Das Projekt NDS-AAI

ZKI-AK Verzeichnisdienste,

Hamburg, 11.-12.10.2007

Peter Gietz, CEO, DAASI International GmbH

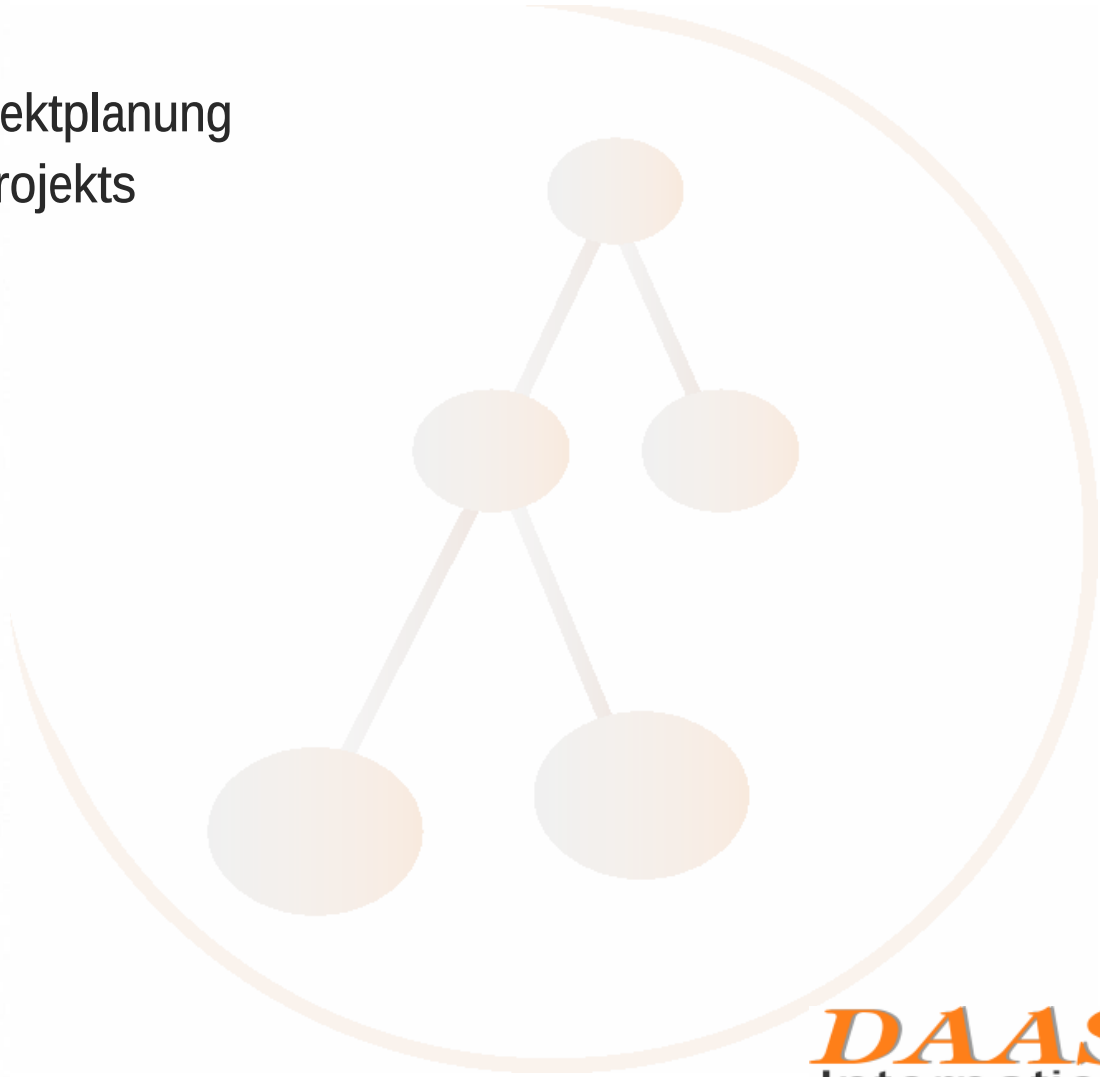
Peter.gietz@daasi.de

DAASI International

Directory Applications
for Advanced Security
and Information Management

Agenda

- Föderation
- Shibboleth
- Nds-AAI Projektplanung
- Status des Projekts



DAASI International

Directory Applications
for Advanced Security
and Information Management

Grundbausteine einer Föderation

- Eine Föderation ist ein Vertrauensbund, der es ermöglicht, verteilte Ressourcen gemeinsam zu nutzen
  - Vertrauen wird durch Einhaltung von Sicherheitspolicies gewährleistet
- Eine Föderation besteht aus drei Bausteinen:
  - Föderationsverwaltung
    - zentraler Vertragspartner für Föderationsmitglieder
    - Verwaltet Zugangsdaten zu den einzelenen Bausteinen
    - betreibt zentrale Infrastrukturkomponenten
  - Identity Provider (IdP)
    - Benutzerverwaltung der Heimatorganisation
    - verantwortlich für Authentifizierung und Attribute
  - Service Provider (SP)
    - Verantwortlich für Ressourcen
    - Entscheided aufgrund von Aussagen des IdP

DAASI International
Directory Applications for Advanced Security and Information Management

Voraussetzungen für eine Föderation 1

- Verwaltung der Föderationsmitgliedschaft
  - Liste der Mitgliedsorganisationen
  - Verträge zwischen den Mitgliedern (n to n, oder 1 to n)
  - Sicherer Datenaustausch zwischen Mitglied und Föderationsverwaltung, z.B. durch X.509-Zertifikate von Zertifizierungsstellen, denen alle Mitglieder vertrauen
  - Sicherer Registrierungsmechanismus
- Metadaten Verwaltung
  - Spezifizierung eines Metadatenformats
  - Mechanismus zur sicheren Übertragung und Verwaltung von Metadaten
  - Gewährleistung der Richtigkeit der Metadaten
  - Sicherer Mechanismus zur Veröffentlichung der Metadaten innerhalb der Föderation

