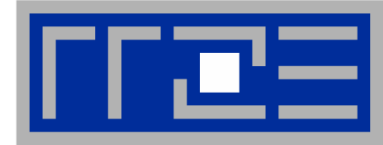


# Erfahrungen mit Web-SingleSignOn am Regionalen Rechenzentrum Erlangen

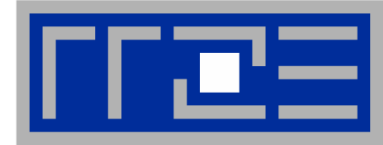
Florian Hänel

Regionales RechenZentrum Erlangen  
Friedrich-Alexander-Universität Erlangen-Nürnberg

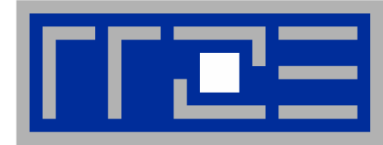
09.04.2007



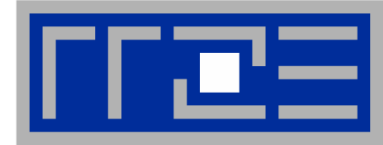
- **Historie**
  - Projektfortschritt
  - Realisierte Anwendungen
  - Ausblick
- **Systeme**
- **HowTo Shibbolethisierung**
- **Offene Fragen**
- **Links**



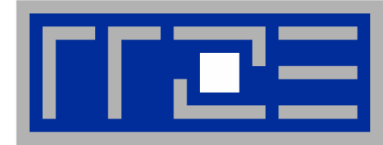
- Sommer 2006: Idee im Rahmen des IDM Projekts
- Herbst 2006: Konkretisierung auf dem AAI-Treffen in Freiburg
- Beginn: Dezember 2006
- Januar: erste Version des Identity Providers aufgesetzt
  - Zertifikate für die AAI Testumgebung erstellt
  - Beitritt der AAI Testföderation
- Februar: erste Version des Service Providers
  - Testbetrieb in der vascoda/AAI Testumgebung
- Einfaches schützen von Dateien und Verzeichnissen
  - Direkt über .htaccess Dateien



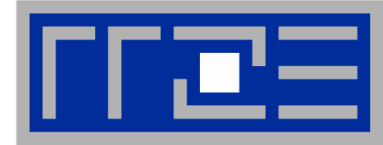
- Erste eigenständige Anwendung: Mediawiki
- Software der Wikipedia
- Anpassung durch extension Script
  - [http://meta.wikimedia.org/wiki/Shibboleth\\_Authentication](http://meta.wikimedia.org/wiki/Shibboleth_Authentication)
  - Installation durch kopieren in extensions Verzeichnis
- Anpassung der Parameter in Localsettings.php
  - Einbinden der extension
    - `require_once('extensions/ShibAuthPlugin.php');`
  - Schreibrechte entfernen für anonyme Benutzer
    - `$wgGroupPermissions['*']['edit'] = false;`
  - Unterbinden von Accounterstellung ausserhalb SSO
    - **`$wgGroupPermissions['*']['createaccount'] = false;`**



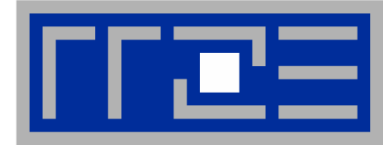
- Weitere Anwendung: Antville
  - Helma.org Mailinglisten leider nicht hilfreich
- Aufbau:
  - Apache->Helma Object Server->Antville
  - Anpassung des Helma Object Servers notwendig
    - Reicht nur wenige ENV Variablen von Apache durch
    - Anpassung macht alle Variablen in Antville verfügbar
  - Anpassung des Antville Codes
    - Einstiegspunkt: Globale Funktion die bei jeder Seite aufgerufen wird um ein evtl gesetztes Cookie zu prüfen
    - Erweiterung dieser Funktion auf Shibboleth Environment Variable
    - Wenn gültig, entsprechenden Benutzer laden
    - Ansonsten neuen Benutzer anlegen



- Das Apache Modul stellt Attribute zur Verfügung
  - Environment Variablen
  - Konfigurierbar über die modul-Konfiguration
- Die Webanwendung wertet diese aus
  - Geeignete Stellen sind Funktionen, die bei jedem Seitenaufruf ausgeführt werden müssen
  - Fehlen die Attribute, wird der Zugang verweigert
  - Link zum Login am Identity Provider muss bereitgestellt werden, oder Benutzer wird automatisch weiterverwiesen beim Fehlen der Attribute
  - Bei gültigen Daten muss der dazugehörige Benutzer gefunden werden
  - Gibt es noch keinen Nutzer lokal, muss dieser angelegt werden

