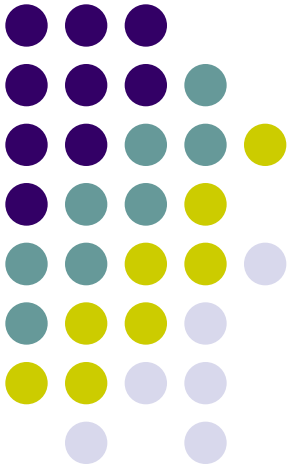
C2G and B2G Authentication and Authorization in Finland

Special Discussion Topic

Kantara Initiative eGov Working Group

Prepared by:
Keith Uber
Ubisecure Solutions Oy

31.1.2011



Agenda

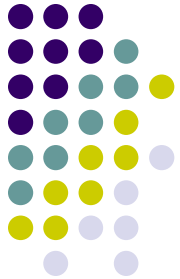
- Citizen Authentication
- Citizen Attributes
- Commercial Identity Providers
- Company Authentication
- Company Authorization
- Higher Education sector
- Authentication of Civil Servants
- Questions / Discussion

kantara INITIATIVE

Finland

- 5.3 million residents
- Parliamentary republic with central government
- 336 local municipalities
- EU member since January 1995

Finnish Personal Identification Number



- National ID number
- Widely used incorrectly for identification
- Format YYMMDD?123X
- Exposes both date of birth and gender

eID in Finland

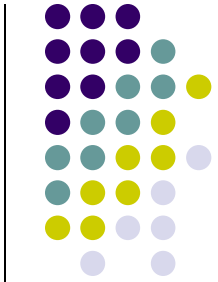
- eID card contains
  - name
  - optionally email address
  - SATU (electronic identification number)
- Not mandatory
- Price 51€
- The SATU number can be converted to a personal identity number through a web services query to the population register

kantara INITIATIVE

eID Statistics

- End of November 2010
  - 341,800 certificates issued to date
  - 272,200 currently valid

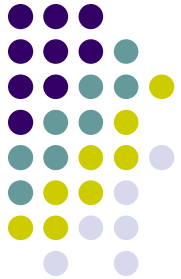
Population Registry



- Provides Web Service interface to population registry data to authorized parties (VTJKysely)
- Interface provides
  - Citizen, building and real estate information
  - Over 80 different types of attributes available
  - Web service interface authentication at connection level using client certificates

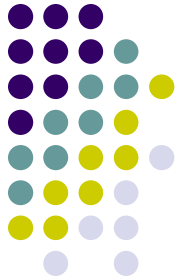
kantara INITIATIVE

Banks as Commercial IdPs for eGov



- TUPAS is a joint bank specification for electronic authentication by the Federation of Finnish Financial Services
- Proprietory protocol
- User must be strongly authenticated
- Typically PIN/TAN list
- Banks provide limited financial liability
- User approves and certifies the personal data released

Banks as Commercial IdPs

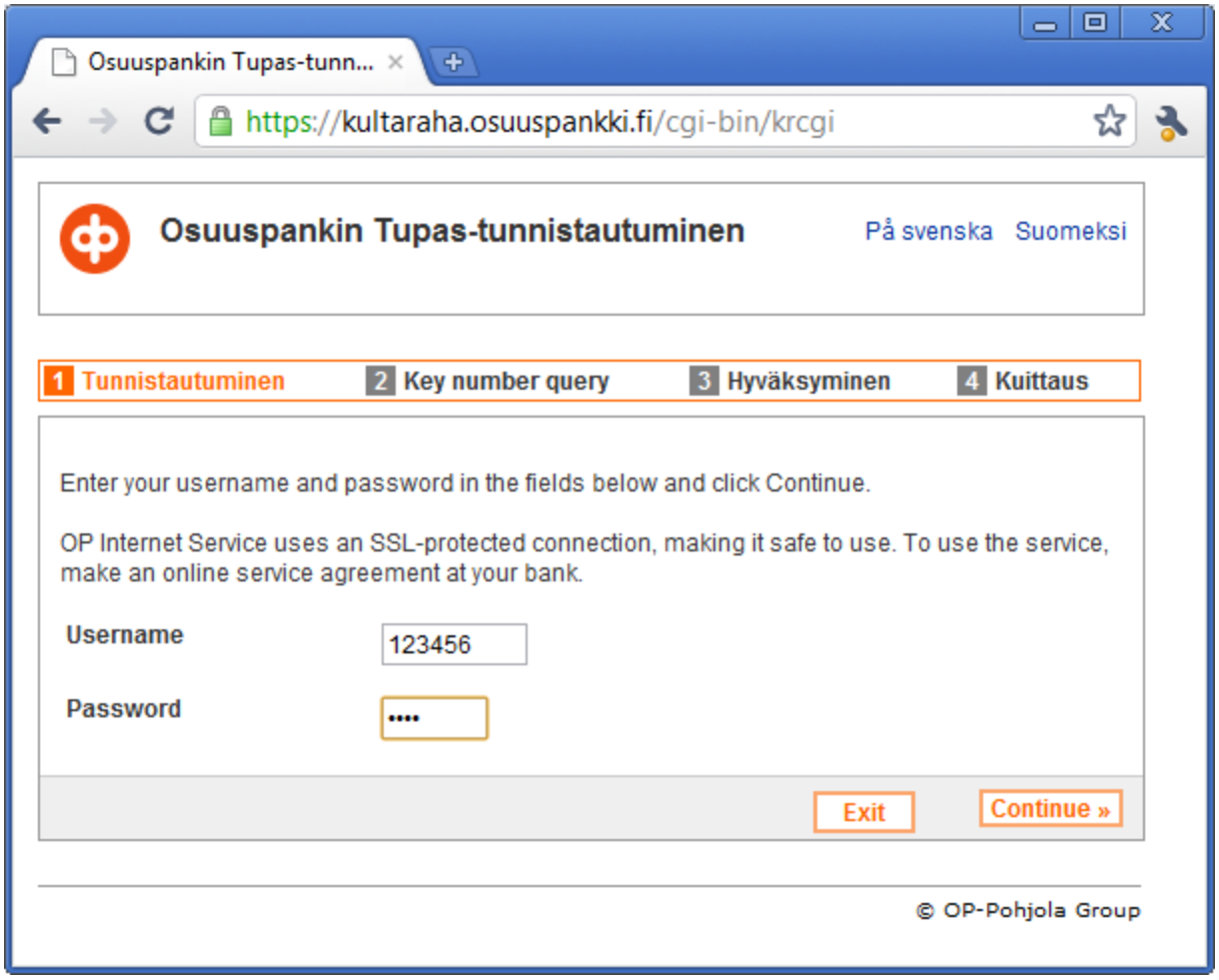


- 10+ banks
- Commercial service
  - Contracts between SP and each bank required including typically
    - Establishment fees
    - Monthly fees
    - Transaction fees
  - Similar process to Verified By Visa etc

