Der Authentifizierungs- und Autorisierungsverbund SaxIS - ein sächsischer Mosaikstein für die DFN-AAI

DFN Kanzlertagung
Potsdam, 20. Juni 2007

Dr. Andreas Kluge
Lars Eberle
Jens Schwendel
Sven Lederer

TU Bergakademie Freiberg

Gliederung

1. Das Projekt SaxIS - Ziele und Vorgehensweise
2. Der Überbau: Identitätsschnittstelle auf der Basis der Software Shibboleth
   - Lösungsansätze
   - Die Software Shibboleth
   - Rolle der Förderation
3. Der Unterbau: lokales Identitätsmanagement
   - Bestandsaufnahme
   - Umsetzung am Beispiel der TU Bergakademie Freiberg – Erfahrungen und Probleme
4. Projektergebnisse
   - Erreichtes und wesentliche Erfolge
   - Aktueller Stand der Umsetzung
   - zukünftige Aufgaben

Anlass und Nutzen übergreifender Authentifizierungs- und Autorisierungsschnittstellen

- Konsortialverträge von Hochschulbibliotheken
- Bibliotheksverbünde
- Nutzung gemeinsamer Softwareplattformen (z.B. Bildungsportal – OLAT, Bibliotheksportal)
- Spezialisierung und Ergänzung kooperierender Rechenzentren
- Nutzung externer Dienstleistungen
- Komfort für die Nutzer (Single Sign On)
- Verbesserter Datenschutz für den Nutzer

Projekt „Gemeinsame Autorisierungs-schnittstelle für Nutzer an sächsischen Hochschulen - SaxIS“

(Gefördert aus dem HWP vom Sächsischen Staatsministerium für Wissenschaft und Kunst)

- **Projektleitung:** Dr. Andreas Kluge (TU Freiberg, Leiter URZ)
  Dipl. Wirt.-Inf Jens Schwendel (BPS GmbH, GF)
- **Projektbearbeiter:** Dipl. Wirt.-Inf. Lars Eberle (TU Freiberg, URZ)
  Dr. Jochen Heinke (TU Freiberg, URZ)
  Sven Lederer (TU Freiberg, URZ)
- **Projektlaufzeit:** 01.03.2005 bis 31.12.2006
- **Personalumfang:** 2 x 0,5 VZ
- **Gesamtfördersumme:** 141.300 € (Personal- und Sachmittel)
- **Projektpartner:** Rechenzentren der folgenden Einrichtungen:

  TU Dresden, Uni Leipzig, TU Chemnitz, TU Bergakademie Freiberg, HTWK Leipzig, HTW Dresden, HS Mittweida, WHS Zwickau, HS Zittau/Görlitz, HfM Dresden, HfMT Leipzig, HGB Leipzig, HfBK Dresden, SLUB Dresden

Projektziele

Phase 1 (2005)

- prototypische Implementierung einer sicheren Authentifizierung der Nutzer von zentralen Services
- zeitnaher Ausschluss unberechtigter oder nicht mehr berechtigter Nutzer
- einheitliche Logins und Passwörter an zentralen Services und Hochschulen
- Komfort für die Nutzer
- Ermöglichung hochschulübergreifender Authentifizierung auch für die Hochschulen

Projektziele

Phase 2 (2006)

- Konzeption und initialer Aufbau einer sachsenweiten Shibboleth-Föderation. Entwicklung und Umsetzung von Policies und Standards als Voraussetzung für den reibungslosen Betrieb einer einrichtungsübergreifenden AAI im Rahmen der Shibboleth-Föderation.
- Unterstützung der Einrichtungen bei der Klärung anstehender datenschutzrechtlicher und sicherheitstechnischer Probleme
- Anbindung der Einrichtungen über die aufgebaute AAI an das Bildungsportal Sachsen und das Digitale Bibliotheksportal Sachsen.
- Beratung und Unterstützung der Einrichtungen bei der Umsetzung interner Identitätsmanagementkonzepte.
- Sicherung des langfristigen stabilen Weiterbetriebs der aufgebauten SaxIS-Dienste.

