



# **Der Einsatz von Shibboleth als Single-SignOn-System in wissenschaftlichen Bibliotheken**

**Das Projekt Authentifizierung, Autorisierung und  
Rechteverwaltung (AAR)**

**Ato Ruppert, UB Freiburg**

**27.3.2007, D-Grid Security Workshop, Göttingen**



# Gliederung

- Das Projekt AAR
- Motivation, Szenario
- Fragen und Lösungsbeispiel
- Aufgaben der Föderation DFN-AAI
- Ausblick



# Das Projekt AAR

- Partner: **UB Freiburg** und **UB Regensburg** (bis 31.3.2007)
- finanziert durch das **BMBF** ([PT-NMB+F](#))
- eingebettet in **vascoda** (<http://www.vascoda.de/>)
- Laufzeit zunächst **3 Jahre** bis Ende 2007:
  - 2 Jahre Entwicklungs- und Testphase mit der Regionalen Datenbank-Information Baden-Württemberg (**ReDI**) und **vascoda als Pilotanwendungen**
  - 1 Jahr Unterstützung von Einrichtungen und Anbietern bei der Einführung des Systems
- **Verlängerung** bis Mitte 2008 zum Aufbau der nationalen Infrastruktur (mit DFN-Verein)





# Was macht das AAR-Projekt?

- **AAR** baut eine **Infrastruktur** zur Authentifizierung, Autorisierung und Rechteverwaltung
- **AAR** implementiert ein **Single SignOn System**, mit dem verschiedene Ressourcen mit einem einzigen Login genutzt werden können („Reference Linking“)
- **AAR** baut auf **Shibboleth** (Internet2-Projekt) auf
- **AAR** basiert auf einem **föderativen Ansatz**:  
Die **Einrichtung** verwaltet und authentifiziert ihre Mitglieder und der **Anbieter kontrolliert den Zugang** zu seinen Ressourcen
- Gemeinsam mit dem **DFN-Verein** wird eine deutschlandweite **Föderation** als nachhaltiger Dienst des DFN aufgebaut (**DFN-AAI**).



# Situation im Bibliotheksbereich

- Viele unterschiedliche Angebote an elektronischen Diensten (Freiburg: mehr als 34.000)
- Verträge mit vielen unterschiedlichen Diensteanbietern (Freiburg: mehr als 500)
- Authentifizierung i.d.R. über IP-Kontrolle
- Aktualisierung der IP-Listen (fast) nicht mehr möglich
- Organisation der Angebote über Portale
- Beispiele:  

ReDI

## Bestandsabfrage

Uni Freiburg

**Titel:** External and internal...

**Journal:** Radiation and envi...

ISSN: 0301-634X

[Kompletter Datensatz](#)

## Elektronische Zeitschriftenbibliothek

Der Volltext der Zeitschrift ist

Readme freigeschaltet.

[Radiation and environmental biophysics](#)

## Kataloge:

[Freiburger Online-Katalog](#)

[SWB Verbundkatalog](#)

[Karlsruher Virtueller Katalog \(KVK\)](#)

[Zeitschriftendatenbank \(ZDB\)](#)

# Elektronische Zeitschriftenbibliothek

## Universitätsbibliothek Freiburg

[Über uns](#) | [Einstellungen](#) | [Zeitschriftensuche](#) | [Kontakt](#)



Der in vascode ausgewählte Artikel ist über ein Online-Abonnement Ihrer Bibliothek freigeschaltet.

Bitte beachten Sie die [Zugangsbedingungen](#)

External and internal irradiation of a Rural Bryansk (Russia) population from 1990 to 2000, followin....  
Erschienen in: [Radiation and environmental biophysics](#)

Der Artikel ist in Ihrer Bibliothek über verschiedene Anbieter zugreifbar.

### Der Weg zum Volltext:

Eine vollständige Quellenangabe zum Artikel liegt uns leider nicht vor.

Bitte kehren Sie zu vascode zurück. Dort erhalten Sie (teilweise kostenpflichtige) Informationen über den Artikel.

