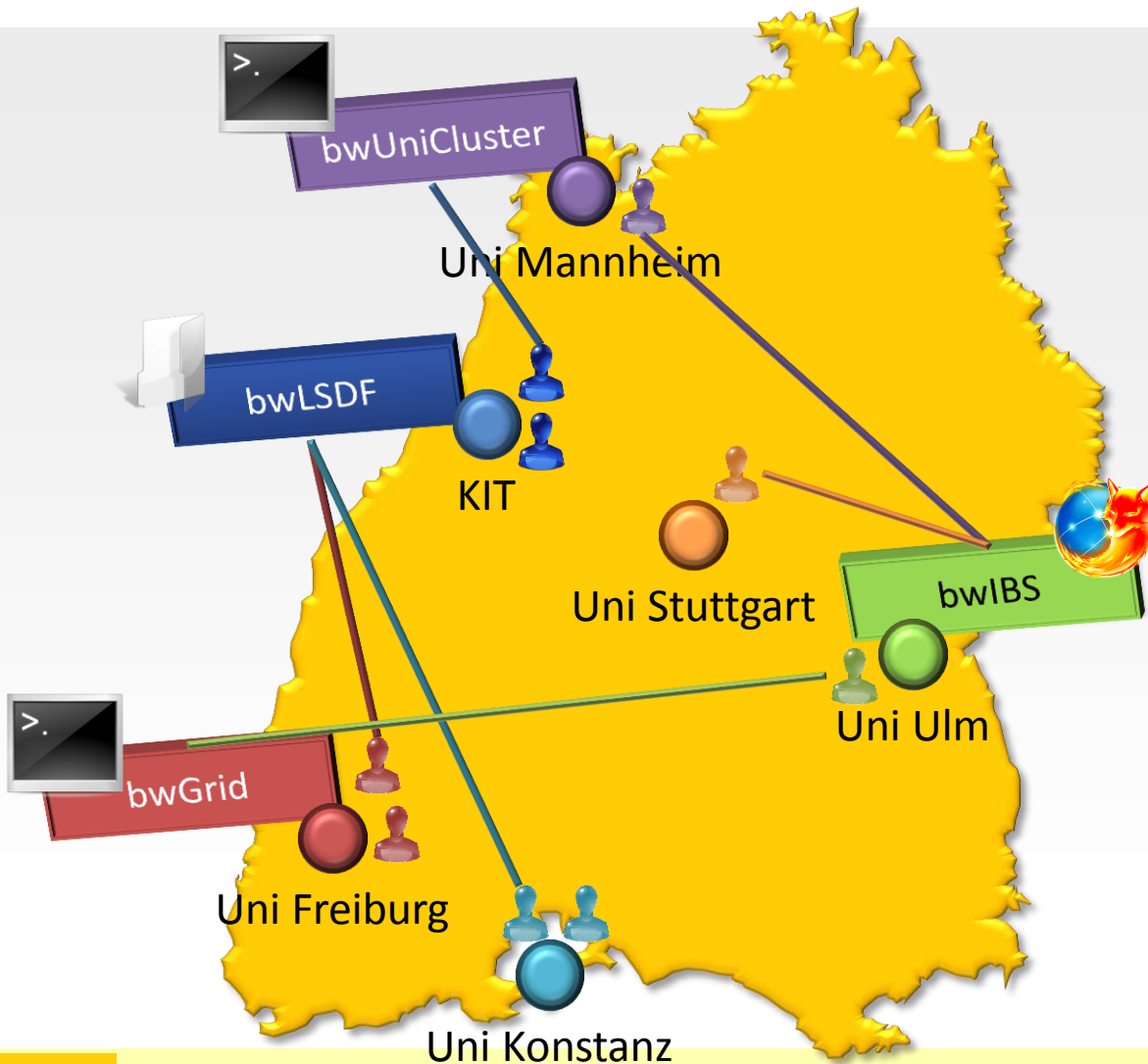


# Integrating non web-based services with identity federations

Jens Köhler, Michael Simon,  
Sebastian Labitzke, Tobias Dussa,  
Martin Nußbaumer



