establish secure eGOV services, the aim was to create a Broker of CAS or Validation Platform (VP) that allows eGovernment Applications to verify the status of all the qualified certificates and eSignatures created in the country
- The Validation Platform is the core element to facilitate among Public Administrations the use of the same digital signature formats and higher levels of trust for eID: Interoperability of different PKI solutions
- The connection to the service provides immediate eID and eSignature Features to eGovernment Portals for all the Qualified Certificates issued in the country (Multiple-PKI Platform)

Lessons learned:

- The VP is a cost-efficient and time-saving service providing eID and electronic signature features in a simple way. In fact, it prevents Public Bodies from investing in validation SW modules and other communications-related infrastructures needed to interconnect eGOV systems to every qualified CA verification service
- The uptake in the use of digital certificates in the public sector is encouraging the private sector to provide secure services based on the national eID card (i.e.: 12 banking entities already incorporating the eID card at on-line banking services)
- Spain is also taking part in the Large Scale Pilots on eIDM within the CIP initiative (STORK Consortium) and will integrate this national infrastructure to the future interoperability framework for eID to accept other EU eIDs

More information can be found:

- On the national eID card:
 - <http://www.dnielectronico.es/>
- On the Multiple PKI Validation Platform
 - <http://www.csi.map.es/csi/pg5a12.htm>
 - http://www.dnielectronico.es/seccion_aapp/platform.html
 - <http://www.epractice.eu/cases/1984>

Questions/Discussions on morning session

At this point in the agenda, there was a Questions and Answers session with the previous speakers:

Comment: With regard to distributions in Ministry databases. In Germany, the databases were decentralized by municipalities. Now there are a number of registers that are decentralized that may need to get accessed from a centralized point of view.

Question: In Germany, long ago, it was necessary to go to the police for these kinds of services. This changed to a more citizen-based service. Is there any stigma attached to this in Spain?

Answer: In Spain, there is no problem or social stigma or rejection with the citizens having to go to the Police directorate to obtain the National ID.

Question: Private companies are included in the process also in the Belgian model. How does this impact if you are **not** a Belgian company and wants to accept a Belgian ID?

Answer: Stork will help you there. A company can download a toolbox to read Belgian identities. You will need to build an application for this.

Question: There is a need for core biographical data needed, how do you manage this when you have municipalities issuing these. Is there a centralized process that sits behind the decentralized process that holds this data.

Answer: Every time the CA wants to set up, they have to make the public certification policy, where it is explained how the registration process occurs. The citizen must go to the registration authority to prove identity (usually against full name, address and ID card number). Typically, this is done by physically presenting a photocopy of the ID card that is validated against the original one also shown by the citizen. For business, a reliable claimed document is mostly requested. For instance, the public notary certificate stating the creation and name of the legal person and also the public notary certificate declaring the natural person that can act on behalf of the business and the legal powers that person is entitled to. However, the database used by Police Directorate for the eID card is a centralized one and therefore, accessible by each Police Station-Registration authority at issuance time

Comment: How do you get a national ID card in a municipality environment? For example, in Germany, when a baby is born, you register the baby in the municipality as a registered inhabitant. You cannot just drop from nowhere. If moving from Frankfurt to Hamburg, you would bring the certificate from Frankfurt with you. It is nice from the data protection perspective but of course it may not be as quick and efficient as a centralized situation. Have to be careful when starting from birth as it might be easy to fake a birth certificate.

Question: In his keynote presentation, Malcolm mentioned policing and laws at state level where the authentication process operates. However, not too much was mentioned about this in the presentations. Is it because this is assumed?

Answer: In Australia, as this information needs to be put across the borders, the efforts have been put into the flow but not about the accountability of the flow of the data. It is currently lop-sided in this respect. There is an increasing proportion of data moving into an "accountability free" zone. Accountability has to be built in with the same level as the data flow processes.

Question: Banking applications – how is it handled in Spain?

Answer: Private sector is concentrating on this more so than the public sector, which needs to keep up. Main private sector methodology is username/password and pragmatic approach. eCommerce take-up hasn't been as well taken up in the public sector.

Question: Regarding the Levels of trust slide in Belgium. These are just 5 different levels. Does it have any technical evaluation?

Answer: No, these haven't been defined or made into any law. These are ones that the Ministry has discussed and seems to think may work.

Question (related to the previous question/answer): How do you inform the user? Most are dealing with the eID and a small piece of paper is issued with the eID that has 24 codes on it. When they have full roll out, it may then be possible to have legislation for this. Does that mean that a code level 4 in Belgium accept a code level 2 from Spain?

