

Update on EU Common Specifications

Porvoo 12 – Grosseto, October 2007



Background – The Manchester Ministerial Declaration (2005)



About eIDs

*By 2010 European citizens and businesses shall be able to benefit from **secure means of electronic identification** [...] made available under the responsibility of the Member States but recognized across the EU*

About eDocs

*By 2010 Member States will have agreed a framework for [...] **authenticated electronic documents across the EU***

Source: <http://archive.cabinetoffice.gov.uk/egov2005conference/documents/proceedings/pdf/051124declaration.pdf>

Background – The i2010 Action Plan (2006)

i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All

"Member States recognize the importance of eIDM for ensuring that **by 2010 European citizens and businesses will be able to benefit from secure and convenient electronic means, issued at local, regional or national levels and complying with data protection regulations, to identify themselves to public services in their own or in any other Member State**"

Source: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0173en01.pdf

Background: i2010 actions (to promote eID as key enabler for e-Government)



- 2006 Agree with Member States ... on the way to a European eIDM framework by 2010 based on interoperability and mutual recognition of national eIDM
- 2007 Agree common specifications for interoperable eIDM in the EU.**
- 2008 Monitor large scale pilots of interoperable eIDMs in cross-border services
- 2009 eSignatures in eGovernment: Undertake review of take-up in public services
- 2010 Review the uptake by the Member States of the European eIDM framework for interoperable eIDMs.

Source: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0173en01.pdf

The project (eID interoperability for PEGS) represents one of IDABC contributions to the i2010 Action Plan



Project details:

- Project name: **eID Interoperability for PEGS**
- Project owner: European Commission (IDABC)
- Contractor: Siemens IT Solutions and Services (Timelex as subcontractor)
- Project start date: January 2007

Entities also involved in the review of the deliverables:

- IDABC eID Interoperability Expert Group
- i2010 eGovernment sub-group of DG INFSO

Main objectives of the project

- To analyze the eIDM and authentication interoperability requirements stemming from the pan-European or cross-border eGovernment services
- To describe the required interoperability functions in eIDM and provide a comparative assessment of existing eID interoperability models
- To derive **common specifications** for interoperable eIDM in the EU.

Status of work (1/2)

Done: analysis of main eIDM schemes, available solutions for interoperability and impact on cross-border e-Gov.

- ✓ Country Profiles of MS (with a comprehensive analysis of current eIDM schemes)
- ✓ Report on Analysis and assessment of similarities and differences of eIDM schemes (with respect to both legal and technical aspects)
- ✓ Report on impact on eIDM interoperability (of the similarities and differences of the various eIDM schemes)
- ✓ Report on interoperable eIDM technical solutions (key attributes of each eIDM model for possible use in a cross-border application)
- ✓ Report on comparison and assessment of eIDM solutions interoperability (technical comparison of the respective models)

Status of work (2/2)

Current & next steps: Multilevel Authentication and Common Specifications models:

- ✓ Draft Common specifications for eIDM interoperable solutions
- ✓ Summary of existing national and other authentication schemes
- ✓ Proposal for multi-level authentication mechanism and a mapping of existing authentication mechanisms
- ✓ Report on the Impact and the implementation of the multi-level authentication mechanism and recommendations for the adoption of a multi-level authentication mechanism

Main results (1/5)

