Freie Universität Berlin

– Nur für den internen Gebrauch bestimmt –

Freie Universität Berlin

FUDIS Antrag

Antrag auf Übermittlung von Daten und Teilnahme an der Authentifizierung durch den zentralen Dienst FUDIS (FU Directory and Identity Service) der ZEDAT

Fassung: Februar 2009
Version 1.3

Inhalt

1 Antragsstatus 3

2 Angaben zum IT-Verfahren 4

2.1 IT-Verfahren 4
2.2 Verfahrensverantwortlicher 4
2.3 Spezieller Ansprechpartner für FUDIS*) 5
2.4 Spezieller Ansprechpartner für FUDIS (1. Vertretung) 5
2.5 Spezieller Ansprechpartner für FUDIS (2. Vertretung) 5

3 Produktauswahl 6

4 Abschließende Regelungen 11

5 Anhang FUDIS-Produkte 13

5.1 Allgemeine Aufgaben 13
5.1.1 Datenübermittlung 13
5.1.2 Authentifizierung 13
5.1.3 Autorisierung 13
5.2 Produkte 13
5.2.1 Produkte zur reinen Datenübermittlung 13
5.2.2 Produkte zur reinen Authentifizierung 14
5.2.3 Produkte zur reinen Autorisierung 14
5.2.4 Kombination von Authentifizierung und Datenübermittlung 14
5.2.5 Kombination von Autorisierung und Datenübermittlung 15
5.2.6 Kombination von Authentifizierung, Autorisierung und Datenübermittlung 15

1 Antragsstatus

	übergeben am	Stellungnahme	Stellungnahmen vorgelegt am
ZEDAT FUDIS		❑ Teilnahme vertretbar / keine Bedenken ❑ Teilnahme vertretbar / geringe Mängel ❑ Teilnahme nicht vertretbar / erhebliche Mängel	
Audit-Stelle		❑ Teilnahme vertretbar / keine Bedenken ❑ Teilnahme vertretbar / geringe Mängel ❑ Teilnahme nicht vertretbar / erhebliche Mängel	
Datenschutz		❑ Teilnahme vertretbar / keine Bedenken ❑ Teilnahme vertretbar / geringe Mängel ❑ Teilnahme nicht vertretbar / erhebliche Mängel	
Personal-vertretung		❑ Teilnahme vertretbar / keine Bedenken ❑ Teilnahme vertretbar / geringe Mängel ❑ Teilnahme nicht vertretbar / erhebliche Mängel	
Verantwortlicher IT-Leiter		❑ Teilnahme wird erlaubt ❑ Teilnahme wird nicht erlaubt	

2 Angaben zum IT-Verfahren

Bei den nachfolgend anzugebenden Anschriften sind immer die Dienstadressen aufzuführen.

2.1 IT-Verfahren

Bezeichnung:	
Signatur[1]:	
Schutzbedarf:	

Das IT-Verfahren wurde bei eAS gemeldet am:	
Es wurde gemäß den in der IT-Grundsatzdienstvereinbarung festgelegten Regeln dokumentiert.	
Es wurde nicht dokumentiert. Eine Kurzbeschreibung gemäß den in der Dokumentation zum Verfahrensablauf definierten Anforderungen liegt dem Antrag bei.	

2.2 Verfahrensverantwortlicher

Name, Vorname:	
Straße:	
PLZ:	
Ort:	
Telefon:	
Fax:	
E-Mail:	

[1] Die Signatur wird vom zentralen Dokumentenmanagement vorgegeben. Wenn die Signatur noch nicht bekannt ist, kann das Feld frei gelassen werden.