**zur Zeitschriftenhomepage \***  
(via SpringerLink)

Hilfe bei Zugangsproblemen

**zur Zeitschriftenhomepage**  
(via SpringerLink)

\* **Die Volltexte dieser Online-Zeitschrift sind Nationallizenzen.** Leider konnten wir nicht eindeutig feststellen, ob der obige Aufsatz in diesen Zeitraum fällt. Bitte versuchen Sie Ihr Glück.

ReDI

### Bestandsabfrage

Uni Freiburg

**Titel:** External and internal...

**Journal:** Radiation and Envi...

**ISSN:** 0301-634X

[Kompletter Datensatz](#)

### Elektronische Zeitschriftenbibliothek

Der Volltext der Zeitschrift ist

Readme freigeschaltet.

[Radiation and Environmental Biophysics](#)

### Kataloge:

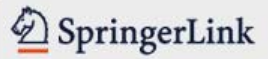
[Freiburger Online-Katalog](#)

[SWB Verbundkatalog](#)

[Karlsruher Virtueller Katalog \(KVK\)](#)

[Zeitschriftendatenbank \(ZDB\)](#)

### Bestellung:



Athens Authentication Point

#### Welcome!

To use the personalized features of this site, please log in or register.

If you have forgotten your username or password, we can help.

#### My SpringerLink

Marked Items

Alerts

Order History

#### Saved Items

All

Favorites

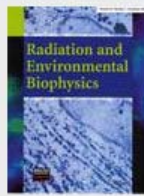
Content Types Subjects

English

Back to: Journal \ Journal Issue \ Journal Issue

Previous Item Next Item

### Journal Article



### External and internal irradiation of a Rural Bryansk (Russia) population from 1990 to 2000, following high deposition of radioactive caesium from the chernobyl accident

Journal	Radiation and Environmental Biophysics
Publisher	Springer Berlin / Heidelberg
ISSN	0301-634X (Print) 1432-2099 (Online)
Subject	Biomedical and Life Sciences, Earth and Environmental Science and Physics and Astronomy
Issue	Volume 44, Number 2 / October, 2005
Category	Original Paper
DOI	10.1007/s00411-005-0007-2
Pages	97-106
Online Date	Wednesday, September 21, 2005

- Add to marked items
- Add to saved items
- Recommend this article

C. Thornberg<sup>1</sup> ✉, R. Vesananen<sup>2</sup>, E. Wallström<sup>3</sup>, I. Zvonova<sup>4</sup>, T. Jesko<sup>4</sup>, M. Balonov<sup>4</sup> and S. Mattsson<sup>1</sup> ✉

- (1) Department of Radiation Physics, Lund University, Malmö University Hospital, 205 02 Malmö, Sweden
- (2) Department of Radiation Physics, Göteborg University, Sahlgrenska University Hospital, Göteborg, Sweden
- (3) Department of Radiology, NÄL, Trollhättan, Sweden
- (4) Institute of Radiation Hygiene, St Petersburg, Russia

**Received:** 25 February 2005 **Accepted:** 30 June 2005 **Published online:** 21 September 2005

**Abstract** In 1990, a joint Nordic-Russian project was initiated in order to make independent estimations of the effective dose to selected groups of inhabitants in a highly

#### Find more options

...

- Within this issue
- Within this journal
- Within all content

#### Export this article

Export this article as RIS|Text

#### Text

#### PDF

The size of this document is 324 kilobytes. Although it may be a lengthier download, this is the most authoritative online format.

Open: Entire document

**ReDI**

**Bestandsabfrage**

**Titel:** External and internal...

**Journal:** Radiation and Envi...

**ISSN:** 0301-634X

[Kompletter Datensatz](#)

**Elektronische Zeitschriftenbibliothek**

Der Volltext der Zeitschrift ist  freigeschaltet.

