

Federated Identity - Haka Federation

TF-CSIRT

September 22nd 2006

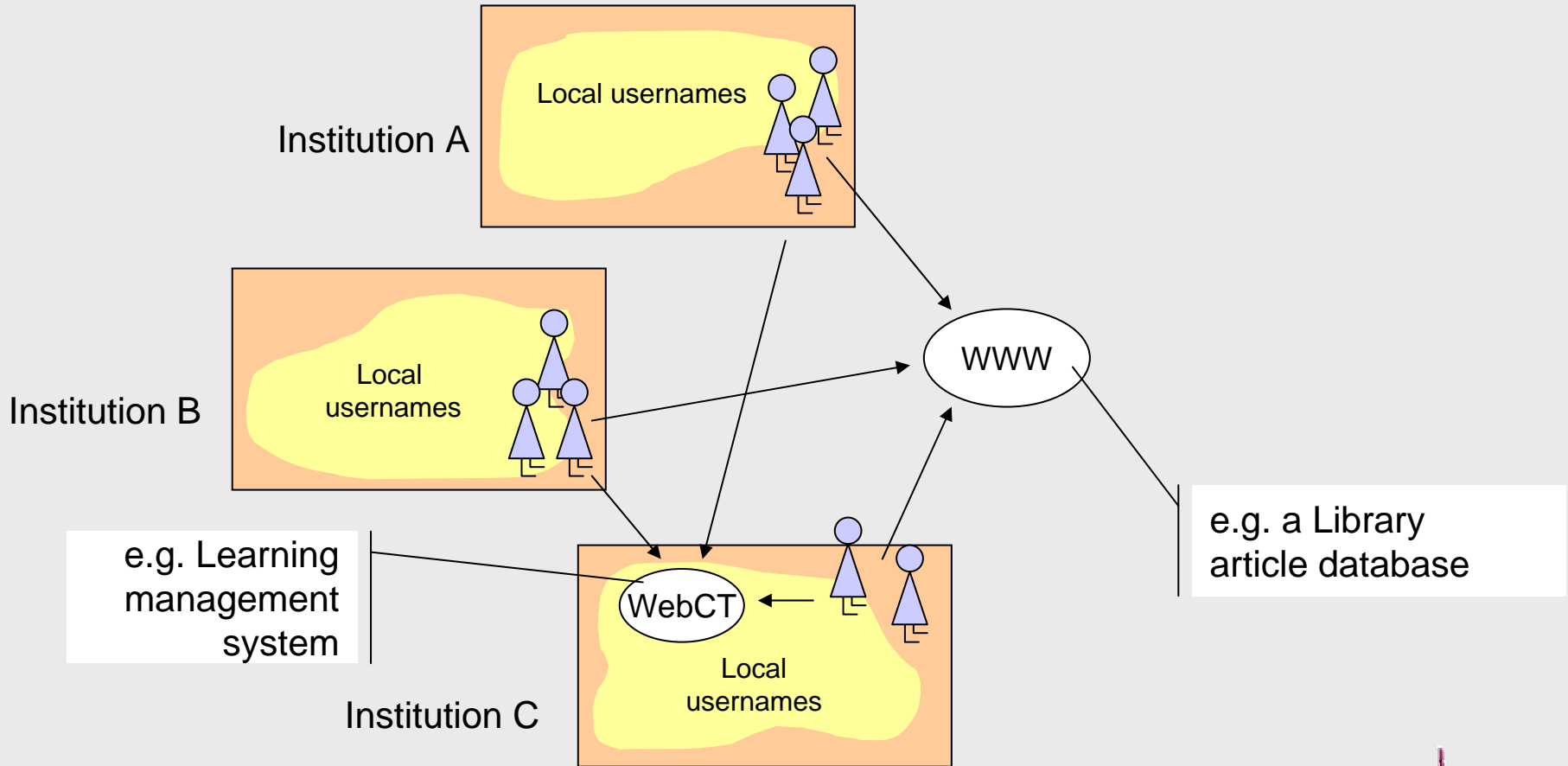
Arto Tuomi,

CSC, the Finnish IT Center for Science

arto.tuomi@csc.fi



What is federated identity management?



