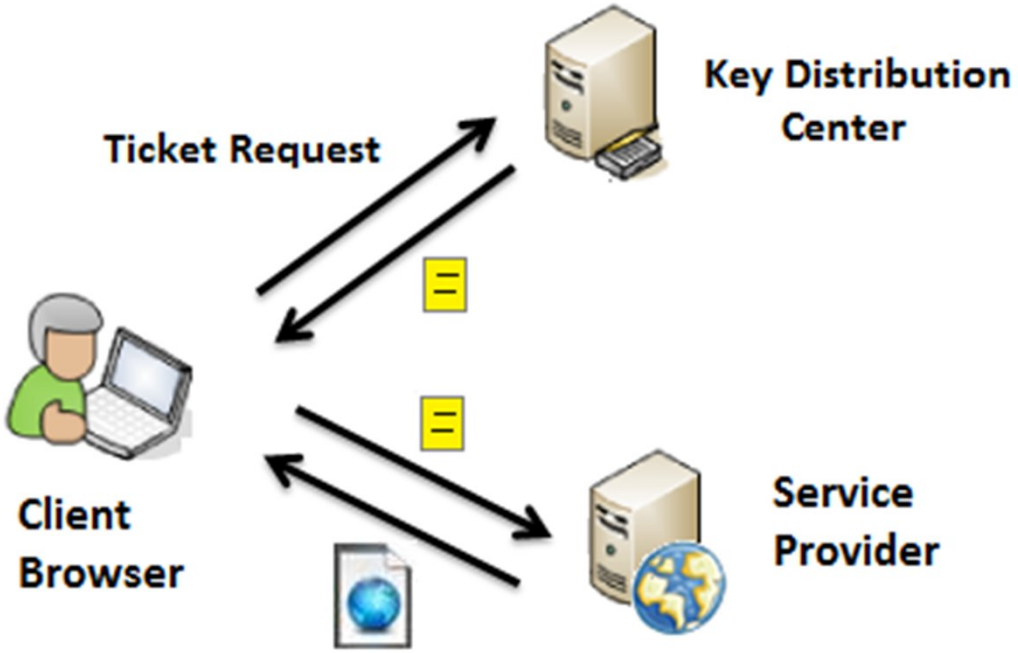
Fachhochschule
Nordwestschweiz

AAI-SSO with Active Directory
Kerberos Login Handler

Project Overview

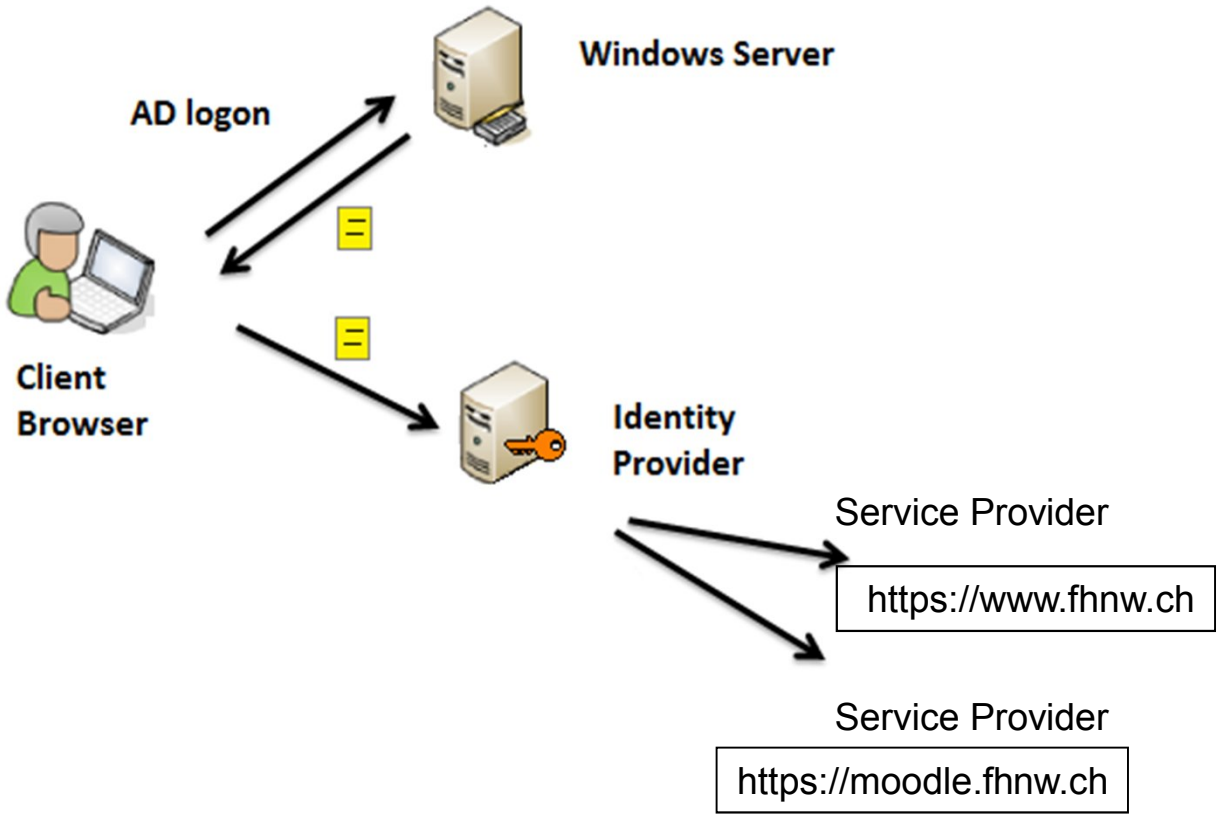
- One of FHNW's AAA projects
- Use case: SSO for AAI Applications with Active Directory domain logins
- Project goal: Development of a Kerberos login handler for the Shibboleth IdP
- Timeframe: April 2010 – March 2011
- Status: In production at FHNW since May 9, 2011 (for Windows users)
- Left to do:
  - Further testing and documentation for typical Mac/Linux scenarios
  - Attribute resolver optimizations



Kerberos

What is Kerberos?

- Kerberos was developed by MIT as part of Project Athena (1983)
- Kerberos is a ticket-based network authentication protocol
- Passwords are never sent over the network



Windows and Kerberos

Using Kerberos in the Windows environment:

- TGT-ticket will be requested at logon time (into AD domain)
- Service ticket will be requested on demand
- The browser will send the service ticket to the IdP
- The IdP will validate the service ticket

Requirements for Implementation

Kerberos Infrastructure

- Key Distribution Center
- Service accounts

Identity Provider

- Kerberos client
- Kerberos login handler installed

Client

- Kerberos client
- Browser configured

Recommended Scenario

Kerberos Infrastructure

- Active Directory
- Domain controller (Win 2003+) as KDC

Identity Provider

- Kerberos client
- Kerberos login handler integrated with «UsernamePassword» login handler

Client

- Windows OS (Kerberos client integrated)
- Centrally managed browser configuration with the help of a software deployment solution or by use of group policies

Kerberos Infrastructure

- Active Directory (out of the box) with domain controller as KDC
- Also possible: other directory service with Kerberos functionality
- Service Accounts (generated keytab files)
- Firewall: Kerberos ports (TCP/UDP 88) open between KDC and IdP