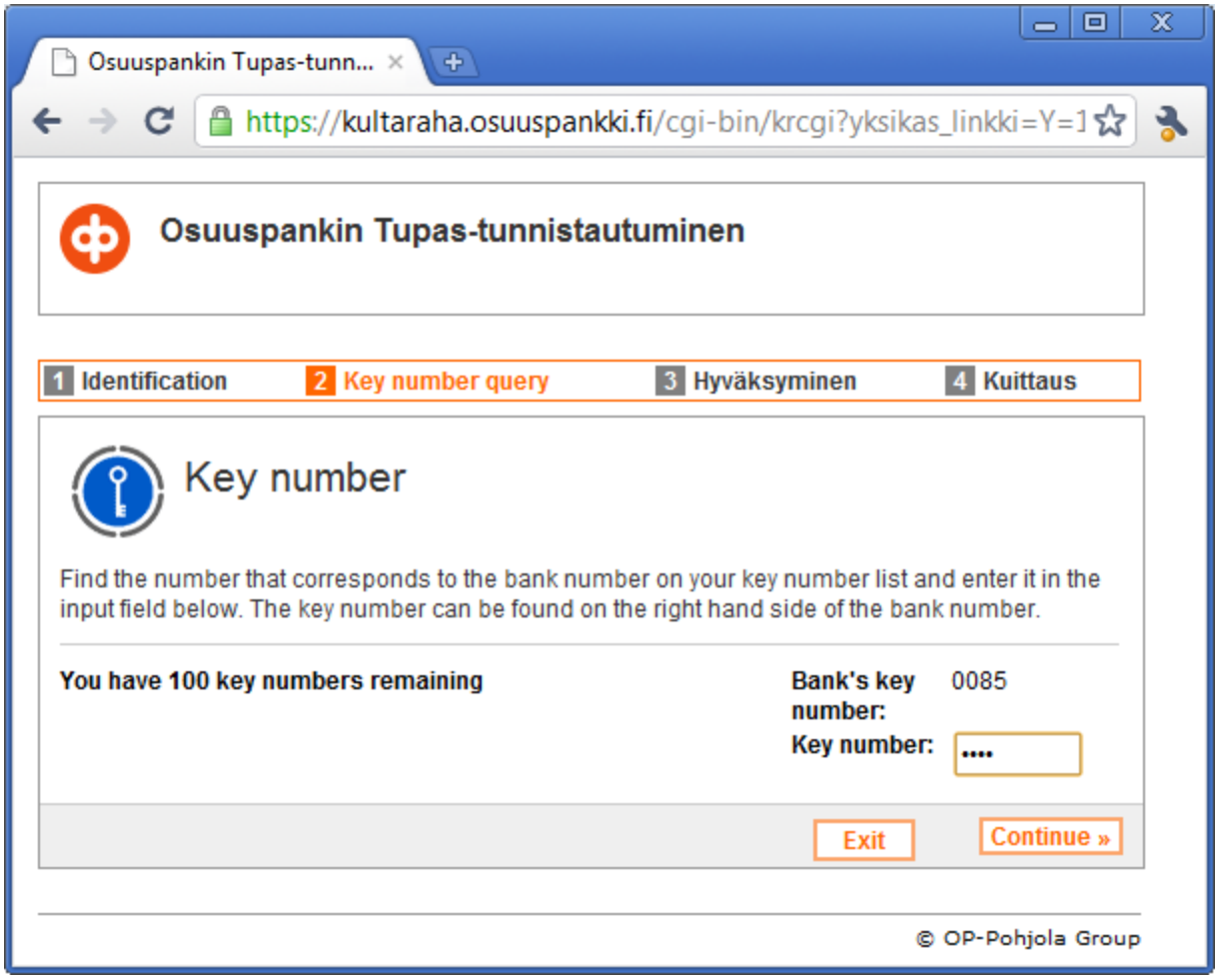
Familiar process

kantara INITIATIVE

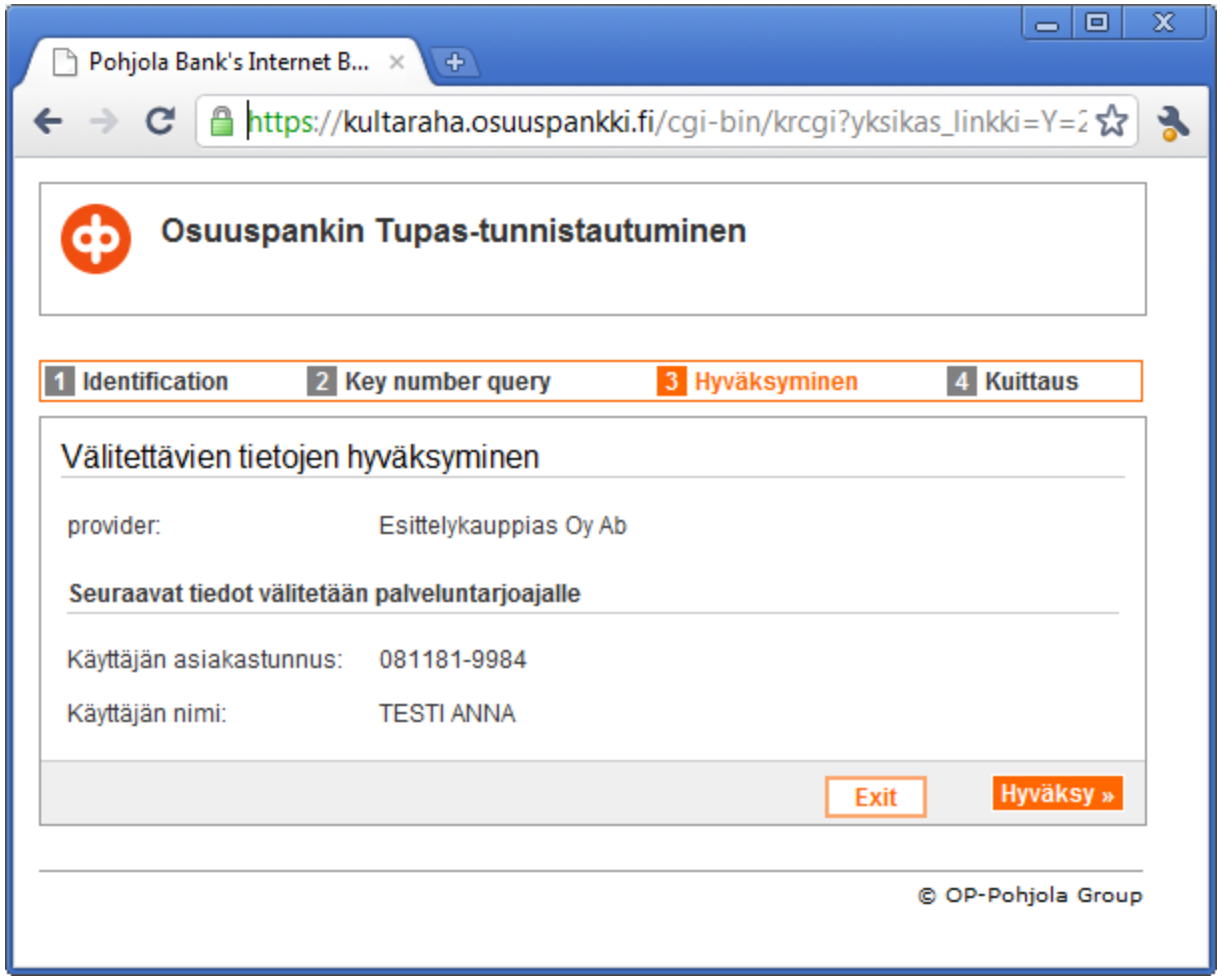
Bank authentication



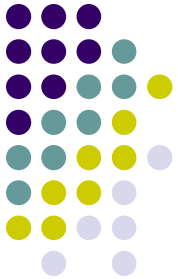
Indexed TAN


Osuuspankin Tupas-tunn...
https://kultaraha.osuuspankki.fi/cgi-bin/krcgi?yksikas_linkki=Y=1
Osuuspankin Tupas-tunnistautuminen
1 Identification
2 Key number query
3 Hyväksyminen
4 Kuittaus
Key number
Find the number that corresponds to the bank number on your key number list and enter it in the input field below. The key number can be found on the right hand side of the bank number.
You have 100 key numbers remaining
Bank's key number:
0085
Key number:
....
Exit
Continue »
© OP-Pohjola Group

Attribute release consent



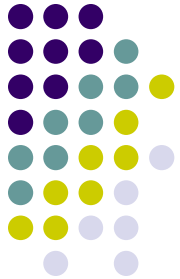
Telcos as Commercial IdPs for eGov



- Commercial Wireless PKI (MPKI, WPKI) service launched 30.11.2010
- Named ”Mobiilivarmenne” Mobile Certificate
- http://www.mobiilivarmenne.fi/en/en_2.html
- Supported by 3 out of 4 national telcos
- Competing with TUPAS service
- Roaming function - one contract with one telco is enough
- ETSI MSS Mobile Signature Service

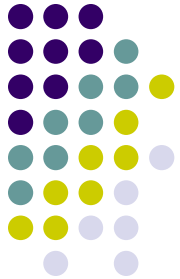
kantara INITIATIVE

Telcos as Commercial IdPs



- Long history – previous studies and commercial trials commencing around 2003 to use national ID in the mobile had failed
- New business model, purely commercial
- Requires government-issued CA license with stringent auditing
- Application embedded in SIM (application toolkit application)

Telcos as Commercial IdPs



- Works while roaming (SMS based transport)
- Pricing for end users
  - Elisa: 0.09 per transaction (Free until Nov 2011)
  - Other telco pricing unknown
- Pricing for SP services
  - Unpublished
- Expected adoption for C2G services in 2011

