SAML to LDAP bridging developments

Marcus Hardt

LSDMA

Motivation

- Allow linux logins, using SAML
  - i.e. non-web => ECP
- Harmonise our existing AuthN infrastructure
  - Give same (UID, [GID]) to user with SAML and X.509 Auth
- Easy to use solutions

- Pilot: ssh-login for users from state of Baden-Württemberg

Harmonisation between X.509 and SAML

- Goal: Map to same (UID, [GID]) regardless of AuthN method
  - Use case:
    - Provide access via [ssh|gsi-ssh|globus-ftp|...] to same filesystem
    - Have credential translation available (DFN-SLCS)
  - Requirement: have single source for user and group information
    - Unity
    - VOMS-SAML
    - REMS
- Procedure
  - Site-local LDAP interface
  - Input: login information, Assertion, Certificate
  - Return: (UID, [GID]) after intelligent analysis of input
- This talk: **SAML + LDAP**

Approach

- Provide a PAM module (in python)
  - Supports many linux services
  - PAM authentication:
    - (username, password) are handed to PAM module
    - PAM module tries to guess home-IdP from username (ka_lo0018@<host>)
    - Try to obtain an assertion from selected home-IdP
    - Return (UID, [GID]) based on attributes found inside assertion
- Update: switch from PAM to LDAP
  - Due to problems with python and one linux distribution

  => **KIT LDAP Facade**
  - Linux services can use the LDAP interface
  - LDAP Facade obtains (username, password)
  - ...
  - LDAP Facade returns (UID, [GID])

Solved Problems on the way

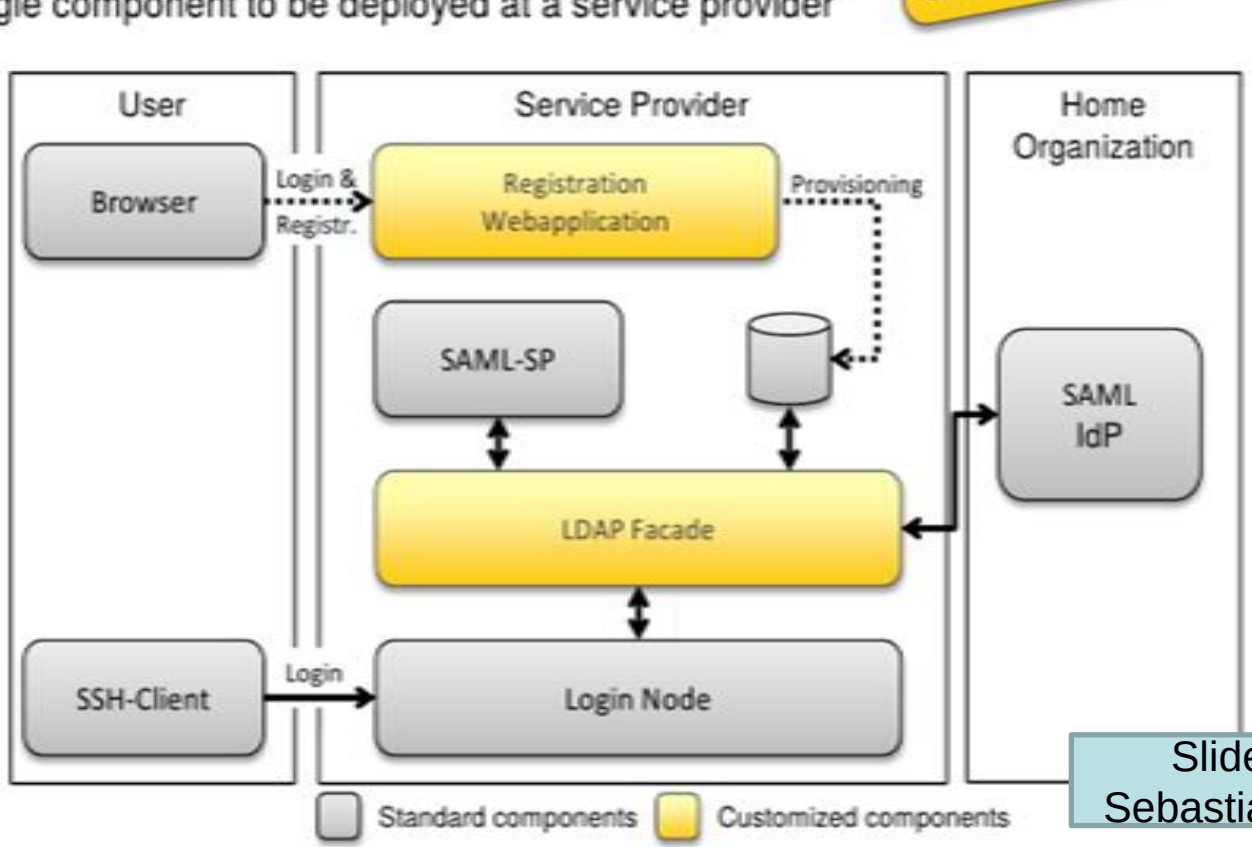
- “German problems”: privacy laws & co
  - Setup of a Sub-Federation
    - Development of Federation Access Policy (FAP)
    - Code of Conduct for the SP
      - Different to the Edugain CoC
    - Requirements for interaction between IdP and User

