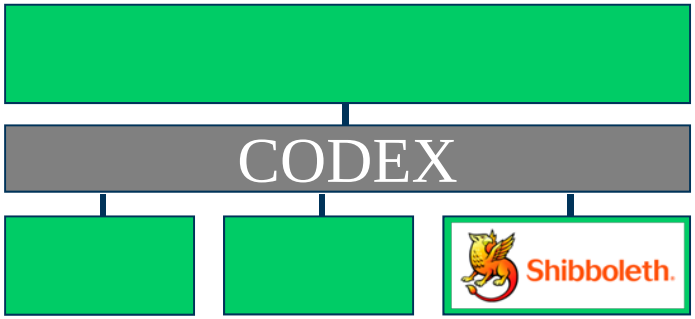
Shibboleth Identity Provider im Thüringer Codex-Projekt

Jena

Schmalkalden

Weimar



Erfurt

Nordhausen

Ilmenau

Consulting mit der Firma DAASI International GmbH

Maike Lorenz FSU Jena
Martin Haase, Peter Gietz DAASI International GmbH
Jörg Deutschmann (Berichterstatter) TECHNISCHE UNIVERSITÄT ILMENAU

Gliederung

1. Einleitung & Aufgabenstellung
2. Kurze Historie der Zusammenarbeit
   - Das Motto der Umsetzung war „Ruck-Zuck“ ☺ .
3. Feinspezifikation im Überblick
   - Dokumentation des Shibboleth-Systems für die TU Ilmenau
4. Gesamtarchitektur der technischen Lösung
5. Betriebshandbuch im Überblick
   - Betriebshandbuch für das Shibboleth-System der TU Ilmenau
6. Resümee und Ausblick

Einleitung & Aufgabenstellung

- Teilnahme der Thüringer Hochschulen an der DFN-AAI
- ➢ Consulting-Auftrag an Firma DAASI International
- Implementierung eines Shibboleth-Systems bestehend aus
  - Identity Provider (Produktivsystem) und
  - Service Provider (exemplarisch)
- Dokumentation des Systems für die TU Ilmenau
- Ausführliches Betriebshandbuch für die TU Ilmenau
- ➢ unter Einbeziehung der am Codex-Projekt beteiligten Einrichtungen, insbesondere Jena und Weimar