Identity Provider

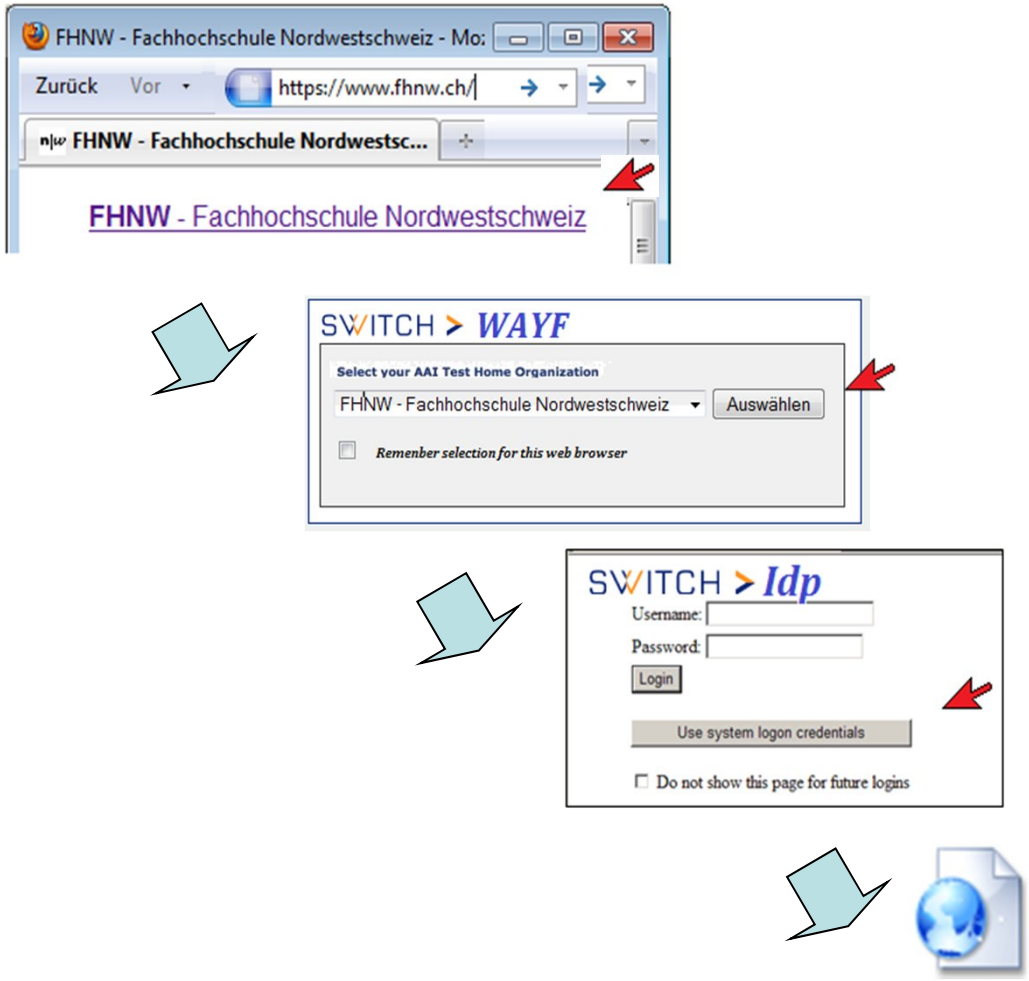
In addition to a standard IdP installation (UsernamePassword)

- Necessary configuration
  - Kerberos Client settings (krb5.conf)
    - KDC (Windows Server)
    - Keytab (generated for the service)
  - Kerberos login handler
    - Servlet (web.xml)
    - Handler (handler.xml)
  - Attribute resolver configuration
    - Configuration for «principal name» in the format: Principal@DOMAIN.COM
- Customization
  - Login form layout, CSS
  - Logging

Client

- Windows client must be joined to the domain
  - Client will receive a ticket
- Browser must be configured
  - allows the ticket to be sent to the IdP