    => IdPs can hand out **any** attribute, **legally**

  => Web registration prior to first login
    - Click “OK” under the AUP (= terms & conditions)
    - Also used for changing preferences in the SP
- All local-state universities enable ECP
  - ....because their users get 10GB Dropbox like + 10GB via scp for free

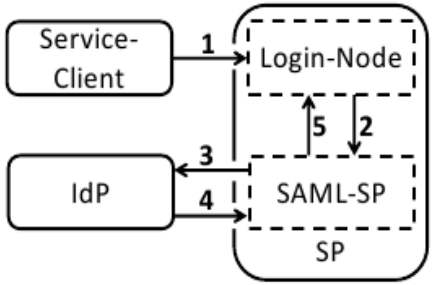
- LDAP-Facade
  - Appears to be a local LDAP directory
  - Includes FACIUS logic (incl. the web registration)
  - Transparent from the perspective of service providers
  - Deployable like any other SAML-based service provider
  - Single component to be deployed at a service provider

Further Information:
J. Köhler, M. Simon, M. Nussbaumer, H. Hartenstein: *Federating HPC access via SAML: Towards a Plug-and-Play Solution*, International Supercomputing Conference, Leipizig, Germany, Juni 2013

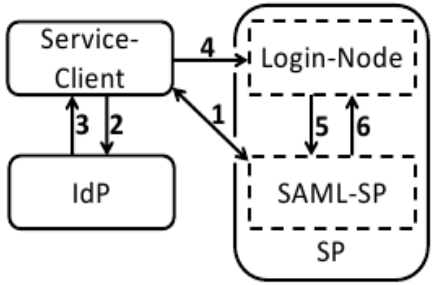


Slide courtesy of Sebastian Labitzke, KIT

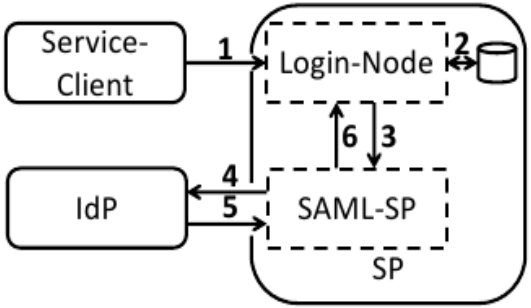
Authentication Scenarios



(a) Remote authentication: SP as Enhanced Proxy



(b) Remote authentication: Service-Client as Enhanced Client



(c) Local authentication