Answer: This is a good question and needs to be explored more in STORK.

Question: Where these 3 eGovernment approaches representative of STORK? Or are there other approaches?

Answer 1: In the UK, Trust levels based on username and password. Another issue is integrating technical approaches – how to use the username and password work in the other Member States.

Answer 2: A clear difference between the 3 presented and Netherlands, eID in NL is an identifier. It is only a number that is accessed by username and password. The other countries would not get anything as they wouldn't have the special number. There seems to be a commitment from the Dutch government to work on it as and when and where needed.

Question: Who is running the interoperability? Would there be contracts for this?

Answer: Stork is working in such a way to make the system work without changing the existing systems. Treaties wouldn't allow changes to be made to the systems to allow for this interoperability. The idea would be that services should still be able to operate even without the Stork PORTAL. But finding the services could be the issue then.

Comment: With regard to submitting on-line submissions for EC, it would be very interesting (and preferred) to have such an approach being discussed today to have the trusted MS authentication instead of having to take care of it on their own and dealing with multiple translations, getting data into the systems, storage issues, etc.

The speakers for the morning were thanked by the Chair Jacques Bus for their interesting presentations and discussions afterwards.

Panel with project presentations focusing on research in digital identity management issues

FIDIS: Martin Meints (Unabhängiges Landeszentrum für Datenschutz)

Martin Meints explained the background and context that eIDS are used in a far more complex environment where Identity management in national and pan EU governmental applications is challenging due to

- size of ID mgmt systems
- requirements of high levels of authentication (namely identification)
- need for offline availability in certain application scenarios
- differences in cultural and legal grounds.

There are interoperability challenges that must be addressed over 3 layers:

1. Informal organization –
2. Formal Organisation (bureaucracy)
3. Technical – connecting identifiers, systems

To reach interoperability over these three layers is a formidable challenge. As a general observation, while technical interoperability can be achieved relatively easy, on the formal and informal layer much more effort is needed. For example:

- Technical interoperability has been demonstrated
- National concepts of governmental sectors, data handling strategies in this sector. Definition of sectors is different, way data is handled is different, etc. so it is difficult to compare the sectors approach and to compare the enforcement regimes. These can be organizational ie. Forbidden as in Switzerland or highly support technically as in Austria.
- Risk: interoperability opens “back doors” endangering data security and protection in neighboring EU countries
- Possible countermeasures

- Data handling, security and privacy policies need to be negotiated, implemented, enforced and audited.
- Harmonisation of governmental sectors in mid and long term

Other recommendations from FIDIS were presented:

1. Concerning PKI, PKI is well established in the context of authentication of devices and citizens, and electronic signing. Interoperable eID schemes should take care not to require verification of citizen's certificates in case of any authentication (risk of tracking).
2. Biometrics are increasingly used to strengthen the link between an ID document and the document holder.
3. With respect to data protection and security the current ICAO standards are far from being state-of-the-art.
4. A mid and long term strategy is needed how to:
 - Reduce or avoid additional information in biometric reference data
 - Protect reference data (e.g. applying measures for template protection, revocability or using encapsulated biometrics)
 - Ensure back up procedures in case biometric verification fails

PICOS: Kai Rannenberg (Goethe University Frankfurt)

PICOS will develop and build a state-of-the-art platform for providing the trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks. A number of interesting trials are planned within the transport sector (taxis) and recreational anglers (fishermen).

Some major questions the project is examining:

1. What are the Trust, Privacy and Identity management issues in new context- rich mobile communications services, especially community-supported services?
2. How can information flows and privacy requirements be balanced in complex distributed service architectures (e.g. in mash-ups)?
3. How can these issues be solved in an acceptable, trustworthy, open scalable manner?
4. Which supporting services and infrastructures are needed?

In the first phase, the project has already come up with a set of interdisciplinary requirements. The next steps are the development of an architecture and a platform prototype that demonstrate the provision of appropriate privacy and trust technologies and are the basis for user centric trials

Please participate to the networking session in ICT 2008 in Lyon – Privacy, Identity Management and Dependability in Emerging ICT-based Interaction Scenarios: Trustworthy Fulfilment of Requirements beyond purely Technological Innovation (Session N.80, Wednesday, 26 November, 16.00 – 17.30)⁵.

SWEB: Petra Hoepner (Fraunhofer Institut Fokus)

SWEB⁶ – Secure, interoperable, cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries.

