Interoperable and Secure Authentication for Organizations on e-government

Tero Pernu
National Board of Taxes
Finland
Start point and challenges back in 2004

- There weren't any sufficient coverage/leverage of organization authentication system
- Various proprietary authentication methods
  - It is practically impossible to utilize existing authentication methods in different services
- **Strategy**
  - Supporting e-government in general: State Information society program and NBT IT-strategy
- **Must increase productivity**
  - Pressure from central government
Feasibility Study Conclusions in Jan 2005

- Support open and standard
- Avoid new proprietary methods and get away of old ones
  - This is the goal, real world is another thing…
  - E.g. mobile PKI with roaming, ETSI-204/Ficom
- Liberty Alliance advantages
  - Secured, privacy oriented and de-centralized
  - Collaboration with other standardization bodies
  - Federation
  - Support not only browsers but clients also
KATSO Schedule

- Requirements gathering was finished in May 2005
- Call for tenders in June 2005
- Selected supplier in August 2005
- Project started in September 2005
- Phase I, November 2005
  - SAML 2.0 WebSSO
  - ID-WSF
- Phase II, January 2006
  - IDP and authorization
- Phase III, February 2006
  - Federation
Katso IDP Features

- Katso OTP authentication method
  - User ID, password and one-time-password
- Katso PWD
  - User ID and password
- Browser and client based authentication
- Authorization service
- Federation
- Administration
  - Front office, Back-office and Master admin
Katso platform and software

- Sun Fire, Solaris, Bea Weblogic, My SQL, Open LDAP
- Ubilogin 3.1 by Ubisecure
- Integrator, support service provider by WM-data
Options for browser implementation

• **SAML 2.0**
  - Service Provider implements SAML 2.0 Service Provider features
  - Authentication according to standard, not integrated with the IDP

• **Ubialogin SAML 2.0 Web Agent**
  - Web agent requires a lot less experience and allow fast implementations
  - Acts as a Service Provider in front of service
  - Integrated to the IDP
Options for clients implementation

- There should be an implementation of Web Service Client (WSC)
  - Makes possible to use Katso authentication straight through e.g. pay-roll system
- For server application Web Service Provider (WSP) is needed
  - User is identified in server, e.g. in tax portal without leaving the tax portal
Authorization

- Katso provides standard interface to attribute provisioning to e-services
  - SAML 2.0 AttributeQuery
- Authorization information is on Katso database
  - Maintained by users themselves
- E-service asks for authorization information from Katso –service
  - Secured and privacy friendly: information is not going through browser or client just between servers
Browser Based Authentication

Welcome TestCompany user!

E-Filing

Please Sign In

Tax Portal

Browser

Credentials

Katso IDP

NetBanks

PKI

MobilePKIs
Katso – SAML 2.0 WebSSO

Web browser

HTTP GET

Redirect / POST

Redirect / POST

UID, PWD [+ OTP]

SAML AuthnRequestResponse

Response

Selected Company?

OrgID

SP

Yritys.tunnistus .fi

IDP

KATSO

KARVA

Authentication (UID, PWD [+ OTP])

Response

Roles (KatoID)

Response

Roles

Response

Attribute Request

Selected Company?

OrgID

Attribute Request: Response

Attribute Request: Response
Katso – ID-WSF 2.0
Provided Attributes

- Katso ID
- Role
- Organization ID
- Organization Type
- Personal ID
- Organization name
- + others

- "tfi.kid : 119453"
- "tfi.role : representative"
- "tfi.bin : 1234567-1"
- "tfi.oid : 1.43.3.56.2.1"
- "tfi.pin : 121245-554B"
- "tfi.corporatename : Company ltd"
- "tfi.[+other]"
Benefits to the Government

- **E-services enables significant cost savings**
  - Every transaction made in office costs 20 – 50 euros and an e-transaction 10 – 50 euro cents
- **Simplified processes**
  - Reduced 5 phases on e-filing
- **New possibilities to arrange e-services**
  - E.g. e-filing straight from Pay-roll –system instead of Tax portal web site
- **Life-cycle management (e.g. changes in management, users, mergers etc.)**
- **Reliable roles and authorization (audit-trail)**
Benefits to organizations

• Prerequisite to be able to use government e-services
• Secured and faster transactions
• Streamlined process
  • No manual work, no papers, no archiving
  • No need to go to an agency
• Cost savings
  • Use of existing data from pay-roll or accounting system
  • Better return on investments on ERP-system
Thank you for your attention

tero.pernu@vero.fi
+358 400 87 94 87