DAASI International
Directory Applications for Advanced Security and Information Management

Voraussetzungen für eine Föderation 2

- Mechanismus zum Auffinden der IdPs
  - Der SP muss wissen, woher der Benutzer kommt
  - Dieser Dienst muss hochverfügbar sein
  - Ein Benutzer kann Mitglied in mehreren Föderationen sein!
- Betrieb des Dienstes
  - Betrieb der Metadatenverwaltung und des zentralen Dienstes zum Auffinden der IdPs
  - Weiterentwicklung der Standards und Technologien beobachten
  - Software-Updates ohne dass der Dienst unterbrochen ist

DAASI International
Directory Applications for Advanced Security and Information Management

Voraussetzungen für einen IdP

- Zugehörigkeit zur Community
- Aktualität und Vollständigkeit der Benutzerdaten
  - am Besten mittels eines IdM-Systems
- Unterstützung des Attributschemas mindestens durch ein Mapping
- Unterstützung eines sicheren Authentifizierungsmechanismus (Passwöter nur über verschlüsselte Verbindungen)
- Implementierung der geforderten Föderationssoftware
- Registrierung bei der Föderation und Lieferung der Metadaten
- Erhebung und Speicherung von Logdaten
- Reaktion bei Betrugsfällen, etc. z.B. Recherchieren der Identität, die zu einer bestimmten TargetedID gehört
- Einhaltung des Datenschutzes

DAASI International
Directory Applications for Advanced Security and Information Management

Voraussetzungen für Service Provider

- Zugehörigkeit zur Community
- Implementierung der geforderten Föderationssoftware
- Registrierung bei der Föderation und Lieferung der Metadaten
- Muss die Föderationsrichtlinien, insbesondere bezüglich des Datenschutzes befolgen
- Muss die Dienste zur Verfügung stellen und Zugriffskontrolle aufgrund der vereinbarten Regeln und Attribute ausüben

DAASI International
Directory Applications for Advanced Security and Information Management