# The bwIDM project

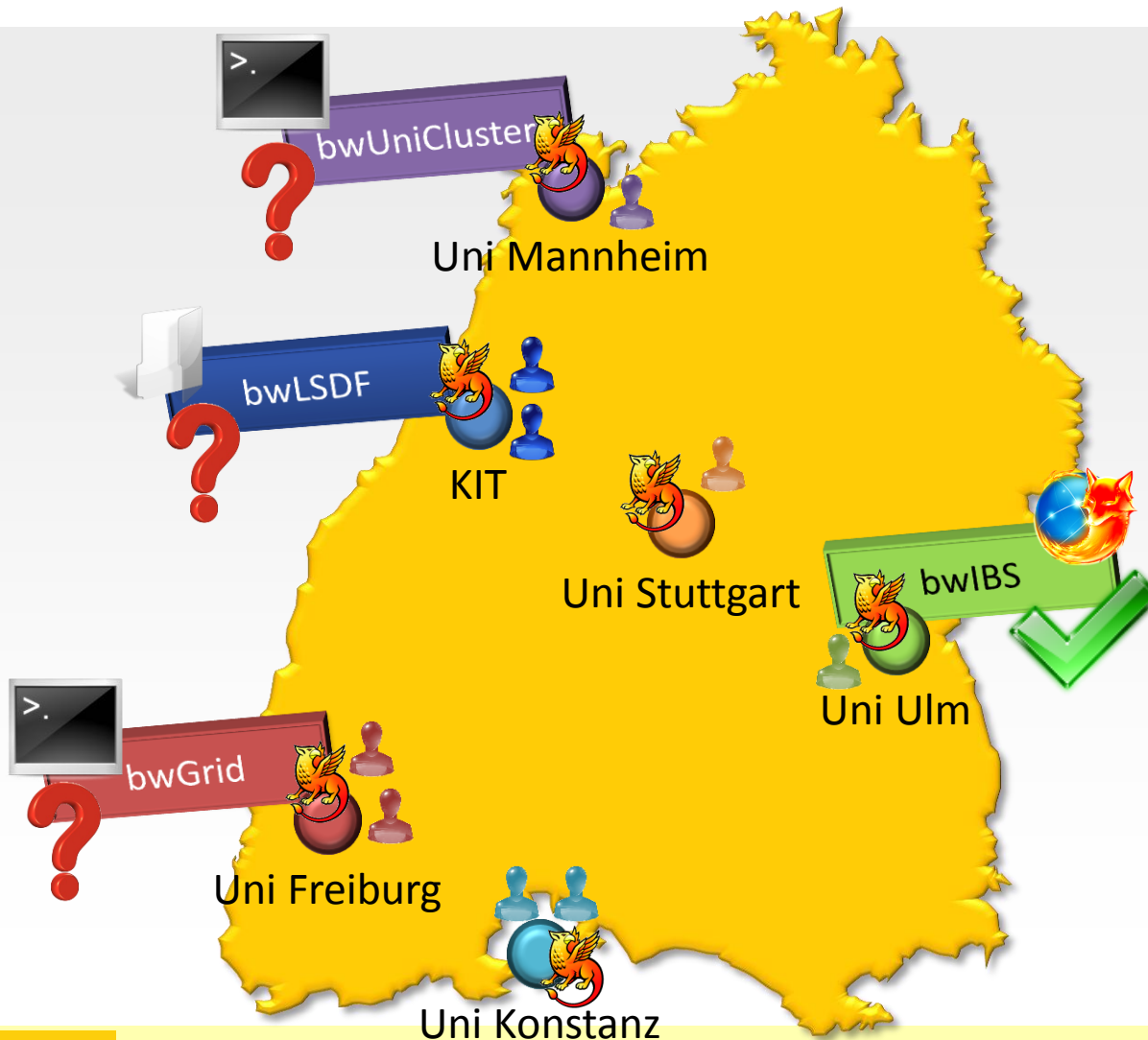


- Services of the state of Baden-Württemberg placed at different locations
- Should be useable by the affiliates of universities
- Affiliates should be able to access them with their familiar accounts of their home organization

**bwIDM:**  
Federated Identity  
Management for Baden-  
Württemberg



# The bwIDM project



- SAML identity providers are already present at each university
- Integrating web-based services into this infrastructure is straightforward
- Integrating non web-based services is a challenge