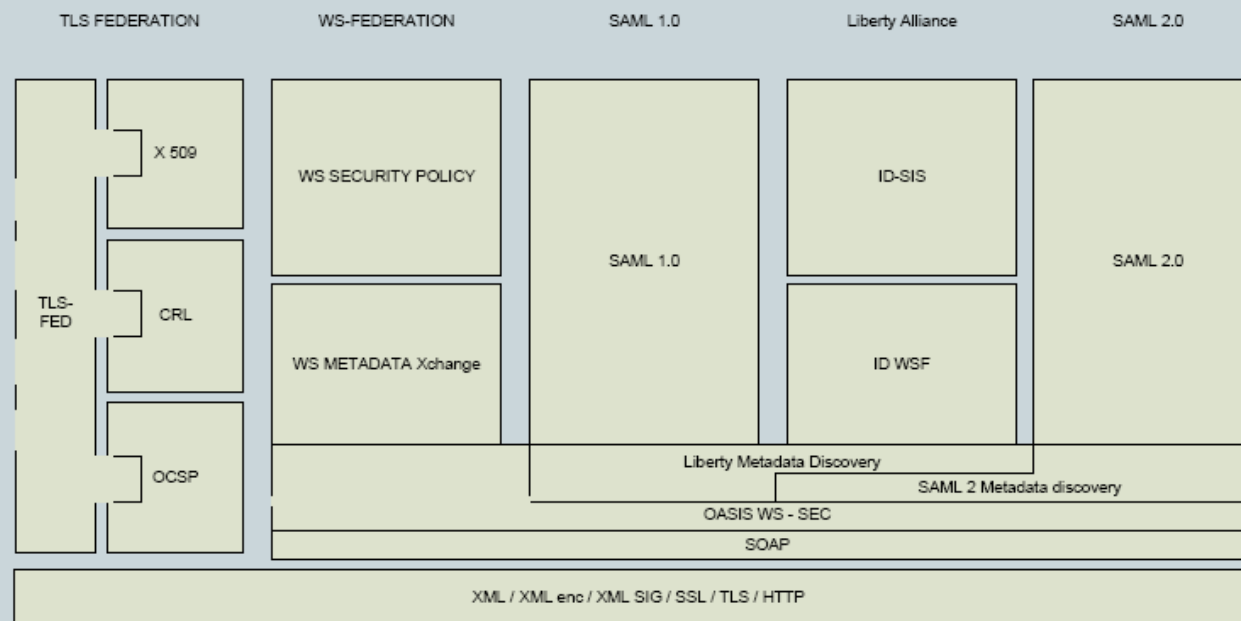
Complexity of the scenario

- ✓ The country survey revealed a heterogeneous scenario with regard to the adoption and use of identity resources. Particularly, with regard to identity tokens, the study found that out of 32 countries, 28 issue identity cards and only 7 are deploying eID cards (Austria, Belgium, Estonia, Finland, Italy, Portugal and Spain)
- ✓ Even unique identification numbers are not always used, due to privacy concern or other reasons
- ✓ However, almost 50% of the MS are in the process of designing eID cards for future roll-out

Main results (2/5)

Complexity of the available technologies

- ✓ The preliminary analysis of the existing eIDM schemes and solution models showed a large number of existing solutions, often similar but sometimes very different and even not interoperable.



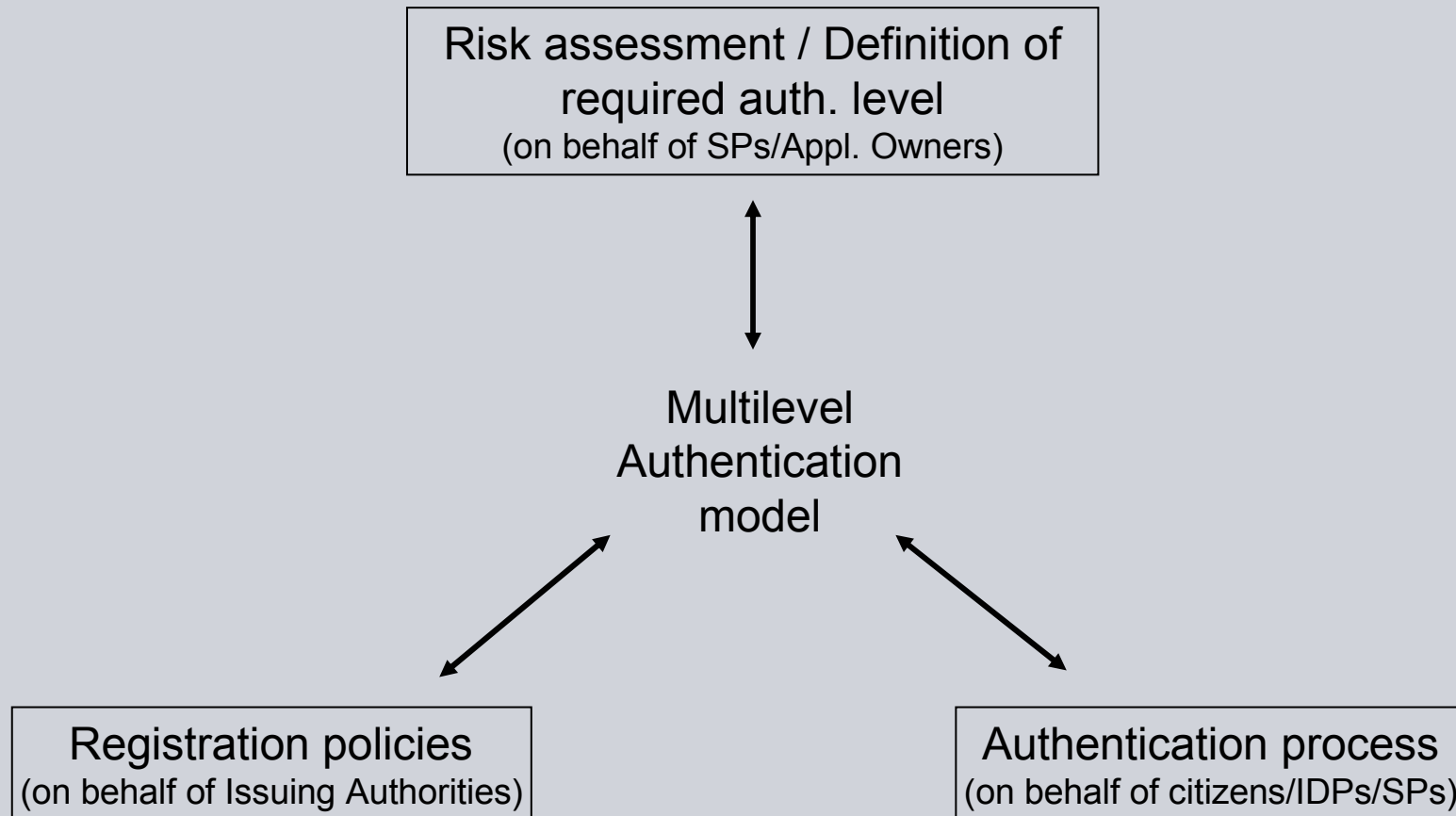
Landscape of IDPs
(source: IDABC site)