An FP6 project addressing SO 2.6.5. International cooperation for eGovernment and eParticipation Target countries West Balkans.

The Objectives of the project are to develop an SWEB platform and services to:

- Establish C2G secure communications through mobile means
- Establish G2G secure communications through electronic means

The SWEB Identity concepts are based on X.509 certificates including roles as attributes. The X.509 certificate is used to request a SAML token from an STS server. The SAML

⁵ http://ec.europa.eu/information_society/events/cf/item-display.cfm?id=821

⁶ <http://www.sweb-project.org>

token is stored on the mobile device and is used for authentication of the citizen at the municipality running the SWEB platform. Based on a policy and the attributes in the token an authorization decision is taken. WS-Secured SOAP communication is used between stakeholders (see figure in slides).

An example of a scenario was given and described: eGovernment Service execution in a local and cross-border case. The SWEB platform and services will be demoed and tested and evaluated starting in December 2008.

Question: how did you select WS over the SAML protocols for securing the SOAP messages?

Answer: The project decided to go with what was available at the time. Since WS was used more frequently, they decided to use this.

Question: What type of technology for encryption – asymmetric?

Answer: Yes, if you are going to connect to a municipality, you will apply WS-encryption on the SOAP messages depending on the target. In case the local municipality has to forward the service request to another municipality, the service request and SAML token are signed and encrypted again.

SWIFT: Amardeo Sarma (NEC Laboratories Europe)

SWIFT⁷ (Secure Widespread Identities for Federated Telecommunications) is addressing Identity convergence for NGN+ and leverages digital identities to solve identity fragmentation and to enable convergence between users/services/networks. The project is intending to extend IdM systems for multiple services at different network layers using the same ID and make a bridge between platforms that transcends layers. The virtual identities concepts have been adapted from the EU Daidalos⁸ project. These were researched and developed to support privacy of the user.

There are a number of goals of the project:

Goal 1. Enhance ubiquity and experience

- liberate user from device(s) by enabling use of several interchangeable device
- ownership of the device should be independent of who uses it – hiring embedded devices becomes part of the model
- facilitate discovery and service usage respecting the user's privacy options
- network access is automatically made available based on service requested
- invisible coordination of network and resources.

Goal 2 Enable Convergence

- Identity can form the bridge between networks, services, content and arbitrary offerings – it becomes a convergence technology
- Currently, a vast range of solutions exist that need to be brought together = SIM and USIM
- Central will be to also impact emerging NGN arch. 3GPP. ITU-T, ETSI
- Bridge the independence.

Identity in the Future Internet

- Bringing ID MGMT to the network
 - o Enable access and reachability across domains
 - o Make identities of people, services, things, software modules a part of the future int. architecture
- FI would be the ...identiNET
- Id as the future end point of communications
 - o Whether user, service, things, device, software module

The duration of the project is January 2008 to June 2010

Question: Are there more than one technical solutions to bridge these technologies?

⁷ <http://www.ist-swift.org>

⁸ <http://www.ist-daidalos.org/>

Answer: the project is not building a supra technology but we are trying to use this layered approach to try to work with these existing aspects. The project is still looking at requirements and the scenarios. It is too early to say which of the technological solutions will be selected.

Question: Are you taking into account other systems like National ID cards?

Answer: Yes, it will be part of the work to explore these.

Question: I am a bit surprised to see User-Network-Service-Centric – how can all of these be linked?

Answer: SWIFT is looking at it from the user down to the network level also and this is a differentiator. From the network level, we are looking at how to anonymise MAC address, and there are some ways to support privacy at this level. At the user level, there are policies that the user can be in the loop to allow them to make the decisions and interact with the system before data is sent one place or another.

PRIME and PRIMELIFE: Jan Camenisch (IBM Zurich Research Laboratories)

The PRIME vision was: ***“In the information society, users can act and interact in a safe and secure way while retaining control of their private sphere.”***

Therefore, within the high level requirements of enhancing privacy for the information society, the solution has to be technically feasible, understandable and manageable by end users, socially desirable and acceptable and legally compliant. The principles include the design should start with maximum privacy and system usage is governed by explicit privacy rules.

Vint Cerf – “We need identification in the Internet. We need both: sometimes we want to be anonymous, sometimes we need to be identified.”

How do we achieve both of these at the same time? This is what PRIME looked at.

A number of scenarios were presented showing the minimal information needed that is still sufficiently authenticated and guaranteed by some government credentials.

