Challenges of eID interoperability: What we learn(ed) from the STORK journey?

Primelife Summerschool, Helsingborg, 3.8.2010

Herbert.Leitold@egiz.gv.at
Presentation Overview

- eID motivation, a little history
- STORK Project Environment
- Interoperability Models and Integration
- Technology
ID - what if something goes wrong ...

- Digital twins, identity theft, ...
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 2\textsuperscript{nd} half 2003

- Government eID projects ...
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
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
  - 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
  - E-Health
  - Services Directive
  - Moving house
  - Social security …

and many, many more private sector applications!

Claim 3: There is a case for cross-border eID
A European eID model must coexist with all three models not compromising privacy.

eID MUST NOT ADD ADDITIONAL PRIVACY RISKS TO EXISTING APPLICATIONS.
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

2006

2007

2008

2009

Authentication Model & Levels

Common eID Framework

Equal Treatment of national eIDs

Personal Data Ownership Model

eID Terminology

Definition of eID

eID Role Management

EU provisions: Recognition of national eIDs

Federated eID Management

eGovernment eID and Authentication
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.
<table>
<thead>
<tr>
<th>Country &amp; sec. level</th>
<th># of cred.</th>
<th>Token Types</th>
<th>Relation to 1999/93/EC</th>
<th>Token Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Smart card</td>
<td>mobile eiD</td>
<td>soft.-certif.</td>
</tr>
<tr>
<td>Austria</td>
<td>3</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Belgium</td>
<td>1</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Estonia</td>
<td>2</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Iceland</td>
<td>2</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Italy</td>
<td>2</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>3</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Portugal</td>
<td>1</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Slovenia</td>
<td>3</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
</tr>
<tr>
<td>Spain</td>
<td>1+80</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
</tr>
<tr>
<td>Sweden</td>
<td>12+</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
</tr>
</tbody>
</table>
Presentation Overview

- eID motivation, a little history
- STORK Project Environment
- Interoperability Models and Integration
- Technology
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 – Member State involvement

Member States/EEA – STORK
Member States Ref Group
STORK-2 (original plan)
The Basis

- 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 ??
Project’s structure

**Project Management (ATOS)**

- **eID inventory, trust & application groups (NL MOI)**
- **eID and upcoming technologies (AT TUG)**

**Communication and Sustainability (Gov2U)**

- **eID process flows (UK IPS)**
- **Common specifications and Stork’s eID models (FEDICT BE; MAP ES)**
- **National integration of Stork models and Common specifications (FEDICT BE, MAP ES)**

**DEFINITION AND ANALYSIS**

**DESIGN OF INTEROPERABLE FLOWS & ARCHITECTURES**

**CONSTRUCTION AND IMPLEMENTATION**

**TESTING & EVALUATION**

**Pilots**
STORK – Roadmap “the way ahead”

Feb 09

- Framework mapping
- Legal interoperability
- Priority technologies

Oct 09

- Cross-border authentication platform
- Assessment on common specifications on eID

May 10

- Quality authenticator scheme
- eID PROCESS FLOWS

May 11

- Construction & Implementation
- Exploitation - Pilots
- Evaluation

Common, SAML 2.0 - based specifications have been agreed by the STORK consortium
Pilots

Pilot 1 – Cross border authentication

Pilot 2 – safer chat

Pilot 3 – eID Student Mobility

Pilot 4 – eID electronic delivery

Pilot 5 – EU Citizen Change of Address
Further services

- A2A services as additional deployments
  - Defined as part of the work programme
  - First focused on specific applications, but …

- Integration with ECAS
  - Obvious option for doing the A2A services with EC
  - Demonstrator as a first step

- Establishing as a full STORK pilot (the 6th pilot)
Presentation Overview

- eID motivation, a little history
- STORK Project Environment
  - Interoperability Models and Integration
  - Technology
One problem tackled: Trust levels

Different technologies and security levels:
- Smart cards
- Software certificates
- Mobile Phones
- Username-password
Approach: Mapping to QAA levels

- Austria: 0, 1
- Estonia: 1
- France: 0, 1, 2, 3
- The Netherlands: 1, 2
- Sweden: 1, 2
- Spain: 1, 2, 3, 4
- UK: 0, 1, 2

STORK-QAA levels:
- Austria: 0, 1
- Estonia: 1
- France: 0, 1, 2, 3
- The Netherlands: 1, 2
- Sweden: 1, 2
- Spain: 1, 2, 3, 4

National Levels
STORK assumes the citizen has online-access with eID.

Four use cases:

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

2. **Attribute Transfer**
   - STORK defines *eID* as the *identifier* (e.g. national citizen ID),
   - “the rest” (name, date of birth, qualification, …) are *attributes*

3. **Attribute Verification**: is a certain attribute presented by the citizen correct?