2.3 Spezieller Ansprechpartner für FUDIS*)

Name, Vorname:	
Straße:	
PLZ:	
Ort:	
Telefon:	
Fax:	
E-Mail:	

2.4 Spezieller Ansprechpartner für FUDIS (1. Vertretung)

Name, Vorname:	
Straße:	
PLZ:	
Ort:	
Telefon:	
Fax:	
E-Mail:	

2.5 Spezieller Ansprechpartner für FUDIS (2. Vertretung)

Name, Vorname:	
Straße:	
PLZ:	
Ort:	
Telefon:	
Fax:	
E-Mail:	

*) Sofern ein Ansprechpartner, der für alle Fragen die im Zusammenhang mit dem Anschluss an den FUDIS-Dienst stehen, vorgesehen ist, sollten die Kontaktdaten dieser Person hier eingetragen werden.

3 Produktauswahl

Produkte zur reinen Datenübermittlung

- LDAP-Data
- LDAP-Data-Anonymous → *individuelles Produkt*
- Flatfile-Data → *individuelles Produkt*

Produkte zur reinen Authentifizierung

- LDAP-AuthN
- Shib-AuthN

Produkte zur reinen Autorisierung

- LDAP-AuthZ → *individuelles Produkt*

Kombination von Authentifizierung und Datenübermittlung

- LDAP-AuthN&Data

Kombination von Autorisierung und Datenübermittlung

- LDAP-AuthZ&Data → *individuelles Produkt*

Kombination von Authentifizierung, Autorisierung und Datenübermittlung

- Shib-AuthN&AuthZ&Data

Für Produkte mit Datenübermittlung:

Falls der Verwendungszweck der benötigten Daten in der IT-Verfahrensdokumentation ausführlich dargelegt wurde, reicht im folgenden Kasten ein Verweis auf die Stelle in der Verfahrensdokumentation aus. Sofern keine detaillierte Beschreibung vorliegt, muss der Verwendungszweck der Daten im Folgenden ausführlich beschrieben werden.

Verwendungszweck der benötigten Daten:

Der oben angegebene Verwendungszweck darf nicht von dem in der IT-Verfahrensdokumentation abweichen.

❍ Die Zustimmung des/der Dateneigner(s) zur Nutzung der oben benannten Daten liegt unterschrieben vor und ist diesem Antrag beigefügt.

Wählen Sie die benötigte Personengruppe aus. Bitte beschränken Sie Ihre Auswahl auf den absolut notwendigen Umfang.

❍ **Mitarbeiter**

Genaue Spezifikation: *(z.B. Mitarbeiter des FB Physik)*	
Begründung:	

❍ **Studierende**

Genaue Spezifikation: *(z.B. Studierende mit Hauptfach Biologie)*	
Begründung:	

❍ **Lehrende**

Genaue Spezifikation: *(z.B. Angestellte der Freien Universität)*	
Begründung:	

❍ **Sonstige**

Genaue Spezifikation: *(z.B.alle Alumni)*	
Begründung:	

Definition der Personengruppen:

Mitarbeiter sind alle Personen, die in einem Beschäftigungsverhältnis mit der Freien Universität Berlin stehen. Hinzu kommen auch korporative Mitglieder der Freien Universität.

Studierende sind alle Personen, die an der Freien Universität Berlin immatrikuliert sind, an einer anderen Hochschule im In- oder Ausland immatrikuliert sind und an einem Kooperationsstudiengang mit der Freien Universität Berlin teilnehmen, Erasmusstudierende sowie Gaststudierende.

Lehrende sind alle Personen, die Lehre an der Freien Universität ausüben. Dies können Mitarbeiter, aber auch andere Personen sein, die einen Lehrauftrag erhalten.

Sonstige Dies sind alle Personen, die nicht zur den Gruppen Mitarbeiter, Studierende und Lehrende gehören. Beispiel: Alumni.

Benötigte Attribute der Personendaten:

- **Benutzername**

Benutzername:	
Begründung:	

- **Vollständiger Name**
  (Bestehend aus Vor- und Nachname, einschließlich Namensvor- und -zusätzen, wie z.B. von, van, Freiherr, Baronin sowie Titeln, wie z.B. Dr. Prof.)

