

# Kerberos Login Handler (IdP)

## The Project

**Main Goal:** Implement a new IdP Handler using client's system credentials to provide a "Single Sign On" mechanism.

### Main Benefit

- Facility for the user
- Single Sign On (The user type username/password once).
- Protection against some kind of attacks (Keystroke loggers)

### Important

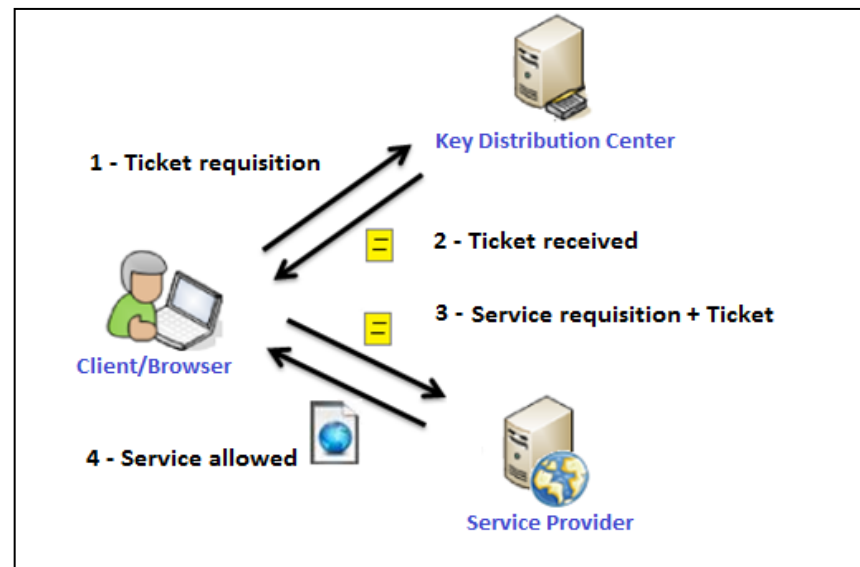
Like other SSO Systems:

- The person who has access to the machine will be able to join the system.

## What is Kerberos?

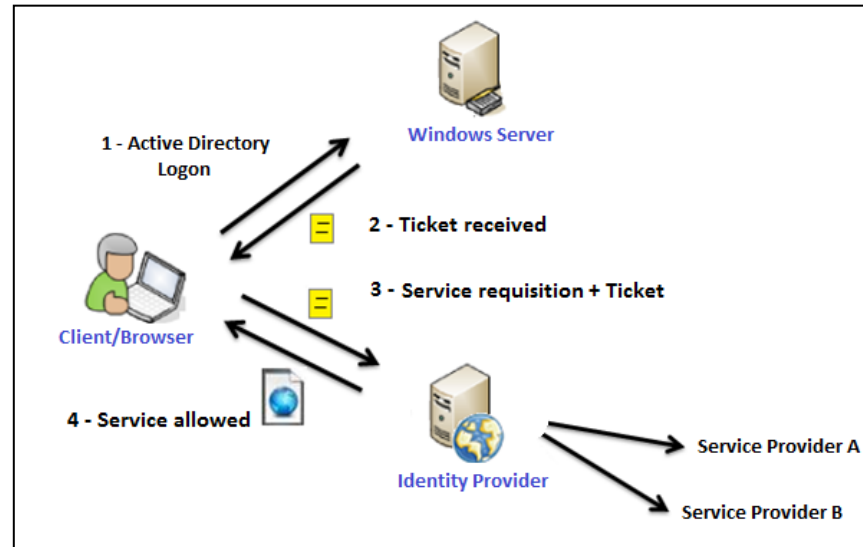
- Kerberos was developed by MIT (Massachusetts's Institute of Technology) as part of Project Athena, which started in 1983 (<http://web.mit.edu/kerberos>)
- Kerberos is a ticket-based network authentication protocol - SSO.
- Microsoft adopted Kerberos as the preferred authentication protocol since Windows Server 2000.
- The user's password is never sent over the Network

### Basic schema



# Kerberos Idp Handler & Active Directory

## Basic schema



1. Log-in in the Active Directory (windows logon)
2. The TGT (ticket-granting-ticket) will be stored at the client
3. The browser will request a resource and send a Service-Ticket.
4. The Identity Provider validates the Ticket and extract the credentials