4. **Certificate Verification**: for electronic signatures
One Interoperability Framework, Two Basic Models

STORK will investigate and pilot 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.
Integration at the Service Provider with smart-cards as means of eID
STORK – Example of Middleware Architectures

Service Provider Domain

Client Domain

Application

MOA-ID (Server-Middleware)

Bürgerkartenumg. (Client-Middleware)

Internet

eID Server (Server-Middleware)

Ausweis App (Client-Middleware)

Internet

Service Provider Domain

Client Domain

Application

MOA-ID (Server-Middleware)

Bürgerkartenumg. (Client-Middleware)

Internet

eID Server (Server-Middleware)

Ausweis App (Client-Middleware)

Internet
STORK – Communalities: Middleware Concept

Application

MOA-ID
(Server-Middleware)

Bürgerkartenumg.
(Client-Middleware)

Internet

eID Server
(Server-Middleware)

Ausweis App
(Client-Middleware)

Internet

MOA-ID
(Server-Middleware)

Application

eID Server
(Server-Middleware)

Ausweis App
(Client-Middleware)
STORK – Making Governments to co-operate

TRUST – STORK’s QAA

Pan European Proxy Services (PEPS)
1. User accesses service provider.
2. Service provider requests identity from Stork National PEPS.
3. User is authenticated through the Authentication Portal.
4. Attributes Providers provide identity information.
5. Identity information is exchanged between Stork National PEPS.
6. Service provider verifies identity and grants access.
Protocol: Federated Identity (SAML 2.0)

1. User logs in to the Service Provider (SP).
2. SP requests identity information from Stork National PEPS.
3. User authenticates with the Authentication Portal.
4. Attributes Providers communicate with Stork National PEPS.
5. Stork National PEPS verifies user identity and returns attributes.
6. SP uses the identity information and attributes for service access.

Flags of Belgium and Iceland are visible, indicating international aspects of the protocol.
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
PEPS example: Swedish student at UK university

Central national PEPSs

UK PEPS

SE PEPS

UK Service

IP

IP
STORK – combined model

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
Integration model “PEPS country”

Service providers

STORK Layer (centralized)

Foreign eID

MS-specific connector

PEPS

V-IDP

middleware

V-IDP
Integration model “MW country”

Service providers

STORK Layer (decentralized)

Foreign eID

V-IDP

MS-specific connector

PEPS

MS-specific connector

middleware
Presentation Overview

- eID motivation, a little history
- STORK Project Environment
- Interoperability Models and Integration
  - Technology
Case 1: Service Provider in PEPS State

- eGov Service in PEPS country
- STORK interface – V-IDP
- PEPS AB
- STORK delegation component
- eCardAPI (Server) + acc. cert.
- MOAID
- PEPS Plug-In
- STORK interface – PEPS
- V-IDP
- Internet

Internet

- eCardAPI (Client)
- Thin-Client Middleware

Internet

- PEPS Plug-In
- V-IDP
- MOAID
- PEPS AB
- STORK interface – PEPS

Internet

- PEPS XY
- STORK interface - PEPS

Internet

- Browser
- username password

Internet

- Proxy and IDP
- IDP
- Credential

Internet

- PEPS Plug-In
- STORK interface – PEPS

Internet

- eCardAPI (Client)
- Thin-Client Middleware

Internet

- PEPS Plug-In
- V-IDP
- MOAID
- PEPS AB
- STORK interface – PEPS
Case 2: Service Provider in MW State

STORK interface – V-IDP
STORK delegation component
V-IDP

eGov Service in MW country

Internet

eCardAPI (Client) CardInfo

Thin-Client Middleware

Internet

STORK interface - PEPS
PEPS

MOA-ID

Internet

username password

Browser

PEPS Plug-In

Internet

STORK int. - PEPS

Proxy and IDP

IDP

Internet

PKCS#11, CSP, TLS-Fed, ...

Internet

Client Middleware

Credential

other token

STORK interface – V-IDP

Internet

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORK

STORA
**Authentication Process Flow: WP4.1 Diagram A**

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

---

**Identification phase**

1. **MS A Resident**
   - Select to authenticate to Service Provider in MS B
   - Request eID with trust level >= x

2. **Service Provider MS B**
   - Request eID with trust level >= x
   - Select MS from the provided list. User choice
   - Redirect to MS A PEPS. Authentication request and trust level

3. **MS A PEPS**
   - Provide list of MS A eIDs with trust level >= x
   - MS A specific interaction with the user for validating eID. Include Consent
   - Create assertion with the authentication statement. Including unique, minimum, persistent representation of a persons identity

4. **MS A Identity Provider**
   - MS A specific interaction with the user for validating eID. Include Consent
   - Process Consent

---

**Assertion validation and login phase**

1. **Inform User I&A failed**
   - Proceed with Service

2. **Convert assertion to internal MS B standard**
   - Select eID
   - MS A Specific
   - Validation

---

Notes:

- **MS-specific elements remain**
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

- Select eID
- User selects data to be transmitted
- Forward provided credentials to the IdP for validation
- Validation of provided eID
- Authentication Request
- Validation
- Uses credentials to authenticate
- Yes
- Forward

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
- 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
- Virtual IDP
  - Delegate to SPware if the trust level >=x
- MS A SPware
  - Token access initialization