Vollständ. Name:	
Begründung:	

- **Geburtsdatum**

Geburtsdatum:	
Begründung:	

- **Geburtsname**

Geburtsname:	
Begründung:	

- **Geburtsort**

Geburtsort:	
Begründung:	

- **Fachbereich** *(z.B. Fachbereich Physik)*

Fachbereich:	
Begründung:	

- **Status des Personeneintrags** *(aktiv oder gelöscht)*

Status:	
Begründung:	

- **Status des Benutzerkontos** *(aktiv, gesperrt oder gelöscht)*

Status:	
Begründung:	

-

:	
Begründung:	

-

:	
Begründung:	

-

:	
Begründung:	

-

:	
Begründung:	

4 Abschließende Regelungen

Die im Folgenden formulierten Regeln sind für alle Personen verbindlich, die für den Betrieb der an FUDIS teilnehmenden Systeme verantwortlich sind (Verfahrensverantwortlicher, Administrator, Applikationsbetreuer usw.).

- Der Benutzername kann auch für sich allein ein Datum mit Vertraulichkeit sein. Sofern die Veröffentlichung des Benutzernamens weder notwendig noch erwünscht ist, sind von den zuständigen Administratoren Maßnahmen zur Gewährleistung der Vertraulichkeit zu treffen. Auch wenn die Geheimhaltung des Benutzernamens systembedingt oft nicht möglich ist, darf keine vorsätzliche Veröffentlichung durch die Administratoren erfolgen. Bei Systemen, in denen intern die Veröffentlichung des Benutzernamens erwünscht bzw. notwendig ist, muss sichergestellt werden, dass die Veröffentlichung auf den Kreis der Zugriffs- bzw. Informationsberechtigten beschränkt bleibt.
- Die Nutzung der Benutzernamen für die Versendung von Massen-E-Mails ist nicht gestattet, insofern dies nicht durch den Verwendungszweck im Antrag ausreichend begründet wird. Vor dem Versand von Massen-E-Mails sind die technischen Rahmenbedingungen mit der ZEDAT abzuklären.
- Es muss sichergestellt werden, dass eingegebene Passworte ohne jede Zwischenspeicherung direkt an die Authentifizierungsserver weitergeleitet werden, um ein vermeidbares Risiko des Passwort-Ausspähens zu verhindern.
- Die Übermittlung sämtlicher Daten, insbesondere der Passwörter, haben stets über verschlüsselte Verbindungen zu erfolgen.
- Der Verfahrensverantwortliche verpflichtet sich, die teilnehmenden IT-Systeme einem Sicherheits-Audit zu unterziehen. Das Audit wird von der dafür zuständigen Stelle in der Freien Universität durchgeführt. Das positive Ergebnis des Audits ist eine notwendige aber nicht hinreichende Bedingung zur Teilnahme an FUDIS.
- Der Verfahrensverantwortliche stellt sicher, dass für die teilnehmenden Systeme ein sicherer IT-Betrieb gemäß den Anforderungen und Maßnahmen der IT-Sicherheitsrichtlinie gewährleistet ist. Jeder Sicherheitsvorfall, der potentiell die Sicherheit der von FUDIS übermittelten Daten oder der an FUDIS angeschlossenen Systeme beeinträchtigen kann, muss zum Zweck der Schadensbegrenzung sofort der ZEDAT gemeldet werden.
- Die Anzahl der Personen mit administrativem Zugriff ist möglichst gering zu halten.

Neben den oben genannten Regeln gelten insbesondere das Berliner Datenschutzgesetz (BlnDSG), das Berliner Hochschulgesetz (BerlHG), die IT-Sicherheitsrichtlinie der Freien Universität Berlin sowie die FUDIS-Benutzungsordnung in der jeweiligen aktuellen Fassung.