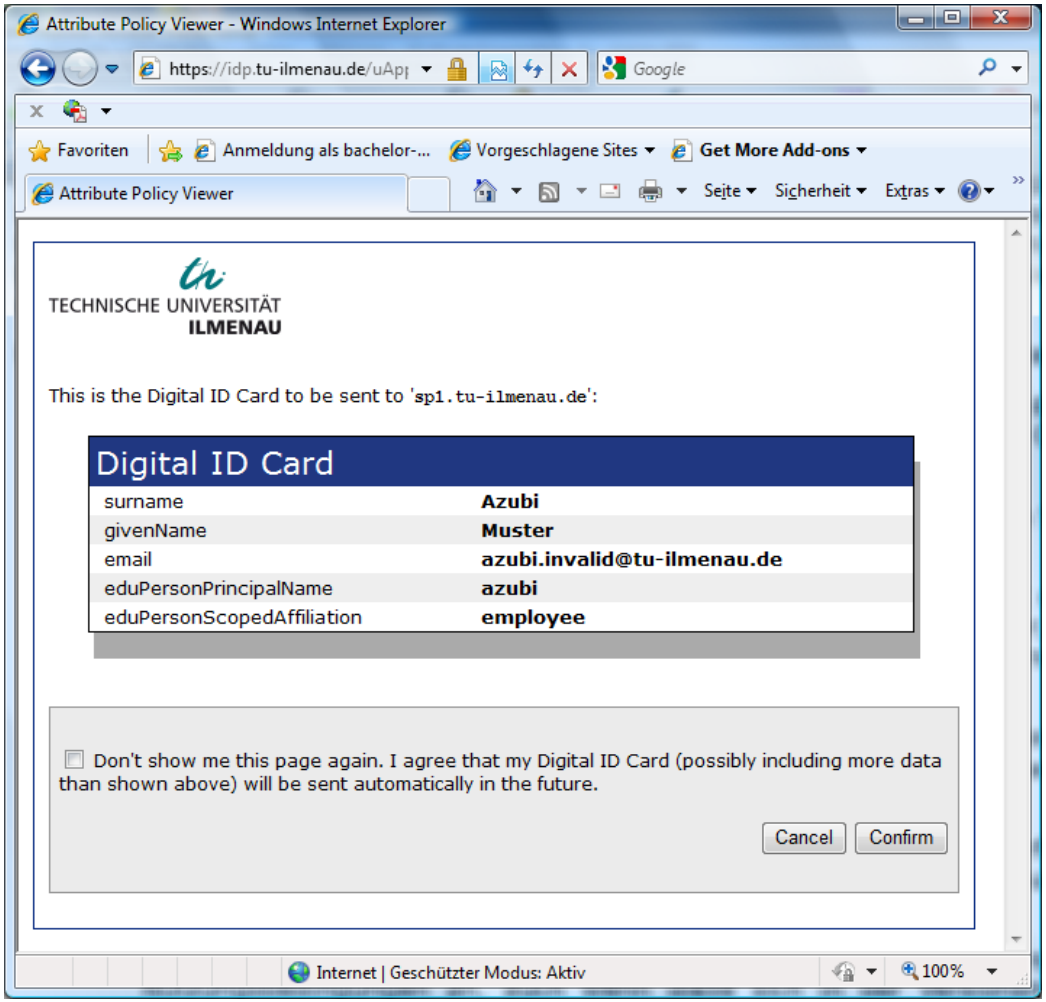
Kurze Historie der Zusammenarbeit

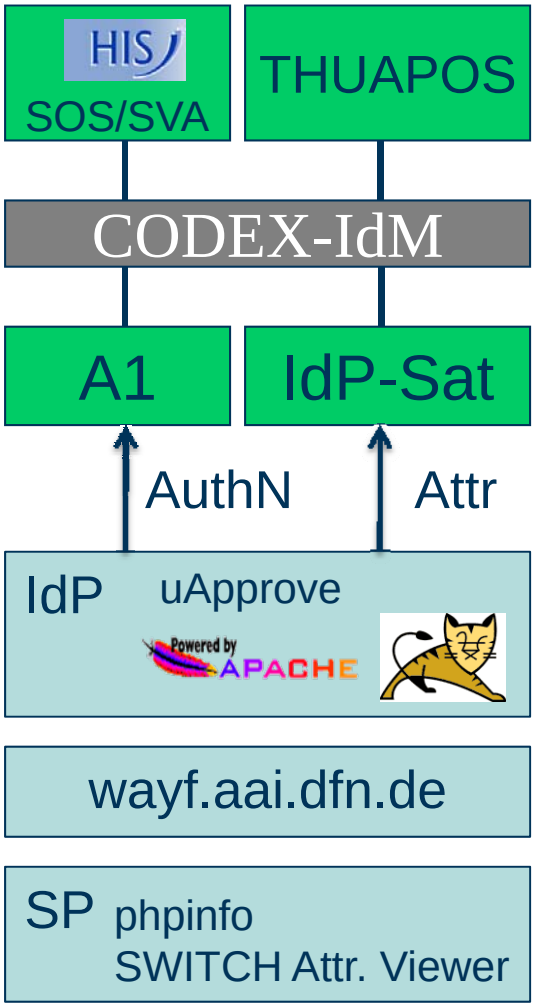
Zeitangabe	Ereignis
06. Oktober 2009	Idee beim ZKI AK Verzeichnisdienste
29. Oktober 2009	Beschlussvorlage bei Codex-Kern
09. November 2009	Angebot der Firma DAASI international
KW 46	Auftrag erteilt
KW 49	Installation IdP und SP; Remote-Zugang
18.11.2009 bis 07.01.2010	Versionierung der Feinspezifikation
17. Dezember 2009	Videokonferenz mit Vorführung des Systems
18.12.2009 / 07.01.2010	Abnahme Feinspezifikation Version 1.0 / Version 1.1
02. Februar 2010	Erste Version 0.1 des Betriebshandbuches

Feinspezifikation im Überblick

- Funktionelle Anforderungen an das System
- Architektur des Gesamtsystems
- Schnittstellenbeschreibung
  - HTTP, SAML, LDAP, PKI
- Spezifikation der einzelnen Komponenten
  - Apache – proxy_ajp – Tomcat
  - LDAP-Server, IdP, uApprove, SP, Metadaten
- LDAP-Schema für Autorisierungsattribute
  - Incl. kurze Beschreibung der von DFN-AAI empfohlenen Attribute
- Anforderungen für den Beitritt zur DFN AAI
- Auflistung der Konfigurationsdateien

Gesamtarchitektur





Codex-IdPSat

Von der DFN AAI empfohlen	Codex-IdPSat
cn (common name)	uniqueID
sn (surname)	Surname
givenName	Given Name
eduPersonScopedAffiliation	{'faculty' | 'student' | 'staff' | 'alum' | 'member' | 'affiliate' | 'employee' | 'library-walk-in'}* + ‘@’ + ‘tu-ilmenau.de’
eduPersonEntitlement	z.B. ‚urn:mace:dir:entitlement:common-lib-terms‘
eduPersonPrincipalName	uniqueID + ‚@‘ + ‚tu-ilmenau.de‘

*Beispielabbildung:

thuEduRoleType	thuEduJobType	DFN-AAI-Mapping
Mitarbeiter	Beschäftigter DM	staff; member; employee
Mitarbeiter	Prof. im Ruhestand	faculty; member; employee
Mitarbeiter	Hilfskraft	employee

Betriebshandbuch im Überblick

- Maßnahmen zur Aufnahme des IdP in die DFN-AAI
  - Organisatorisch, Beispiel für „Terms of Use“, Anmeldung technisch
- Beschreibung der Konfigurations- und Logdateien
- Liste der in ein Backup zu integrierenden Dateien
- Howto‘s und betriebliche Aufgaben
  - Cronjobs zur Auswertung der Log-Dateien
  - Beschreibung zur Nagios-Integration
  - Freigabe von Attributen und Integration neuer SPs
  - Layout-Anpassungen für Login-Seite und uApprove
  - Fehlerfallbehandlung u. Bemerkungen zur Ausfallsicherheit

Resümee und Ausblick

- Im Rahmen eines Consulting-Auftrages an die Firma DAASI International wurde
  - die technische Basis zur Teilnahme an der DFN-AAI in Ilmenau geschaffen, leicht von den Thüringer Hochschulen übernehmbar
  - die organisatorische Basis detailliert vorbereitet
- Im Rahmen des Codex-Projekts werden
  - die technische Basis an die beteiligten Einrichtungen „transferiert“, u.a. durch flexible Reisemitarbeiter
  - die organisatorischen Rahmenbedingungen geschaffen durch
    - eine exemplarische Anlage an die Dienstvereinbarung zum Meta Directory in Ilmenau
    - Aufnahme ins Verfahrensverzeichnis des Datenschutzes
    - Abschluss der Verträge mit dem DFN