

Services for Kalmar Union: Short lived credential service (SLCS)

Kalle Happonen (HIP),

and

Pekka Lehtovuori

Development Manager, Grid technologies, CSC

pekka.lehtovuori@csc.fi

www.csc.fi



Background about grids: Local vs Grid Authentication

- **Local resources**

- User name and password
- “Login” authenticates and usually also authorizes to use local resources

- **Grid environment**

- Authentication based on X.509 certificates granted by a third trusted party, Certificate Authority (CA)
- Each user has his/her own personal certificate
- Authentication is separate from authorization => having a valid certificate does not automatically give access to resources



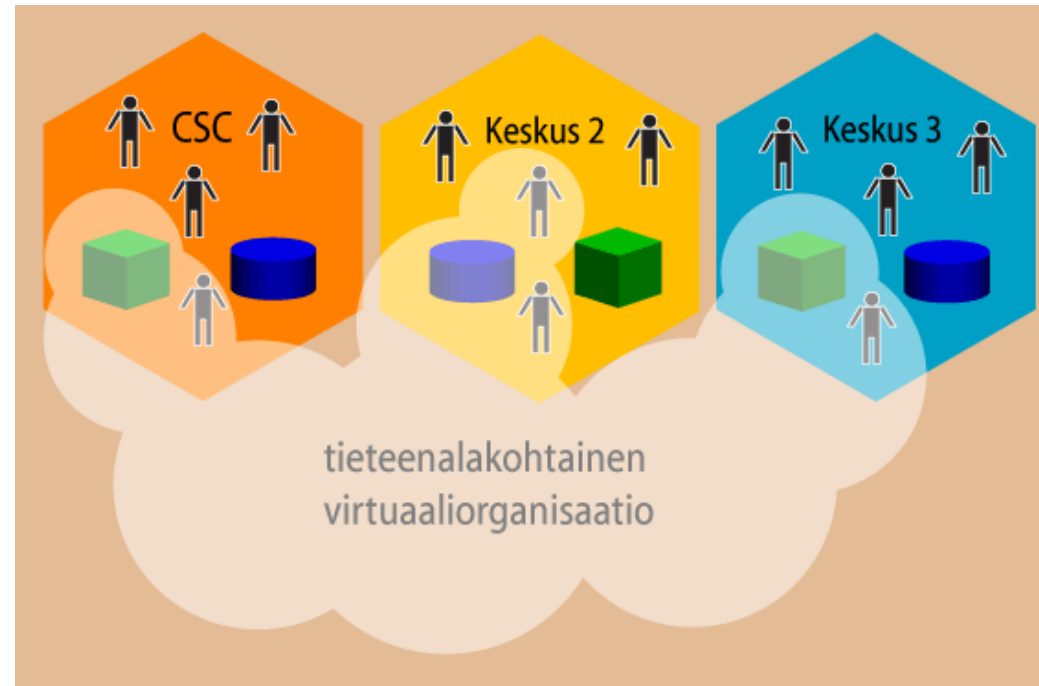
Authorization on the Grid

- **Users are grouped into Virtual Organizations (VO)**
 - Based on a common research area, nationality, funding agency, project, etc.
 - The same user can belong to several VOs
- **Resource providers grant access to VOs**
 - Scales better than managing individual users at every resource
 - Implies trust towards the organization managing the VO
 - E.g. in the M-grid the users of each site form one VO, and we could combine all to a larger "M-grid VO" when negotiating with external parties



Virtual organization (VO)

- Shares / owns resources from several organizations
- Has it's own trust and attribute domain
- Resource provider needs an interest in supporting the VO
- users can act independently from their own organisation
- Typically group of users, research laboratories, institutes working around some special field of science



Grids usually span over multiple administrative domains!



