

Case Study:

The Finnish National Board of Taxes Makes a Business Case for E-Authentication



Building the Finnish Information Society

The Finnish Government is deeply committed to developing an advanced Information Society. The aim is to increase competitiveness and productivity, promote social and regional equality, and to improve citizens' well-being and quality of life through effective use of information and communications technologies. As a Member State of the European Union, Finland advocates an efficient single market, and a clear and consistent tax system. The National Board of Taxes project is a key element of the advanced e-government initiative.

Challenges

The Finnish Board of Taxes has many responsibilities, including overseeing the tax information flow from business to government, and the authentication of those businesses and individuals who work there, to the government.

The Finnish Board of Taxes sought to improve the taxation e-collection process and to create an authentication model to first improve productivity within their own operations, and then be leveraged to other government areas and functions.

"We were faced with a situation where there were several proprietary authentications being used, but none of them could be leveraged to support a total initiative," said Tero Pernu, planning manager, Finnish Board of Taxes. "We wanted to find a way to support the Finnish e-government initiative and the State Information Society program that was in-line with our IT strategy at the Board of Taxes."

Studying the Situation

The Finnish Board of Taxes introduced a range of e-services in the late nineties including an e-filing service.

"For income tax, you have to have strong authentication, so basically you have to know who exactly is doing the filing for legal reasons," said Tero Pernu. "Another important consideration for us is that authentication and authorization activities need a reliable audit-trail to prevent tax frauds."

Today, the authentication system is implemented so that it can be used in any e-service that the Board of Taxes, or any other governmental agency, introduces. Like e-filing, another typical e-service is the single tax account. How it works is a business will have one tax account and only one balance on this account. Instead of paying company income tax or value-added tax separately to different accounts with different references, businesses will pay taxes in a very flexible and straightforward way to one account.

"These kinds of services need definitively strong authentication because it is a question of trust," explained Finland's Pernu.

"We determined that Liberty is quite good for our purposes. They have done all the work for us, by defining the identification framework and the service framework proposal."

Tero Pernu
Planning Manager
Finnish Board of Taxes

The Requirements of Strong Authentication

In order to determine the requirements for a solid strong authentication system, Tero Pernu and his team carefully evaluated their options and decided on the following:

The solution would be open and standards-based. As part of the feasibility study, they looked closely at the Liberty Alliance. "We determined that Liberty is quite good for our purposes," said Pernu. "They have done all the work for us, by defining the identification framework and the service framework proposal." One of the most important issues was that all the SAML 2.0 and ID-WSF 2.0 specifications could be reviewed by anyone. He added that layered security, a model separating channels, and message security were also seen as major advantages.

New proprietary methods would be avoided and old proprietary methods would be eliminated. According to Tero Pernu, this is a challenging goal. Today, old proprietary methods have been unified to the Katso system during the project. "We moved existing user accounts to the new system. Now old users can utilize all the features that the Katso system provides, including authorization. In old systems, this wasn't possible," he said.

Clear policy for privacy. The EU and Finnish regulations mandate user privacy on e-services. Liberty was attractive because it has excellent documentation relating to privacy issues and details how privacy should be taken into consideration when implementing e-services.

The Solution

Today, the Katso system, the nickname for authentication methods used by the Tax Board, is up and running and serving 120,000 businesses. Katso now enables businesses to file and interact with the government.

Today, Katso acts as the identity provider, and provides the standard interface to a range of e-services. Katso also provides authorization services; e.g., a shop owner can authorize his bookkeeping company to do income tax declaration on his behalf. Bookkeepers must accept the authorization before it is valid.

In addition, the solution utilizes Web service interfaces so businesses and citizens can do the e-filing straight from their payroll system without accessing any of the Board of Tax portals, simplifying the process and making it as short as possible.

"We think that it is easier for the businesses if they are able to do authentication and e-filing seamlessly from their payroll or accounting system, without going to a tax administration's Web page. It is in our interest that our customers can fulfill their legal obligations as easily as possible. There is still room for browser-based solutions, but in service-oriented architecture, businesses want to take more out of their investments in ERP systems," said Pernu.

In this new environment, all business authorization information is on the Katso database and maintained by the users themselves. When an e-service asks for authorization from Katso, it is secure and privacy friendly. Information is not moving between browser and client---just between server back-ends.

Once the Web service interfaces are made to taxation purposes, they are available to other purposes as well.

In addition, any mobile device that supports SAML 2.0 and ID-WSF 2.0 can use all the Katso elements.

"It is in our interest that our customers can fulfill their legal obligations as easily as possible. There is still room for browser-based solutions, but in service-oriented architecture, businesses want to take more out of their investments in ERP systems."

Tero Pernu

Planning Manager
Finnish Board of Taxes

Liberty Alliance Benefits All Participants:

- The specifications are based on open standards
- Liberty's work represents a collaboration with other standards bodies
- Liberty enables federation
- It supports not only browsers, but clients as well

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 administration)

The Technology Solution

- Sun Solaris Enterprise System
- Sun Fire Server
- BEA WebLogic
- MySQL
- OpenLDAP
- Ubilogin 3.1 by Ubisecure (<http://www.ubisecure.com/>)
- WM-Data (<http://www.wmdata.fi>) for integration and support services

The Solution Rollout

Phase I was inaugurated in November of 2005 with the release of SAML 2.0, supported Web-based single sign-on, and ID-WSF. Phase II was rolled out in January of 2006 with the IDP and authorization elements. In February, Phase III introduced federation.

How Government Benefits from Katso

Lower Cost of Service Delivery: Pernu's staff has calculated that every Internet transaction costs their office around 10-30 Euros. If the transactions were made physically to the Tax Board office, the cost would be around 20-50 Euros. "As you can see, the difference is huge," said Pernu. "Lower costs are the most compelling, and only practical, reason for us to support e-transactions and e-services in general."