kantara INITIATIVE

eGov Shared Identity Services

C2G	B2G	Civil servants	Education
Tunnistus.fi	KATSO	VIRTU	HAKA
Vetuma			

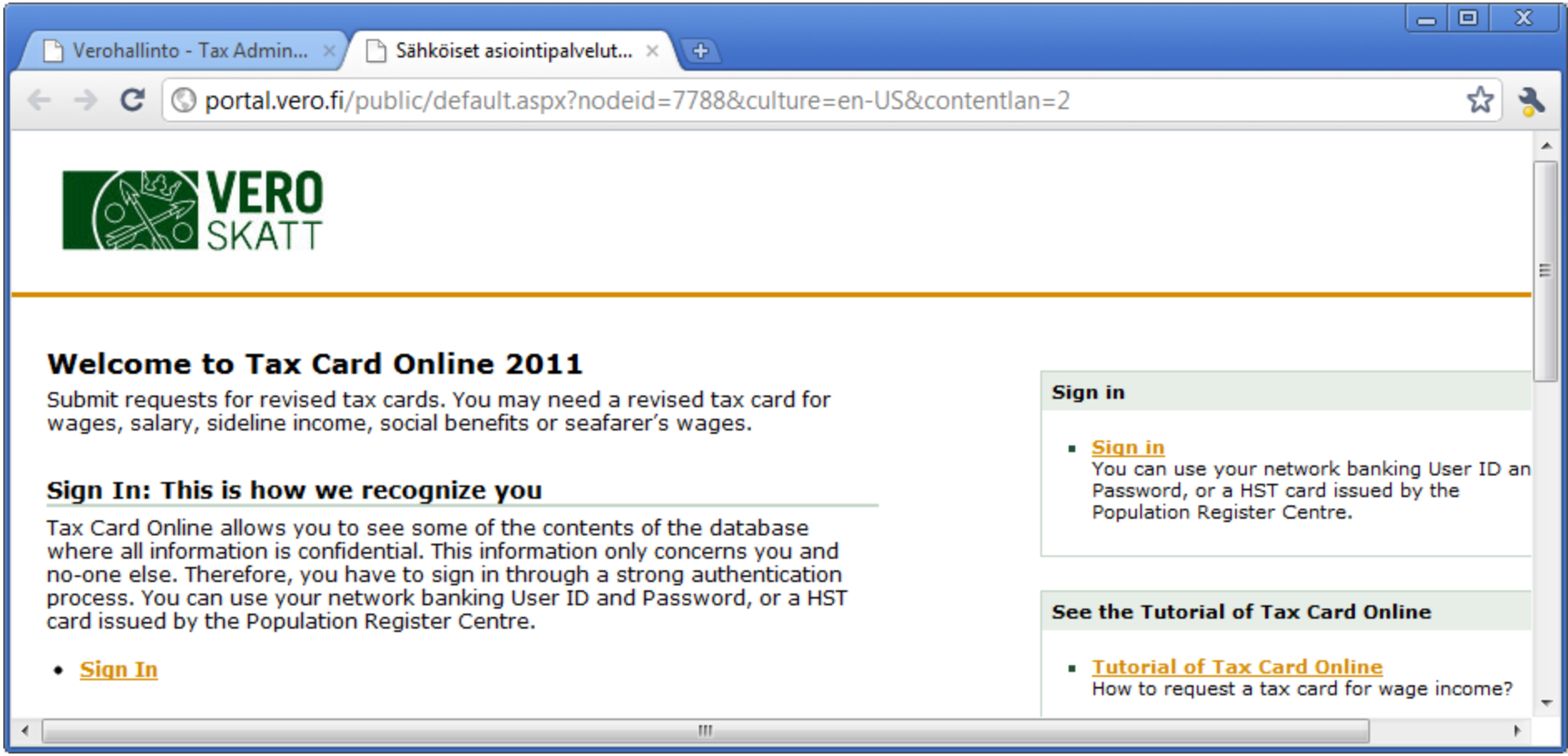
kantara INITIATIVE

Tunnistus.fi Identity Provider

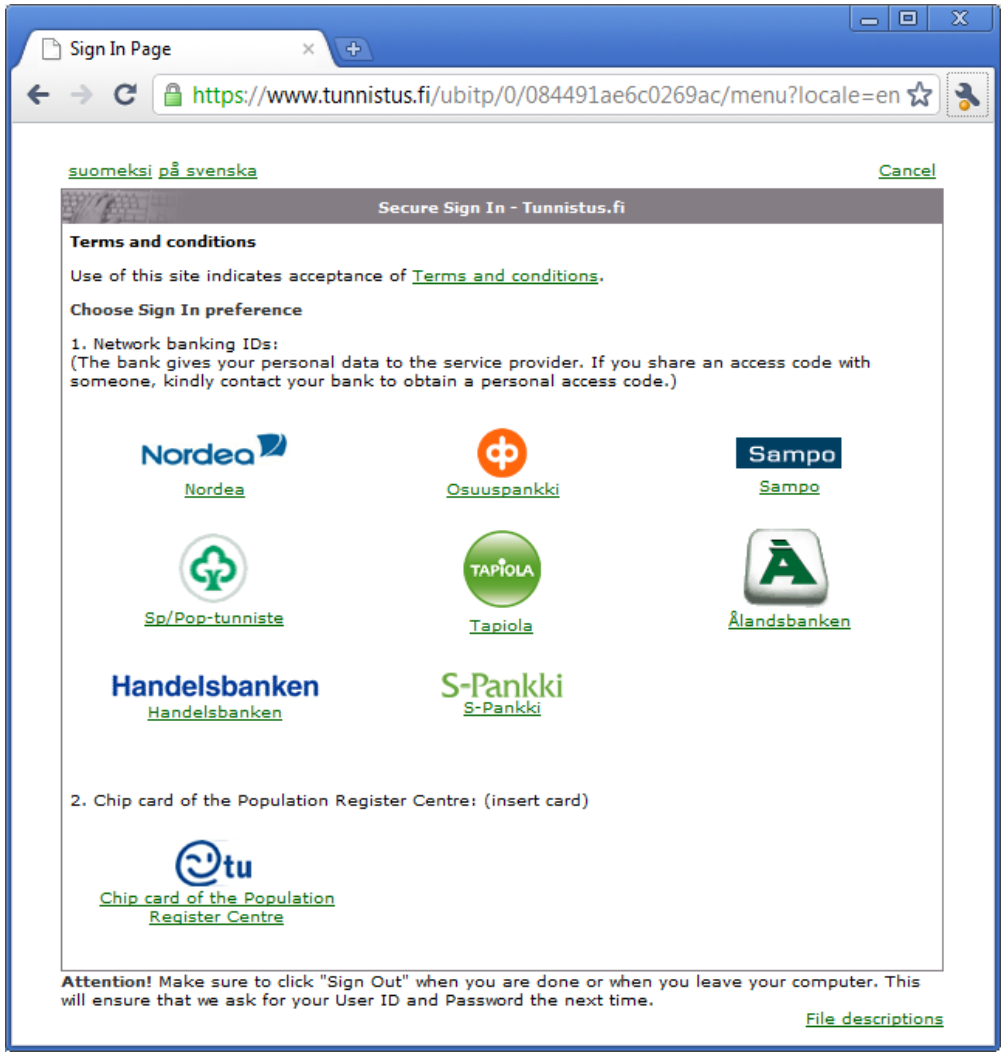
- Tunnistus means Identification
- Joint project of the Tax Administration, Ministry of Employment and the Economy and the Social Insurance office
- IdP Proxy service for Banks and eID cards
- Joint venture consortium contract signed March 2003
- RFQ March 2003, Implementation 5 months
- Operational January 2004

kantara INITIATIVE

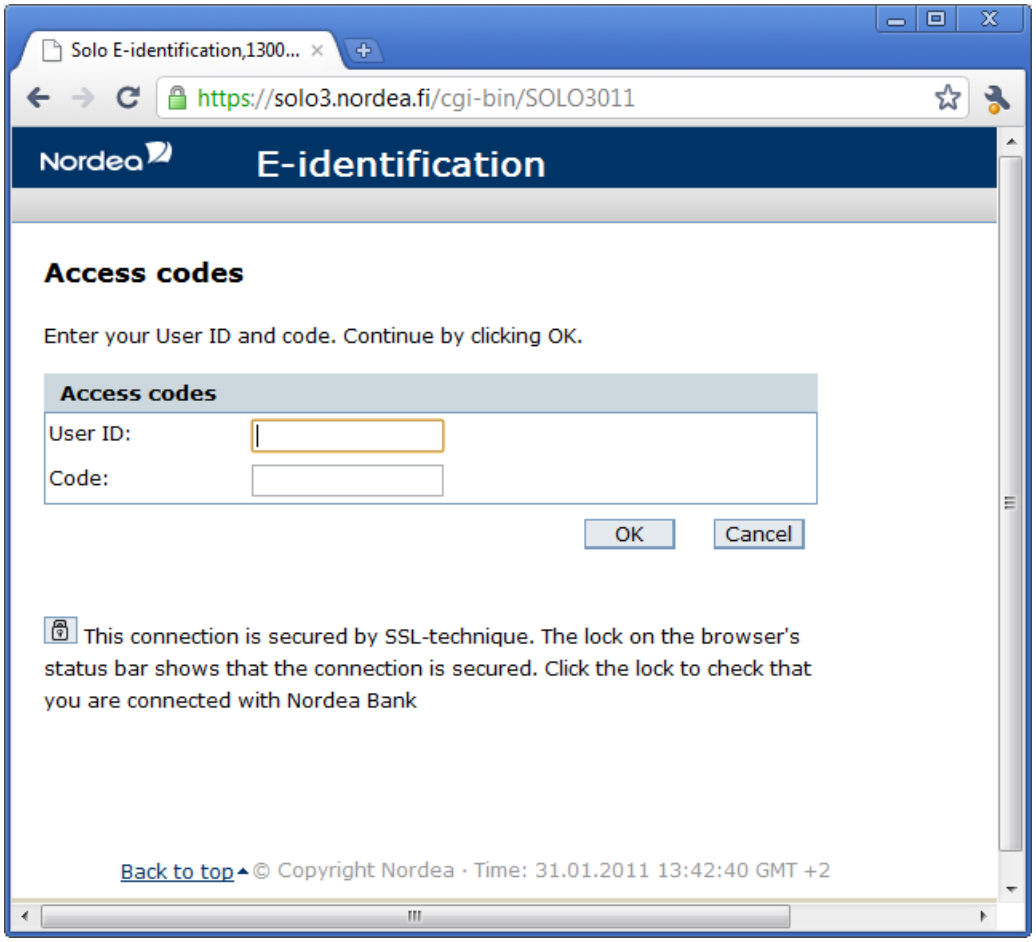
Accessing a service



IdP Discovery

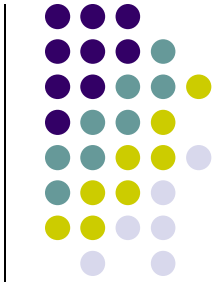


Authenticate at bank (PIN/TAN)