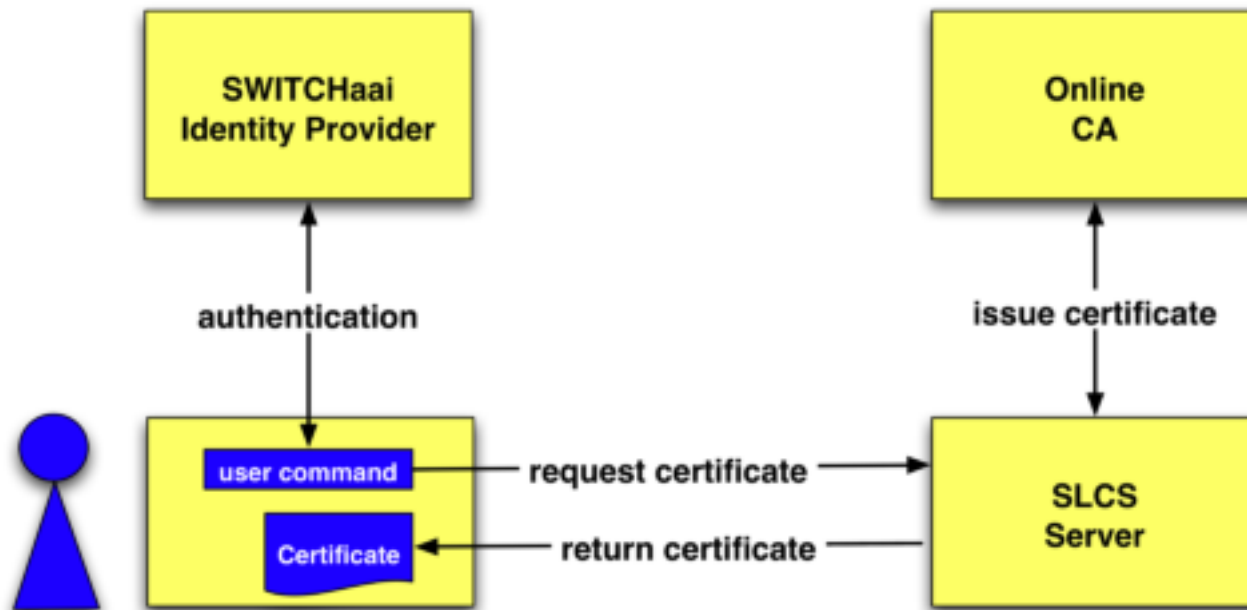
Why we need on-line Certificate Authority (CA) service

- One of the biggest obstacles in starting to use grids is the use of X.509 certificates because:
 - **It takes some time to get a certificate**
 - **scientist will lose the window of opportunity to familiarize him-/herself with grids**
 - **People are not familiar with certificates**
 - **Certificates are not necessarily handled as cautiously as they should be**
- On-line CA would ease the grid usage through portals