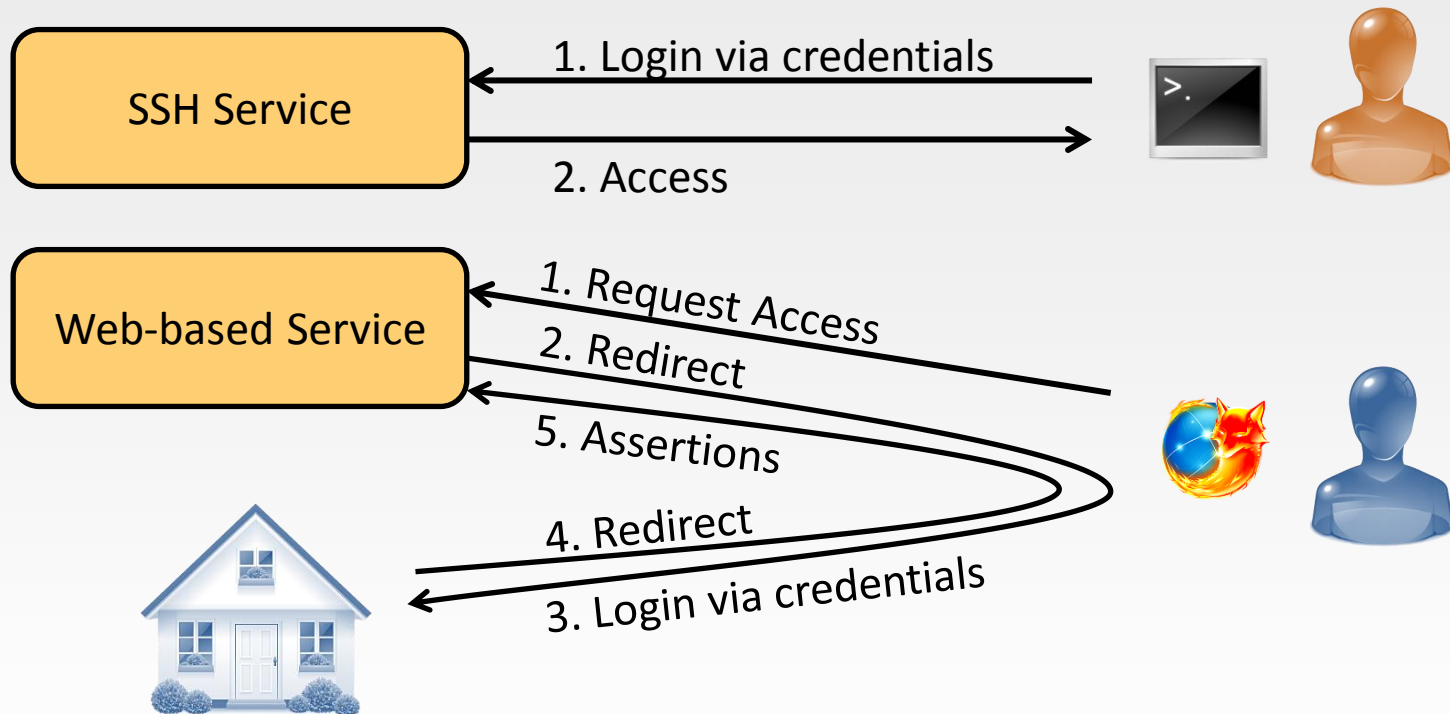
## FACIUS:

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



# Non web-based services vs. SAML

- Non web-based services: **Authentication via the Service Provider**



- Main characteristic of SAML: **Authentication via the Home Organization**
- SAML-ECP profile can be used to „SAMLfy“ arbitrary applications  
→ Technical foundation to enable non web-based services to use SAML exist



# Requirements

## Service Provider requirements

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

# Deployability

- Alternative authentication methods
- Transparency
- Use of home credentials

- Legal aspects
- Necessary software adaptations

## User requirements

## Home Organization requirements



# A users perspective: Getting access to the service

## Registration

- Via a Registration-Webapplication (Browser)
- Authentication based on the account at the Home Organization

## Provisioning of a local context

- In the SSH case:  
Establishment of a UID, a home directory, ...

