Workshop „SAP and AAI“

Daniel Emch, Universität Zürich

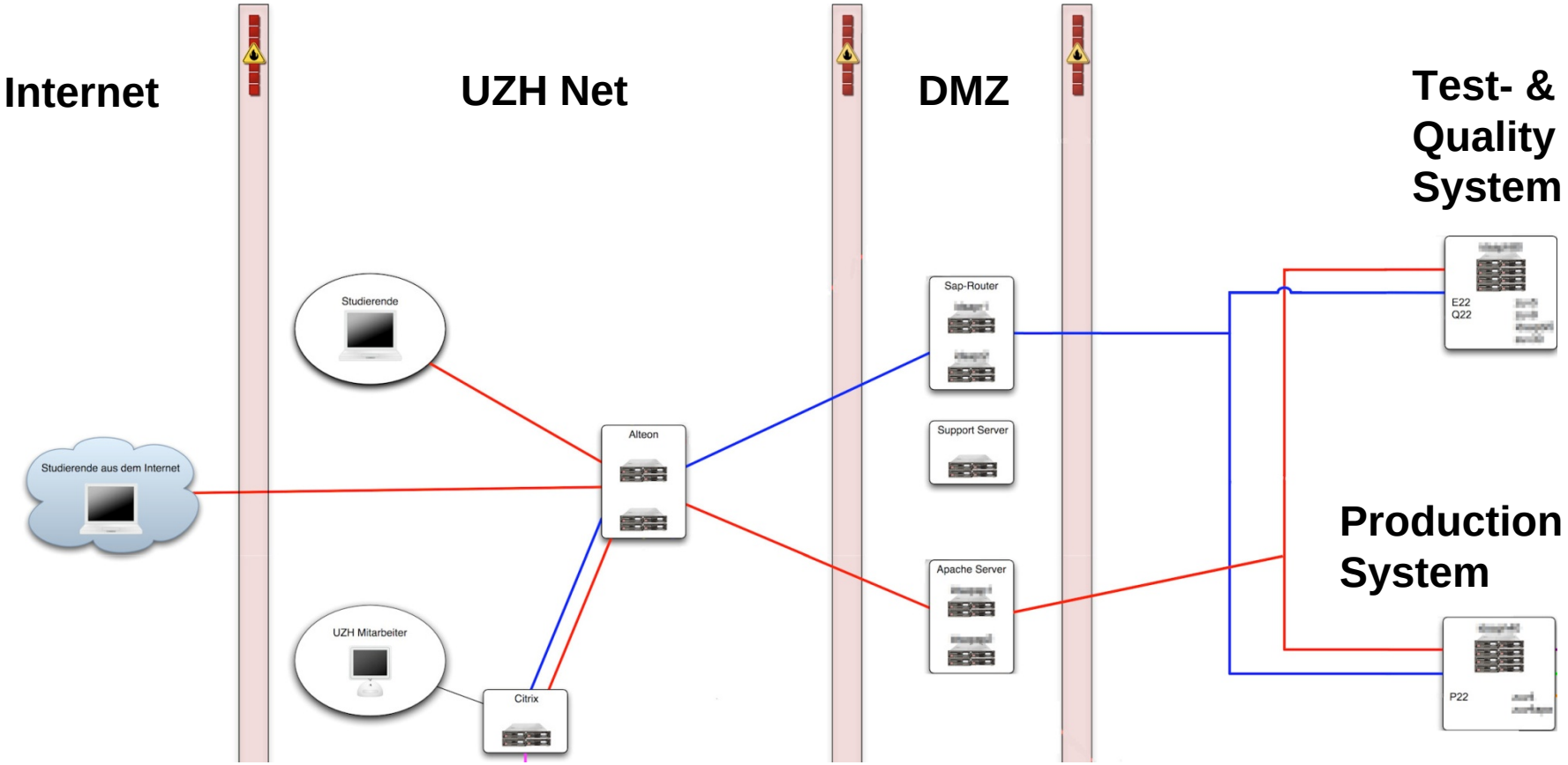
8. February 2010

Agenda

- Overview of the UZH SAP architecture
- User authentication using header variables
- Actual Implementation at UZH
- Advantages
- Drawbacks
- Live Demo
- Question & Answers
- Contact

SAP System- and Network Architecture

Universität Zürich



User Authentication using Header Variables

- Authentication is handled by a own application
  - In our case through Apache reverse proxies together with the Shibboleth module mod_shib
- After a successful authentication, a HTTP header variable with the user's ID is added to the HTTP Request
  - In our case we use a UZH internal AAI attribute, which contains the user's SAP user ID as HTTP header variable
- Applications protected by AAI authentication can read the user's ID from the HTTP header variable for authorization
- There is no password transfer between the reverse proxy and the application server!

Why did we use AAI for the Module Booking?

- The SAP ERP LDAP connector is in our eyes a bad piece of software
- At each start of a module booking period (between 800 and 1500 students try to book at the same time) we had a lot of performance problems
- Moving the authentication to a different system increases the resources for other parts of the application
- Through this measure we were able to increase the amount of concurrent users by factor 10!

- Another reason was to enable SSO with other UZH application, e.g. OLAT

Header Authentication - Where used at UZH?

- BSP custom application module booking.
  - Used in the Production, Test- and Development-System
  - Students: authentication in order to book modules
  - Staff: authentication in order to “simulate” students

- SAP Netweaver Enterprise Portal
  - Used on the Test-System only
  - For “simulation” purpose only

Header Variable Authentication - Advantages

- Easy to implement
  - Define AAI Attribute used for header variable authentication: existing or custom attribute
  - Load and configure Apache module mod_shib
  - Custom BSP: Change of the authentication service to read the user's ID from the HTTP header
  - Portal: Adjust the login module stacks to read user's ID from the HTTP header (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/8f/ae29411ab3db2be10000000a1550b0/frameset.htm)
- Low application requirements
  - SAP BSP or Web Dynpro Application not running inside the portal can easily be adopted
- "Simulation" mode can be achieved through reverse proxy configuration

Header Variable Authentication - Drawbacks

- Security. To minimize security concerns do:
  - Harden and keep the reverse proxy used for AAI authentication up to date. Optionally use a application firewall, e.g. mod_security (Open Source)
  - Use SSL between client – reverse proxy and reverse proxy – backend system
  - Put a firewall between reverse proxy (→ DMZ) and backend server. On the firewall, limit the web access to the backend system(s) to the reverse proxy IPs
  - Use a certificate between the reverse proxy and the backend system

Why didn’t we use AAI for the Portal?

- Missing ability to specify a certain validity period for a password

Live DEMO – student module booking

Universität Zürich

https://idagreen.uzh.ch/mb/

Question & Answers

Universität Zürich

Contact

Daniel Emch

Universität Zürich / Informatikdienste

Rämistrasse 42

CH 8001 Zürich

Tel. +41 (0)44 63 44035

E-Mail daniel.emch@id.uzh.ch