Shibboleth

- Föderationssoftware vom US-amerkanischen Internet2-Projekt
- Open Source Software
- zusätzlich eine Single Sign On-Lösung
  - nach einmaliger Authentifizierung hat der Nutzer für eine bestimmte Zeit föderationsweit Zugriff auf verschiedene Anwendungen
- *Fertige Software für SAML-basierte Föderationen*
- *unterstützt Single Sign On*
- *viele Anwendungen werden „shibbolethisiert“*
- *Version 1.3. ist produktionsreif*
- *Neue Features wie Single Log Out werden erst in Shibboleth 2.0 implementiert*
- *http://shibboleth.internet2.edu*

DAASI International
Directory Applications for Advanced Security and Information Management

Federations mit Shibboleth

- Shibboleth im Wesentlichen besteht aus:
  - Identity Provider (IdP), der an die lokalen Benutzerverwaltungen (z.B. LDAP Server) angeschlossen wird
  - Service Provider (SP), der vor zu schützende Ressourcen bzw. Dienste gestellt wird
  - Where Are You From Server, über den der Benutzer seine Heimatorganisation auswählen kann
- Provider sind als Apache-Module implementiert
- Baut auf eine eigene SAML-Bibliothek auf

DAASI International
Directory Applications for Advanced Security and Information Management

