# 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.

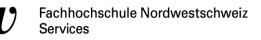
#### **Main Benefit**

- 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.

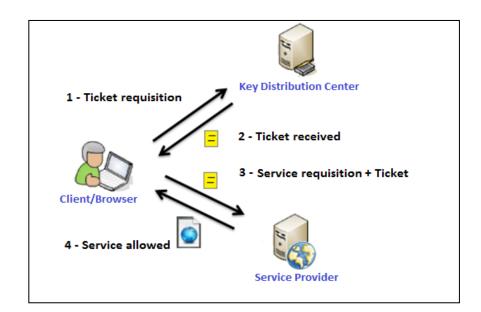


# What is Kerberos?

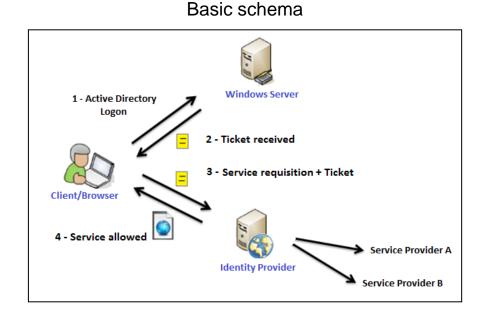
- Kerberos was developed by MIT (Massachusetts's Institute of Technology) as part of Project Athena, which started in 1983 (<u>http://web.mit.edu/kerberos</u>)
- Kerberos is a ticket-based network authentication protocol SSO.
- Microsoft adopted Kerberos as the preferred authentication protocol since Windows Server 2000.

**Basic schema** 

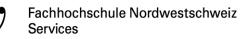
- The user's password is never sent over the Network



# Kerberos Idp Handler & Active Directory



- 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

n

- Kerberos Client
- Browser (must to be configured)

 $\mathbf{n}|w$ 

## Examples

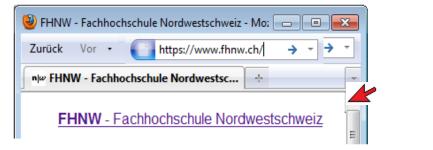
#### Browser configuration – Internet Explorer:

sthe local intranet zone.	Local intranet	1
Automatically detect intranet network	Local Intranet	2
🗖 Include all local (intranet) sites not	You can add and remove websites from this zone. All websi	ites in
$\square$ Include all sites that bypass the pr	this zone will use the zone's security settings.	
🗹 Include all <u>n</u> etwork paths (UNCs)		
	Add this website to the zone:	
vhat are intranet settings Advanced	https://aai-logo???main-a.com Add	
	Websites:	
	Remov	ve
Custom		
Custom settings. - To change the settings, click Custom		
- To use the recommended settings, cl		
	Require server verification (https:) for all sites in this zone	
<u>C</u> ustom level	Close	
	Close	

n

#### **Examples**

Some screens



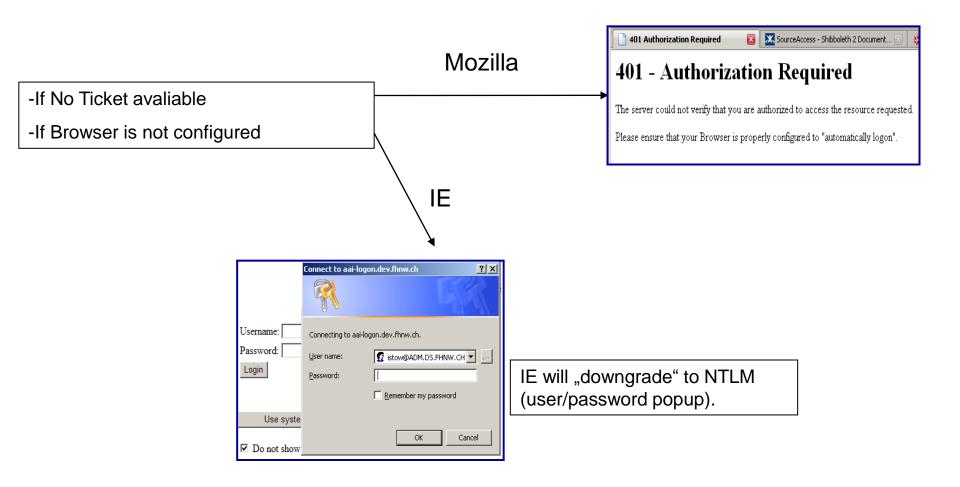


SWITCH > Idp Username: Password: Login	4
Use system logon credentials	
Do not show this page for future logins	



## Examples

If the client's browser is not properly configured.





## 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