Access to service

Tunnistus.fi



- Web single sign-on based on both proprietory and SAML2 protocols
- Liberty Interoperable tested
- Single logout

kantara INITIATIVE

Tunnistus.fi Statistics

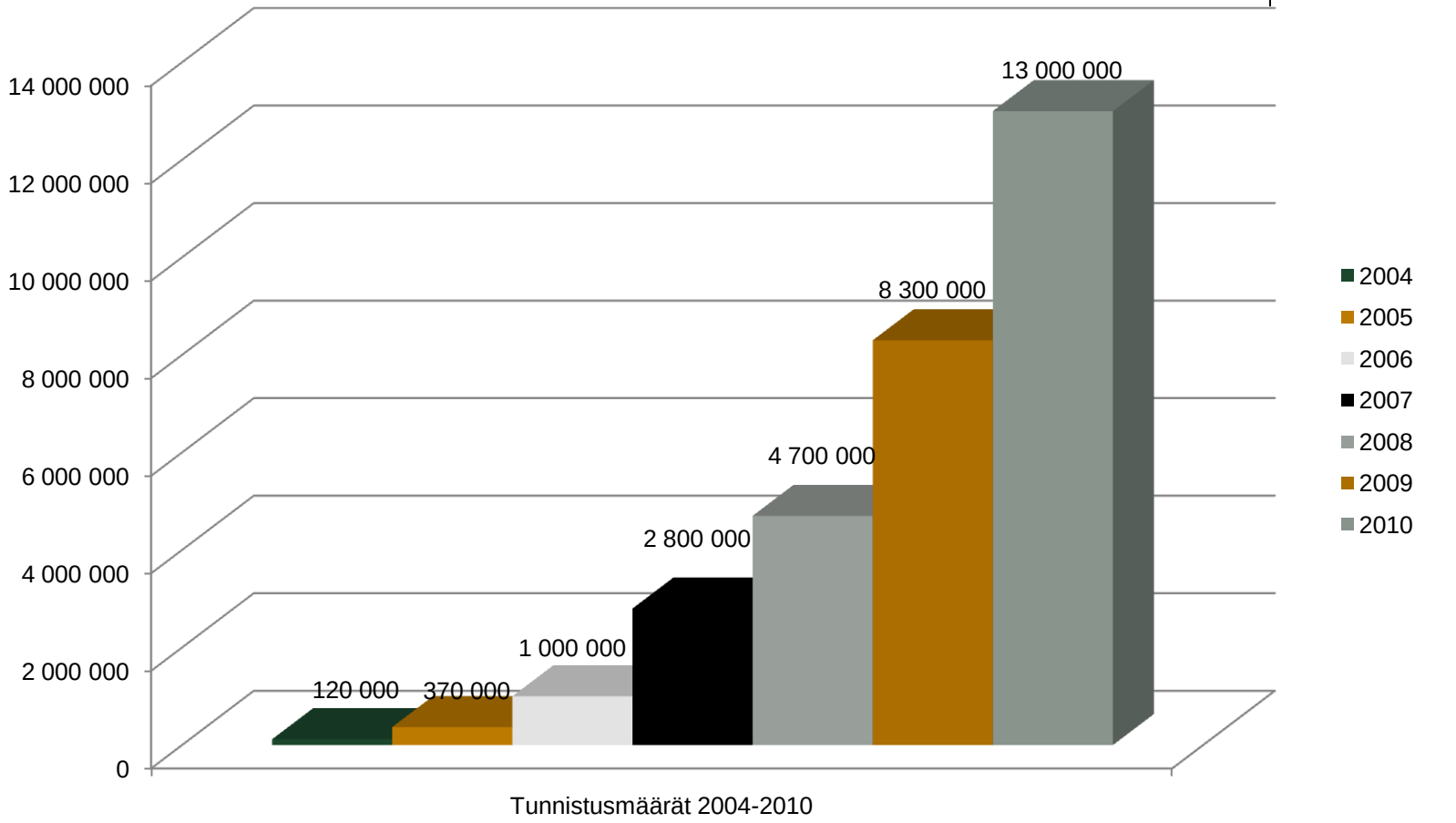
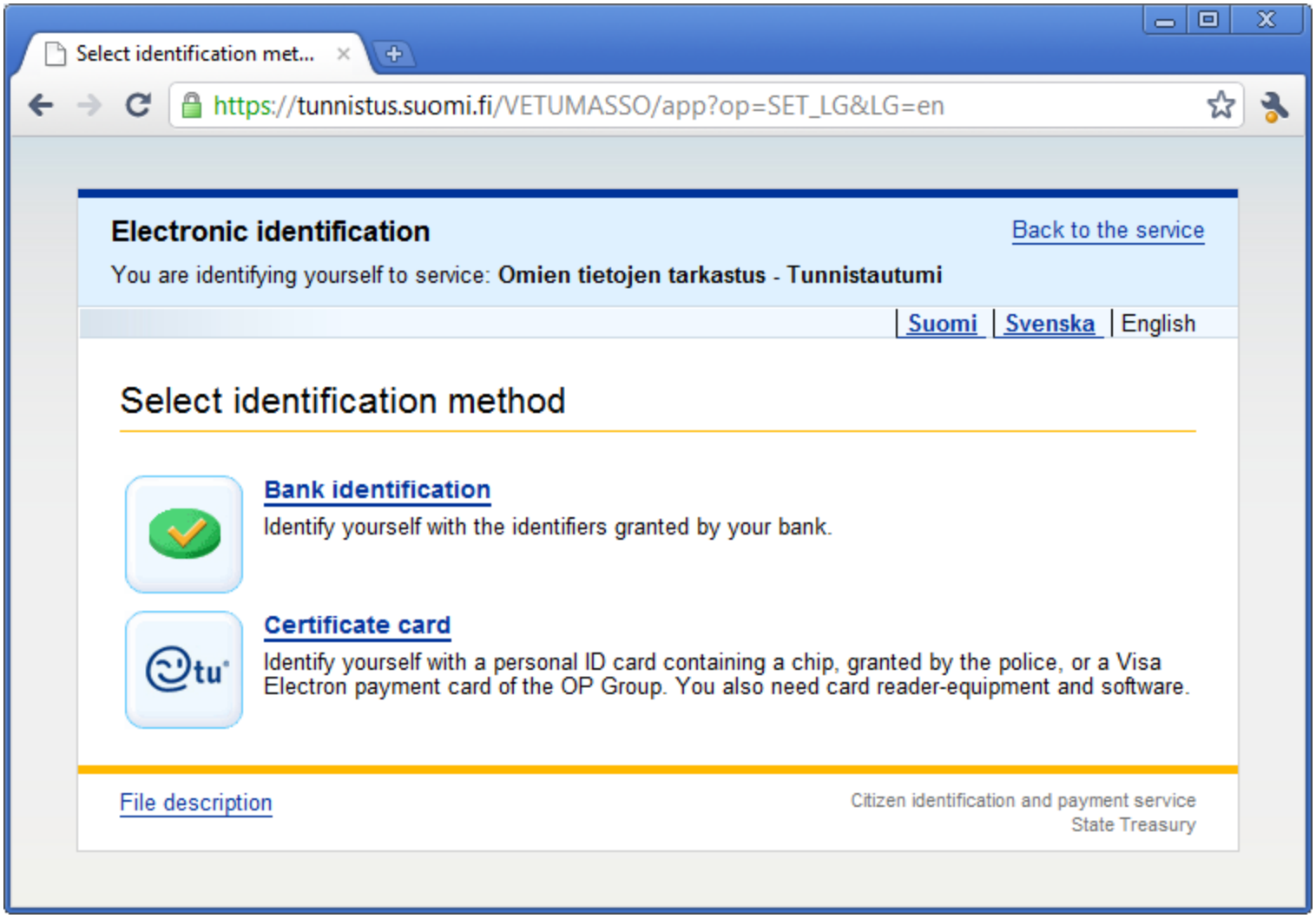
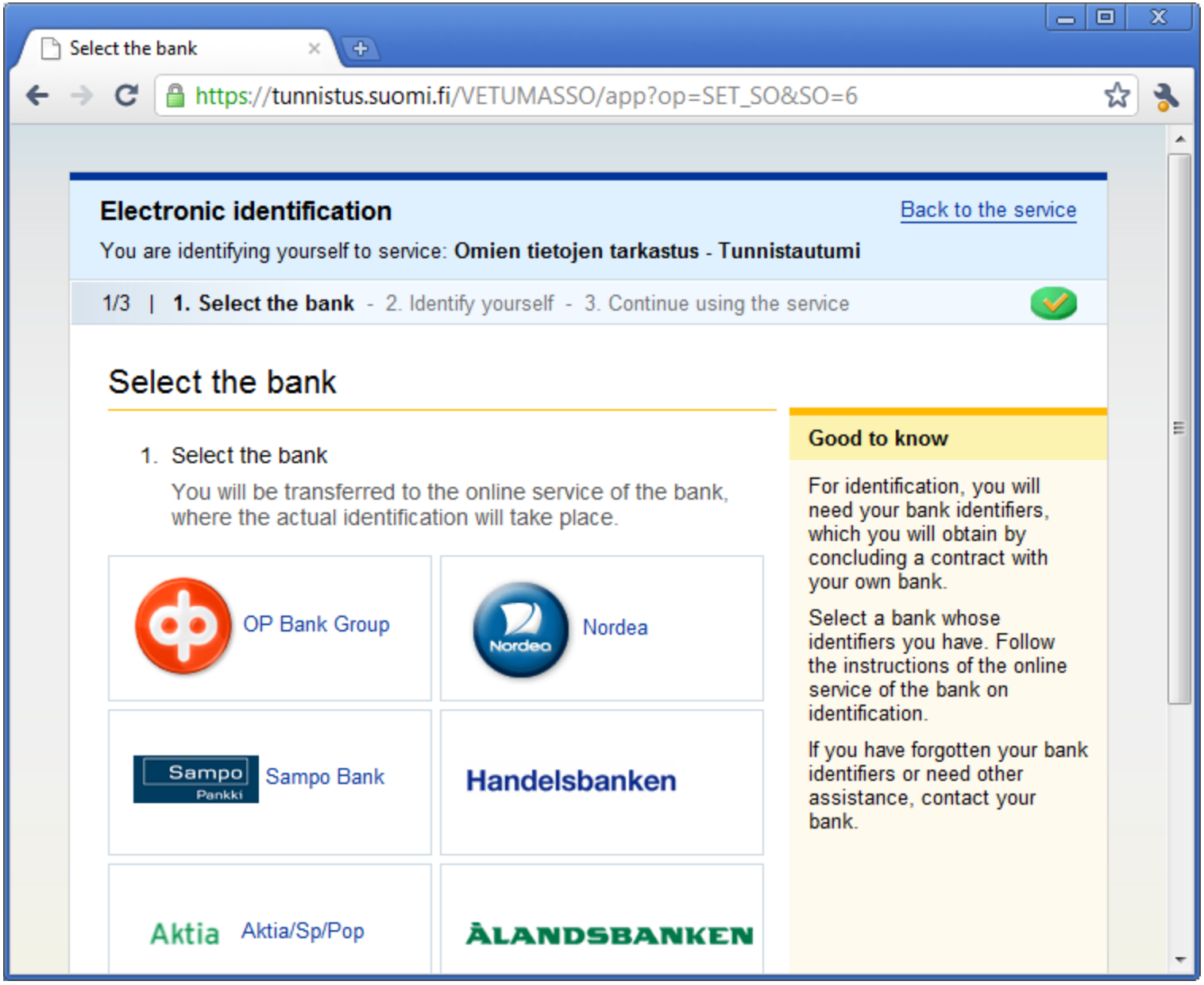