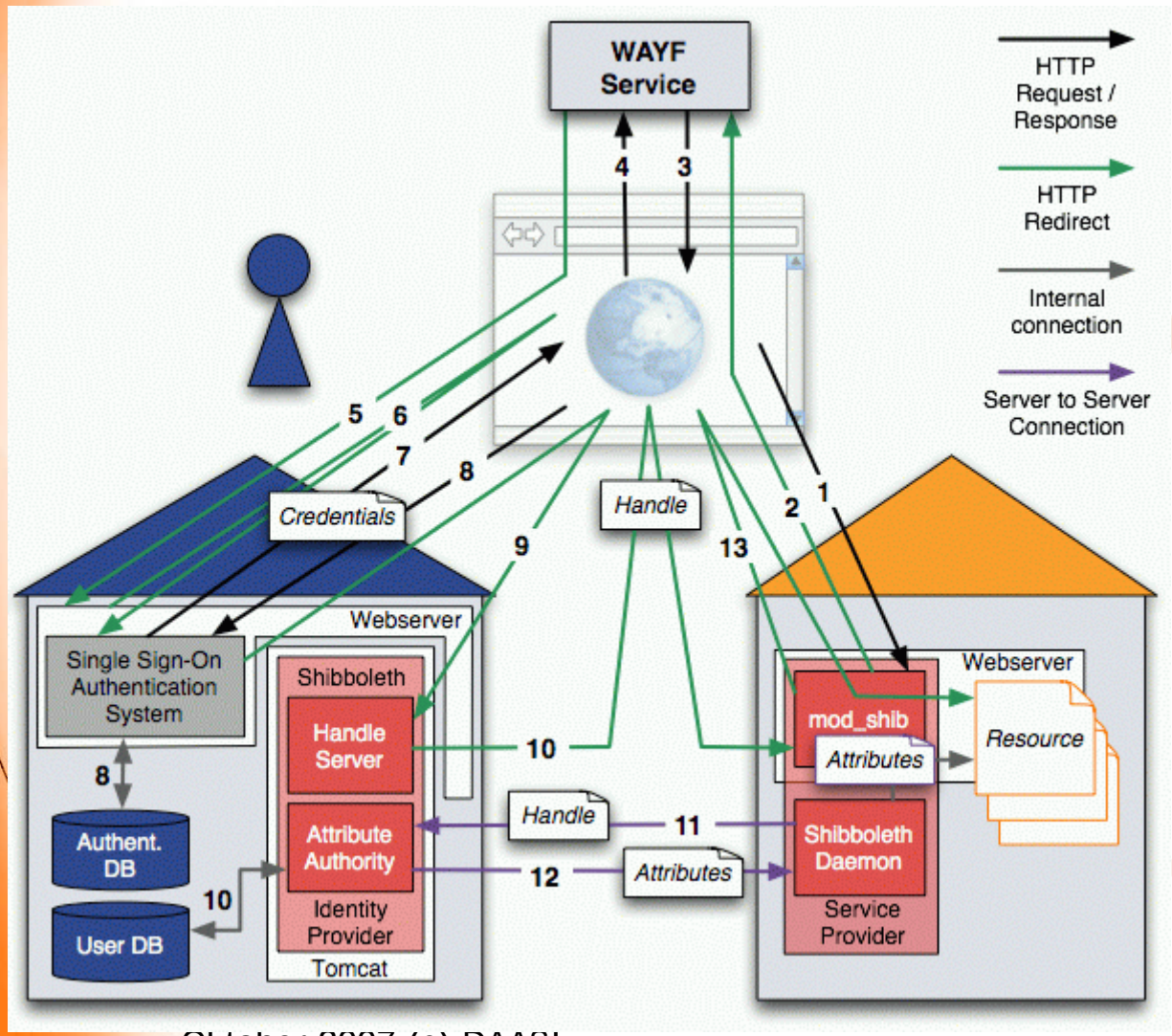
SAML

- SAML (Security Assertion Markup Language) (OASIS)
  - XML-Dokumente enthalten Zusicherungen (Assertions) die ein IdP über Benutzer macht:
    - Authentication Statements, Zusicherung, dass sich ein Benutzer Authentifiziert hat
    - Authorization Statement, Zusicherung über bestimmte Zugriffsrechte
    - Attribute Statement, Zusicherung über bestimmte Eigenschaften eines Benutzers, die in Form von Attributen weitergegeben werden und dem SP bei der Entscheidung über Zugriff unterstützen
  - Profile spezifizieren welche Assertions wie zwischen IdP und SP ausgetauscht werden

DAASI International
Directory Applications for Advanced Security and Information Management

Shibboleth Architektur

© Switch-AAI



DAASI International

Directory Applications for Advanced Security and Information Management

Das Projekt Nds-AAI

- Das Projekt Nds-AAI ist eine Initiative von LANIT
  - Landesarbeitskreis Niedersachsen für Informationstechnik der Hochschulrechenzentren
- Finanziert vom Niedersächsisches Ministerium für Wissenschaft und Kultur
- Durchgeführt im Wesentlichen durch die DAASI International GmbH

DAASI International
Directory Applications for Advanced Security and Information Management

Motivation für Nds-AAI

- Das Projekt Nds-AAI baut eine landesweite Föderation auf, die es auf Grundlage einer technischen Infrastruktur ermöglicht, den lokal in ihren Heimatorganisationen verwalteten Benutzern Ressourcen der gesamten Föderation kontrolliert zur Verfügung zu stellen.
- Diese Infrastruktur soll insbesondere Studierenden ermöglichen, Lerninhalte von E-Learning-Plattformen der verschiedenen Hochschulen zu nutzen, ohne in all diesen Hochschule einen Benutzeraccount haben zu müssen.
- Die erste Anwendung, die über die Nds-AAI zugänglich gemacht werden soll,
  ist die E-Learning-Software StudIP.