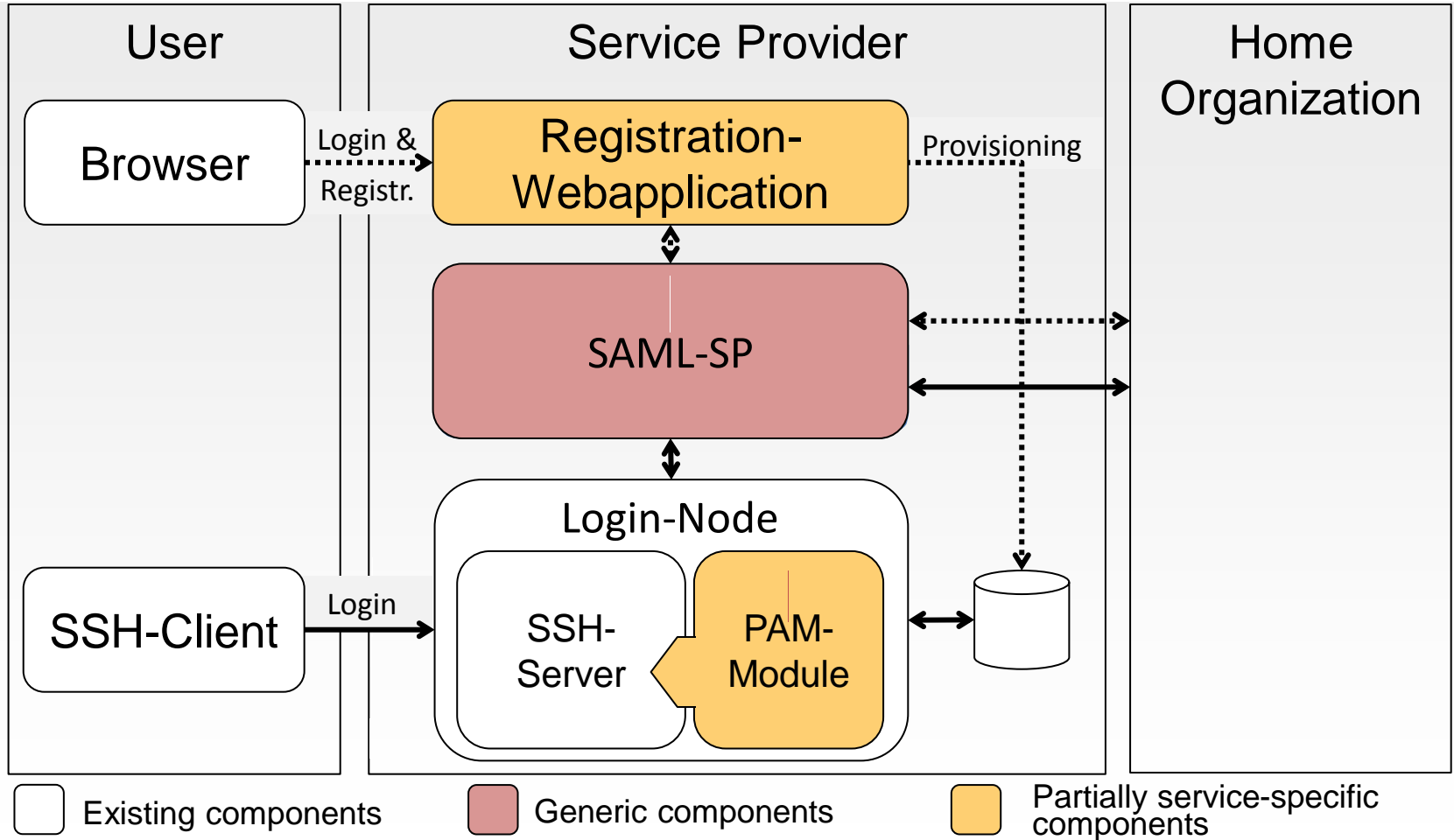
## Accessing the service

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

Just has to be performed once.