Main results (3/5)

Necessity of a country inclusive and user protective approach

- ✓ The proposed specification has to preserve or at least to take into account local preferences and existing infrastructures of 30+ MS
- ✓ A must is the protection of citizen data, so that their amount has to be minimized and an informed consent of their owners clearly obtained; use of general unique identification numbers should be excluded.
- ✓ Data protection regulations should be addressed in a set of standardized policy documents to be used by the application owners.
- ✓ Electronic identity should be defined to be technology neutral, require a minimal data set of user data, comply with legal restrictions and be commonly accepted by all MS
- ✓ Multiple authentication levels supported in favor of trust

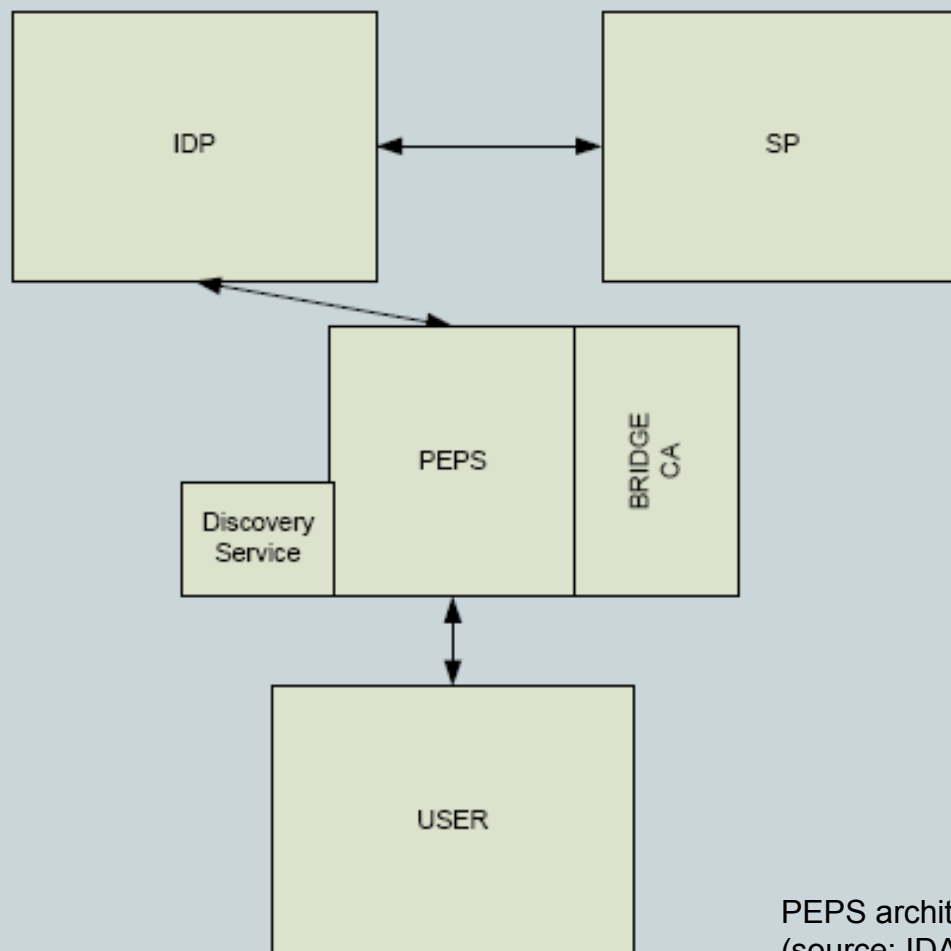
Main results (4/5) – Common specification of a multilevel authentication model



Multilevel authentication – Example matrix

| | Risk assessment / Definition of required auth. level | Registration policy | Authentication Process |
|---------|--|---|--|
| Level 1 | Low risk/damages | Claim based; no requirements for proving the claimed identity | Standard passwords accepted |
| Level 2 | Low-medium risk/damages | No personal presence of the applicant still acceptable, but basic validation of claimed identity attributes is required | Authentication based on ID Tokens (SW or HW) always acceptable; no passwords, except OTPs |
| Level 3 | Medium-high risk/damages | Personal presence of applicant is required, or availability of official identity resources for secure on-line verification of claimed id | OTP is still tolerated, but ID Tokens (SW or HW) strongly recommended |
| Level 4 | High risk/damages | Personal presence of applicant required; on-line registration only possible if qualified signatures of official identity resources are used | Only hard crypto tokens are accepted (e.g. eID cards) |

Main results (5/5) – Common specification of a Pan European Proxy Service



PEPS architecture
(source: IDABC site)



SIEMENS

Thank you for your attention!

Andrea Biasiol
Siemens IT Solutions and Services
andrea.biasiol@siemens.com

Copyright © Siemens AG 2006. Alle Rechte vorbehalten.