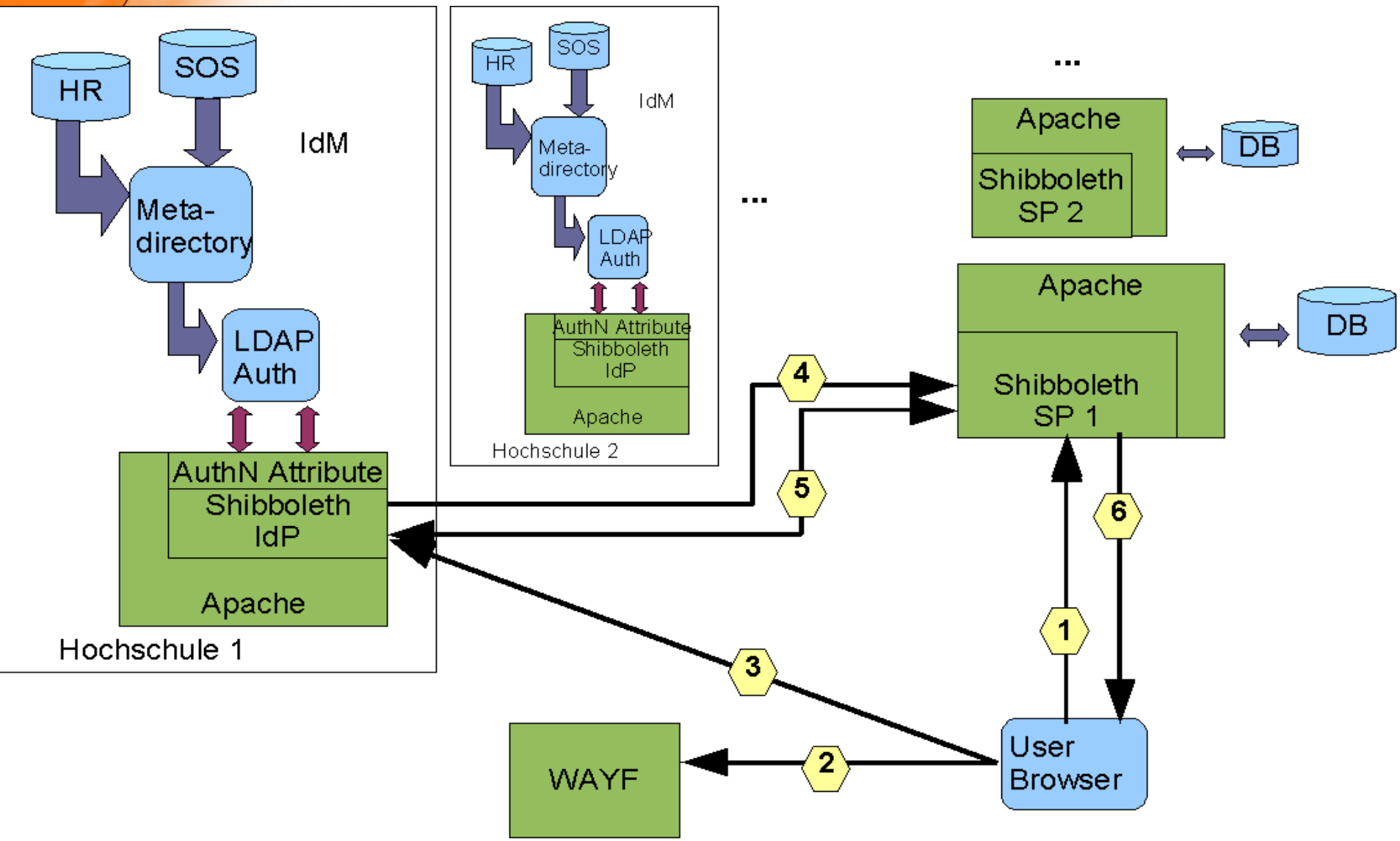
DAASI International
Directory Applications for Advanced Security and Information Management

Warum nicht gleich DFN-AAI?

- Festdefinierter Kreis der Mitglieder: Hochschulen in Niedersachsen
- Nds-AAI ist zunächst für einen bestimmten Zweck gedacht: eLearning mit StudIP
  - Es gibt bereits eLearning-Kooperationen in Niedersachsen
- Anforderungen an die Benutzerverwaltungen können flexibel den Einsatzszenarien angepasst werden
- Im Projekt können die Hochschulen gemeinsam Voraussetzungen für die Teilnahme an der DFN-AAI erarbeiten
- Sie können aber zu unterschiedlichen Zeitpunkten der DFN-AAI beitreten
- Hochschulen können mit dem selben IdP an verschiedenen Föderationen teilnehmen

DAASI International
Directory Applications for Advanced Security and Information Management