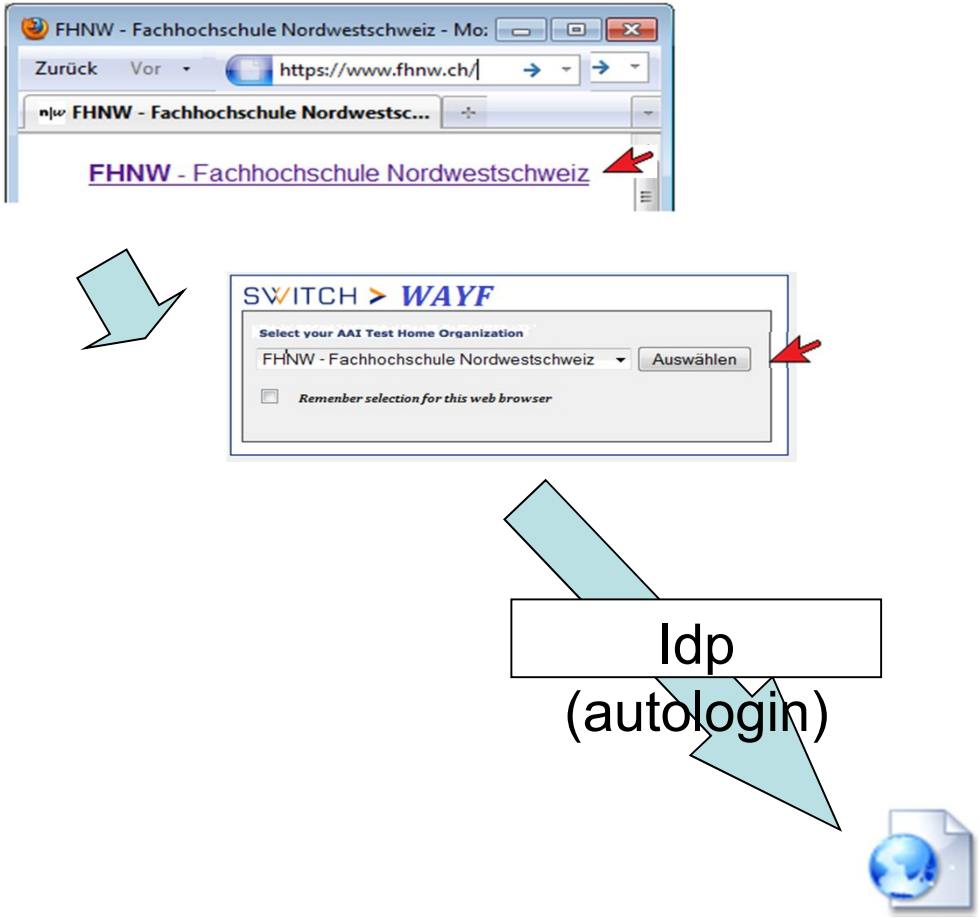
Demonstration



The «Auto Login» Option

- The Kerberos login handler optionally sets a cookie «_idp_krb_autologin=true»
- This cookie can be used for automatic redirection

The «Auto Login» Option

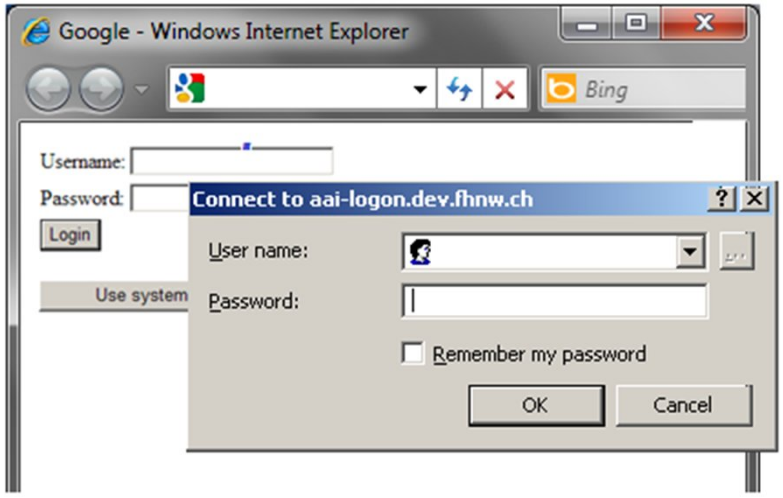


Client

How can a bad user experience be avoided?