Finnish higher education overview

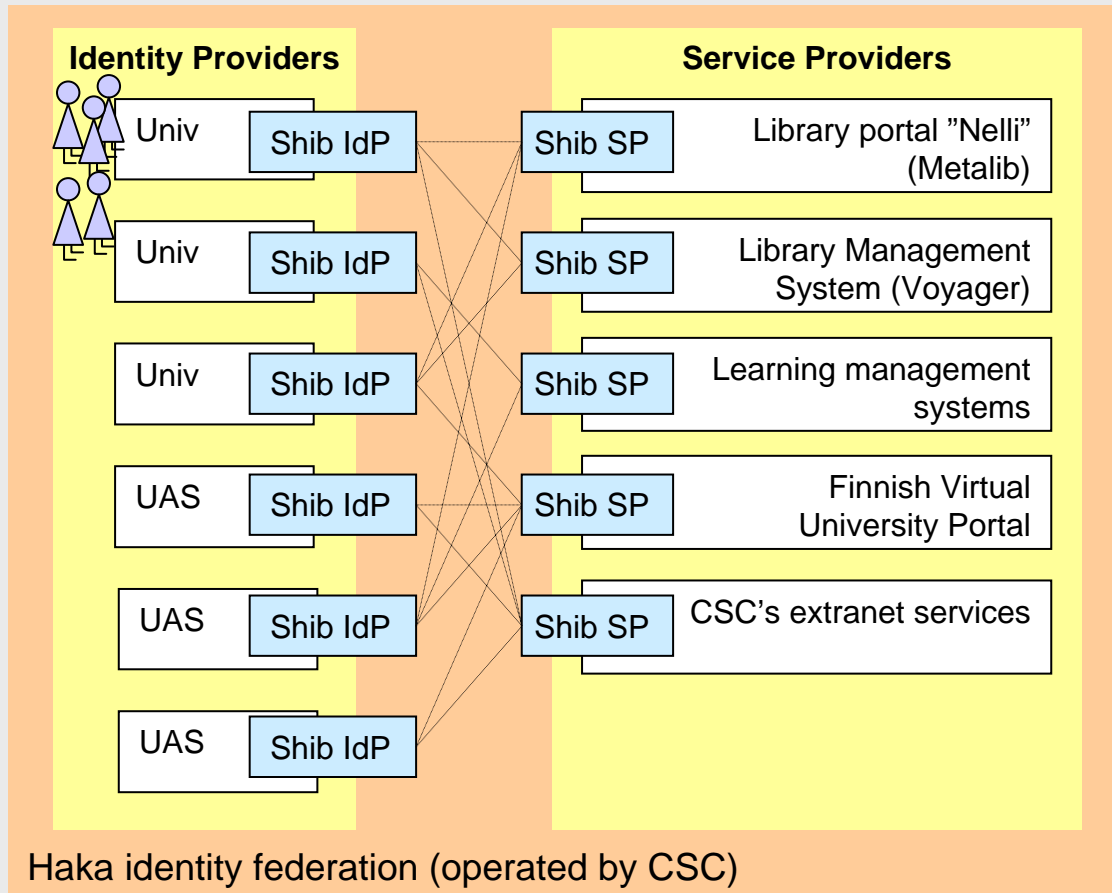
- **20 universities, 29 polytechnics (universities of applied sciences)**
 - Small units spread throughout the country
- **300 000 degree students, 40 000 employees**

CSC, the Finnish IT Center for Science

- **Non-profit company owned by the ministry of education**
- **To provide centralised IT services to higher education and research**
 - Scientific computing, supercomputing
 - Funet – the Finnish national research network (NREN)
 - Haka identity federation