Projekt SaxIS - Globalziel

Einführung einer sachsenweiten Identitäts-Schnittstelle für Nutzer (Beschäftigte und Studenten) an sächsischen Universitäten und Fachhochschulen

Lösungsansatz im Projekt

1. Identitätsmanagement war **nicht** Ziel von SaxIS, die Nutzer werden weiterhin an den Hochschulen verwaltet
2. was realisierbar war, ist eine AAI (Authentication and Authorization Infrastructure)
3. deutschlandweit liefen bereits einige vergleichbare Projekte und Vorhaben an, internationale Erfahrungen waren verfügbar
4. die Wahl der Software fiel Shibboleth, das sich mittlerweile fast zum einem Standard entwickelt hat (http://shibboleth.internet2.edu/)
5. entstanden aus einem ähnlich gelagerten Projekt in den USA, vielfach produktiv im Einsatz

Shibboleth – Die Grundlagen

Vier Parteien:

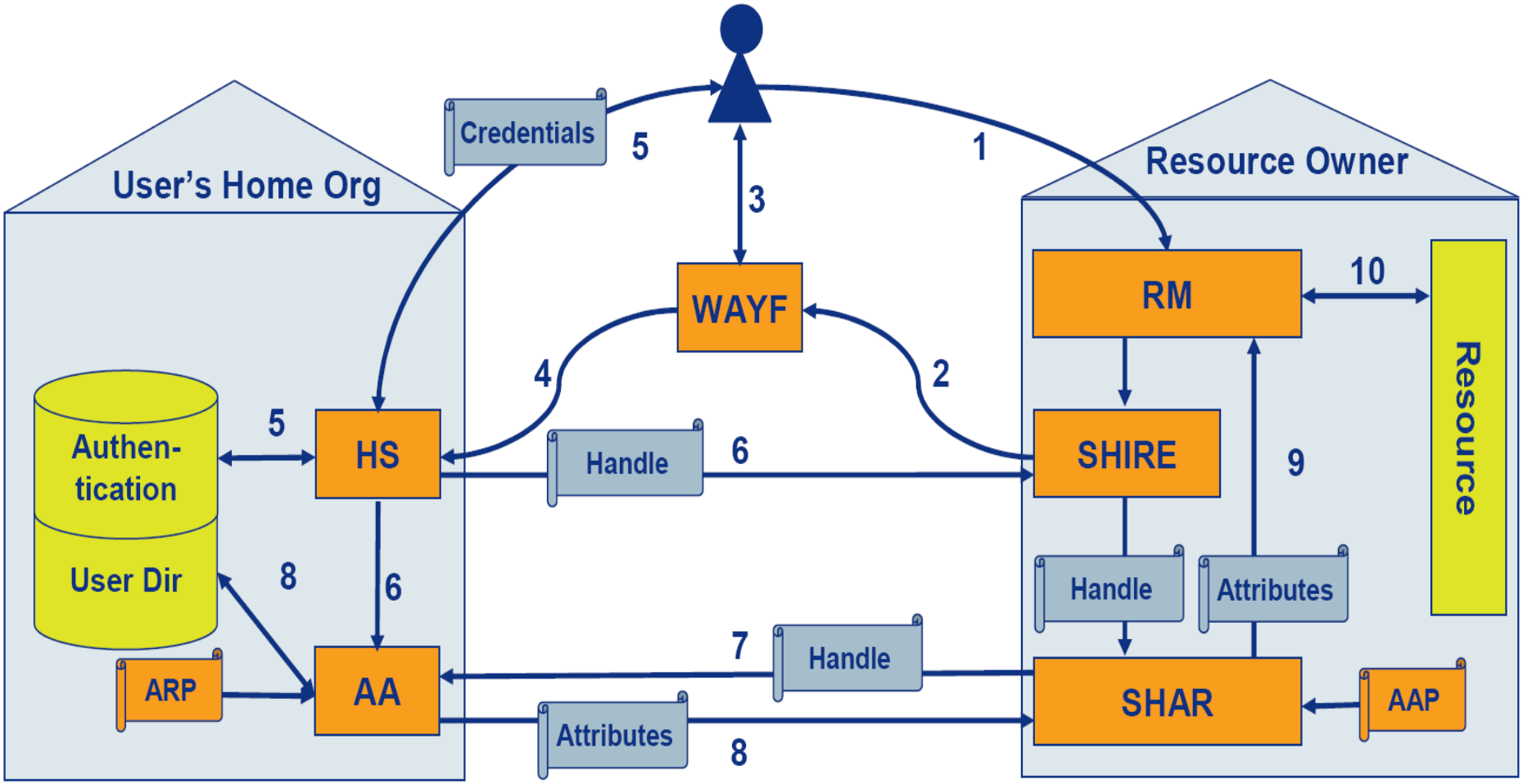
- **Nutzer** (gehören einer/mehreren Einrichtung an)
- **Identity Provider**
  (die Einrichtungen, haben Nutzerdaten gespeichert)
- **Service Provider**
  (bieten Services an, benötigen dazu evtl. Nutzerdaten)
- **Föderation**
  (regelt Standards, verwaltet Überblick über die Identitäsverwalter, Policyverwalter -> Details folgen)

