A Review of the Danish Public Sector Federation

Burton Group Catalyst Conference Europe 2007
Barcelona, 23rd October, 2007

Center for Service Oriented Infrastructure
Danish National IT and Telecom Agency
IT Architect Søren Peter Nielsen
My relation to the Danish Public Sector Federation

The Danish public sector federation team is hosted at the Danish Agency for Governmental Management and lead by Ms Clea Bach

I work as an IT Architect in National IT and Telecom Agency’s Center for Service Oriented Infrastructure (CSI) with a mission to build out the shared IT-infrastructure in Denmark

In this respect I’m part of the federation team being responsible for architecture and standards
Agenda

- Facts about Denmark
- The federation
  - Planning History
  - Business Case
  - Federation Principles
  - Development Plan
  - Architecture and Standards
- Danish SAML 2.0 profile
- The Operator Solution
- On-Boarding
- Some Lessons Learned
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, regions (5), municipalities (98) )
- Public sector makes up 1/3 of workforce
- Consensus culture in a multiparty system
- In the top of e-Readiness and eGov surveys
Danish eGovernment

- In 2012 all relevant written communication between companies, citizens and the public sector should be electronic.
- Parliament decision in June 2006 regarding mandatory use of open standards in public sector solutions
- eGov strategy covering 2007-10 with many initiatives
- The public sector today is digitalized to a large degree
  - First national citizens register implemented in 1968
  - Nation wide registers covering citizens, businesses, housing, geodata, livestock, income data etc
The challenge...

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

Daughter - Louise
Moving

Son - Anders
Student

Mother - Irene
Company owner

Local Gov rental subsidiary

Educational loan & support

"EasyAccount"

Tax Auth

Business services Portal

Local Gov Case-sys

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
There is clearly a need for better integration across government and private sector

- First challenge is almost always to pass assertion of user identity around in a scalable and secure manner
- Given the decentralized structure of public sector federation seems to be the best fit for a solution
- Thus the Danish Public Sector was formed
But it wasn’t as easy as that

History
- Architecture and standards work since 2004
- Business Case report in 2005
- Analysis of potential operators in 2006
- November 2006 – Decision to start planning forming the federation
- January 2007 – Proof of Concept
- May 2007 - Federation formed and operator chosen

“My Page” at the Danish Citizens Portal became the compelling reason to act
Our Business Case

Restricted Scope
- Mainly Local Government to Central Government
- Used benchmark data from internal IAM
  - Heterogeneous: 3 + 9 FTE / 1000 users
  - Homogenous: 1 + 8 FTE / 1000 users
- At 30.000 users
  - Expect a direct saving per year at approx. DKK 20-30 million (~2.7 – 4 million Euro) using federation

My opinion: Direct savings is not the point – Federation is an infrastructural enabler
Principles for the Federation

- It is an Open Federation!
- Open and Flexible Architecture
- Standards Based!
- Phased Development
- Extra Support for First Comers
Federation Development Plan Phases

1) Web SSO
   - Primarily for citizens and employees logging in with Digital Signature

2) Power of Attorney & Consent
   - Shared solutions/standards

3) Government-to-Government SSO
   - Webservices, Each authority can have their own authentication point

4) Federated Provisioning
   - Enables one-stop administration

5) Analysis of potential for common roles
Denmarks chosen standard for federation is SAML 2.0 – by now clearly the standard for Web SSO
We need to align with and try to influence the rest of the world

- It is important to have support in markets beyond our local for our architectures and standards
- We participate various standardization and EU efforts
- In the federation space we have particular benefit from being a member of Liberty Alliance
  - E-Government Special Interest Group
  - Not just Technology
  - Privacy, Policy, Federation Agreements, etc.
Still - We have a special Danish SAML profile

Describes

- Web SSO – using redirect/POST binding
  - With attribute mapping
  - With persistent pseudonyms
- Single Logout – using redirect/SOAP binding
- Attribute Query – using SOAP binding
- Attribute profiles that describe extra attribute sets that can be transferred as part of authentication assertions or in attribute assertions
Why a special Danish SAML profile?

Two reasons:
- Cultural extensions – e.g Attributes like Business number, etc.
- Remove complexity in subset of standard that fulfills our use cases
  - Less variations to test
  - Less variations to do risk analysis on
  - Less implementation requirements for federation members that want to implement their own SAML-integration

The profile is to a very large degree adopted from the US eAuthentication SAML profile. Liberty eGov SIG is studying feasibility of common eGov profile
## Subset of OASIS Conformance Modes that are applicable to Danish Requirements

<table>
<thead>
<tr>
<th>Feature</th>
<th>IdP</th>
<th>IdP Lite</th>
<th>SP</th>
<th>SP Lite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web SSO, AuthnRequest, HTTP redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Web SSO, Response, HTTP POST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Web SSO, Response, HTTP artifact</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Artifact Resolution, SOAP</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Enhanced Client/Proxy SSO, PAOS</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Name Identifier Management, HTTP redirect (IdP-initiated)</td>
<td>MUST</td>
<td>MUST NOT</td>
<td>MUST</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Name Identifier Management, SOAP (IdP-initiated)</td>
<td>MUST</td>
<td>MUST NOT</td>
<td>OPTIONAL</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Name Identifier Management, HTTP redirect</td>
<td>MUST</td>
<td>MUST NOT</td>
<td>MUST</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Name Identifier Management, SOAP (SP-initiated)</td>
<td>MUST</td>
<td>MUST NOT</td>
<td>OPTIONAL</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Single Logout (IdP-initiated) – HTTP redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Single Logout (IdP-initiated) – SOAP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>Single Logout (SP-initiated) – HTTP redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Single Logout (SP-initiated) – SOAP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>Identity Provider Discovery (cookie)</td>
<td>MUST</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
</tr>
</tbody>
</table>