[Radiation and Environmental Biophysics](#)

**Kataloge:**

[Freiburger Online-Katalog](#)

[SWB Verbundkatalog](#)

[Karlsruher Virtueller Katalog \(KVK\)](#)

[Zeitschriftendatenbank \(ZDB\)](#)

**SpringerLink**

Athens Authentication Point

**Welcome!**

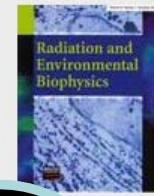
To use the personalized features of this site, please [log in](#) or [register](#).

If you have forgotten your username or password, you can [help](#).

Content Types Subjects

English

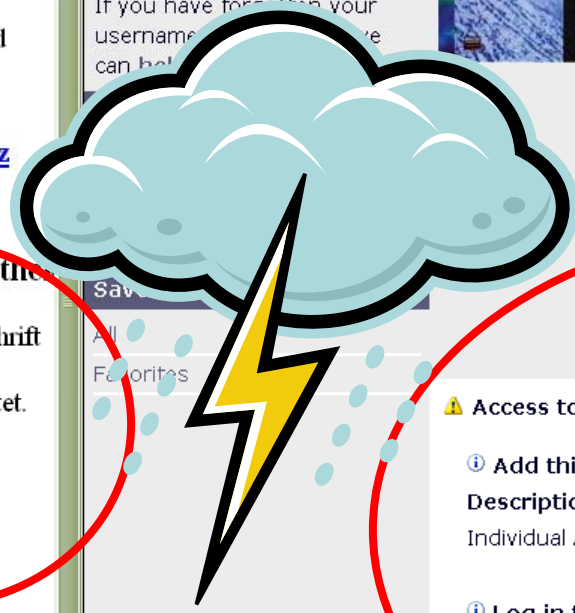
**Resource Secured**



**External and internal irradiation of a Rural Bryansk (Russia) population from 1990 to 2000, following high deposition of radioactive caesium from the chernobyl accident**

Journal	Radiation and Environmental Biophysics
Publisher	Springer Berlin / Heidelberg
ISSN	0301-634X (Print) 1432-2099 (Online)
Subject	Biomedical and Life Sciences, Earth and Environmental Science and Physics and Astronomy
Issue	Volume 44, Number 2 / October, 2005
Category	Original Paper
DOI	10.1007/s00411-005-0007-2
Pages	97-106
Online Date	Wednesday, September 21, 2005

Add to marked items



**⚠ Access to this resource is secured.**

**ℹ Add this item to your shopping cart for purchase later.**

Description	Price
Individual Article (Electronic Only)	\$30.00 <input type="button" value="Add"/>

**ℹ Log in to verify access**

Username

Password

Find   more options

(Within all content)

Frequently asked questions | General information on journals and books | Send us your feedback

© Springer. Part of Springer Science+Business Media  
Privacy, Disclaimer, Terms and Conditions, © Copyright Information





# Probleme der IP-Authentifizierung für Bibliotheksbenutzer

- **Lösungsmöglichkeiten des Ortsbindungsproblems:**
  - **VPN:** Komplexe technische Lösung, Probleme bei der Softwareinstallation und Konfiguration sowie mit Firewalls
  - **Proxies:** spezielle Browserkonfiguration nötig, Probleme mit Nutzern in privaten Netzwerken, die andere Proxies für den Internetzugang benötigen
  - **Rewriting Proxies** (HAN, EZProxy):
    - Benötigen spezielle Links um die Inhalte zu adressieren (in Katalogen, LinkResolvern, Portalen, ...)
    - Erschweren oft die Integration von Inhalten
    - Skalieren nicht besonders gut. Denken Sie an spezielle Links zu 10000 und mehr elektronischen Zeitschriften
    - Erhebliche Probleme beim ReferenceLinking
- **Unsicherheiten:**
  - Fälschbare IP-Adressen
  - Offene Proxies