Sicherheit: SSL und Zertifikate sind obligatorisch

Shibboleth – Der Ablauf

- Nutzer kommt zu einem Service Provider (z.B. BPS)
- dieser kann ihn zuerst nicht authentifizieren und leitet ihn an den „Where are you from“-Server (WAYF) der Föderation weiter
- dort wählt der Nutzer seinen Identity Provider
- er wird zu diesem weiter geleitet
- er authentifiziert sich dort lokal (völlig egal, wie)
- wenn erfolgreich wird er zurück zum Service Provider geleitet
- dieser kann ihn nun identifizieren
- Service Provider fragt Attribute des Nutzers beim Identity Provider ab
- Nutzer wird angemeldet

Interaktionen (am Beispiel Shibboleth)



Quelle und Erläuterung der Abkürzungen: www.switch.ch/de/aai/

Shibboleth - Interna

- Authentifizierung
  - Shibboleth authentifiziert nicht selbst
  - zur Anwendung kommen Apache oder Tomcat-Authentifizierung, die die einfache Anbindung der bereits vorhandenen Authentifizierungsmechanismen erlauben
- Attribute
  - welche Attribute ausgeliefert werden bestimmt nur der Identitätsverwalter und/oder Nutzer selbst
    (aber nie mehr als angefragt)
  - einfache Anbindung von LDAP oder JDBC-Datenbanken
  - fein konfigurierbar, beliebig erweiterbar, Mehrfachattribute möglich

Shibboleth – Die Fakten

AAI mit Shibboleth

- Shibboleth bietet **keine**
  - Rechteverwaltung
  - Identitätsmanagement
  - Datenspeicherung
- Shibboleth bietet
  - sichere Authentifizierung bei Vertrauen zwischen Teilhabern
  - sichere Datentransfers unter Beachtung des Datenschutzes
  - Single Sign On

Shibboleth – Die Vorteile

einrichtungsintern:

- **ein** Identitätsverwalter, beliebig **viele** Services
- einfache Anbindung der bereits vorhandenen Nutzerverwaltung und Authentifizierungsstrukturen
- effektiver Zugriffsschutz aller Webservices (über Apache oder Tomcat)
- Single Sign On
- Logindaten werden den Webservices dabei nicht bekannt (PHP-Problem beseitigt)
- ermöglicht anonyme Berechtigungsweitergabe
- einfache Konfiguration

Shibboleth – Die Vorteile

einrichtungsübergreifend:

- zentrale Services können Nutzerdaten der Hochschulen verwenden -> keine mehrfache Datenhaltung
- Daten sind immer aktuell
- ihnen werden die Logindaten der Nutzer nicht bekannt -> mehr Vertrauen der Nutzer
- Datenschutz voll gewährleistet
- Single Sign On funktioniert auch übergreifend
- in Hochschule nur minimale Konfigurationsänderungen notwendig, um zusätzliche Services anzubinden

Warum Shibboleth?