Nds-AAI Architektur



Projektplan

- Phase I: Planung
  - Ist-Analyse an 17 Hochschulen
  - Spezifikation der Anforderungen
  - Spezifikation einer Plattform (Hardware/Software)
  - Implementierungsplan
  - Erstellung eines Feinkonzepts
  - Sicherheitsanalyse zum Feinkonzept

DAASI International
Directory Applications for Advanced Security and Information Management

Projektplan

- Phase II: Aufbau und Test eines Prototypen
  - Aufbau Prototyp
  - Spezifikation von Testszenarien und deren Implementierung
  - Installation von Shibboleth 2.0 IdP und SP auf drei Rechnern, Installation eines WAYF-Servers auf einem der drei Rechner
  - Implementierung der Shibbolisierung von StudIP
  - Konfiguration und Dokumentation der Konfiguration
  - Gesamtdokumentation Prototyp
  - Test Prototyp

DAASI International
Directory Applications for Advanced Security and Information Management

Projektplan

- Phase III: Implementierung und Pilot
  - Implementierung
  - Installation und Test des getesteten Prototyps auf 18 Rechnern
  - Implementierungsbericht
  - Anschluss an die lokalen Infrastrukturen
  - Hochschulspezifische Betriebsdokumentationen
  - Exemplarische Anbindung an bestehende Förderationen
- Dokumentation des Gesamtsystems
- Pilotbetrieb, einschließlich Helpdesk über 4 Wochen
- Abschlussbericht

DAASI International
Directory Applications for Advanced Security and Information Management

Projektplan

- Phasenbegleitende Maßnahmen
  - Schulungs- und Marketingmaßnahmen
  - Durchführung eines Workshops zur Einführung in Shibboleth, Diskussion der individuellen Voraussetzungen an den einzelnen Hochschulen und Projektvorstellung
  - Durchführung eines Workshops zum Betrieb der Infrastruktur
  - Vorträge zum Nds-AAI-Projekts in einschlägigen Arbeitskreisen, insbesondere im ZKI-AK Verzeichnisdienste und DFN-AAI-Veranstaltungen

DAASI International
Directory Applications for Advanced Security and Information Management

Projekt – Phase I

- Ist-Analyse an 18 Hochschulen
  - Interview-Fragebogen definieren
  - Erhebung der Kontaktdaten der an den einzelnen Hochschulen zuständigen Mitarbeiter
  - Datenerhebung während der Telefoninterviews
  - Erstellung von Interview-Protokollen
  - Analyse der Interview-Ergebnisse
- Erstellung eines Bericht zur Ist-Analyse

DAASI International
Directory Applications for Advanced Security and Information Management

Projekt – Phase I

- Erstellung eines Feinkonzepts
  - Funktionelle Beschreibung des Gesamtsystems
  - Architektur des Gesamtsystems
  - Schnittstellenbeschreibung (LDAP, SAML, PKI)
  - Spezifikation der Authentifizierungsvorgänge und Autorisierungsvorgänge
  - Spezifikation eines LDAP-Schemas für Autorisierungsattribute
  - Spezifikation eines SAML-Profile
  - Mindestvoraussetzungen an die Identity-Management-Systeme der Einzelhochschulen
  - Spezifikation der einzelnen Komponenten des Gesamtsystems (PKI, IdP, SP, WAYF, Policy-Server)

DAASI International
Directory Applications for Advanced Security and Information Management

Projekt – Phase I

- Sicherheitsanalyse zum Feinkonzept
  - Datenschutzanalyse (Datenarten, Datenhoheit, Datenübertragung, Einverständnis der Teilnehmer)
  - Spezifikationen der Sicherheitsmaßnahmen
  - Sicherheitsanalyse (mögliche Angriffe auf das System, Analyse, ob Sicherheitsmaßnahmen solche Angriffe verhindern können)
  - Anpassung der Datenschutzvereinbarung

DAASI International
Directory Applications for Advanced Security and Information Management