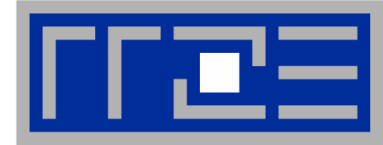


- **Benutzernamensräume**
  - Lokale Benutzerverwaltung bei vielen Anwendungen nötig
    - Speicherung von Benutzereinstellungen
    - Sessions
  - Möglichkeit: Unix-Kennung verwenden
    - Unschön, nichtssagend, und nicht jeder besitzt eine solche
  - Alternative: VornameNachname
    - Problem: Mediawiki und antville legen neue Benutzer an falls der Nutzer die Seite zum ersten mal besucht
    - Namenskollisionen

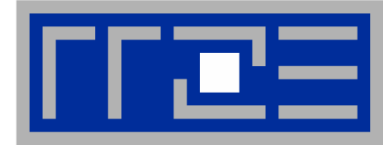


- Szenario: Nicht im IDM verwalteter (externer) Nutzer erzeugt sich einen Account in der Anwendung mit Namen HansMüller. Nun greift ein anderer Hans Müller über Shibboleth auf die Anwendung zu und wird als der bereits existierende Nutzer eingeloggt -> „Identitätskonflikt“
- Lösungsansatz: Namensräume
  - Prefix: „rrze:HansMüller“
  - Postfix: „HansMüller@rrze.uni-erlangen.de“
  - Externe Benutzer anlegen unterbinden

# Roadmap



- Antville soll durch Wordpress  $\mu$  ersetzt werden
  - Antville wird nicht mehr weiterentwickelt
  - Wordpress weiter verbreitet
- Typo3 Content Management System
- Ilias e-Learning Plattform
- Virtuelle Hochschule Bayern
  - Warten auf VHB-Service Provider
- Beitritt der DFN-PKI
  - Ersetzen der selbstsignierten Zertifikate durch OpenCA basierende Zertifikate
- Mit Wiki und Blog sind die wichtigsten Teile des RRZE-Intranets abgedeckt



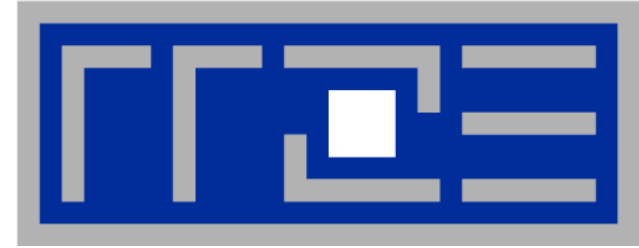
- VMWare Virtual Machines
- Hardware:
  - HP Xeon 2x3,0 GHz
  - 6GB Speicher
  - ~10 VMs
- Software
  - SuSE Enterprise Server 10
  - Apache 2
- Probleme:
  - Anfangs Probleme mit Zeitsynchronität
  - Kommunikation zwischen Service und Identity Provider enthält timestamps
  - Auseinanderlaufen der Zeiten führte zu Fehlern
  - Vmware-tools und deaktivieren der ntp daemons beheben das Problem



- Rpms im Projekt verwendeter und angepasster Software
  - <http://hp-test2.rrze.uni-erlangen.de/home:/unrz139-idm/>
- AAR Projekt Freiburg (Testföderation)
  - <http://aar.vascoda.de/>
- Internet2 Shibboleth
  - <http://shibboleth.internet2.edu/>
- RRZE Demo-Seite
  - <http://idmvm4.rrze.uni-erlangen.de>



Vielen Dank an das  
**AAI Team von der Universität Freiburg**  
für die Hilfe bei den vielen kleinen Stolpersteinen und  
Verständnisproblemen im Laufe des Projekts!



Vielen Dank für ihre geschätzte  
Aufmerksamkeit

Florian Hänel

[florian.haenel@rrze.uni-erlangen.de](mailto:florian.haenel@rrze.uni-erlangen.de)

Peter Rygus

[peter.rygus@rrze.uni-erlangen.de](mailto:peter.rygus@rrze.uni-erlangen.de)