- weltweit bereits oft erfolgreich in Betrieb
- sehr einfache und flexible Anbindung vorhandener Authentifizierungs- und Datenverwaltungsstrukturen
- dezentraler Betrieb – unabhängig von einer zentralen Instanz
- OpenSource – kann modifiziert und jedem Anspruch angepasst werden
- DFN wird eine Föderation betreiben und damit für Nachhaltigkeit stehen

Shibboleth - Föderation

- Eine Föderation ist ein Zusammenschluss von Einrichtungen und Anbietern auf Basis gemeinsamer Richtlinien.
- Sie schafft das für Shibboleth notwendige Vertrauensverhältnis zwischen Identity und Service Providern und einen organisatorischen Rahmen für den Austausch von Benutzerinformationen.

Shibboleth - Föderation

Aufgaben einer Föderation sind:

- Vorgabe von Richtlinien (Policies)
- Verwaltung der Metadaten der Mitglieder
- Betrieb des Lokalisierungsdienstes (WAYF)
- Betrieb einer Zertifizierungsstelle
- Technischer Support

Der Unterbau – lokales Identitäts-management

- **Bestandsaufnahme: vertrauliche Gespräche mit allen Projektpartnern (i.d.r. Leiter der RZ, für die Nutzerverwaltung verantwortliche Mitarbeiter)**
- **Diskussion von internen Lösungsansätzen**
- **Vermittlung von Erfahrungen aus anderen Einrichtungen**
- **Vorgabe verbindlicher Minimalziele (übergreifende Schnittstelle, Authentizität, Aktualität der Daten)**
- **Praktischer Druck durch Anwendungsfall Bildungsportal**

Grundsätzliche Ergebnisse der Bestandsaufnahme

- IDM ist zumindest für größere Einrichtungen eine aktuelle Aufgabe
- Status bei Projektbeginn (3 generelle Zustände):
  1. RZ besitzt eine mehr oder weniger umfassende Nutzerdatenbank, gleicht +/- sporadisch mit Verwaltung (HIS-Datenbank) ab („kleinere“ Unis, viele FH's)
  2. Es existieren mehrere unabhängige Nutzerdatenbanken (fakultätsbezogen, dienstbezogen, ...) ohne Abgleich mit Verwaltung (Größere Unis)
  3. Es existiert keine oder nur eine rudimentäre Nutzerverwaltung (kleinere Kunsthochschulen)

Strategiefestlegung:

- Konzentration auf die zentrale Nutzerdatenbank im RZ
- Regelmäßiger Abgleich mit HIS-Datenbanken (SOS/SVA)
- Eindeutige Kennzeichnung von aktuellen Studenten und Mitarbeitern

Umsetzung der Strategie am Beispiel TU Bergakademie Freiberg

Status bei Projektbeginn

- Zentrale Nutzerdatenbank im URZ: ZNDB (mysql)
- „historisch“ gewachsen
- nur sporadisch mit HIS-SOS abgeglichen
- Einrichtung neuer Studenten aber semesterweise auf der Grundlage eines HIS-Datenauszuges
- Abmeldung mit Laufzettel -> Löschung manuell
- Verknüpfung über Scriptesystem mit NIS und Windows PDC bei Einrichtung (radius wird aus NIS gespeist)
- Authentifizierung auf zentralem Webserver funktioniert mit NIS
- Es existieren dezentrale Windows PDC -> tw. Abgleich über Datenbankauszug

Probleme:

- Ältere Angaben unvollständig (fehlender eindeutiger Identifikator: Matrikel-Nr., Personal-Nr)
- Schreibweise von Namen abweichend (Umlaute, Transkriptionen)
- Jede Menge „Karteileichen“
- Vermischung persönlicher und institutioneller Accounts
- Unvollständig gegenüber HIS-SOS und HIS-SVA