Der Verfahrensverantwortliche verpflichtet sich, die benötigten Daten ausschließlich für den oben genannten Zweck zu verwenden. Wesentliche Änderungen an den angeschlossenen Systemen oder deren administrative Verwaltung sowie Änderungen des Verwendungs-

zwecks der Daten sind sofort eAS mitzuteilen und unterliegen grundsätzlich dann einer erneuten Prüfung, wenn Datenschutz- oder Sicherheitsbelange berührt werden.

Der Verfahrensverantwortliche hat alle Personen in dem Antrag aufgeführt, die über administrative Rechte verfügen. Er stellt sicher, dass diese Personen die Regeln des Datenschutzes und der Sicherheitsrichtlinien innerhalb der Hochschule kennen und beachten. Personal von Fremdfirmen, die im Auftrag der Hochschule administrativen Zugang zu Systemen erhalten, werden über die Regeln des Datenschutzes und der Sicherheitsrichtlinien der Freien Universität Berlin belehrt. Die erfolgte Belehrung ist vom Belehrten durch Unterschrift dem Verfahrensverantwortlichen zu bestätigen. Dieser Nachweis über die Belehrung ist dem Antrag beizufügen.

Der Wechsel des Verfahrensverantwortlichen muss sofort schriftlich eAS mitgeteilt werden. Dies gilt auch für die anderen Rolleninhaber.

Sollte sich die im Antrag aufgeführte Stelle nicht an die vorstehenden Regeln halten, so kann die ZEDAT sofort die Übermittlung der Daten sowie den Zugang zur zentralen Authentifizierung einstellen.

Im Schadensfall sind von der verursachenden (Kosten-)Stelle bzw. Organisationseinheit alle Folgekosten zu begleichen. Als Beispiel sei hier der Postversand neuer Passwörter aufgeführt.

Eine Kopie des Antrags dient zugleich als Datenschutzmeldung und wird den behördlichen Datenschutzbeauftragten der Freien Universität Berlin übermittelt.

Berlin, den

_____

Unterschrift Verfahrensverantwortlicher

5 Anhang FUDIS-Produkte

5.1 Allgemeine Aufgaben

FUDIS (Freie Universität Directory and Identity Service) bietet Produkte an, die die folgenden drei Aufgaben erfüllen können:

5.1.1 Datenübermittlung

Bei der Datenübermittlung werden in der Regel personenbezogene Daten von einem System zu einem anderen System transportiert. Ob eine permanente Speicherung der Daten im Zielsystem erfolgt, hängt von dem jeweiligen Anwendungsfall ab.

5.1.2 Authentifizierung

Unter Authentifizierung wird der Vorgang verstanden, bei dem eine Person oder eine zu ihr gehörende Identität anhand bestimmter Authentifizierungsmerkmale (engl. credentials) überprüft wird. In der Regel werden ein Benutzername und ein Passwort überprüft.

5.1.3 Autorisierung

Wird einer Person der Zugriff auf eine Ressource gewährt, so spricht man von Autorisierung. Autorisierung umfasst dabei die Zuweisung und die Überprüfung von Zugriffsrechten.

5.2 Produkte

5.2.1 Produkte zur reinen Datenübermittlung

- **LDAP-Data**

  Das Produkt LDAP-Data stellt über einen LDAP-Server personenbezogene Daten bereit. Die Daten können nach einer erfolgreichen Authentifizierung eines Funktionsbenutzers abgerufen werden.
  (Wird aktuell verwendet für: ZEDAT Portal, ZEDAT Passwortserver, Institut für Informatik Benutzerverwaltung, CeDiS Blackboard, CeDiS CMS)

- **LDAP-Data-Anonymous → *individuelles Produkt***

  Ausgewählte Dienste müssen in sehr kurzer Zeit viele Daten abrufen können. Für diesen Zweck wird ein LDAP-Server angeboten, der unverschlüsselte Verbindungen zulässt. Aufgrund der IP-Adresse des Servers kann auf den Dienst ohne weitere Authentifizierung zugegriffen werden.
  (Wird aktuell verwendet für: ZEDAT E-Mail-System, ZEDAT Print-Service-Server)