# Beispiel: Nationallizenzen: Die Situation heute – institutionelle Nutzer

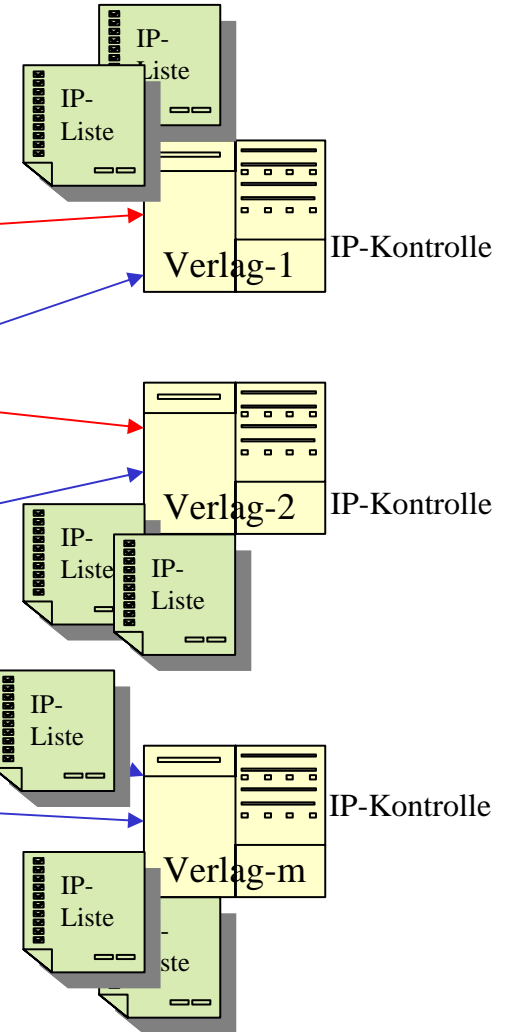
Zugangsvermittlung mit  
proprietären Verfahren



Einrichtung-1



Einrichtung-2



IP-Kontrolle



# Was wollen wir mit Shibboleth erreichen?

## Nutzer

- Der Zugriff auf lizenzierte Inhalte soll **unabhängig vom gewählten Arbeitsplatz und dem Zugriffsweg** möglich sein.
- Alle lizenzierten Inhalte sollten nach nur einmaliger Anmeldung zur Verfügung stehen (**Single SignOn**).

