Building a portal for citizens in Norway with secure authentication and single sign on

Dag Efjestad
Agenda

- Overview
- Authentication – ID
- MyID solution
- Integration with MyID
- MyPage
Norway

- 4.600.000 citizens
- Everyone has an unique id
- 2005:
  - 75 % has a pc and 60% use it every day
  - 60 % has Internet access at home
  - 50 % has access to xDSL
Public sector in Norway

- About 1800 different organizations
- Three main levels
  - Local
  - Region
  - Central
- IT
  - Variations is size/complex/advanced
  - Often very independent institutions
  - Some common portals – Altinn/Region portals
**eNorway 2009**

- All relevant public services shall be digital.
- Enable the vision of the digital citizen
  - From 2007 shall everyone be able to choose how to communicate with the public sector
- All services from the public sector shall be based on open standards
- During 2009, all public services will be available in MyPage
Before MyPage ....

- Industry
- Altinn.no
- Public institutions
- Local authorities
- Security
- Services
- Citizen
- Security
- Services
After MyPage …

Industry
Altinn.no
Other Portals
MyPage

Citizen

Common Services

Services from public sector
MyPage – makes the day for the citizen

For citizens:
- Common portal – don’t need to know public sector.
- Don’t have to deal with different authentication mechanism
- Can get information about themselves that are registered in public sector

For public sector:
- Get more digital services in public sector and easier marketing against the public.
- Establish common architecture and standards for public sector.
Autentication
What is available?

- PKI based solutions
  - BankID
  - Skandiabanken
  - Buypass – Tippekortet
  - SIM-card
  - ++

- Push vs Pull

- PIN code from TAX – Almost everyone 😊
- Almost everyone know have to use it
- Pushed out to over 3.5 mill.
PIN Codes from TAX department

- TAX Form - printed out once per year
- Each pin is 5 chars long
- 20 numbered codes per TAX form
- We will establish an order service. Here we will have 100 codes per order.
- Only used for login on to TAX dep. and MyID

<table>
<thead>
<tr>
<th>NR</th>
<th>KODE</th>
<th>NR</th>
<th>KODE</th>
<th>NR</th>
<th>KODE</th>
<th>NR</th>
<th>KODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6345</td>
<td>6</td>
<td>3244</td>
<td>11</td>
<td>89732</td>
<td>16</td>
<td>21213</td>
</tr>
<tr>
<td>2</td>
<td>32223</td>
<td>7</td>
<td>65672</td>
<td>12</td>
<td>43424</td>
<td>17</td>
<td>12933</td>
</tr>
<tr>
<td>3</td>
<td>54603</td>
<td>8</td>
<td>78377</td>
<td>13</td>
<td>86513</td>
<td>18</td>
<td>78146</td>
</tr>
<tr>
<td>4</td>
<td>32390</td>
<td>9</td>
<td>65456</td>
<td>14</td>
<td>56167</td>
<td>19</td>
<td>32948</td>
</tr>
<tr>
<td>5</td>
<td>45089</td>
<td>10</td>
<td>76893</td>
<td>15</td>
<td>76346</td>
<td>20</td>
<td>27189</td>
</tr>
</tbody>
</table>
MyID and PIN Codes

- Only 1 pin code card/paper is active
- Yearly updates from TAX for all Norwegians
- Daily updates from TAX ordering service.
- Possible to disable a user/pin code
MyID solution
MyID solution

MyID

LDAP Repository

Authentication module

SAML 2.0

Users from Tax

Web interface

Integration with SP’s
What is Federated Identity?

- “The agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.”

Federation Concepts

- Federation starts with a group of companies that agrees to join together to exchange user authentication information and user profile information.
- The group forms a Circle Of Trust which centers around one or more one Identity Providers and a number of Service Providers.
- These companies have related products to offer the customers in each of their databases.
- The union of the person's identity information in each of provider's databases is called the user's federated identity.
Federation Concepts (continued)

- Federated identity information is shareable amongst the members of the circle of trust, shareable under controlled policy restrictions.
- Federated identity allows Single Sign On (SSO): a user logs in to one of the service provider sites and can click through to another service provider part of the CoT without having to re-authenticate or reestablish their identity.
- Once logged in, a user can log off using single log off which logs the user off all the Federated web sites.
SAML

SAML is from OASIS: http://www.oasis-open.org

- The OASIS Security Services Technical Committee is in charge of defining, enhancing, and maintaining the SAML specifications.
- SAML is an XML-based standard to enable the exchange of security information between a security system such as an authentication authority, and an application that trusts the security system.
- Standard for communicating authentication, authorization and attribute information among members of a circle of trust.
- Allows organizations to securely send assertions between partnered organizations regarding the identity and entitlements of a principal (an example principal is a user).
Scenario
Integrating with MyID
Verification of products/suppliers

- Sun
- IBM
- CA
- Oracle
- Novell
- Software Innovation
- HP
- Kantega
How to?

