

Data Management Related Activities in Switzerland



SWITCH

Serving Swiss Universities

Christoph Witzig

Christoph.witzig@switch.ch

Background: Co-operation projects in CH

- Federal government subsidizes co-operation projects between Swiss universities
- In the past: AAI 2004-2007 (ended March 31, 2008)
 - Roll-out of SWITCHaai infrastructure
 - A series of projects of various sizes around AAI
- In the future: AAA/SWITCH 2008-2011
 - AAA (“the third A”)
 - Grid
 - E-Learning
 - Support for virtual organizations

Project DocExchange

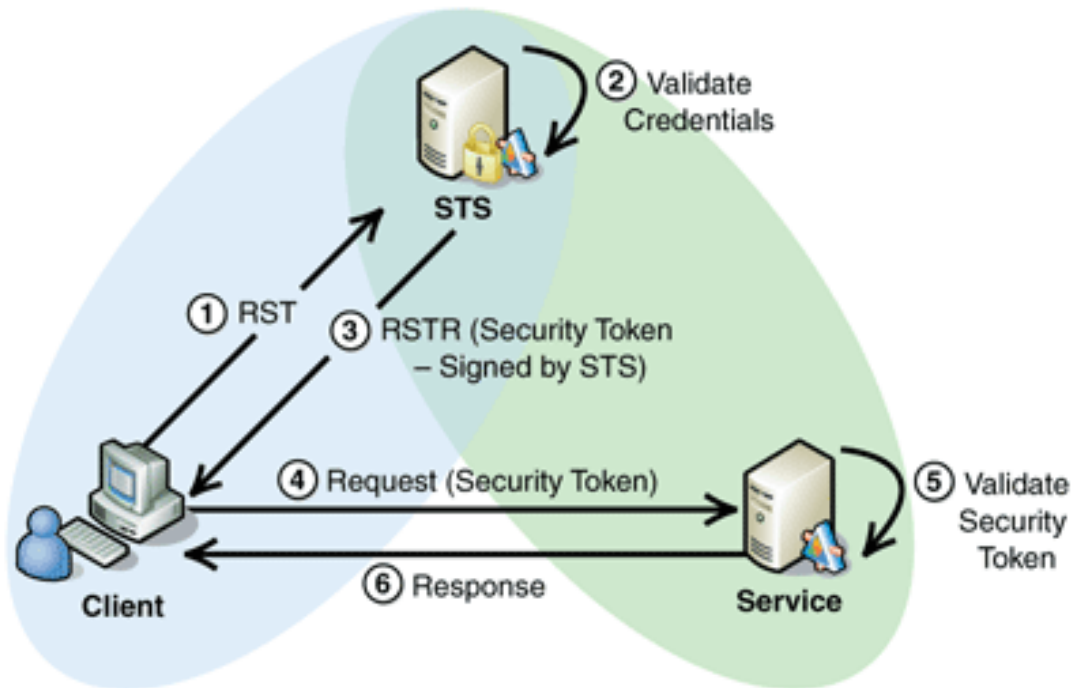
- Projects in AAI 2004-2008 by University of Basel
- Idea: Exchange of data (“documents”) between two user
 - Exchange of CD/DVDs should be possible
- Use-cases:
 - Both have AAI account
 - Sender has AAI account
 - Receiver has AAI account
- Key features:
 - AAI protected (either sender or receiver must have AAI account)
 - Data encrypted (DES)
- Prototype in advanced stage, used internally, release planned for summer 2008

Nation-wide afs Project

- AAA 2008-2011
- Use-cases:
 - A bio-informatics institute has to provide
 - Home directory and
 - Data directoryto users from different universities
 - Making grid middleware and/or application specific code available to several sites on the grid
- Idea:
 - Project idea in proposal stage
 - Use afs
 - Leverage against Shibboleth-based AAI using a Security Token Service

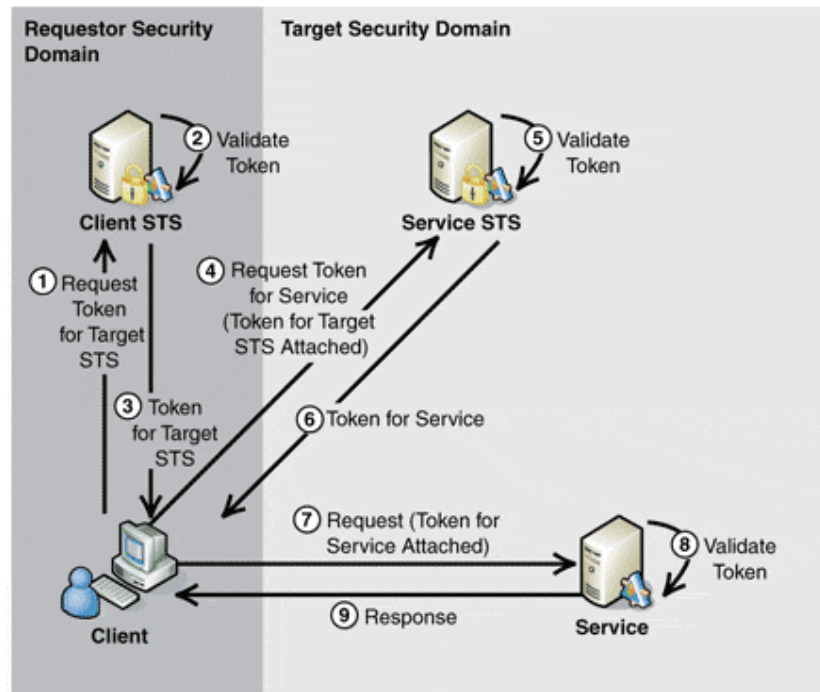
Security Token Service

- WS-Trust defines mechanisms for brokering trust to an authority called Security Token Service (STS)
- The Security Token Service have a trust relationship with both the client and the service.



Multiple Security Domains

- A client may need to communicate with services that operate across trust boundaries (i.e. Shibboleth SAML vs Grid X.509)
- Multiple STS can be used in a trust chain across security domains (delegated trust)



Use Cases

- STS issuing kerberos tokens
 - AFS
 - GPFS
- Non-browser based Shibboleth applications:
 - User agent contacts Shibboleth IdP with credential (e.g. username, password)
 - User agent receives SAML assertion to be sent to a Shibboleth SP
- Grid:
 - Shibboleth user wants to access a Grid resource (e.g. WMS, File Catalogue, Storage Element...)
 - He needs to obtain security token that the Grid services understand (X.509)
- SWITCH is developing such an STS service to be deployed as
 - IdP endpoint
 - Independent service