## Einrichtungen (etwa Hochschulen)

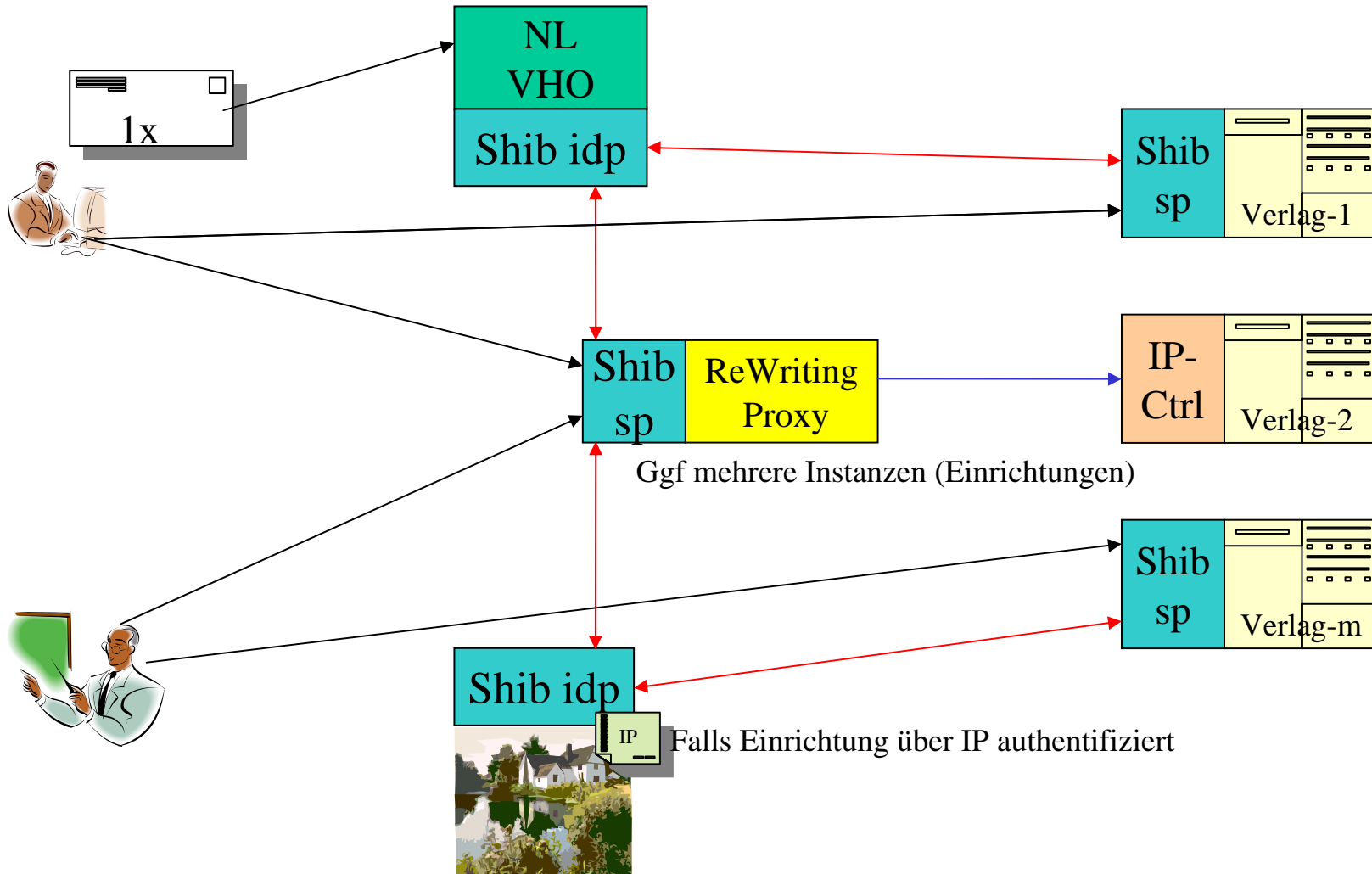
- Die Einrichtung soll ein **beliebiges Authentifizierungssystem** wählen dürfen.

## Anbieter

- Die lizenzpflichtigen **Inhalte** der Anbieter sollen vor unberechtigten Zugriff **geschützt** werden.



# Nationallizenzen ...und das Ziel mit Shibboleth





# Die Föderation DFN-AAI

- **Wo ist das Problem?**
  - Anbieter muss dem Anwender **vertrauen**.
  - Es geht um **Geld**.
  - „**Vertrauen**“ heißt im Geschäftsleben: „**Vertrag**“.
  - Es müssen **belastbare vertragliche Regelungen** getroffen werden.
- **DFN-AAI** ist ein Dienst des DFN-Vereins für Wissenschaftseinrichtungen und (auch für kommerzielle) Anbieter von (Informations)-Ressourcen. (<https://www.aai.dfn.de/>)
- **DFN-AAI** schafft das für notwendige **Vertrauensverhältnis** und einen **organisatorischen, technischen Rahmen** für den Austausch von Nutzerinformationen zwischen vielen Anwendern und vielen Anbietern.