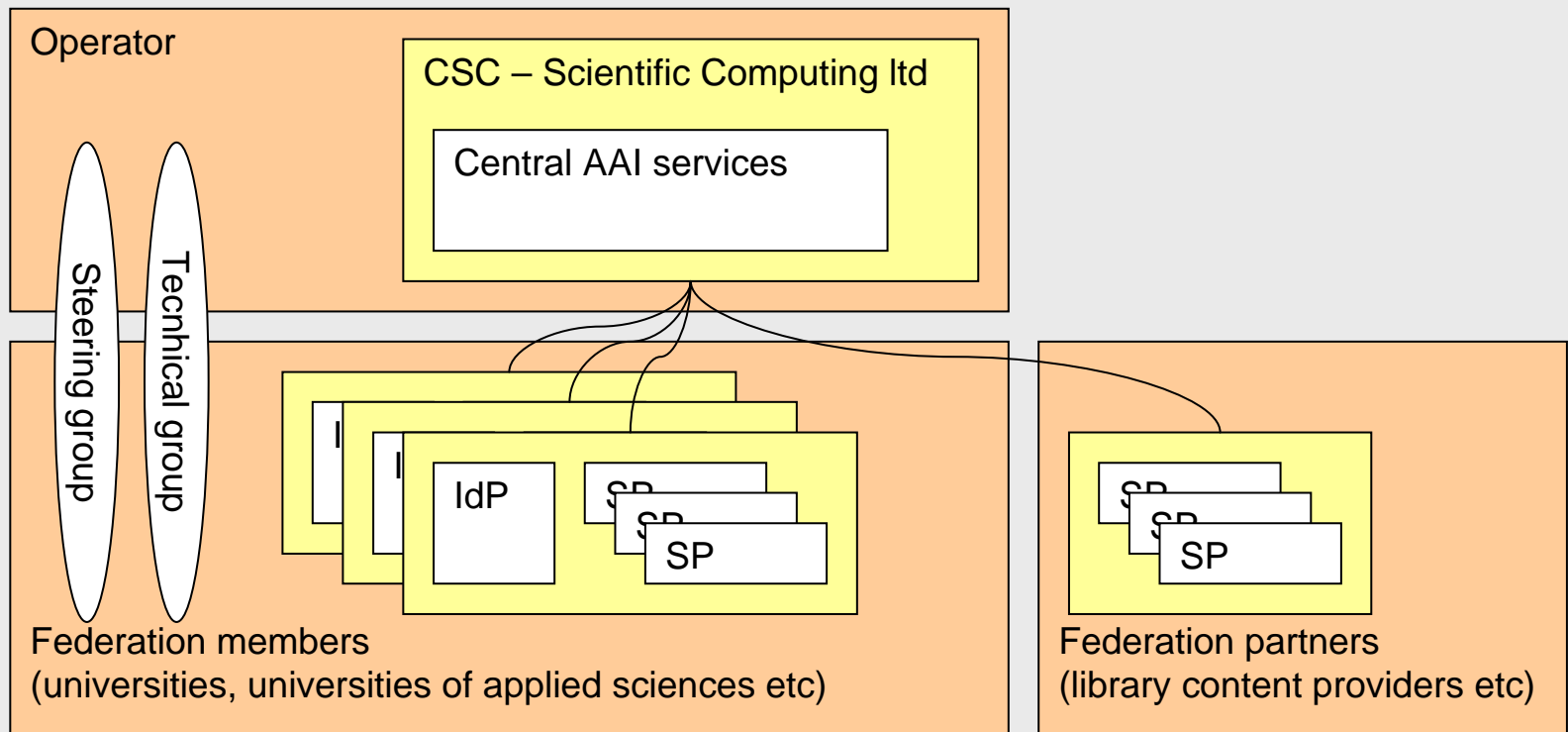


Haka federation, the identity federation of Finnish higher education



- User's home institution (Identity Provider, IdP) maintains user's identity and attributes (name, contact info, role, major etc)
- Home institution authenticates the user (e.g. by password)
- Home institution releases attributes to the Service Provider (on user consent)
- Based on the attributes, service provider decides what kind of service the user gets

Haka is a service provided to the institutions by CSC ("the operator")