- If the client's browser is not properly configured
- If no ticket is available

IE

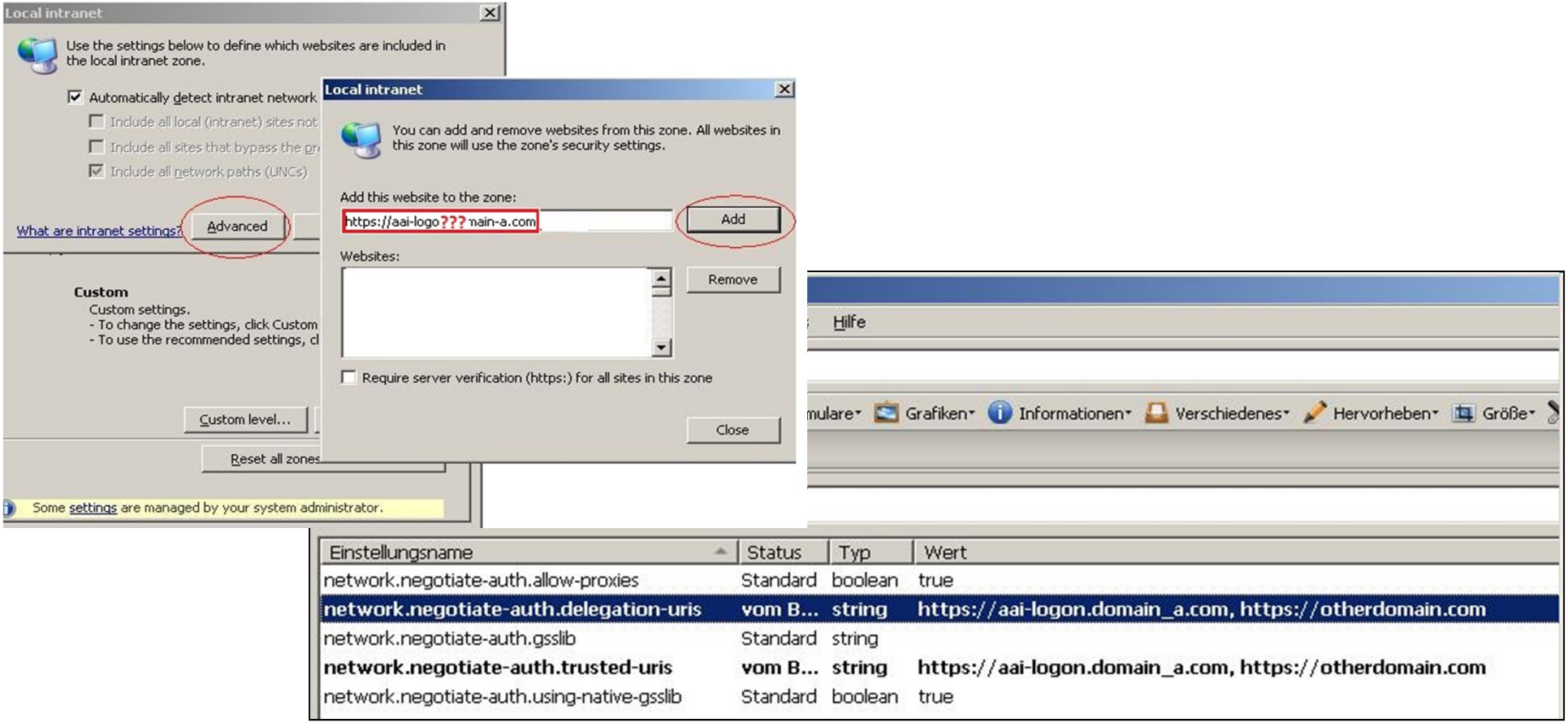


IE will “downgrade” to NTLM and request username and password

Firefox

Client

Manual configuration can be difficult for the user:



Client (example solution FHNW)

How can correct browser configuration be ensured?

- Internet Explorer
  - Browser configuration by group policy
  - User-agent header changed to confirm the configuration:

	Value
Accept encoding	gzip, deflate
[redacted]	
User-agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; FDM; IENW110)

- Firefox
  - Browser configuration by software deployment solution
  - Browser type and version is checked