Langfristiges Stragetieziel

- Zentrales Verzeichnis
- “heißer“ Kandidat: **HIS-PSV** mit Datenreplikation nach LDAP bzw. Active-Directory (MS-AD)
- MS-AD für Single-Sign-On auf Betriebssystem- bzw. Nicht-Web-Dienstebene bereits jetzt im Aufbau (Status: Testlauf)
- „Hoffen“ auf HISinOne für eine saubere Abbildung von Identitäts- und Strukturdaten

Realistischer Zwischenschritt (Status Quo)

- Zentrale Nutzerdatenbank (ZNDB) als Puffer zwischen HIS (SOS und SVA) sowie NIS/Radius und Windows AD
- (teil-) automatischer Abgleich der Mitarbeiter- und Studentendaten
- Shibboleth holt Autorisierungsdaten aus ZNDB, Authentifizierung über .htaccess -> Radius
- Einhalten der DFN-AAI-Vorgaben: Angaben zu Mitarbeitern und Studenten sind authentisch, Änderungen werden tagesaktuell (Mo-Fr) wirksam

Datenabgleich HIS-ZNDB

Probleme:

- ZNDB ist nicht auf mehrere Studiengänge ausgelegt -> nur Erststudiengang wird übernommen
- Mitarbeiter sind gleichzeitig als Studenten eingeschrieben -> nur der höhere Status (Mitarbeiter) wird gespeichert
- Verfahren besitzt noch eine zeitliche Lücke, da die Einrichtung als neu erkannter Studenten max. 1 Tag benötigt
- Der Geschäftsprozess ist derzeit nicht vollständig automatisierbar, Zwischenschritte erfordern noch manuelles Eingreifen

Datenabgleich HIS-ZNDB

Erfahrungen:

- Einmaliger, sehr großer Aufwand bei initialer Korrektur unkorrekter Mitarbeiter- und Studentendaten (iterativer Prozess, nur teilweise algorithmische Unterstützung möglich)
- Nach Abschluss dieses Prozesses gelingt die Neuaufnahme von Zugängen auf der Basis der HIS-Datenbankauszüge weitgehend automatisiert (Problem: bereits vergebene Logins/E-Mailadressen)
- Problematischer ist das Löschen von Abgängen:
- Die Löschung der Nutzungsberechtigungen erfolgt grundsätzlich nur zweistufig manuell, auf Entscheidung der Sachbearbeiterin durch einen Operator (4-Augen-Prinzip)
- Vor der “physikalischen” Löschung des Accounts erfolgt eine “Nominierung” zur Löschung mit sofortigem Entzug des Status („M“ bzw. „S“) -> wirkt auf AAI durch
- Gast-Accounts, Institutionelle Accounts und „Altaccounts“ (z.B. Emeritierte Professoren, Mitarbeiter in Altersteilzeit etc.) werden ausschließlich in ZNDB verwaltet (als nicht verifizierte Accounts sind diese im Moment aber von der AAI ausgeschlossen)

Zusammenfassung: Erreichtes im Projekt SaxIS

Wesentliche Erfolge

- Die RZ sind mit sanftem Druck (AAI und Bildungsportal!) bewegt worden, technische und organisatorische Element eines hochschulübergreifenden Identitätsmanagements umzusetzen
- Die Kontakte zur Verwaltungs-EDV wurden in allen beteiligten RZ ergebnisorientiert intensiviert, es wurden neue übergreifende Geschäftsprozesse konzipiert und umgesetzt
- In diesem Prozess wurden die ansatzweise vorhandenen zentralen Nutzermanagementsysteme in den RZ qualitativ und qantitativ verbessert (Authentizität der Daten, Vollständigkeit der Daten)
- Im Hochschulaußenverhältnis können (wenn auch wegen des Datenschutzes äußerst sparsame) authentische Nutzerdaten zur Autorisierung und Authentifizierung über eine einheitliche Schnittstelle genutzt werden