Chart credit: Verohallinta, Finnish tax administration

Vetuma

- Authentication and payment gateway for eGov-services for citizens
- Operational July 2006
- Largely used for regional goverment (local council) services
- Based on both proprietory and SAML2 protocols
- State Treasury service

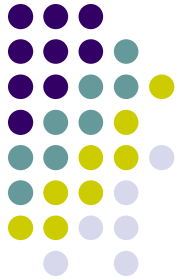

Select identification met...
https://tunnistus.suomi.fi/VETUMASSO/app?op=SET_LG&LG=en
Electronic identification
Back to the service
You are identifying yourself to service: Omien tietojen tarkastus - Tunnistautumi
Suomi
Svenska
English
Select identification method
Bank identification
Identify yourself with the identifiers granted by your bank.
Certificate card
Identify yourself with a personal ID card containing a chip, granted by the police, or a Visa Electron payment card of the OP Group. You also need card reader-equipment and software.
File description
Citizen identification and payment service
State Treasury


Select the bank
https://tunnistus.suomi.fi/VETUMASSO/app?op=SET_SO&SO=6
Electronic identification
Back to the service
You are identifying yourself to service: Omien tietojen tarkastus - Tunnistautumi
1/3 | 1. Select the bank - 2. Identify yourself - 3. Continue using the service
Select the bank
1. Select the bank
You will be transferred to the online service of the bank, where the actual identification will take place.
OP Bank Group
Nordea
Sampo Bank
Handelsbanken
Aktia/Sp/Pop
ÅLANDSBANKEN
Good to know
For identification, you will need your bank identifiers, which you will obtain by concluding a contract with your own bank.
Select a bank whose identifiers you have. Follow the instructions of the online service of the bank on identification.
If you have forgotten your bank identifiers or need other assistance, contact your bank.

VETUMA Statistics

- Services using authentication (t)
  - 47 local government
  - 25 government services
- http://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_-maksaminen_vetuma/yleiset_materiaalit/vetuma_palvelun_tilanne_joulukuussa_2010/VETUMA_tilastot_3_2010.pdf

Tunnistus.fi and VETUMA federation



- Two similar systems cover different target groups under different government budgets with different service mandates
- New government portal service started in 2011 is driving increased authentication volume
- Tunnistus.fi and VETUMA will be federated together in Q1 2011 using discovery based on the CDC approach
- Stakeholders developed the eGov Deployment Profile for Finnish public sector SAML2 WebSSO deployment profile. The profile is based on the Kantara eGov implementation profile 2.0 and the SAML2int.org ver 0.2 deployment profile[1].

kantara INITIATIVE

KATSO B2G AuthN & AuthZ

- Self-service authentication and authorization service for government e-services

- User self-registration
- Role delegation (to other sub-user)
- Power of attorney (user to user, user to organization, organization to organization)
- Self-service credential management