For example, a person wants to rent a car. The person needs a driver’s license and insurance to rent the car. These aspects can be described similarly into the electronic domain. However, if we use more than the minimal data, the data can be mined and used for illegitimate purposes. Therefore, the solution is Anonymous credentials.

In this scenario, can use pseudonyms and get Driver’s license confirmation as Alice, insurance confirmation as Eve and rent car as Bob. Thus, only the data you are willing to reveal will be revealed. It is up to the user only as to what is revealed. However, more information may need to be available if there is a car accident so the car agency can go to a third party using encrypted data to get the car repaired or take the escalated scenario further. The technology allows you to specify the minimum data in the normal operation. If the car gets broken, it is pre-established what additional information is needed for the car fixing company to figure out how you are identified to the insurance company. For these base and escalated scenario, there are 2 definitions of minimum information needed here –

1. data for the ordinary situation and
2. data for the escalated situation when something goes wrong.

We have to consider all of these situations ahead of time. In 1., there is minimum disclosure in the normal context but in 2., there could be additional disclosure required for these escalated contexts.

PRIMELIFE is Making PRIME real. PRIMELIFE intends to go beyond data minimisation and towards trust building and enforceable data protection (end to end policies). The research will focus on main issues uncovered by PRIME – HCI, Policies and infrastructures (and some mechanisms). It will be looking to cooperate with others especially since the technology will be via Open Source for HCI, tools (cryptography) and policy languages and standards.

Beyond data minimization

- social networks, Web 2.0, Lifelong
- Research focus on main issues uncovered by Prime
- HCI, Policies and infrastructures and some mechanisms
- Make privacy enhancing technologies uptake more.

Conclusions

1. authentication and privacy is possible...
2. and ready for pilots
3. still a long twisted road for widespread use
4. HCI
5. Devices and protocols and infrastructures
6. standards, standards, standards

Question: For Normal case and escalated case – are you giving the data encrypted for the excessive case at the same time as the normal case or would it be given only in the context requiring the additional data?

Answer: Technologically, we can do it either way. But we need to be able to get back to the person in case we get into this other situation.

Comment: In today's world, the process is usually the other way around – normally most data is required initially and then less data is needed. We are trying to move to the situation where we start with the minimalist data and put in the additional data only when needed. Otherwise, it wouldn't be possible to track someone if they don't want to be tracked in the escalated situation where more data is needed.

Question: Is the project looking at the future impact the technologies described in, for example the car rental and escalated example, would have if it led to a court case and the burden of proof would be made more difficult whereby the underlying technologies would have to be explained and understood by lay persons on a jury to link the person back through their pseudonyms.

Answer: The project wasn't addressing these aspects apart from having tutorials to explain to users of the technologies.

Recent work on user-centric identity meta system

This was a joint presentation by Reinhard Posch and Kai Rannenberg on their paper co-authored with Kim Cameron entitled "Proposal for a common identity framework: A User centric Identity Metasystem". Reinhard Posch presented a number of the application background points, which led to the work in the paper and Kai Rannenberg presented the technical aspects of the paper. See slides and distributed paper.

From the introduction of the paper:

"The paper proposes a framework for protecting privacy and avoiding the unnecessary propagation of identity information while facilitating exchange of specific information needed by Internet systems to personalize and control access to services. It also sets out factors to be taken into consideration when deciding where the standardization of such a framework should be brought about."

A central concept of the paper are so-called Claims. A Claim is an assertion made by one subject about itself or another subject that a relying party considers to be "in doubt" until it passes "Claims Approval", but that it can use based on its own policy and risk assessment of granting access.

With respect to Standardisation, there are essential properties of an organization to standardize the Identity Metasystem.

- the ownership of the standards must be clear, and it must be with a respected and open organization.

- There must be transparent, agreed and accessible process how to develop the standards and how to process amendments e.g. in regular time intervals.
- Neutral with regard to specific implementations and must cope with regional and cultural
- Aim for general standardization instead of sector specific.

Minimal disclosure tokens

- approach significantly enhanced through a new crypto technology (U-Prove/PRIME)
- allows packages of claims to be validated and signed by the claims provider in such a way that it knows they are true when it gives them out, but:
 - o cannot track the usage of the claims by different users unless they are abused
 - o provides strong disincentives to “lending” one’s claims to others.
- package of claims can be revoked
 - o users can demonstrate their claims have NOT been revoked without divulging ANY information

In conclusion, feedback to the paper would be highly valued. Especially if participants would check the model by using it to structure their respective application of Identity Management, this would be very useful. It is impossible to cover all aspects in a short presentation and the authors are happy to share the paper with those **who promise to send their comments** – and they will pass your ideas to Kim Cameron. It was noted that the Paper is not for large distribution just yet. Its purpose is to keep the discussions centralized by the authors.