## Minimal requirements

### **Kerberos Infrastructure**

- Kerberos - Key Distribution Center
- Service Accounts

### **Identity Provider**

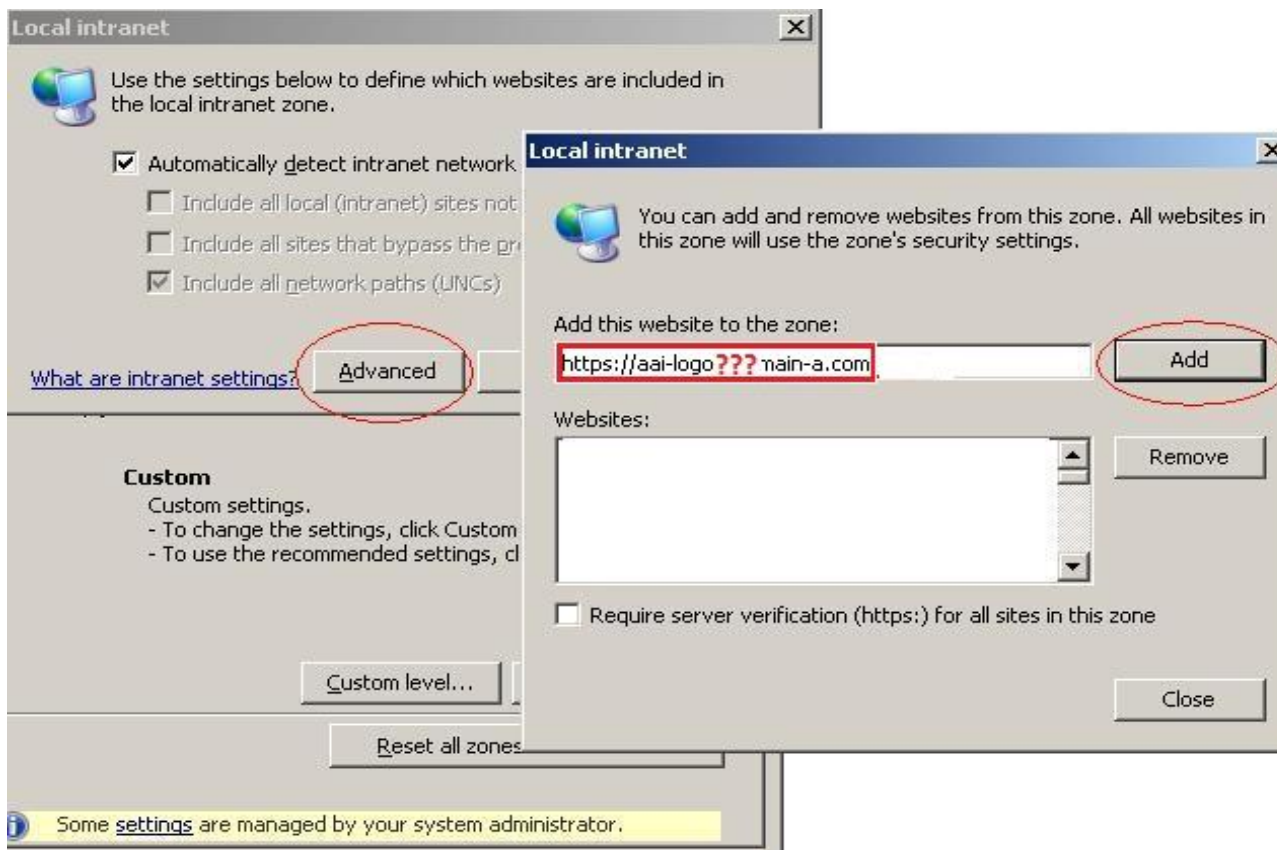
- Kerberos - Client
- Kerberos Idp Handler

### **Client**

- Kerberos - Client
  - Browser (must to be configured)
-

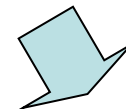
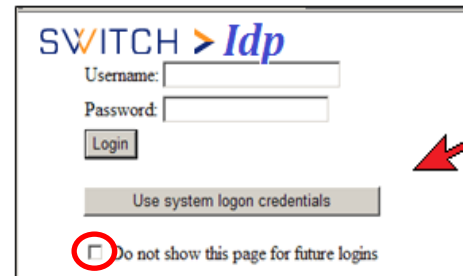
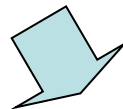
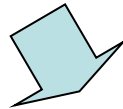
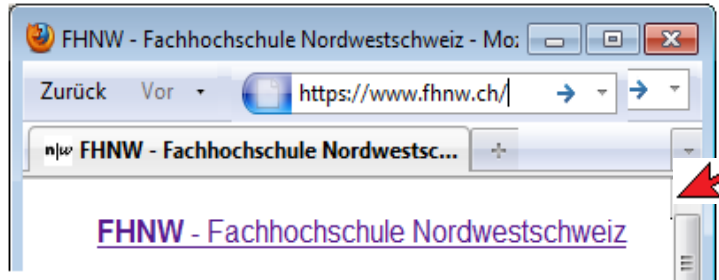
## Examples

### Browser configuration – Internet Explorer:



# Examples

Some screens

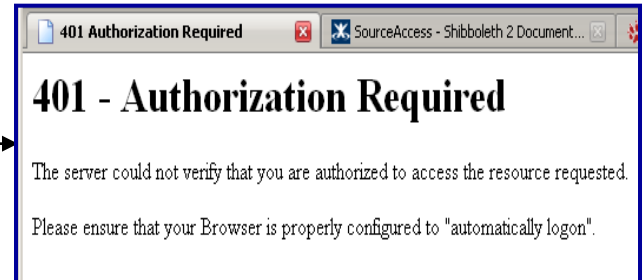


## Examples

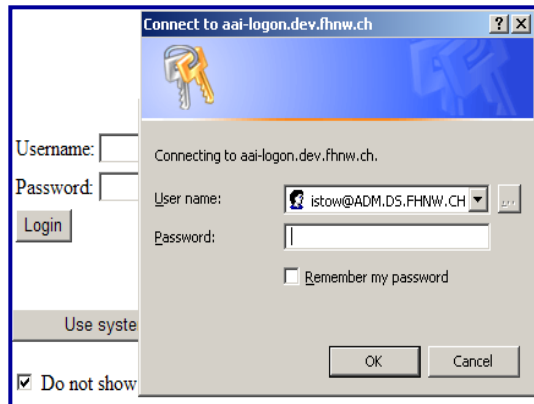
If the client's browser is not properly configured.

- If No Ticket available
- If Browser is not configured

Mozilla



IE



IE will „downgrade“ to NTLM  
(user/password popup).

For more Information:

Wiki

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

Project page (bugs, features)

<https://forge.switch.ch/redmine/projects/java-idp-kerberos-login-handler>