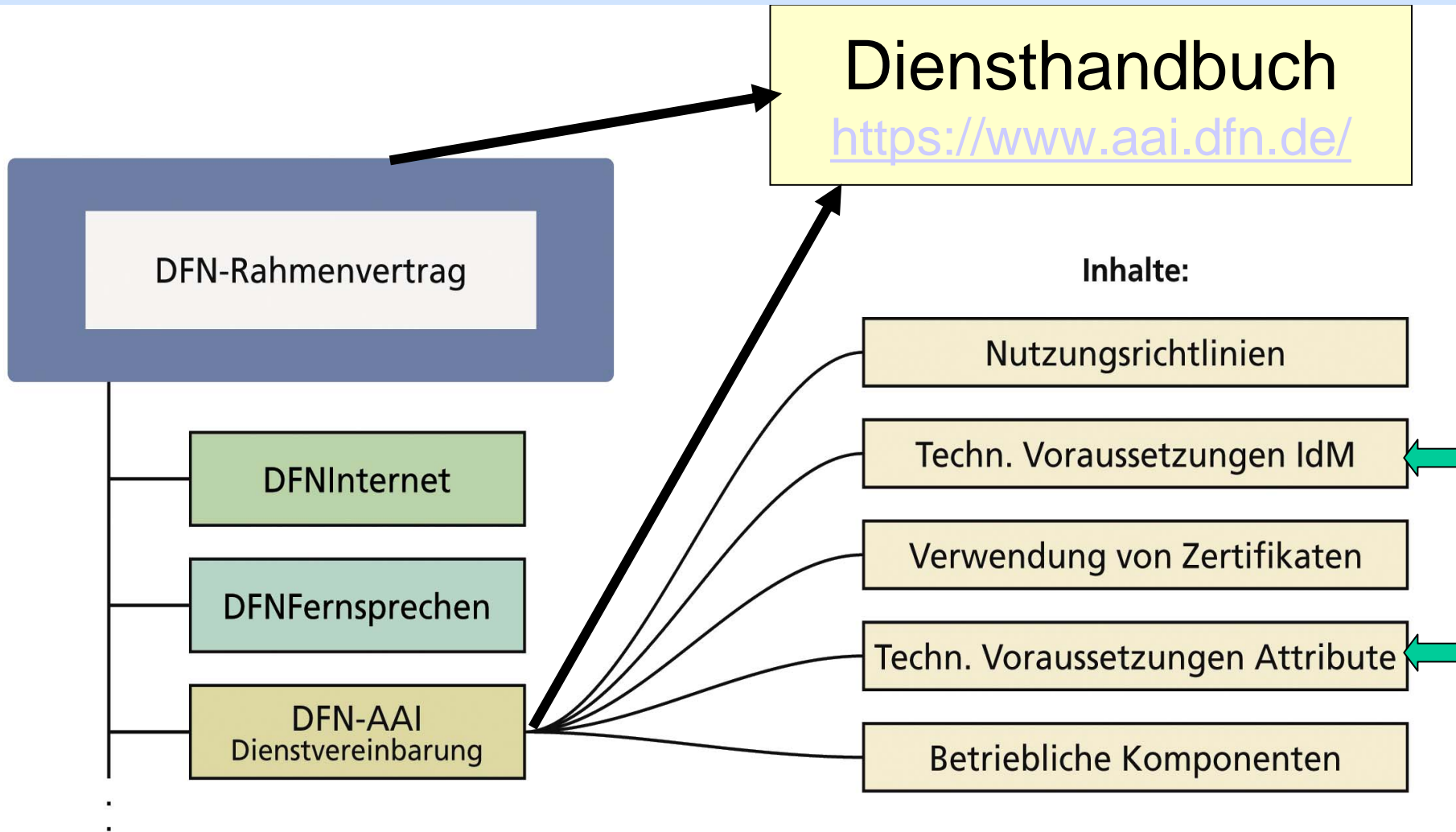


# Aufgaben der DFN-AAI

- Vorgabe von Richtlinien (Policy)
- Vertragsgestaltung und -abschluss
- Public Relations & internationale Vertretung
- zentrale betriebliche Aufgaben
  - Metadatenverwaltung
  - WAYF-Server (Discovery-Service)
  - Testsystem
  - Web-Portal
  - Schulung, Beratung
- Die DFN-AAI steht allen Shibboleth-Anwendern (und darüber hinaus) zur Verfügung!