Zusammenfassung: Schritte zum Identitätsmanagement

Zukünftige Aufgaben

- Die begonnenen Arbeiten müssen bis zur Etablierung umfassender interner Identitätsmanagementsysteme fortgeführt werden
- Die bisher gefundenen Lösungen bauen auf historisch “Ererbtem” auf und sind durchweg heterogen. Die einrichtungsinternen Schnittstellen zwischen den beteiligten Datenbanken sind nicht volländig transparent und automatisierbar
- Fragen des Datenschutzes müssen in der organisatorischen Umsetzung verbessert werden
- Zumindest den größeren Hochschulen wird der “schmerzvolle“ Weg zur Einführung und Umsetzung eines umfassenden Identitätsmanagementkonzeptes trotzdem nicht erspart bleiben.

Aktueller Stand SaxIS / DFN-AAI in Sachsen

Technische Umsetzung

Einrichtung	Shibboleth-Instanz	Einbindung in Bildungsportal	Bemerkung
TU Chemnitz	√	√	
TU Dresden	√	√	
Uni Leipzig	√	-	Datenabgleich fehlt noch
TU Freiberg	√	√	
HTWK Leipzig	√	√	
HTW Dresden	√	√	
HS Mittweida	√	√	
WHS Zwickau	√	√	
HS Zittau/Görlitz IHI Zittau	√	√	
HfM Dresden	√	√	nur Testbetrieb mit BPS
HfMT Leipzig	√	√	nur Testbetrieb mit BPS
HfGB Leipzig	√	√	nur Testbetrieb mit BPS
HfBK Dresden	√	√	nur Testbetrieb mit BPS

Aktueller Stand SaxIS / DFN-AAI in Sachsen

Nutzung durch Service-Provider

1. schrittweise Einbindung der dezentralen Shibboleth-Instanzen in die Lernplattform des Bildungsportal Sachsen
   - Anbindung an das Bildungsportal Sachsen (https://bildungsportal.sachsen.de/)
   - läuft stabil im Produktionsberieb
2. Aufbau einer Lösung für die Anbindung der Digitalen Bibliothek Sachsen an die Shibboleth-Föderation
   - Anpassung von Sisis Elektra als SP ist prototypisch erfolgt
   - Authentifizierung über Libero-Radius-Anbindung der TUD
   - eine Shibboleth-Schnittstelle für Libero ist angekündigt
3. Hochschulinterne Nutzung
   - Vorreiter ist hier die TU Chemnitz

Perspektive SaxIS: DFN-AAI

Erarbeitung und Bewertung von Varianten für die Sicherung des langfristigen Betriebes der SaxIS-Dienste

Organisatorisch

- einzig sinnvolle weil nachhaltige Lösung: Inanspruchnahme der DFN-Föderation
- alle beteiligten Hochschulen sollten dieser beitreten
- Ansprechpartner bleibt bis dahin das Bildungsportal Sachsen

Technisch

- Status Quo: Weiterbetrieb des technischen Betriebs der zentralen SaxIS-Server durch die TU Chemnitz bis zur Ablösung durch die entsprechenden DFN-Strukturen
- Zentraler Radius-Proxy: Überführung in DFN Roaming
- Metadaten/WAYF-Server: Betrieb durch DFN-Föderation

Aktuelle Aufgaben in Sachsen

Aufgaben für die Hochschulen und ihre RZ

- Sicherung des stabilen Betriebs des IdP
- **Kommunikation und Unterzeichnung der Dienstvereinbarung DFN-AAI durch die jeweilige Universität/Hochschule**
- Vertragsentwürfe sind den RZ-Leitern am 24.4.07 übergeben worden
- Technischer Kontakt mit der DFN-AAI (Zertifikat, Austausch von Konfigurationsdateien)
- **Sicherung der Konsistenz und Authentizität der Daten in Zusammenarbeit mit der jeweiligen Hochschulverwaltung**
- Sicherung des technischen Datenschutzes in der Einrichtung

Vielen Dank für Ihre Aufmerksamkeit!

DFN Kanzlertagung
Potsdam, 20. Juni 2007