Comments please to Kai.Rannenberg@m-chair.net and Reinhard.Posch@cio.gv.at

Discussion

Question: [U. Helmbrecht] If you want a high assurance level that a claim is true, you will need to go back to the identity provider. If within the policy of the relying party that they want to contact them directly, there is no way around that. If you live in Germany with an identity card, you have no chance to prove if correct. You believe it is correct. If you move and don’t change the card’s address, it is wrong. Will we change this if we move into the digital world?

Answer: [R Posch] The notion of government is that you use authentic documents. Eg. Birth certificate, certificate of marriage, ... In the electronic world, you sometimes want to have things in between e.g. Registers or things in between that go cross border and these things have to be put into the legal system.

[J. Camenisch] Sometimes, revocation is not necessary. It depends on the scenario: an expired drivers license can still be used to buy a beer – paper based has a very different process.

[Jacques Bus] There are two distinct developments - Mechanisms that allow trackback to individuals. Technology also inspires people, it is vitally important for technologists to explain to the ones making the administrative systems and work flows and laws what technology can do to ensure privacy and other issues like data minimization so that the cultures of these people are changing from “I want to know everything just in case” to a more “need to know” basis. This is not something you create just by creating technology. We need these discussions like today and broader discussions.

Question: [Amardeo Sarma] For other types of data – eg. context data, how are they represented in the ID metasytem.

Answer: [Kai Rannenberg] This is included in the slide on administrative domains [side 35] – the context data is incorporated into the transactions. An example: I want to find a pharmacy in the next 30 minutes. The core of the paper is more about the metasytem. As soon as the application is of high enough quality in the administrative area, then more context data can be used to “endure” the identification chain.

Question [Amardeo Sarma]: There should be mechanisms in place to reduce the precision of data. It may be sufficient to know we are in Europe, OR Belgium, OR Brussels, OR Beaulieu etc.

Answer [Kai Rannenberg]: On the Metasystem parties and flow slides [slide 25], on the right hand side, the relying party has a Claims policy which can do this – it can say “I only want to know what city people are in now”. User centricity is guaranteed with the policies within the Claims selector and these are only feeding the right information to the Relying party.

Comment [Jacques Bus]: Clearly, there are 3 facets when talking about identity data: Personal data of owner, how to manage data in the identity system and organization commercial value of data. It would be interesting to work these out in more detail in use cases. Therefore, we would invite everyone to read the paper in more detail and apply it to activities you are doing yourself and see if the meta-system is general enough to cover the data and tell the authors what you think about it. Check to see if it is a more general perspective on what you are doing every day and see if this is the right direction to go.

Wrapping up and next steps

The final part of the workshop was dedicated to general discussions on whether the particular topics in the meeting were useful or whether meetings should be held more regular. We should discuss about whether it is necessary to bring more people from the field of research with the people from Policy levels together or not.

[R Posch]: From the STORK perspective, it was very useful and it is the projects mission to communicate with other communities. We should extend into the operation of the government research services as they are a major player in the eID world.

[Jacques Bus] I am part of the board related to research services, including eID. It is a good idea to bring these together and we are working towards this direction. If we have another meeting, we can invite someone from there.

[R. Leenes]: Although STORK is aiming at building upon what is currently available in the MS, it would be worthwhile to have STORK people sit at the table with Prime/PrimeLife/Swift/etc.... to discuss use cases to see what the world would look like if we used anonymous credentials. This should be done in the immediate future but not sure who should take the lead on this.

[K. Rannenberg]: The 3 authors are also interested in use cases for their framework thinking so it would be a good idea to set up such a workshop.

[A Varghese]: In order to be concrete, the STORK partners and some of the ICT projects know one another, so when you have a use case to discuss together, you are free to look at other research going on following a subset level. The STORK WP leaders can do this on a case by case basis. This sort of implementation can take place without a big meeting if necessary.

[J. Camenisch]: For Primelife, we foresaw workshops like this are needed and would welcome STORK people also to participate.

[J. Bus]: This can be done both ways: organise a use case at a time together and if you want to do a couple of use cases at one time, Primelife could organize a larger workshop.

[R Posch]: Stork feels it is best that Primelife take this action since they are more of a visionary approach.