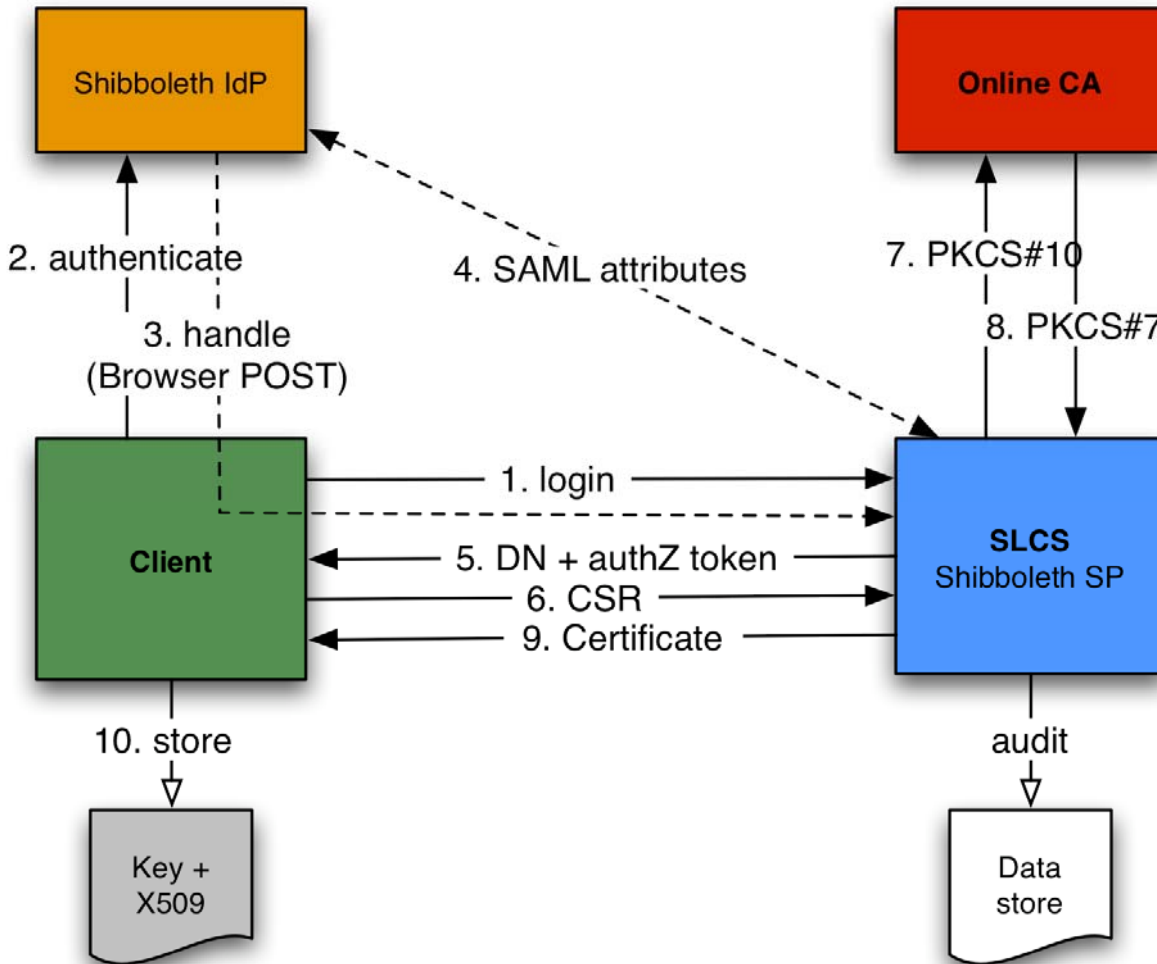


SLCS (Short Lived Credential Service)

- an X.509 certificate factory that issues him/her a certificate with which he/she can access grid resources
- Integrates Shibboleth (developed within the Internet2 project) and Grid infrastructures



Shibboleth messaging in SLCS



1. Request for a new short-lived certificate
2. Redirect to the Shibboleth IdP, user is authenticated.
3. The IdP issues a handle to the SLCS Service Provider.
4. With the handle the SLCS SP retrieves the SAML attributes of the user and generates a certificate subject derived from the user's attributes.
5. User generates locally a private key and a Certificate Signing Request (CSR).
6. CSR and authorizing token back to the SLCS SP.
7. The SLCS receives the CSR and after verification sends a request to the Online CA for signing.
8. The Online CA sends a short-lived certificate back to the SLCS server.
9. The SLCS server sends the signed short-lived certificate back to the UI as an XML message. The audit log is updated.
10. The user's certificate is stored on the UI.



Why SLCS / on-line CA is of interest for us?

- **At least Finland (CSC) and Norway are already setting up their own SLCSs for national usage**
- **Nordugrid has a firm user community and resources in every Nordic country**
- **Eases the co-operation between national grids and pan-Nordic research communities**
- **Lot of potential new grid users in each country**



Questions

- **One SLCS server for Nordic countries or one in each country?**
- **Association to Nordugrid CA?**
 - Are certificates valid in all science grids or just within the services operated under Kalmar union?
- **Proposition: Start first with the local installations, later merge the services if seen feasible**



Contact:
Pekka.Lehtovuori[at]csc.fi
Kalle.Happonen[at]cern.ch
Jussi.Hynninen[at]csc.fi