Support of E-Government: The Finnish Board of Taxes will support e-government actively when it is appropriate and when they have legal framework in place. This includes e-filing straight from the payroll, instead of via the tax portal Web site.

Efficiencies via Standards: On the technological side, the Finnish Board of Taxes wanted to support an open and standards-based solution. "We anticipate that there will be commercial solutions (IDPs) available later on that are based on Liberty specs, because it makes our work much easier," he said. "It is simply easier to use existing interfaces and add new authentication methods that are based on the same standards."

Simplified Processes: Five phases in the e-filing process were eliminated.

Life Cycle Management: (changes in management, users, mergers, etc. ...)

Reliable Roles and Authorization: All authentication transactions and usage of the authorization service will be written to the log, which can be reviewed simply through a Web browser.

Definition of Terms

Circle of Trust (n) 1. a trusted group of identity and service providers who share linked identities and have pertinent agreements in place
2. where an individual or a business inputs a password once and minimal necessary credentials are shared among the Circle of Trust's members
3. a step strongly linked to federation, where multiple entities are involved, and there are business, policy and technical relationships in place
4. also known as "trust circle"

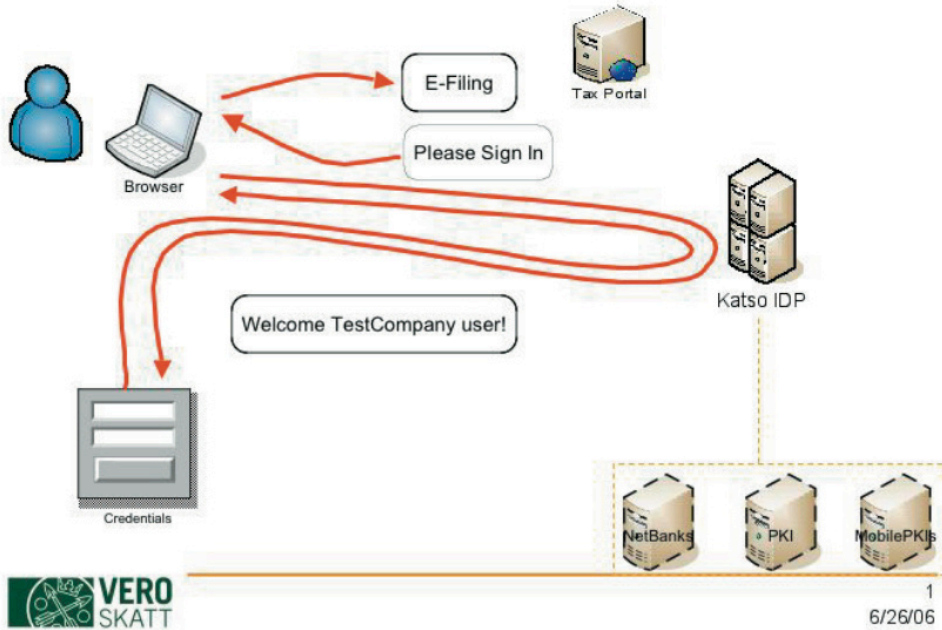
Federation (n) 1. an association comprising of any number of service providers or organizations
2. a model based upon trust in which user identities and security are individually managed and distributed by the service providers or member organizations
3. where the individual organization is responsible for vouching for the identity of its own users and the users are able to transparently interact with other trusted partners based on this first authentication
4. resembles the credit card model in that vendors accept an individual's ability to pay and then that ability is authenticated/verified through a single location

ID-DAP (n) 1. a well-known protocol for looking up information. ID-DAP enables an entirely new business model wherein an application can access information about a principal known only by their federation pseudonym

Identity (n) 1. the most basic element in a high value relationship
2. the individual characteristics by which a person, business, business partner, government agency or other entity is recognized or known

Identity Provider (IdP) (n) 1. a service that authenticates identity; often a trusted party such as a bank, mobile operator, or an Internet Service Provider (ISP)

Browser Based Authentication



How Organizations Benefit from Katso

Access to Government E-Services Secured, Faster Transactions, and Streamlined Processes

- No manual work, no papers, no archiving
- No need to go to an agency

Cost Savings

- Use of existing data from payroll or accounting
- Better return on investments through existing ERP system

Definition of Terms

ID-MM7 (n) 1. MM7 is a specification that has been long used by operators for relaying MMS and SMS traffic. ID-MM7 enables an entirely new business model wherein the content providers know their subscribers only pseudonymously – thus providing unprecedented ability to thwart spam, identity theft and fraud

MM7 (n) 1. a protocol standardized by the 3GPP to allow the delivery and submission of messages between valued-added Service Providers and mobile operators

Mobile Web Services (n). 1. where Web services technologies expose and integrate the value they hold in the mobile domain 2. an opportunity to lower integration costs between operators and content partners

Service Provider (SP) (n) 1. a federation partner that provides services to an end user; service providers typically do not authenticate users but instead request authentication decisions from an identity

About Liberty Alliance

Liberty Alliance is the only global identity organization with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trusted Internet by addressing the technology, business and privacy aspects of digital identity management. The Liberty Alliance Management Board consists of representatives from AOL, BT, France Telecom, HP, Intel, Novell, NTT, Oracle and Sun Microsystems. Liberty Alliance works with identity organizations worldwide to ensure all voices are included in the global identity discussion, and regularly holds and participates in public events designed to advance the harmonization and interoperability of CardSpace, Liberty Federation (SAML 2.0), Liberty Web Services, OpenID and WS-* specifications. More information about Liberty Alliance as well as information about how to join many of its public groups and mail lists is available at www.projectliberty.org.