[U. Helmbrecht]: From the German perspective, it is in the process of rollout of the German ID card, rollout 2010 beginning a pilot towards the end of this year or beginning of next year. So attendance at this workshop was very useful from that perspective. In follow-up meetings, the German experience can be fed back into the future meeting.

[A Varghese]: STORK is one big building block but it is not the end. It is a starting point. It is good to look ahead to the future and what needs to be done there together. If ideas can be

brought in or thinking outside the Stork contractual obligations, it is very useful to follow up in this regard.

[J. Bus]: The objective of the Workshop was to have initial contacts together and look forward to further collaboration. The EU needs strategic thinking on how in the next 20 years to progress a common ID management framework. A framework to support the EU Member States enabling real business and enterprise activities necessary for the EU to stay very competitive. A common strategy is needed and it would be useful in coming workshop to think about the instruments within the different funded areas in the Framework programme present today and possibly including other e.g. Procurement on how to address this long term strategy. It is too large a task to implement an ID management strategy overnight and we all need to work together to be successful.

Annex I. Agenda

- 09:30–10:00 Registration
- 10:00–10:15 **Welcome and introduction**
Jacques Bus (INFSO-F5), Mechthild Rohen (INFSO-H2)
- 10:15–10:45 **Introductory keynote** (setting the scene)
Malcolm Crompton (Information Integrity Solutions, former Privacy Commissioner, Australia)
- 10:45–11:15 **Presentations of the STORK project**
Antonio Paradell (Project Manager), Frank Leyman & Jim Purves (Co-Chairs of the project)
- 11:15–12:00 **Presentations of Member States**
- Austria: Reinhard Posch (Chief Information Officer Austria)
 - Belgium: Frank Leyman (Manager International Relations, FEDICT)
 - Spain: Miguel Alvarez Rodriguez (Ministerio de Administraciones Públicas)
- 12:00–12:30 Questions
- | |
|-------------------------|
| 12:30–13:30 Lunch break |
|-------------------------|
- 13.30–15:00 **Panel with project presentations focusing on research in digital identity management issues**
- FIDIS: Martin Meints (Unabhängiges Landeszentrum für Datenschutz)
 - PICOS: Kai Rannenber (Goethe University Frankfurt)
 - SWEB: Petra Hoepner (Fraunhofer Institut Fokus)
 - SWIFT: Amardeo Sarma (NEC Laboratories Europe)
 - PRIME: Jan Camenisch (IBM Zurich Research Laboratories)
 - PRIMELIFE: Jan Camenisch
- 15:00–15:15 Break
- 15.15–15:45 **Recent work on user-centric identity meta system**
Reinhard Posch & Kai Rannenber
- 15:45–16.15 **Discussion**
- 16:15–16:30 **Wrapping up and next steps**

Annex II. List of Attendees

Surname, First Name	Affiliation
Alvarez Rodriguez, Miguel	Ministerio de Administraciones Públicas, Spain
Camenisch, Jan	IBM Zürich Research Laboratories
Clarke, Jim	Waterford Institute of Technology, Ireland
Crompton, Malcolm	Information Integrity Solutions Pty Ltd, Australia
Dean, Roger	EEMA
Gorniak, Slawomir	ENISA
Helmbrecht, Udo	Bundesamt für Sicherheit in der Informationstechnik, Germany
Hoepner, Petra	Fraunhofer Institut, Fokus
Koulolius, Vasilis	
Leenes, Ronald	Tilburg University, NL
Leyman, Frank	Federal Public Service ICT Fedict, Belgium
Meints, Martin	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Orre, Anders	Global Trust Center, Sweden
Paradell, Antonio	Atos Origin, SAE
Pasic, Aljosa	Atos Origin.
Posch, Reinhard	Austrian government
Purves, Jim	Home Office, Identity and Passport service, UK
Rannenberg, Kai	Goethe Universität, Frankfurt
Sarma, Amardeo	NEC Europe
European Commission	
Surname, First Name	Affiliation
Bus, Jacques	INFSO, F5
Gérard Galler	INFSO, A3

Hansteen, Kjell	INFSO, H2
Maghiros, Ioannis	JRC Sevilla
Paindaveine, Yves.	INFSO, F5
Rohen, Mechthild	INFSO, H2
Skordas, Thomas	INFSO, F5
Stienen, John	DIGIT.01/IDABC
Van Rooy, Dirk	INFSO, F5
Varghese, Aniyam	INFSO, H2
Verhoest, Pascal	INFSO, H2