eID Large Scale Pilot STORK: Status and Results

Herbert Leitold
Leuven, March 17th, 2011
A common framework for cross-border use of electronic identity and authentication

- In online-processes
- Respecting national infrastructure
- Allowing different deployment models
  - Centralized (aka “PEPS”)
  - Decentralized (aka “middleware”)
  - Combined
- Pilot in real-world environment

We did that from 2008 until now – and will continue for a few more months
Presentation Outline

- Motivation - History
- Project Environment
- Interoperability Models
- Pilots and Integration
ID - what if something goes wrong …

- Digital twins, identity theft, …

Claim 1: There is a case for quality (e)ID
Government eID projects...

- Early birds started late 1990’s early 2000
  
  Finish eID card: December 1999
  
  Estonian eID card: from January 2002
  
  Austrian citizen card: from 2003, mass-rollouts 2005
  
  Italian CIE / CNS: test phase 2003 (CIE)
  
  Belgian eID card: from 2nd half 2003
Government eID projects ...

- Early birds started late 1990’s early 2000

  Finish eID card: December 1999

  Estonian eID´card: from January 2002

  Austrian citizen card: from 2003, mass-rollouts 2005

  Italian CIE/CNS: test phase 2003 (CIE)

  Belgian eID card: from 2nd half 2003

Evolved as national islands
National eIDs landscape

- Heterogeneous in various dimensions
  - Technology
    - Smartcards: AT, BE, EE, ES, FI, GE, IT, PT, SE, …
    - Mobile eID: AT, EE, FI, LU, NL, NO, UK, …
    - Soft certif.: ES, SE, SI, …
    - usern./pass.: NL, UK, …
  - Operational
    - Issued by public sector, private sector, combined
    - Issued at federal, local, regional level
    - Use of identifiers
  - Legal
    - (limited) use of identifiers: flat, sectoral, combined

Claim 2: None is the “better” system, they’re just different
Cross-border cases

- A few examples …
  - Student mobility
  - Migrant workers
  - Social security
  - E-Health
  - Services Directive
  - Moving house …

… and many, many more private sector applications!

Claim 3: There is a case for cross-border eID
A little history: eID ad hoc group (2004-2005)

... discussed possible interoperability models

Claim 4: Real-world pilots needed
A little history: eID ad hoc-group (2004-2005)

... developed signposts with a roadmap
By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU.
Presentation Outline

- Motivation - History
  - Project Environment
  - Interoperability Models
  - Pilots and Integration
eGovernment objectives (ICT-PSP call 2007)

**Type A**
- eProcurement
- eID
- interoperability
- eHealth

**Type B**
- Electronic documents
- Accessible & inclusive eGovernment
- Combined delivery of social services

**Thematic Networks**
- eParticipation
- Impact & user satisfaction
- Brokering pan-EU eGov solutions & services online
STORK: Who we are

14 ORIGINAL MS PARTNERS

ENLARGEMENT:
3 ADDITIONAL MEMBERS

12 IN REFERENCE GROUP
- Member States have eID projects
  planned, deploying, or operational
- Heterogenous environment
  Technology: smartcards, username/passwords
  Operational: e.g. centralized, decentralized
  Legal: e.g. persistent identifiers, sector-specific IDs

STORK does not change the MS situation, but aims at interoperability on top of it
Issues to be tackled

- Consensus needed
- Legal
  - e.g. MS limit use of national identifiers
  - can prohibit using the identifier cross-border
- Data protection
  - Processing needs to be legitimate
- Liability
  - What if something goes wrong?
- Trust
  - MoUs, Accreditation, self-assessment ??
Common, SAML 2.0 - based specifications have been agreed by the STORK consortium.
One problem tackled: Trust levels

Different technologies and security levels:
- Smart cards
- Software certificates
- Mobile Phones
- Username-password
Approach: Mapping to QAA levels
## eID profile of STORK pilot countries

<table>
<thead>
<tr>
<th>Country &amp; credentials</th>
<th>Token Types</th>
<th>Relation to 1999/93/EC</th>
<th>Token Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country &amp; credentials</td>
<td># of cred. Smart card mobile eID soft.-certif.</td>
<td>qualified cert (signature-cert) is a SSCD</td>
<td>public sector private sector</td>
</tr>
<tr>
<td>Austria</td>
<td>3</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Belgium</td>
<td>1</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Estonia</td>
<td>2</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Finland</td>
<td>1</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Iceland</td>
<td>2</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Italy</td>
<td>2</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Lithuania</td>
<td>1</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>3</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Portugal</td>
<td>1</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Slovenia</td>
<td>3</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Spain</td>
<td>1+80</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Sweden</td>
<td>12+</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
Presentation Outline

- Motivation - History
- Project Environment
  - Interoperability Models
  - Pilots and Integration
STORK assumes that the citizen wishes to have online-access to an eGOV service with her eID.