KATSO Roles

- Different role groups
  - Internal system roles
  - General roles
  - Service specific roles
- Total roles: 51 See role descriptions
- Roles provided by KARVA SAML2 Attribute Authority
- SP queries role information after authentication using SAML2 Attribute Query

kantara INITIATIVE

KATSO Web Services

- KATSO operates a Liberty Alliance ID-WSF 2.0 WSIDP also enabling integration of non-browser clients

KATSO History

- Introduced 2006
- 2009: over 30 services
  - Top 3
    - Unemployment registration (Tax)
    - Tax card ordering (Tax)
    - Registering as a job seeker (Social insurance)

KATSO Statistics

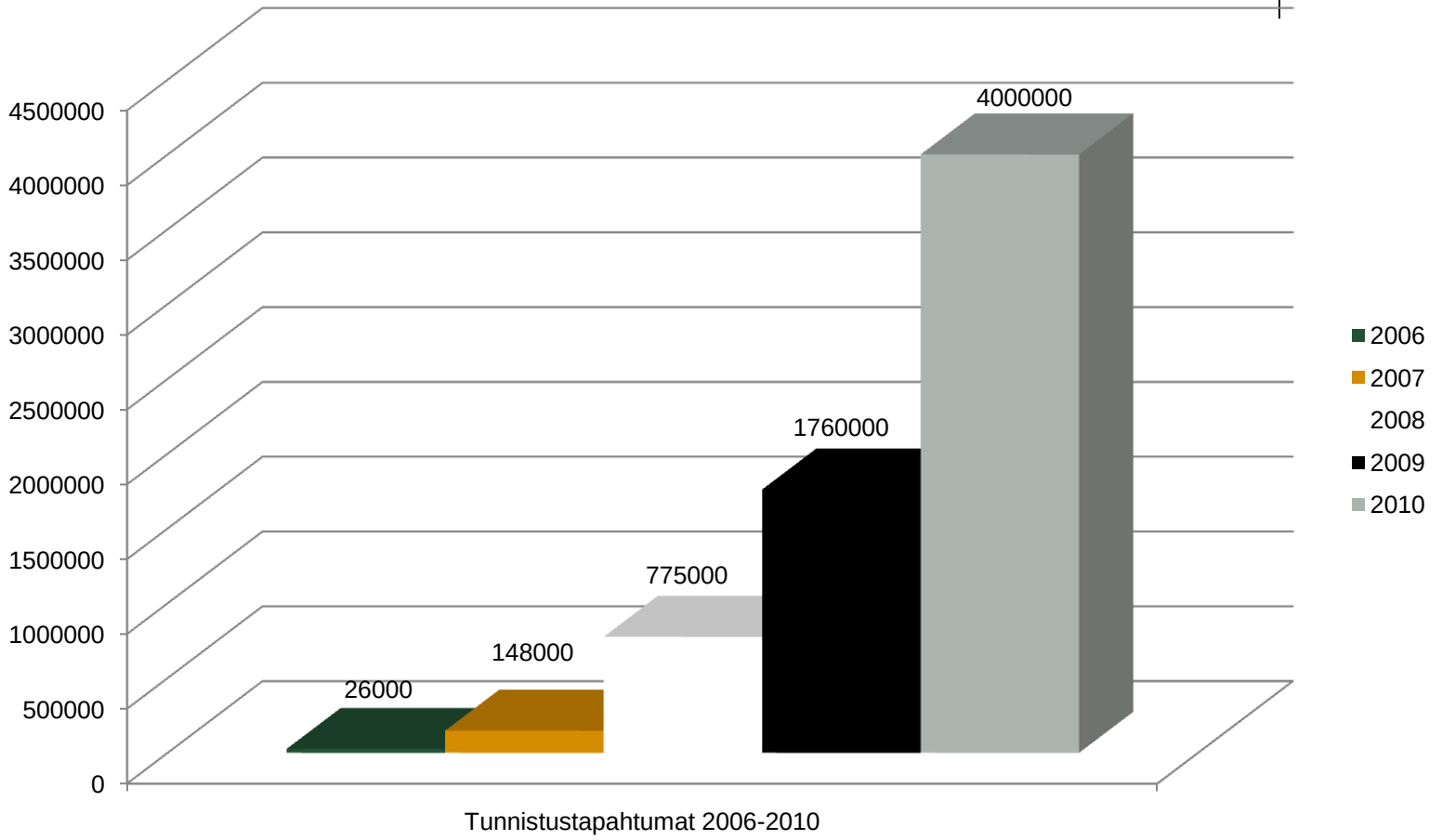


Chart credit: Verohallinta, Finnish tax administration

KATSO

- Two types of authentication
  - Strong: Katso OTP (One time password PIN/TAN)
  - Weak: PWD (Username and password)
- Strong authentication initial registration based on bank assurance (TUPAS) or physical visit

KATSO

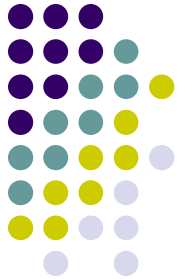
- Use of KATSO initially limited to consortium members
- Legislation changes have permitted wider use
- Use outside of government services still limited by legislation

kantara INITIATIVE


Katso
www.vero.fi/katso_etusivu/?language=ENG
Katso
På Svenska | Suomeksi
Katso Identification System and Authorization management
As a representative of your organization, you can sign in to Katso to set up a Katso ID, manage organization data, manage Sub-IDs and Authorizations.
The Katso ID is used for signing in, so you can safely enter the authorities´ Online and electronic filing services.
Katso Identification Service
Go to Katso
Set up Katso ID
Forget your Password?
New passwordlist
Run out passwords (help)
Still some passwords (help)
Electronic filing services
Tax
Kela
The Finnish Centre for Pensions
Keva
Customs
News releases
News archive
Tips and facts
FAQ
Tips (on Passwords etc.)
Katso roles
Developers of e-services
www.vero.fi/katso
Support
+358 20 697 040
katso@vero.fi
The Katso Identification services are provided free of charge.

