Federation in e-Government

Case: Denmark

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

June, 2006 – Søren Peter Nielsen – spn@itst.dk
Agenda

- A Few Facts about Denmark
- The Danish Reference Model
- Requirements for Federation in Phase 1
- Reference Architecture for SSO
- Criteria for Choosing Federation Standard
- Next Steps in Denmark
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
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.
Danish e-Government so far has been through a Decentralized Approach

A “common” Danish family on a “common” day

Mother - Irene  
Company owner

Daughter - Louise  
Moving

Son - Anders  
Student

Local Gov  
rental subsidiary

Local Gov  
Case-sys

Educational loan & support

“EasyAccount”

Tax Auth

Business services Portal

Service center

Police

Dad - Kenneth  
Public employee

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
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 provisioning, workflow, delegation/self service.

Issuing of Credentials

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.

Logging and Audit

Registration and protection of information, that enables creation of an audit trail
Services includes logging, history/archiving, proactive monitoring, reporting etc.

Authentication

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

Authorization

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
Deliverables under the Umbrella of the Reference Model Includes

- Administration and Mgt.
- LDAP
- OCES
- SPML
- SAML
- XACML
- RBAC
- Logging and Audit

Business case for shared login svc
Recommendations to local Gov

Policies, Reference architectures, Information mdl, Standards, Profiles, Reference implementations, Pilots, etc.
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
It was also a goal to define an architecture with associated standards that allows for a decentralized approach where several smaller federations over time can grow into larger coherent federations without having to make changes to foundational policies and standards.
Reference Architecture for Cross-organizational Single Sign On

Identity Provider (IdP)

Service Provider (SP)

"Portal"

Conceptual Architecture is adopted from US Federal e-Authentication initiative

SAML 2.0 is the recommended federation standard

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

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

Conceptual Architecture is adopted from US Federal e-Authentication initiative

SAML 2.0 is the recommended federation standard
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 Testning/Certification
Next Steps in Denmark

- Creating shared services for federation
  - Authentication
  - Catalog of common roles
    - Primarily for authentication by proxy
- Discussion paper about the Agreements and Structures required to create scalable Trust between many organizations
  - Including Privacy considerations

While supporting and making the initial deliverables operational with profiling, detailed specifications, pilots etc
Additional Info

Søren Peter Nielsen
E-mail: spn@itst.dk

Also watch the following as we update it:
http://www.oio.dk/arkitektur/brugerstyring/english