Three use cases:

1) **Authentication**: in an online access to a service provider

2) **Attribute Transfer**
   STORK supports the attribute transfer of personal identification attributes (national ID number, name, date of birth, qualification). These are retrieved form the eID credential and if needed from an Attribute Provider (Governmental source)

3) **Certificate Verification**: for electronic signatures
STORK – Interoperability Models

One Interoperability Framework, Two Basic Models

STORK investigated and pilots two interoperability models:

1. Middleware (MW)
2. Pan-European Proxy Services (PEPS)

.. and combine them ($MW \Rightarrow MW, PEPS \Rightarrow PEPS, MW \Rightarrow PEPS, PEPS \Rightarrow MW$)

The common specifications have been designed so that major components operate on the same protocols, irrespective of the model or its combinations.
STORK – Example of Middleware Architectures

Service Provider Domain

Client Domain

MOA-ID
(Server-Middleware)

Bürgerkartenung.
(Client-Middleware)

Internet

Bürgerclient
(Client-Middleware)

Internet

eID Server
(Server-Middleware)

Application

Application
STORK PEPS data flow (logical)
Protocol: Federated Identity (SAML 2.0)
The “combination hat trick” V-IDP

Virtual Identity Provider

- provide a MW access at a PEPS or
- a PEPS interface at the SPware
MW ⇒ MW example: Austrian student at German University
STORK – PEPS Interoperability Model

PEPS example: Swedish student at UK university

Central national PEPSs

SE PEPS

UK PEPS

UK Service

IP

IP
MW ⇒ PEPS example: Austrian student at Swedish university,

“Virtual IDP” concept
General considerations

- **Middleware**
  - No intermediaries between user & SP
    - SP remains data controller
  - Needs to integrate all tokens (pure model)
  - End-to-end security

- **PEPS**
  - Third party
    - Liability shift
    - Data processor or data controller
  - Hides national complexity
  - Segmented trust-relationships

In both cases consent as basis for data processing legitimacy
(two variants data type and data value)
Data-type consent example

Slovenia

Portugal
Data value consent examples

Austria

**Authentication Data:**

**Personal Data**
- Name: Herbert Leitold
- Date of Birth: 12.08.1965

**Application Data**
- Name: Demo-SP AT
- Country: Austria

**Technical Parameters**
- URL: https://apps.ogiz.gv.at/mao.stork.web/RetrieveMOAAuthData
- AnyNumber: urn:publicid:vg.at:storkid+AT+EE
- Identifier: eyHeJ+UvD+Dak=8613
- Date: 12.12.2010
- Time: 12:46:26

Spain

**Servicio Español para la Identificación electrónica Transfronteriza**

Los siguientes datos personales han sido encontrados, ¿desea enviarlos a ECAS-SP?

- **Atributos obligatorios**
  - Nombre
  - DNI: ES/BE/1234

- **Atributos opcionales**
  - e-mail

Al enviar sus datos al extranjero, puede aplicar otra normativa de protección de sus datos de carácter personal. Asegúrese de leer con detalle las condiciones de uso de la aplicación de destino de sus datos.

Nota sobre el Domicilio: Aunque el ciudadano tiene la obligación de tener actualizado este dato, no se garantiza que estos sean los datos de empadronamiento actual del ciudadano.

Doy consentimiento | No doy consentimiento
Presentation Outline

- Motivation - History
- Project Environment
- Interoperability Models
  - Pilots and Integration
Our success story

- Six pilots live as “pioneering applications”
  - Online authentication
  - Safer Chat
  - Student Mobility
  - eDelivery
  - Change of Address
  - ECAS
Integration model “PEPS country”

Service providers

STORK Layer (centralized)

Foreign eID

MS-specific connector

Middleware

PEPS

V-IDP

card

Service providers

STORK Layer (centralized)

Foreign eID
Integration model “MW country”

Service providers

STORK Layer (decentralized)

Foreign eID

PEPS

MS-specific connector

V-IDP

middleware
### Authentication Process Flow: WP4.1 Diagram A

**MS A Resident, Identity Provider and PEPS in MS A, Service Provider and PEPS in MS B**

<table>
<thead>
<tr>
<th><strong>Identification phase</strong></th>
<th><strong>Assertion validation and login phase</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select to authenticate to Service Provider in MS B</td>
<td>MS A Specific</td>
</tr>
<tr>
<td>Select MS from the provided list. User choice</td>
<td></td>
</tr>
<tr>
<td>Request eID with trust level $\geq x$</td>
<td>Create assertion with the authentication statement. Including unique, minimum, persistent representation of a person's identity</td>
</tr>
<tr>
<td>Which MS issued your eID for authentication?</td>
<td>Provide list of MS A eIDs with trust level $\geq x$</td>
</tr>
<tr>
<td>Redirect to MS A PEPS. Authentication request and trust level</td>
<td>Authentication interaction with IDP</td>
</tr>
<tr>
<td>MS A specific interaction with the user for validating eID. Include Consent</td>
<td></td>
</tr>
<tr>
<td>Select eID</td>
<td>MS A specific</td>
</tr>
<tr>
<td>Provide list of MS A eIDs with trust level $\geq x$</td>
<td></td>
</tr>
<tr>
<td>Create assertion with the authentication statement. Including unique, minimum, persistent representation of a person's identity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Validation</td>
</tr>
<tr>
<td></td>
<td>MS B Specific</td>
</tr>
</tbody>
</table>