1. Must have a transaction service in MyPage
2. Establish an agreement with norge.no
3. Install and configure an infrastructure for acting ServiceProvider – SAML 2.0
4. Establish and verify an connection against the MyID verification environment.
Documents

- Design guide
- Implementation guide
- Verification process
- Agreement
Mine kjøretøy

Du er her: Forside > Mine kjøretøy

Følgende kjøretøy er registrert på deg hos Statens vegvesen

<table>
<thead>
<tr>
<th>Kjønnemerke</th>
<th>Merke</th>
<th>Modell</th>
<th>Registreringsår</th>
<th>Eierforhold</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP 25647</td>
<td>SEAT</td>
<td>TOLEDO 1998</td>
<td></td>
<td>REGISTRERT EIER</td>
<td></td>
</tr>
</tbody>
</table>

Vis flere detaljer om dette | Utskriftsvennlig visning

Kontaktinformasjon for eier av tjeneste

- Henvendelser vedrørende dine personlige opplysninger retter du til Statens vegvesen. Telefon: 0 66 50 E-post: kontaksentera@vegvesen.no

Vis relevant informasjon utenfor MinSide
Services on MyPage

- Access to information like: My Vehicles, My properties…
- Access to services like: apply for health card, apply for child support, apply for driver license….
- Information about my community
- Messages from public sector
- Important dates
Service types on MyPage

- **Transaction service**
  - Url to a service on another site with SSO.
- **Data retrieval service**
  - Webservice which retrieve data of the citizen
- **Message service**
  - A citizens mail box on Internet for public sector
- **Calendar service.**
  - Public and personal events
Transaction service

- Url to another web site with SSO
- Language support
- WAI requirements

Future:
- Transaction services with web services
- WSRP?
Data retrieval service

- Standardized web service call.
  - WS-I Basic Profile 1.1
  - Only read
  - Secured by VPN
  - XSL – Detail view, Summary view, print view, filtering
  - Standardized XSD for calling and errors
  - SERES?
Data retrieval service (Continued..)

- Liberty ID-WSF?
- Not secured by VPN but WS-S
- WS-I Basic Security profile 1.0
- Common registry UDDI/ebXML
- Use of a common tool and repository for creating schemas. (SERES?)
- Also transactions
Messages

- Based on ordinary e-mail
- Also support structured messages (XML)
- SMS and e-mail alerts
- SSL/TLS (STRATLS)
- Future:
  - web service based?
Avsender: Oslo kommune
Tittel: Kvittering på søknad om barnehageplass
Dato: 01.02.2006 12:45
Referanse: OK938451

Du sendte inn søknad 29.01.2006. Dersom du ønsker å se på innsendt søknad eller endre på opplysninger kan du klikke på linken under som vil åpne nytt vindu med utfylt skjema.

Referanse til sak: OK938451

Du kan også se på tilgjengelige barnehager i din bydel, dine rettigheter samt utskrivingsvennlig visning av relevant informasjon i melding.
Jeg ønsker ikke fornyelse

Avsender: Vegdirektoratet
Tittel: Du må fornye førerkort
Dato: 01.02.2006 12:45

Ditt førerkort av type G går ut 03.04.2006 og må fornyes. Ta kontakt med din Vegdirektorats kontor i Oslo.

Svar

Mottaker: Vegdirektoratet
Tittel:

Svar på: Du må fornye førerkort

- Jeg ønsker ikke fornyelse
- Jeg har ikke førerkort
- Jeg trenger utsettelse

LASTE OPP VEDLEGG
Email catalogue

- Possible to retrieve email addresses with LDAPS.
- The register shows only registered users of MyPage.
XFORMS

- Rendering of XFORMS schemas
- Use external schema repositories
- Delivery of schema with email, web service or http to the service provider.
MyPage/MyID – software

- Sun JES
  - Portal server
  - Access manager
  - WebProxy med SSL
  - Application Server
  - Mail server
  - Calendar server
  - Directory server
- Fatwire Spark Web Content management
Questions