Status of Haka identity federation

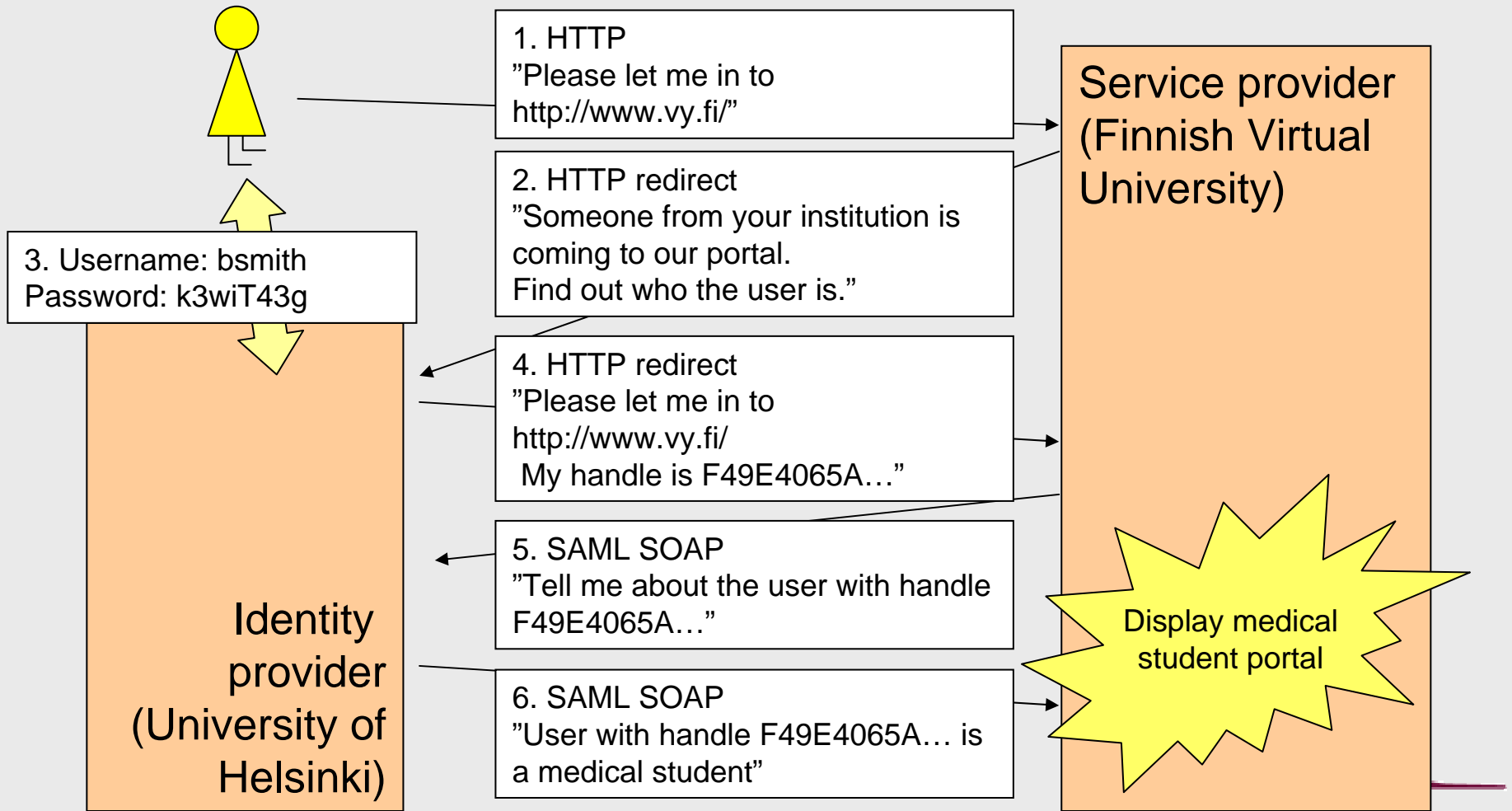
- **Pilot federation operational 12/2003**
- **Production level federation operational 8/2005**
- **Current members: 10/20 universities, 8/29 polytechnic, 2 partners**
 - Big universities; coverage 72% of end users in universities
 - Goal: 12/2006 14/20 universities, 15/29 polytechs
- **Identity Providers (IdP) and Service Providers (SP)**
 - 9 IdPs
 - 8 SPs



Technology in Haka federation

- **Protocol: Shibboleth ver 1.2/1.3**
 - protocol specified by Internet2 (US), based on standards (SAML 1.1, SOAP, XML)
 - free open source implementation by Internet2 available since 2003
 - version 2.0 compatible with Liberty Alliance
 - available for Apache and Microsoft IIS
- **Schema: funetEduPerson**
 - specification of attributes (name, mail, affiliation, study subject...)
 - based on eduPerson of Internet2
 - version 2.0 fall 2006
- **Certificates: Sonera CA (a commercial Finnish CA)**
 - only server certificates needed

