Now SAML takes it all: Federation of non Web-based Services in the State of Baden-Württemberg

Sebastian Labitzke
Karlsruhe Institute of Technology (KIT)
Steinbuch Centre for Computing (SCC)
labitzke@kit.edu
My home organization ;-) 

- **Karlsruhe Institute of Technology (KIT)**
  - Merger of the University of Karlsruhe (TH) and the Research Center Karlsruhe (FZK)
  - >9,200 employees, almost 24,000 students

- **Steinbuch Centre for Computing (SCC)**
  - Computing Center of the KIT
  - 223 employees
    - about 50% scientist and 50% technicians and administrative staff
  - Two locations (Campus North and South), about 10km distance
  - Identity and Access Management, R&D in scientific computing, HPC, Big Data, Grids, Clouds, …
  - Mission statement:

  Science for Services – Services for Science
The bwIDM Project: Vision

- Federated access to services of the State of Baden-Württemberg
- Access control based on local accounts of the home organizations

**Vision:** In the state of Baden-Württemberg, researchers can access decentralized web-based AND non web-based services by the use of their local account

„bwIDM is not about establishing IDM systems, it’s about federating existing IDM systems and services.“
The bwIDM Project: Key Facts

• Project Management
  – Prof. Dr. Hannes Hartenstein (KIT)
  – Dr.-Ing. Martin Nußbaumer (KIT)

• Partners
  – Core-Team: KIT and the Universities of Ulm, Konstanz, and Freiburg
  – Partner Universities: Stuttgart, Mannheim, Hohenheim, Heidelberg, and Tübingen

• Funding: Baden-Württemberg Ministry of Science, Research and the Arts (MWK)
• Period of time: 2011-07 to 2013-12
Outline

• The Challenge
• Today‘s Federated Identity Management
• Requirements for Federating non Web-based Services
• FACIUS: Easy-to-Deploy Concept to Federate Non Web-based Services
• Current Work
• Conclusions
The Challenge

- HPC resources
- LSDF
- employee or student portal
- online publishing
The Challenge

- HPC resources
- LSDF
- Employee or student portal
- Online publishing

- Possibly stale identity data.
- Different credentials for different services.
- Security risks due to password reuse.
Today's Federated Identity Management

- **HPC resources**
- **LSDF**
- **employee or student portal**
- **online publishing**

**NON WEB-BASED SERVICES**
Cannot be seamlessly applied to non web-based services, yet.

**WEB-BASED SERVICES**
Well established for web-based services.
(e.g. SAML, OpenID, WS*)

Home Organization 1
Home Organization 2
Home Organization 3
Federated Identity Management

**CONSTRUCTS**

No **new** federated identity management framework for non web-based services

Most services to be federated are already deployed and operational

NON WEB-BASED SERVICES

Cannot be seamlessly applied to non web-based services, yet.

WEB-BASED SERVICES

Well established for web-based services.

(e.g. SAML, OpenID, WS*)
How can existing solutions for Federated Identity Management be leveraged to federate non web-based services?

**FACIUS**

An easy-to-deploy concept to federate non web-based services based on the SAML standard.
Requirements

Service Provider requirements

- Integration effort
- Legal aspects
- (De-)Provisioning
- Security
- Performance
- Maintainability

Deployability

User requirements

- Alternative authentication methods
- Transparency
- Use of home credentials

Home Organization requirements

- Legal aspects
- Necessary software adaptions

15.05.2013
Sebastian Labitzke - Now SAML takes it all
Outline

• Motivation

• Today’s Federated Identity Management

• Requirements for Federating non Web-based Services

• FACIUS: Easy-to-Deploy Concept to Federate Non Web-based Services

• Current Work

• Conclusions

Technical foundation to enable non web-based services to use SAML exists

➡️ SAML-ECP profile can be used to „SAMLfy“ arbitrary Apps
Getting Access to the Service

**REGISTRATION**

**web application**

SAMLfied: User can make use of credentials of his/her home org.

**ACCESS**

- Via a native service client
- Authorization based on assertions of the Home Organization

Get federated service access by just one single registration process

Provisioning of a local context
- In the SSH case:
  - Establishment of a UID, a home directory, ...
FACIUS - Overview

User
- Browser

Service Provider
- Registration-Webapplication
- SAML SP
- Login-Node
  - SSH-Server
  - PAM-Module

Home Organization
- SAML IdP

Existing components
- SSH-Client

Generic components
- Login & Registr.

Partially service-specific components
- Provisioning


15.05.2013 Sebastian Labitzke - Now SAML takes it all
Three Login Alternatives

Enhanced Proxy

Enhanced Client

Local Authentication

Service Provider

Home Organization

Service Provider

Home Organization

Service Provider

Home Organization

15.05.2013

Sebastian Labitzke - Now SAML takes it all
## Evaluation

### User Requirements:

- **Unmodified client usable**: ✅
- **Login with credentials of the Home Organization**: ✅
- **No harm by malicious Service Providers**: ❌
- **Operable in parallel to other login alternatives**: ✅

### Service Provider Requirements:

- **Integration effort**: Integration of the Pluggable Authentication Module with the Service Access Point
- **Maintainability**: Based on existing frameworks
- **Performance (SSH-Login)**: 1.01 s vs. 0.30 s (regular login)
- **Integration into existing Federations**: SAML-based federations
- **Provisioning/Deprovisioning**: ✅
- **Legal aspects**: User consent to policies can be requested

### Home Organization Requirements:

- **Legal aspects**: User consent to policies can be requested
- **No software adaption**: ✅
Current Work: The plug-and-play solution

- **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:**
Conclusions

• **bwIDM**
  – …federation of 9 universities of the state of Baden-Württemberg ➔ (non) web-based services
  – …federates the access to non web-based services such as grid, cloud, and HPC resources.

• **FACIUS**
  – Deployable, operable, and maintainable approach to federate non web-based services:

   If you have to bring non web-based services together with SAML, make use of the FACIUS approach!

   • FACIUS makes active use of the SAML-ECP and AssertionQuery profile
   • FACIUS offers users a high usability in trustworthy federations

• Easy-to-deploy solution for service collaborations of universities (and companies as well)
• Single registration process per service ➔ service access
• Successfully deployed in testing environments
  ➔ Production by the end of June

Special thanks to Jens Köhler, Michael Simon, and Dr. Martin Nußbaumer!