Projekt – Phase II

- Aufbau Prototyp
  - Spezifikation von Testszenarien und deren Implementierung
  - Installation von Shibboleth 1.3 IdP und SP auf drei Rechnern, Installation eines WAYF-Servers auf einem der drei Rechner
  - Implementierung der Shibbolisierung von StudIP
  - Konfiguration und Dokumentation der Konfiguration
  - Gesamtdokumentation Prototyp
- Test Prototyp
  - Durchführung der Testszenarien
  - Testbericht und Abnahme
- Erstellung eines Betriebskonzepts
- Erstellung von Schulungsunterlagen

DAASI International
Directory Applications for Advanced Security and Information Management

Projekt – Phase III

- Anschluss an die lokalen Infrastrukturen
  - Vorbereitung der lokalen IdPs und Beratung der einzelnen Hochschulen (LDAP-Schema, Attribut-Mapping, Hilfe bei eventuellen Datenmigrationen, etc.)
  - Anschluss der IdPs an die vorhandenen Identity Management Systeme, zentralen Authentifizierungs-Server oder zentralen Benutzerverwaltungen
- Hochschulspezifische Betriebsdokumentationen
- Pilotbetrieb
- Abschlussbericht

DAASI International
Directory Applications for Advanced Security and Information Management

Anforderungen an Anwendungen

- Folgende Fragen sind bei einer Shibboletisierung relevant:
  - Wie werden die Ressourcen bisher geschützt (Apache, Tomcat, eigenes Verfahren, ...)?
  - Existiert ein eigenes Session-Management?
  - Kann dieses weiter verwendet werden, z.B. indem eine Sitzung über Shibboleth aufgebaut wird?
  - Existiert eine eigene Rechteverwaltung?
  - Können die dafür notwendigen Informationen per Shibboleth über Attribute bereitgestellt werden?
  - Wie werden Personalisierungsinformation gespeichert

DAASI International
Directory Applications for Advanced Security and Information Management

Anforderungen an die Plattform

- Serversystem mit Xeon/Opteron
- Linux (OpenSuse 10.2)
- 4 GB RAM
- 120 GB HD (ideal zweifach über Raid 1)
- Gigabit Ethernet Netzwerk-Karte
- redundantes Netzteil
- redundante Netzwerkkarte
- 64-Bit-Architektur wird zwar noch nicht von Shibboleth offiziell unterstützt, funktioniert aber

DAASI International
Directory Applications for Advanced Security and Information Management

Projektstatus

- Phase I: Design: fast abgeschlossen:
  - Erhebung, Anforderungen, Feinkonzept
  - Die Sicherheitsanalyse ist im Entstehen
- Phase II: Prototyp: fast abgeschlossen
  - Testsystem aus drei Rechnern installiert
  - Stud.IP (1.5 und 1.6) erfolgreich shibboletisiert (Dank an E. Ludwig, Virtuos)
  - Testszenariendefinition und Entwicklung von Testclients für Belastungstests fertiggestellt
  - Basistests und Belastungstests wurden bereits erfolgreich durchgeführt
  - Installationsanleitung für OS und Shibboleth erstellt
- Phasenbegleitende Maßnahmen
  - Mehrere Workshops durchgeführt

DAASI International
Directory Applications for Advanced Security and Information Management

Projektstatus

- Phase III: Implementierung findet gegenwärtig statt
  - Rechner wurden an die einzelnen Hochschulen geschickt
  - Anleitung für eine AutoYast-gestützte SuSE-Installation erstellt
  - Beschreibung der Installation und Konfiguration von Shibboleth erstellt
  - Erste Rechner an den Hochschulen werden gegenwärtig angeschlossen
  - Pilotphase wird in Kürze starten

DAASI International
Directory Applications for Advanced Security and Information Management

Ausblick

- Shibboleth 2.0 kommt langsam, aber es kommt
  - insbesondere Single Log Out interessant
- Weitere Anwendungen sollen angeschlossen werden
  - weitere eLearning-Systeme
  - andere Anwendungen
- Anschluss einzelner Hochschulen an die DFN-AAI

DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- Kontakt und weitere Informationen:
  - DAASI International GmbH
    Wilhelmstr. 106
    D-72074 Tübingen

    Web: http://www.daasi.de
    Mail: info@daasi.de

  - Mail: peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management