* IdP MUST support SOAP binding for Single Logout. SP and SP Lite MUST support IdP Discovery.
Initial timeline for the operator solution

Contract signed

Budget approved

Analysis

Approved Solution design

Development, Customization and internal test

External test

Acceptance test

SSO Ready!

However, Contract could not be closed within budget and uncertainties could not be mitigated. Further operator solutions were analysed over the summer. Conclusion: Go for tender, Standard-enable existing login community
Existing Login Community

Current traffic:
220,000 logins per month ~ 100,000 users per month
... to Standards Based ...

"No Extras" solution – Still operational 2Q 2008

In 2008 we expect two waves of federation build-out:
First: 1 Portal, 12 SP’s, 30 Apps,
Second: 3 Portals, 25 SP’s, 75 Apps
On-Boarding

- Efficient on-boarding a huge focus
  - Need major effort for first wave
  - Proof-of-Concept includes tuning the on-boarding process
  - Supplier “integrator certification”
  - Further usage of metadata files
  - Not so pessimistic about technical and organisation scaling once trust scales
- Different categories of Service Providers has different solution requirements
- Strategies to lower the standard-based integration cost
  - Aiding Market Transparency
  - Framecontract for SP-“box” – maybe
  - Description of requirements – and asking the market to respond – maybe more likely
  - Open Source components – target authorities that anyway are comfortable applying open source
Some Lessons Learned

**Operator**
- Hard to promote part of enterprise solution to shared component
  - Identity as a service is still far away
- More choice/easier to evaluate/compare solutions with a standards based function set
- Standard logging may not be sufficient for legal requirements
- Not all federation products support HW storage of certificates

**Risk Analysis**
- No compromise on Integrity and Confidentiality while availability can be adjusted as SP volume grows
Some Lessons Learned - continued

- **Profile**
  - No support beyond basic profile for Attribute Service

- **Proof of Concept**
  - Great advantage from Configuration via metadata
    - Some products required deleting a few lines from metadata file before being able to read it – should be fixed by now
  - Need to create concept for coexistence with “local” federations
  - IE may behave different when running on “non-standard” ports
A concluding remark

While federation may have had it’s 10 minutes of fame among the industry thought leaders...
...this may just be a sign that federation is maturing into being an ordinary thing
Federation will enable new and exiting solutions as well as efficiencies in utilizing existing solutions
Obviously other barriers than the protocol wars have delayed implementation, but just like millions of lives could have been saved if WWII had ended in ’44 we could have been further up along the curve with new innovative federated business applications if the industry had been able to converge on one common federation “plumbing”
</end>
Risk Analysis for the solution

- 1st phase [Requirements specification]: Determining Consequences
- 2nd phase [Solution Design]: Evaluation of threats, vulnerabilities and risks
- 3rd phase [Implemented solution]: Control/Security evaluation of actual solution

First phase is done
First phase

Found consequences with regard to

- Availability, Confidentiality and Integrity

In the areas

- Economic loss/liability, Proces, Reputation, Policy, Stakeholder, Personal safety, Privacy, and Legal violations

Reviewing the following use cases

- User: Service access, document signing
- Authority: Service access, document signing
- Private Business: Service access, document signing
No compromises on the integrity of the solution - However, downtime up till 4 hours not critical to same degree
Why “last century” still is very relevant for people building real-world business solutions:

**Strategic Implications of IT**

<table>
<thead>
<tr>
<th>Local/Functional Optimization</th>
<th>IT Efficiency</th>
<th>Process Optimization</th>
<th>Strategic Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific Business Needs</td>
<td>Local Knowledge Worker Support</td>
<td>Non-core Business Needs</td>
<td>Local Customization</td>
</tr>
<tr>
<td>Data Center</td>
<td>Technology Standardization</td>
<td>Core Process Integration</td>
<td>Wired Business Core</td>
</tr>
<tr>
<td>Application Silo</td>
<td>Standardized Technology</td>
<td>Shared Product &amp;/or Customer Data Bases</td>
<td>Accessible Core Data Objects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rationalized Data</td>
<td>Modular</td>
</tr>
</tbody>
</table>

**Architecture Maturity**

©2003 MIT Sloan CISR, Ross. Used with permission. All rights reserved.
Danish e-Government Maturity

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

Challenges of having competing standards - The question is

Should federation be considered an integration technique that is used to allow several organisations share a limited set of applications? – or –

Should federation be considered an underlying necessary infrastructure to allow citizens, businesses and authorities to collaborate broadly?

Can we fulfill the goals in the EU eGovernment i2010 action plan without taking the infrastructure perspective?
Federation is similar to creating an efficient railroad infrastructure

This cannot be studied as
- a single station issue
- as an individual line issue

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...