# FACIUS - Overview

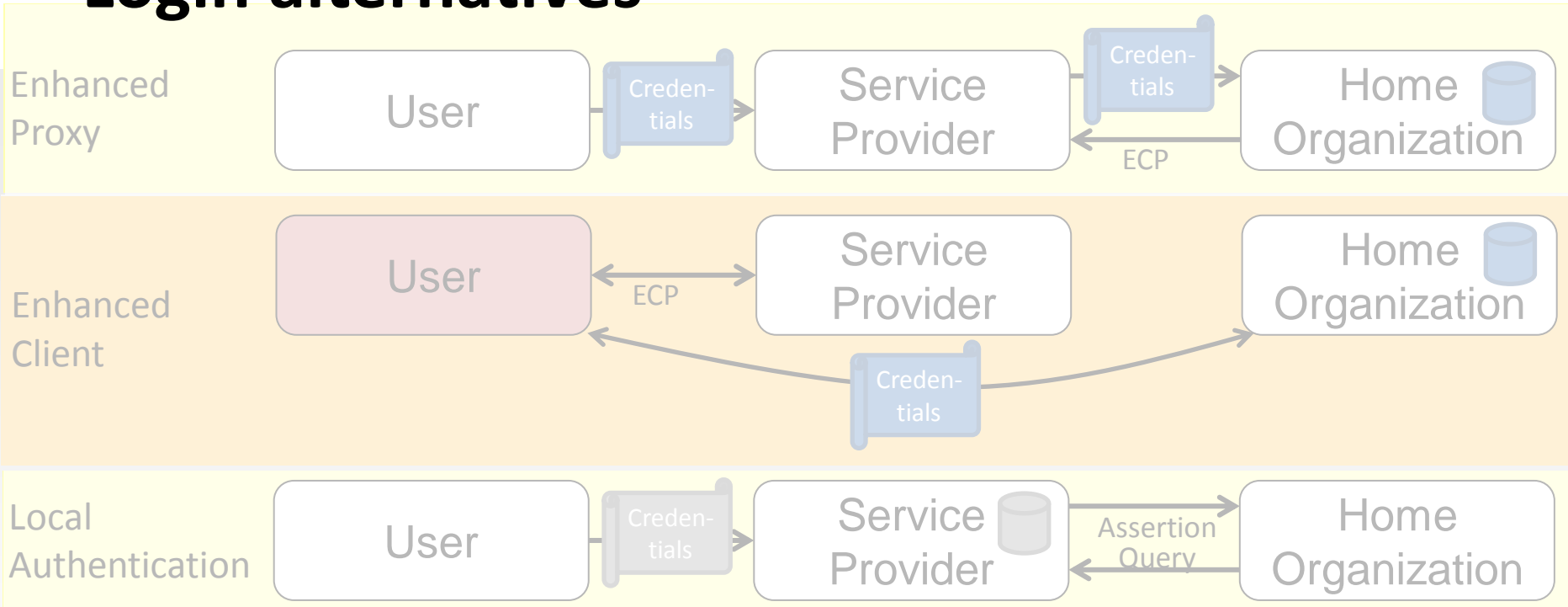


Further Information:

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



# Login alternatives



## User requirements:


	Enhanced Proxy	Enhanced Client	Local Authentication
Unmodified client usable	✓	✗	✓
Login with credentials of the Home Organization	✓	✓	✗
No harm by malicious Service Providers	✗	✓	✓
Operable in parallel to other login alternatives	✓	✓	✓





# Evaluation

- Service Provider requirements:

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

- Home Organization requirements:

<b>Legal aspects:</b>	User consent to policies can be requested
<b>No software adaptations:</b>	



# Conclusion

- bwIDM....
  - ...is a project to establish a federation of 9 universities and services of the state of Baden-Württemberg.
  - ...has the goal to federate access to non web-based services such as grid resources.
- FACIUS...
  - ...enables non web-based services to join SAML-federations.
  - ...aims to be easily deployable for existing service providers.
  - ...makes active use of the SAML-ECP and AssertionQuery profile.
  - ...offers users a high usability in trustworthy federations.
  - ...has been successfully applied to federate SSH services.
- We are planning to...
  - ...federate an operational cluster by the end of the year.
  - ...federate additional services based on FACIUS.



# How does FACIUS fit into the EGI federated identity management platform?