# Vertragsgestaltung / -abschluss





# Attribute

- **Personen erhalten elektronische Identität**
  - **Attribute** beschreiben die Rolle der Person
- **Attribute** bilden die Grundlage für die **Autorisierung und Zugriffskontrolle** in Shibboleth:
  - Identity-Provider stellen mit Attributen die notwendigen Informationen über ihre Benutzer zur Verfügung.
  - Service-Provider werten die Attribute anhand ihrer Regeln aus und gestatten oder verweigern je nach Ergebnis den Zugriff.
- Hierfür sind **Absprachen zwischen Identity- und Service-Providern** notwendig, die durch Verwendung eines einheitlichen Schemas vereinfacht werden!
- Voraussetzung sind verlässliche Benutzerdaten, also ein funktionierendes lokales **Identity-Management!**





# Anforderungen an IdM

- Qualitätsanforderungen
  - Verlässlichkeit: Sicherheitsstufen, Missbrauchsverhinderung
  - Aktualität: zeitnahe Änderung
  - Nachvollziehbarkeit: Dokumentation, Logging
  - Ausfallsicherheit: Back-up-Systeme
- Einklang mit rechtlichen Vorgaben
  - Datenschutzgesetz



# Einsatzmöglichkeiten von SSO

- Zugang zu geschützten (auch und gerade kommerziellen) elektronischen Informationsangeboten:
  - E-Zeitschriften, Datenbanken, E-Bücher, ...
  - Portale (z.B. *vascoda*, ReDI)
  - DFG-Nationallizenzen
  - Repositories (z.B. MyCoRe)
- e-Learning
- e-Science
- Verwaltungssysteme
- Grid-Computing
- [Beispiele Freiburg](#)



# Wer macht im Bibliotheksbereich schon mit?


## Index of Shibboleth-Enabled Applications and Services (Quelle: internet2)

## in Deutschland:

- ArtSTOR
- Blackboard
- Bodington.org
- **CSA**
- Darwin Streaming Server
- Digitalbrain PLC
- eAcademy
- **EBSCO Publishing**
- **Elsevier Science Direct**
- ExLibris-SFX
- Fedora
- Higher Markets
- Horde
- Hupnet
- ILIAS
- **JSTOR**
- Moodle
- Napster
- NSDL
- **OCLC**
- OLAT
- **Ovid Technologies Inc.**
- **Proquest Information and Learning**
- Serials Solutions
- SYMPA
- **ThomsonGale/ISI**
- TWiki
- Useful Utilities-EZproxy
- Web Assign
- WebCT
- **GENIOS/GBI**
- **IZ Soz (Infoconnex)**
- **DIPF**
- **vascoda**
- **ReDI**
- **SaxIS**
- **GBV/NL**
- **FIZ-Technik**
- **FIZ-Karlsruhe(?)**
- **Springer (2007)**



# Zum Abschluss: Stand und Ausblick zum Projekt

- Alle Komponenten von Shibboleth sind in einer **Testumgebung** verfügbar ( bei [AAR](#) und [DFN-AAI](#))
- Portal **ReDI** (Ba-Wü) wurde auf Shibboleth umgestellt (mit einer „internen“ Föderation, etwa 60 Identity Provider und zwei Anbietern: CSA, GBI)
- Die Betriebssoftware IPS von  **vascoda** ist auf Shibboleth umgestellt (Einsatz in Freiburg)
- Für den Bereich der Nationallizenzen wird z.Zt. eine VHO als Grundlage zur Einführung von Shibboleth aufgebaut (vom GBV in Göttingen).
- Und...



# Ausblick auf Shibboleth 2.0

## Shibboleth 2.0 bietet

- viele neue Funktionen auf Basis der erweiterten Möglichkeiten von SAML 2.0 und
- viele Verbesserungen, basierend auf den Erfahrungen mit Shibboleth 1.x
- Vor allem ein Single Log Out (SLO)
- Kompatibilität mit Shibboleth 1.3
  
- daher: Bitte warten Sie mit eigenen Arbeiten nicht auf Shibboleth 2.0





**Vielen Dank für Ihre Aufmerksamkeit!**

AAR ist ein Projekt der  
UB Freiburg und UB Regensburg.  
Gefördert vom BMBF (PT-NMB+F )  
**AAR kooperiert mit dem DFN-Verein**

[aar.vascoda.de](http://aar.vascoda.de)

[info@aar.vascoda.de](mailto:info@aar.vascoda.de)

[ruppert@ub.uni-freiburg.de](mailto:ruppert@ub.uni-freiburg.de)