Importance of Federation to Danish Government

IT Architecture Office
National IT and Telecom Agency
Danish Ministry of Science, Technology and Innovation

October 17, 2006 – Søren Peter Nielsen – spn@itst.dk
Agenda - Importance of Federation to Danish Government

- Architecture & deployment plans
- Importance of a standards-based approach
- Value of participation in eGovernment special interest group
Danish e-Government so far has been through a Decentralized Approach

A "common" Danish family on a "common" day

Mother - Irene
Company owner

Son - Anders
Student

Daughter - Louise
Moving

Local Gov rental subsidiary

Local Gov Case-sys

Educational loan & support

"EasyAccount"

Tax Auth

Business services Portal

Service center

Police

This is just an example – showing a few selected services – It is not representative of the full set of Danish eGov services

E-Government services are delivered by many different organizations
Advancing eGovernment - Finding the right balance...

Bottlenecks
Catch 22’s
...

Centralization

Decentralization

Fragmementation
Complexity
...

We want to advance eGovernment with various parallel initiatives, and at the same time with a common approach to identity and access management

*Federation is critical for this to happen*

Work with architecture and standards has been going on for several years
Important Goals in the First Phase of the Work

- Support the ability of different authorities to use a shared login-service
- Single Sign-On (SSO)
- Establish a structure that can be the basis for exchanging authorisation information between independent organisations
- Embrace the use of different mechanisms for - and levels of - authentication
Reference Architecture for Cross-organizational Single Sign On

"Portal"

Identity Provider (IdP)

- Includes recommendations about
  - Levels of Authentication
  - Core user identity attributes
  - Unique key to link user accounts

Service Provider (SP)

Conceptual Architecture is adopted from US Federal e-Authentication initiative

SAML 2.0 is the recommended federation standard

Approved by Danish Government IT Architecture Committee after public hearing in Autumn 2005
Levels of Authentication – not bound to any particular technology

- **Level 1** - Little or no confidence in asserted identity
- **Level 2** - Some confidence in asserted identity
- **Level 3** - High confidence in asserted identity
- **Level 4** - Very high confidence in the asserted identity

- Recommended level is found through risk assessment
Matching risc with level of authentication

Tabel 1 – Maksimale størrelser af risici for hvert sikkerhedsniveau

<table>
<thead>
<tr>
<th>Risiko i forhold til sikkerhedsniveau</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kategorier af risici ved fejl i forbindelse med autenticitetssikring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ulempe, kval, eller tab af anseelse</td>
<td>Lille</td>
<td>Moderat</td>
<td>Moderat</td>
<td>Stor</td>
</tr>
<tr>
<td>Økonomisk tab eller ansvarspådragelse</td>
<td>Lille</td>
<td>Moderat</td>
<td>Moderat</td>
<td>Stor</td>
</tr>
<tr>
<td>Skade på myndighedsinitiativer eller andre offentlige interesser</td>
<td></td>
<td>Lille</td>
<td>Moderat</td>
<td>Stor</td>
</tr>
<tr>
<td>Ikke-autoriseret frigivelse af sensitiv information</td>
<td></td>
<td>Lille</td>
<td>Moderat</td>
<td>Stor</td>
</tr>
<tr>
<td>Brud på personlig sikkerhed</td>
<td></td>
<td></td>
<td>Lille</td>
<td>Moderat</td>
</tr>
<tr>
<td>Mulighed for at begå/modvirke opklaring af ulovligheder</td>
<td></td>
<td>Lille</td>
<td>Moderat</td>
<td>Stor</td>
</tr>
</tbody>
</table>

Tegnet ”-” angiver ikke relevant
Current focus: Establishing a shared login solution

- To give better user experience for citizens, businesses and public sector employees
- To spare authorities from establishing redundant infrastructure solutions
- Current model:
  - Based on creation of a trust organisation that vouch for the trust in relation to each participant in the federation – and then
  - One (or maybe more) operators delivering the actual login-service – where the operator likely could be an authority that already has invested in an access solution for external users
- Mandat/politisk tyngde
- Overordnet koordinerede og beslutgende aftaleorgan for hele modellen, inkl. i forhold til arkitektur og standarder for operatør og tilslutningskrav til systemejere
- Sikrer overholdelse af fællesoffentlige standarder
- Overordnet ejerskab i forhold til implementering og almindelig 'drift' af modellen

- Arkitektur
- Teknologi
- Standarder
- Processer
- Organisation

- Teknologi
- Standarder
- Processer
- Organisation

Fastsættet af 'trust'-organisationen

- Fastsættet af 'trust'-organisationen

Kommuner/Borgere/Virksomheder/Brugerorganisationer
No Federation without Trust

Not just a technical thing with servers exchanging certificates
Also trust in that your partners have measures for control/responsibility, well defined processes, perhaps a third party auditing federation partners etc.
Thus we are authoring a discussion paper about Trust in the Danish context
- To get best trust model
- To get ownership from stakeholder to the outcome trust model

Work in Liberty eGovernment Special Interest Group has brought valuable input here
Importance of standards

- **Strategic - Open standards**
  - The Danish Parliament imposed earlier in 2006 the government to ensure that the use of IT is based on open standards.
  - The government is required to maintain a set of open standards (January, 2008).
  - A comply-explain demand to the authorities to follow the use of open standards in new solutions.
  - Open standards should after January 2008 be the foundation for the development and procurement of IT to ensure competition.