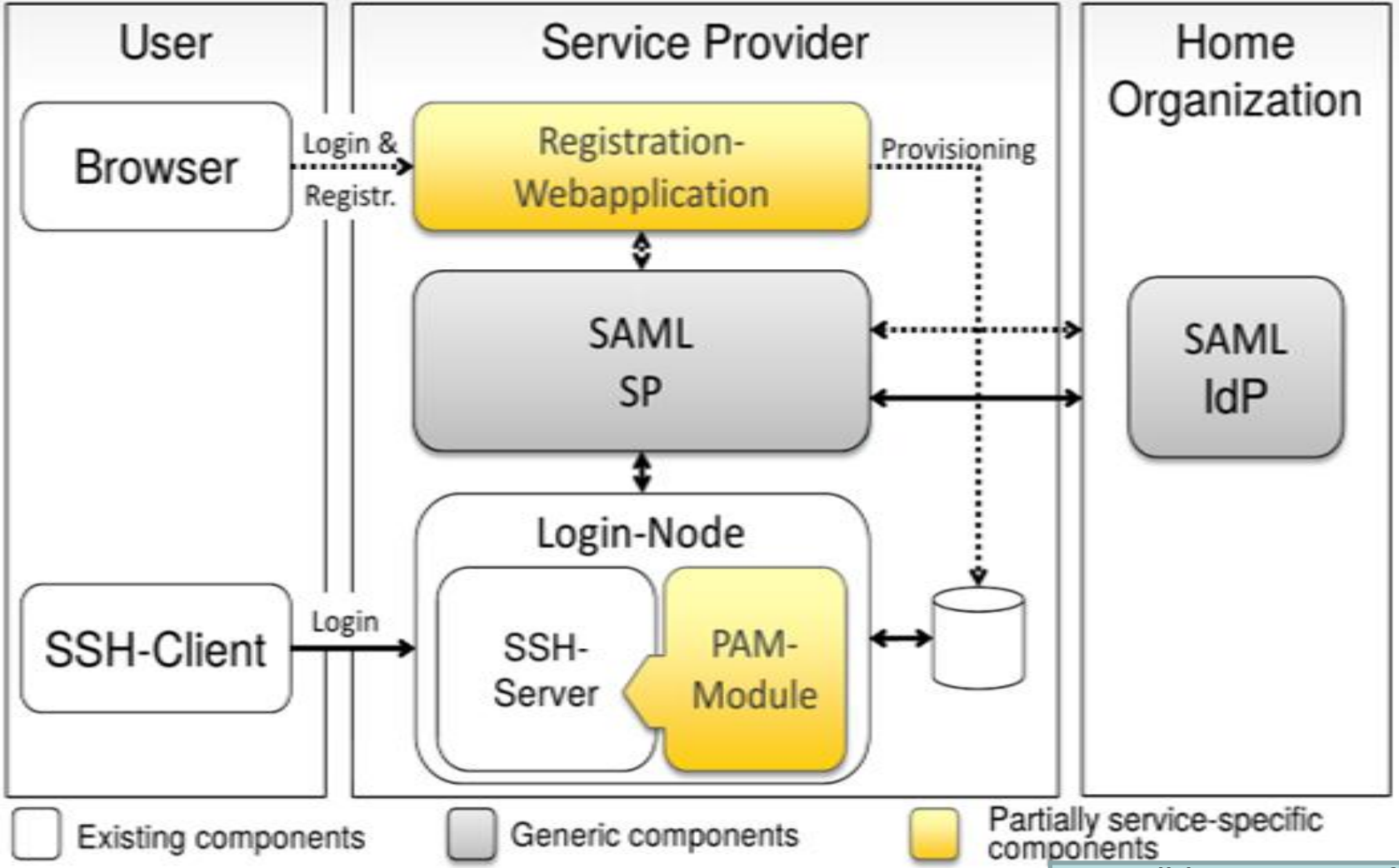
- (a) Enhanced Proxy (ECP)
  - Client sends password to LDAP Facade
  - Login at home-IdP on your behalf ;)
- (b) Enhanced Client (ECP)
  - Local client handles creation of assertion
  - Assertion passed to LDAP Facade
- (c) Local authentication
  - Login via other means (e.g. ssh-keys)
  - LDAP Facade runs Assertion query to verify user is still active

Image courtesy of Jens Köhler, KIT

Summary

- We can now use non-web based SAML via ECP
  - e.g. authenticate SSH with home-IdP
- Unmodified client and server (thanks to LDAP)
- Future work
  - Prototype of the above in place for Baden-Württemberg users in place
  - National prototype under way

  - Integration with
    - grid-security-infrastructure (i.e. globus-ftpd uses LDAP-Facade for (UID, [GID])
    - SLCS service at DFN
  - Extend LDAP Facade to support external AA (e.g. Unity, VOMS-SAML, ..)
  - Missing: the SSO in ECP



Further Information: J. Köhler, S. Labitzke, M. Simon, M. Nussbaumer, H. Hartenstein: *FACIUS: An Deploy SAML-based Approach to Federate Non Web-Based Services*, Proc. of Trustcom 2012

Slide courtesy of Sebastian Labitzke, KIT