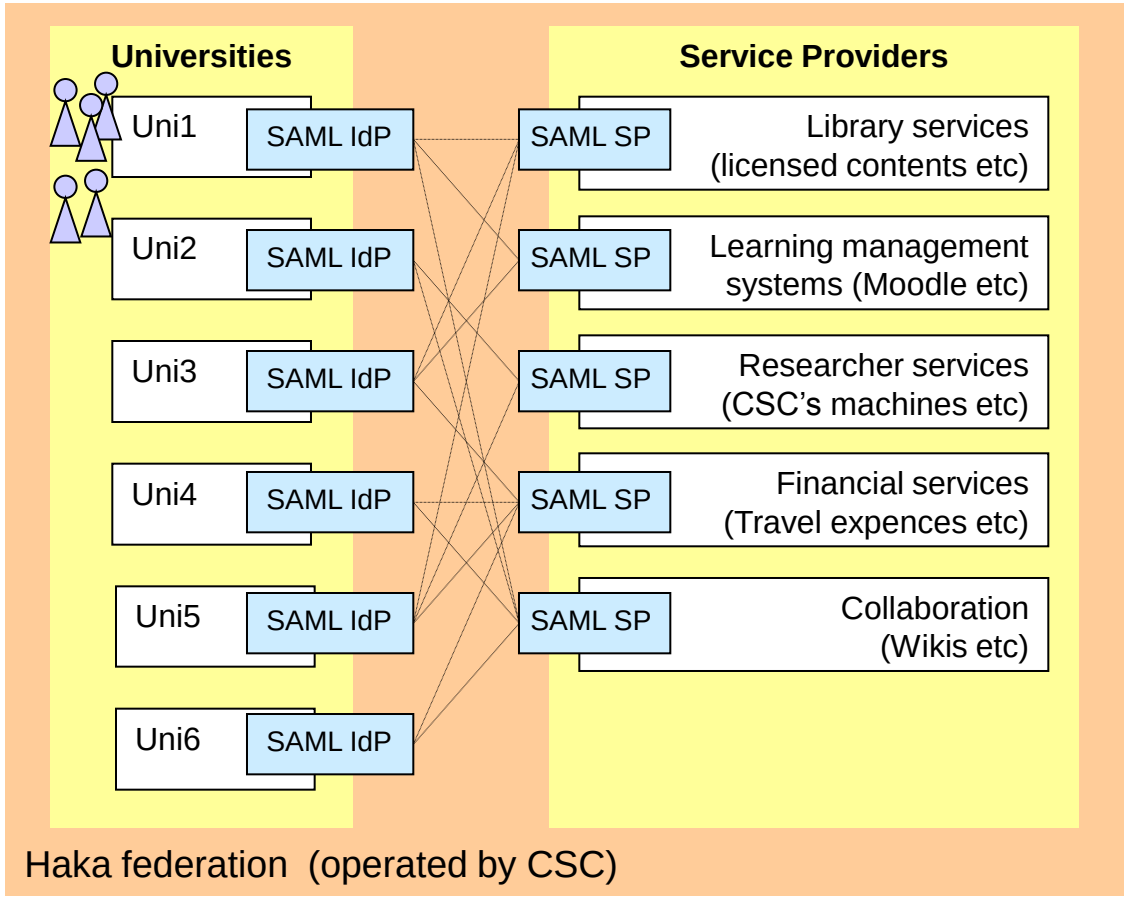
Self service enrolment

Haka Federation for Education

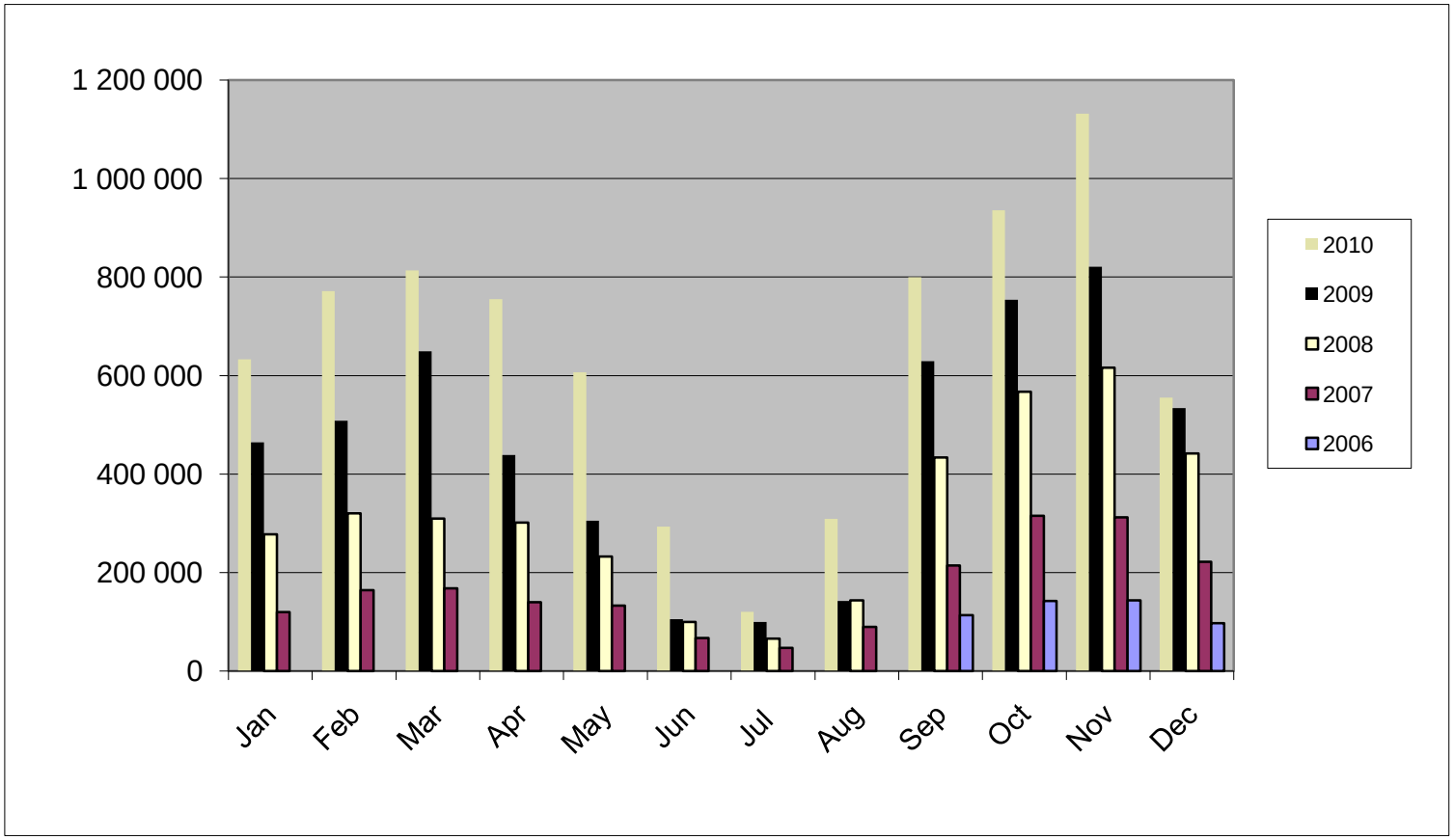


- Identity federation for higher education
- SAML2 (almost 100%)
- Used by 42 out of 43 higher education institutions
- Operated by CSC
- More info

Haka Federation



Haka: 7.7 million logins in 2010



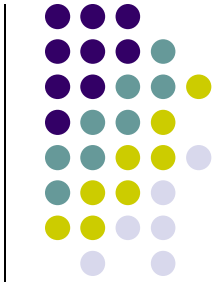
Virtu

- Authentication for Public Servants
- A service of the State Treasury
- Operated by CSC
- In production since August 2009
- IdP requires external security audit
- State Treasury Government IT Shared Service Centre
- Possible future presentation?

Summary

- Many sources of strong identities, both commercial and government operated
- Early adopter with some legacy pre-SAML components
- Open interfaces, standards-based where standards exist
- Continued growth in all services
- Extensible to support new authentication methods (eg WPKI)

kantara INITIATIVE



Questions / Discussion

kantara INITIATIVE