**Key Concepts**
- Identification phase
- Service selection phase
- Assertion validation and login phase
- MS A Identity Provider
- MS B PEPS
- Service Provider MS B
- MS A Resident
- MS A PEPS
- MS B Specific

**Notes**
- MS-specific elements remain
- STORK – Process Flow PEPS-PEPS Authentication
STORK – Process Flow PEPS-PEPS MS-specific

Member State Specific Identification Phase WP 4.1 Diagram B

MS A Resident, Identity Provider and PEPS in MS A, Service Provider and PEPS in MS B

- **MS A Resident**
  - Select eID
  - User selects data to be transmitted

- **Service Provider MS B**
  - Yes
  - Validation of provided eID
  - Forward provided credentials to the IdP for validation

- **MS B PEPS**
  - No
  - Authentication Request
  - Validation

- **MS A PEPS**
  - Yes
  - Validation of provided eID
  - Validation

- **MS A Identity Provider**
  - Select eID
  - Uses credentials to authenticate
  - Authentication Request
  - Validation

EG SPAIN

EG UK
Authentication Process Flow: WP4.1 Diagram C

MS A Resident, Middleware from MS A, Service Provider and PEPS in MS B

### Service selection phase
- **MS A resident**
  - Select to login/register to Service Provider in MS B
  - Select MS from the provided list. User choice

### Identification phase
- **Service Provider MS B**
  - Request eID with trust level >= x, gather needed attributes
  - Which MS issued your eID for authentication?
  - Delegate to VIDP including the trust level, SP_ID, attributes
  - Delegate to SPware if the trust level >= x

- **Virtual IDP**
  - Delegate to SPware if the trust level >= x

- **MS A SPware**
  - Token access initialization
  - MS A specific interaction with the token
  - Validation of Provided eID
  - Create assertion with the authentication statement

### Assertion validation and login phase
- **User interacts with service**
  - Proceed with Service
  - Convert assertion to internal MS B standard
  - Validation
  - Yes

**MS-specific elements remain**

**STORK – Process Flow MW-PEPS Authentication**
STORK – Process Flow PEPS Attribute Transfer

Attribute Transfer Process Flow: WP4.3 Diagram D

Identity Provider and PEPS in MS A with PEPS and Service Provider in MS B

MS A Resident

- MS Defined User Consent
  - MS A specific interaction with the user for validating eID. Include Consent
  - Displays attributes to the user.
  - Provides Consent
  - Users transfer attributes
  - Yes: Transfer attributes
  - No: MS A asks for additional information

Service Provider MS B

- Service requires attributes. Displays list of the required attributes

PEPS MS B

- Receives Attribute Request. Passes request to MS A PEPS
- MS B Specific

PEPS MS A

- Receives Attribute Request. Passes request to correct Attribute Provider

Identity and Attribute Provider MS A

- MS Decision on Session
- Resident Interacting with SP in a Authenticated session
- MS A specific interaction with the user for validating eID. Include Consent
- Displays attributes to the user.
- Provides Consent
- Users transfer attributes
- Yes: Transfer attributes
- No: MS A asks for additional information

Service Provider MS B

- Receive attribute, pre-fill form and display to the user. Request user to submit attributes
- Stores Attributes
- Send Attributes to Service Provider

Stores Attributes

Authentication Process Flow: WP4.1 Diagram C

MS A Resident, Middleware from MS A, Service Provider and PEPS in MS B

1. Service Provider MS B
   - Service requires attributes
   - Displays list of the required attributes and terms and conditions

2. MS A resident
   - Resident interacting with SP in an Authenticated session
   - User selects to continue

3. MS B PEPS
   - Attribute request, delegate to VIDP, include eID.

4. Virtual IDP
   - Proceed with Service

5. MS A SPware
   - Token access initialization
   - MS A specific interaction with the user for validating eID
   - Show list of attributes
   - MS A specific interaction with the user for validating eID
   - Create assertion with the authentication statement

Service selection phase
Identification phase
Assertion validation and login phase
PEPS Architecture
Common MW architecture

Common MW architecture includes the following components:

- **SP DE**: SOAP
- **SP AT**: Web
- **S-PEPS**: STORK
- **SP MS A**: MS A Specific

The Modular Authentication Relay Service (VIDP core) is at the center, with interfaces to:

- **eID Service Connector**: DE Specific
- **MOA-ID Connector**: AT Specific
- **C-PEPS Connector**: STORK

Possible Extension

- **Common Functionality (SAML, Logging)**
Conclusions 1: It works
Conclusions 2: The missing links

- Mutual recognition and missing legal basis
Conclusions 3: Looking forward to Digital Agenda Key Actions 3 & 16

Propose by 2012 a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector)

In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems
Time is flying …

… so I thank You for Your patience and attention.