**Identification phase**
- Service Provider MS B
  - Provide token for selected eID
  - MS A specific interaction with the user for validating eID. Show list of attributes
  - Select attributes, enter PIN
  - Inform user I&A failed. END
- Virtual IDP
  - Validation
  - MS A SPware
  - Create assertion with the authentication statement
  - Proceed with Service
- MS B Specific
  - Convert assertion to internal MS B standard

**Assertion validation and login phase**
- User interacts with service

---

MS-specific elements remain

---

STORK – Process Flow MW-PEPS Authentication
Identity Provider and PEPS in MS A with PEPS and Service Provider in MS B

Attribute Transfer Process Flow: WP4.3 Diagram D

1. **Identity Provider and PEPS in MS A with PEPS and Service Provider in MS B**
2. **Identity Provider and PEPS in MS A with PEPS and Service Provider in MS B**
3. **Identity Provider and PEPS in MS A with PEPS and Service Provider in MS B**
4. **Identity Provider and PEPS in MS A with PEPS and Service Provider in MS B**
**STORK – Process Flow MW-PEPS Attribute Transf.**

**Authentication Process Flow: WP4.1 Diagram C**

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

- **Service Provider MS B**
  - Resident Interacting with SP in a Authenticated session
  - User selects to continue
  - Service requires attributes. Displays list of the required attributes and terms and conditions

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

- **Virtual IDP**
  - User interacts with service

- **Service requires attributes. Displays list of the required attributes and terms and conditions**
  - MS A Specific interaction with the user for validating eID. Show list of attributes
  - Select attributes, enter PIN
  - Inform user &A failed. END

- **Validation**
  - yes
  - no
  - no
  - yes

- **Create assertion with the authentication statement**
  - MS A specific interaction with the token

- **Show list of attributes**
  - yes
  - no

- **Service selection phase**
  - Service requires attributes. Displays list of the required attributes and terms and conditions

- **Identification phase**
  - Token access initialization
  - MS A specific interaction with the token
  - Validation of Provided eID

- **Assertion validation and login phase**
  - Create assertion with the authentication statement
  - Proceed with Service
  - Convert assertion to internal MS B standard

---

**Same as MW-Autentication**
Common MW architecture

- SP DE
- SP AT
- S-PEPS
- SP MS A

- WS Interface
- SP AT Interface
- V-PEPS
- S-PEPS

- eID Service Connector
- MOA-ID Connector
- C-PEPS Connector

- DE Specific
- AT Specific
- STORK

Modular Authentication Relay Service (VIDP core)

Possible Extension

Common Functionality (SAML, Logging)

MARS
**Security Assertion Markup Language (SAML)**

- XML-based standard for exchanging authentication and authorization data between security domains

**Typical Use Cases:**
- Web Single Sign-On (SSO)
- Identity Federation
- Attribute-Based Authorization
- Securing Web Services
SAML architecture

Profiles
Combinations of assertions, protocols, and bindings to support a defined use case

Bindings
Mappings of SAML protocols onto standard messaging and communication protocols

Protocols
Requests and responses for obtaining assertions and doing identity management

Assertions
Authentication, attribute, and entitlement information

SSO Profiles, Single Logout Profile, Attribute Profiles, …

SOAP Binding, HTTP-Artifact, HTTP-Redirect, HTTP-Post Binding, …

Authentication Request Protocol, Single Logout Protocol, …

Authentication, Attribute, Authorization Decision Assertion

Source: SAML 2.0 Technical Overview
SAML example

- SAML via SOAP over HTTP

Source: SAML 2.0 Technical Overview

XML code:

```
1: <?xml version="1.0" encoding="UTF-8"?>
3:   <env:Body>
4:     <samlp:Response
5:       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
6:       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
7:     Version="2.0"
8:     Issuer="urn:oasis:names:tc:SAML:1.1:nameid-format:inf":
10:   <saml:Issuer>http://idp.example.org/saml:Issuer>
11:     <samlp:Status
13:     ...SAML assertion...
14:     </samlp:Status
15:   </env:Body>
16: </env:Envelope>
```
SAML and STORK

Profiles
Combinations of assertions, protocols, and bindings to support a defined use case

Bindings
Mappings of SAML protocols onto standard messaging and communication protocols

Protocols
Requests and responses for obtaining assertions and doing identity management

Assertions
Authentication, attribute, and entitlement information
PEPS – Environment and Frameworks

- Linux/Windows
- Java 1.5
- Application Servers – Web application
  - Tomcat 5/6
  - JBoss 5
  - Glassfish V3
- Frameworks:
  - Spring
  - Struts
  - OpenSAML
  - log4j
VIDP – Environment and Frameworks

- Linux/Windows
- Java 1.5
- Application Servers – Enterprise application
  - Glassfish V2
- Frameworks:
  - EJB
  - Velocity (Web presentation, JSP)
  - OpenSAML
  - slf4j/log4j
  - JAXB/JAX-WS
Presentation Overview

- eID motivation, a little history
- STORK Project Environment
- Interoperability Models and Integration
- Technology
Key Action 3: 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;

Key Action 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);
Conclusions
THANK YOU FOR YOUR ATTENTION

info@eid-stork.eu