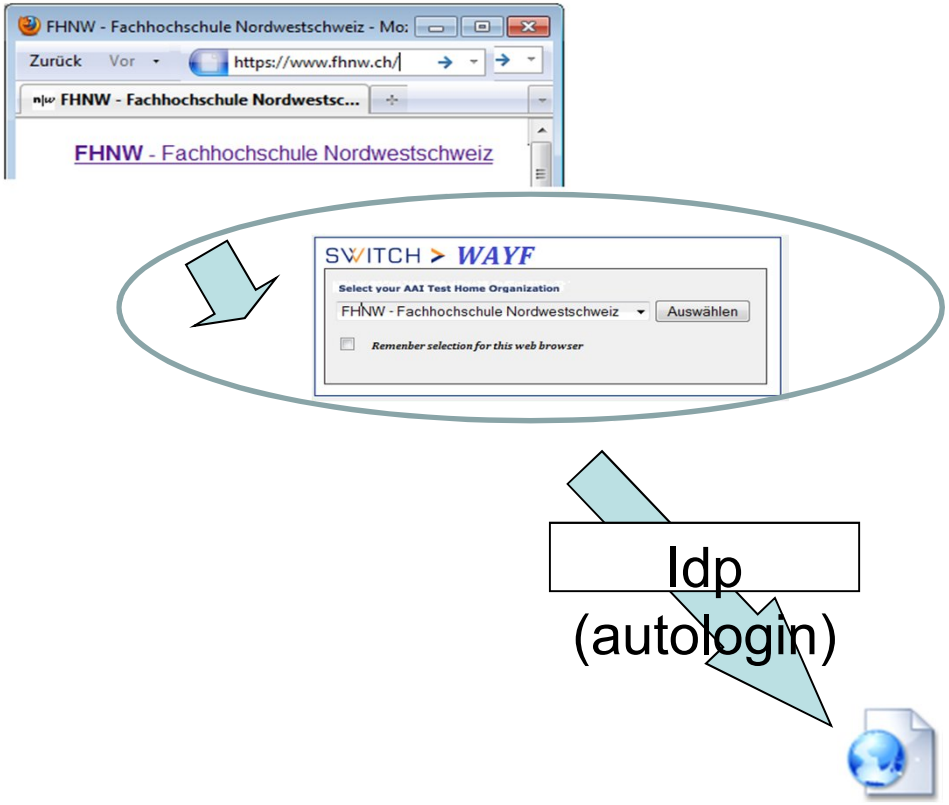
Client (example solution FHNW)

Is the client able to get and provide a ticket?

- The client IP is checked to detemine the user's network location (on campus, connected by VPN or outside FHNW network)

User experience (example solution FHNW)

How can the WAYF page be avoided when auto-login is active?

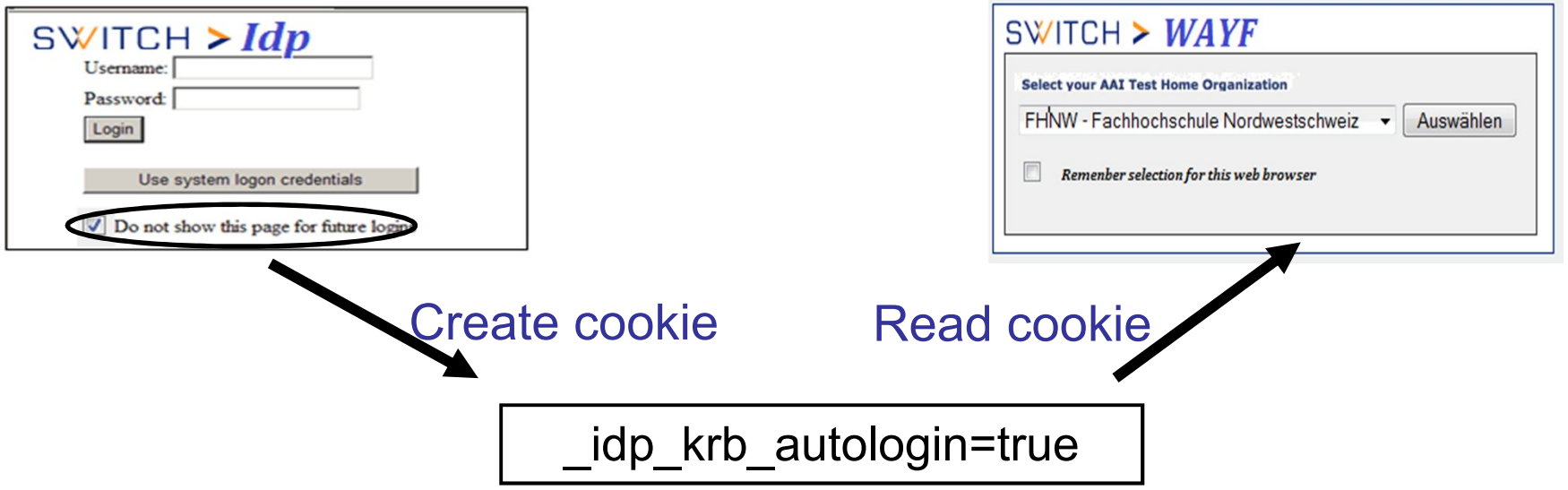


User experience (example solution FHNW)

How can the WAYF page be avoided when auto-login is active?