Shibboleth in action



Shibboleth experiences in Haka

- **Stable**
- **Low maintenance**
 - Few patches and problems
- **Deployment difficulties**
 - Installation and configuration require experience in many areas
 - Single Sign-On unfamiliar for many
- **Dependencies**
 - Authentication system
 - User attribute database
- **Considerable improvements within last 18 months in**
 - Documentation
 - Ease of installation

Service categories so far

1. Library services

- The library management system (Voyager), the library portal (Metalib), the digital content repository (Encompass, work in progress)
- The content providers (work in progress)

2. eLearning services

- Learning management systems (Moodle, A&O, Optima)
- Electronic application form for becoming a visiting student in another Finnish university (www.joopas.fi)

3. Nationally provided services

- CSC's extranet services to researchers
- Research funding application form (work in progress)

4. ASP services in the administration of an institution

- Circulation of travel expense reports & incoming invoices (work in progress)
- HR software/Employee self-service (work-in-progress)



Haka federation and privacy

- **In Finland, Personal data act implements the data protection directive**
- **Only relevant attributes are released to a SP**
 - When a new SP is registered to the federation, the SP provides a list of necessary attributes to the operator
- **IdP asks user's consent for attribute release beforehand**
 - After Shib IdP authenticates the user, before s/he is redirected back to the SP
- **To make the consent *informed*, the Privacy Policy of the SP is provided to the user**
 - The operator has a centralised service that gathers links to the Privacy Policies of the SPs in the federation



Haka federation and the quality of institutional identity management

- **High-quality institutional identity management is a necessity for an IdP joining Haka**
 - The typical problem: accounts not closed as students/employees leave the organisation
 - Best practice: link the IdP's user database to student&HR registry
- **When a new IdP is being registered to the federation, the institution makes an IdM self-audit**
 - The operator checks that the minimum requirement is fulfilled

Supporting institutions to improve IdM: "School in user administration"

- **CSC's workshop of 3 days for staff in IT departments in HEIs**
- **1st day 1/2005**
 - **Theory, best practices, commercial/open source products...**
 - **First homework: evaluate your current institutional IdM**
- 2nd day 5/2005**
 - **homeworks gone through**
 - **The concept of an identity federation introduced**
 - **Second homework: set target for your institutional IdM**
- 3rd day 11/2005**
 - **Again, homeworks gone through**
 - **More best practices and products...**

Other supporting activities

- **Identity management projects for HEIs**
 - CSC provides funding and coordination
 - HEIs implement
 - Since 2003 >10 projects
- **Projects in 2006**
 - Integrate Microsoft CMS to Shibboleth and Grouper (an open source group management toolkit)
 - Learning Management System related projects
- **Shibboleth installation and configuration workshops**
 - One day workshops twice a year
- **Test environment**

Challenges

- **Shibboleth/SAML 2.0**
- **Focus from new IdPs to new SPs**
- **Monitoring, reporting and configuration management**
- **Trying to catalyse commercial companies to provide IdP hosting for small institutions**
- **More ASP services**
- **Cross-national confederation**

Forums for federated identity in Higher education

- **TERENA (the association of European NRENs)**
 - Terena Task Force TF-EMC2
 - EuroCAMP events (2/year)
 - annual Terena Networking Conference (TNC)
- **Geant2 (GN2) project**
 - funded by European Commission
 - GN2/JRA5 to bridge the national federations
- **MACE (Middleware Architecture Committee for Education)**
 - international, US driven group of campus IT architects
- **Nordic co-operation**
 - Gnomis: regular meetings of identity management experts in NRENs and universities

Identity federations in higher education

Shibboleth technology

- **SWITCHaai (Switzerland)**
 - since 7/2004
- **InCommon (the United States)**
 - since 9/2004
- **Haka (Finland)**
 - since 8/2005
- **UK Access Management Federation**
- **Projects in Sweden, Denmark, Australia, Belgium, France, Germany**

Other technologies

- **Norway (FEIDE)**
- **UK (Athens)**
- **Spain (PAPI)**
- **Croatia**



More information

- <http://www.csc.fi/suomi/funet/middleware/english/>