- **Tactical - Interoperable standards**
  - Federation with more than one standard requires the applied standards to be interoperable
  - Translation Gateways are often just a “powerpoint fix”
SAML 2.0 is the recommended standard for federation in the Danish public sector

- Approved by IT Architecture committee in April 2005
- Reconfirmed in March 2006 together with decision to work for convergence among the different federation standards/specifications
- Choice of SAML 2.0 validated by Gartner in October 2006 report
Basis for Recommending SAML 2.0

Based on an evaluation of

- Functionality according to requirements
- Support for the standard in commercially available products
- Usage of SAML in other public sector solutions
- Statements from research and analyst companies
- Ratified open standard
- “Composability” with other ratified standards like XACML and SPML
- Future development of the standard
- Availability of 3rd party Interop Testing/Certification
Participation in Liberty eGov SIG

- The Danish Government joined Liberty Alliance earlier in 2006
  - As part of the dialogue with suppliers and standard creating bodies
  - To input public sector requirements into the standards process
  - To share experiences and collaborate with other governments

- Denmark co-founded with participants from Finland, New Zealand, USA, France, UK, and others the Liberty Alliance eGovernment Special Interest Group
eGovernment SIG - Goals and work items

- Discuss challenges associated with building Circles of Trust, e.g. agreements, eGov use cases, etc
- Share solutions and/or technical approaches to avoid ‘reinventing the wheel’, drive standards based solutions
- Contribute to development of Deployment Guidelines
- Discussion around Identity Providers and Identity Brokers – cooperation between public and private sectors or not, Business Models for Federation -
- Work to identify and agree upon two to three SAML deployment profiles
Next Steps in Denmark

- Making the initial deliverables operational
  - with profiling, detailed specifications, pilots etc
  - Establishing the shared Authentication service for federation
  - Discussion paper about the Agreements and Structures required to create scalable Trust between many organizations

- Looking into federated authorization
  - Catalog of common roles?
    - Primarily for authentication by proxy
  - Definition and standards profiles for "Attribute Service"

- Federation of web services
  - Pilot currently running in the health sector
  - Can Liberty ID-WSF and WS-SX end in happy collaboration?

- Federated provisioning

*Guiding frame for all work on Danish public sector*  
*Id&Acc Mgt is the reference model →*
The High Level Reference Model for Identity and Access Management

The Reference model is to be used as a tool for thinking through, creating and sharing processes, services, & technologies for Identity and Access Mgt
High level reference model for Identity and Access Management

Administration and Management includes processes and solutions to handle Identity life cycle.

Services includes provisionering, workflow, delegation/self service

Creation, maintenance and revocation of credentials

"Digital signature", userid/password, tokens, biometric data (e.g. finger prints), Smart Cards, etc.

Collection and protection of the attributes, that are part of a users digital identity

Services includes storage and search/attribute service

Technologies includes virtualization, metadirectory services, enterprise directories.

Registration and protection of information, that enables creation of an audit trail

Services includes logging, history/archiving, proactive monitoring, reporting etc.

Verification or validation of the authentication of a user (or service) based on a collection of attributes from the digital identity of the user/service

Services includes validation of credentials

Verification or validation of the authorization for a user (or service) to use a specific service based on a collection of attributes from the digital identity of the user/service

Services includes storage of policies

Role based, rule based, attribute based, purpose-based access control etc.

The model is inspired by a model from Booz Allen Hamilton
Additional Info

Søren Peter Nielsen
E-mail: spn@itst.dk
What if somebody in the public sector wants to use something for federation that is different from SAML 2.0 and does not interoperate with SAML 2.0?
Creating a working federation is in some ways similar to creating an efficient railroad infrastructure.

We cannot get an efficient railroad if there is not agreement on the width between rails - and

We cannot study this problem as a station-to-station issue.
Creating a working federation is in some ways similar to creating an efficient railroad infrastructure.

We cannot get an efficient railroad if there is not agreement on the width between rails - and we cannot study this problem as an individual rail line issue.
Creating a working federation is in some ways similar to creating an efficient railroad infrastructure.

We cannot get an efficient railroad if there is not agreement on the width between rails -

This is a question about creating an overall efficient infrastructure – and how we best spend the tax payers money while creating it.

Having different width tracks side-by-side probably isn’t the best way to do it...
Currently the WS-Federation specification cannot maintain the integrity of the user when trying to interoperate with SAML 2.0

The issue for the gateway scenario is when the service provider requires high confidence in asserted identity’s validity. This requires the assertion to be signed at the point of origin. However, even if WS-Federation allows for signing the SAML 1.1 token this signature cannot be maintained when being converted to a SAML 2.0 token.
Denmark - the Fundamentals

- 5.5 mill. inhabitants and one of the richest and most equal countries in the world
- Four levels of government with divided responsibility for tasks – both horizontal and vertical (EU, central government, counties (14), municipalities (268))
- Ongoing major structural reform – fewer regions, larger municipalities
- Public sector makes up 1/3 of workforce
- Consensus culture in a multiparty system
Danish e-Government Maturity

Denmark has been number one in e-Readiness for the last three years according to the Economist Intelligence Unit and The IBM Institute for Business Value.