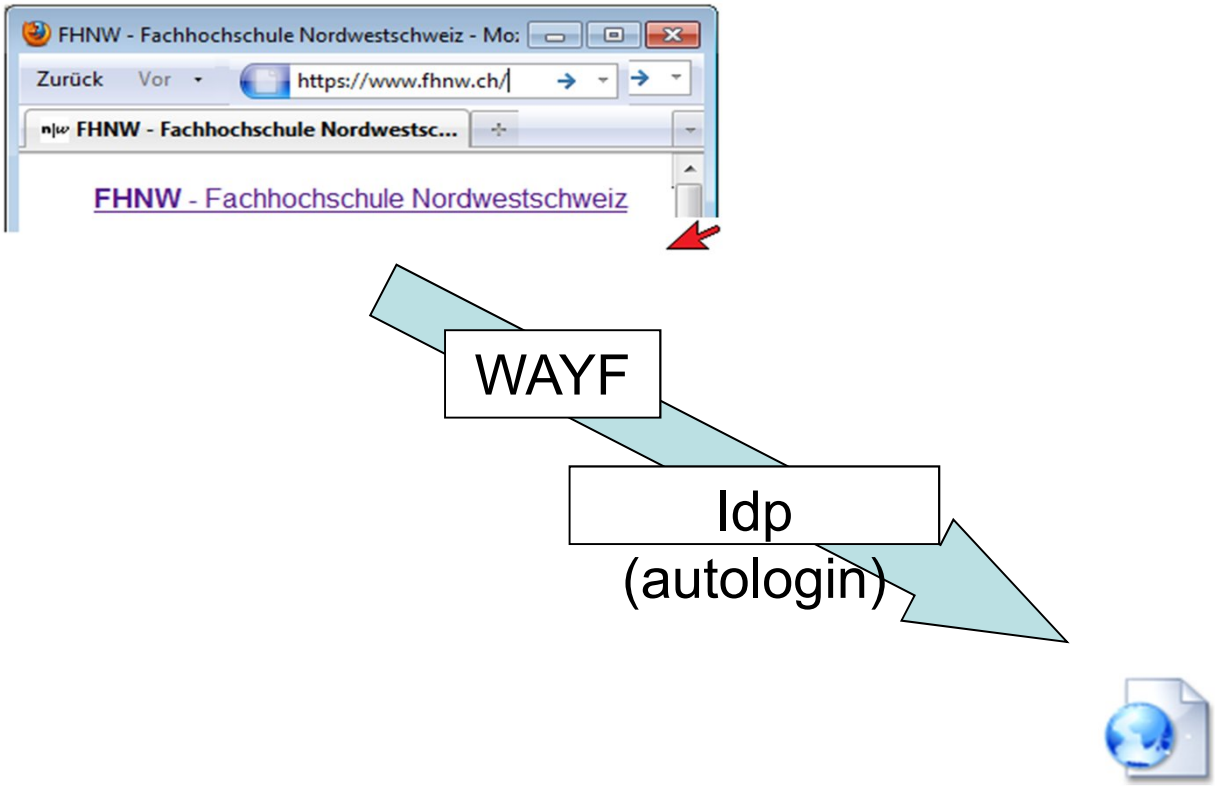
A customization of the WAYF service is necessary:

- Verify that the «auto-login cookie» exists (and is true)
- Redirect to the FHNW Identity Provider



User experience (example solution FHNW)

One-click access to ressource



More Information

https://wiki.shibboleth.net/confluence/display/SHIB2/Kerberos+Login+Handler

- Installation
- Browser configuration
- FAQ
- Examples

Source code will be available starting next month