- **Flatfile-Data → *individuelles Produkt***

  FUDIS exportiert zeitgesteuert Daten aus der zentralen Datenbank, um diese dann in einer strukturierten Textdatei zu einem Kunden zu übertragen.
  (Wird aktuell verwendet für: ZEDAT Print-Service, ZEDAT Telefonanlage, Campus Management Dozentenverwaltung, Immatrikulationsamt SOS, Universitätsbibliothek Aleph, FB Wirtschaftswissenschaften PC-Pool)

5.2.2 Produkte zur reinen Authentifizierung

- **LDAP-AuthN**

  Das Produkt LDAP-AuthN dient der reinen Authentifizierung mit einem Benutzernamen und Passwort gegen einen LDAP-Server. Nach erfolgreicher Authentifizierung werden keine weiteren Daten zurückgegeben. Bei diesem Dienst werden die Benutzernamen und Passwort bei dem jeweiligen Dienstnutzer eingegeben und vom Dienstnutzer an einen LDAP-Server übergeben.
  (Wird aktuell verwendet für: CeDiS Blackboard, Institut für Informatik RT)

- **Shib-AuthN**

  Bei dem Produkt Shib-AuthN ist eine reine Authentifizierung gegen einen Shibboleth Identity Provider möglich. Der Identity Provider ist eingebunden in die Authentifizierungs- und Autorisierungs-Infrastruktur des Deutschen Forschungsnetzes e.V. (DFN-AAI). Bei diesem Dienst erfolgt die Eingabe eines Benutzernamens und Passwortes immer auf einer zentralen Webseite, die von FUDIS betrieben wird. Der Dienstnutzer erhält lediglich ein Ticket, mit dem eine erfolgreiche Authentifizierung für einen Nutzer bestätigt wird.
  (Wird zurzeit NICHT verwendet)

5.2.3 Produkte zur reinen Autorisierung

- **LDAP-AuthZ → *individuelles Produkt***

  Über einen LDAP-Server werden bei AuthZ für Systeme Rollen und Gruppen zur Autorisierung angeboten. Die Verbindung zum LDAP-Server ist verschlüsselt.
  (Wird zurzeit NICHT verwendet)

5.2.4 Kombination von Authentifizierung und Datenübermittlung

- **LDAP-AuthN&Data**

  Dieses Produkt entspricht im Wesentlichen dem Produkt LDAP-AuthN. Jedoch werden nach erfolgreicher Authentifizierung Daten zu dem jeweiligen Benutzer zurückgegeben. Ein spezielles Profil für die Rückgabe der Daten wird bei Linux/Unix-Systemen verwendet, die das so genannte PAM-Modul einsetzen.
  (Wird aktuell verwendet für: ZEDAT CMS-Server)

5.2.5 Kombination von Autorisierung und Datenübermittlung

- **LDAP-AuthZ&Data → *individuelles Produkt***

  Bei diesem Produkt wird ein LDAP-Server bereitgestellt, über den personenbezogene Daten und Rolleninformationen für eine Autorisierung abgerufen werden können.
  (Wird aktuell verwendet für: Campus Management)

5.2.6 Kombination von Authentifizierung, Autorisierung und Datenübermittlung

- **Shib-AuthN&AuthZ&Data**

  Dieses Produkt entspricht dem Produkt Shib-AuthN. Jedoch werden nach erfolgreicher Authentifizierung personenbezogene Daten sowie Rolleninformationen zu dem jeweiligen Benutzer zurückgegeben. Die Benutzer können darüber selbst entscheiden, welche Daten übermittelt werden sollen.
  (Wird zurzeit NICHT verwendet)

Die wichtigsten Informationen zu den Produkten werden in der nachfolgenden Tabelle dargestellt.

Produkt	Datenübermittlung	Authentifizierung	Autorisierung	Benutzer gibt seine Daten für die Übermittlung selber frei	Permanente Speicherung von Daten im Ziel-system möglich	Permanente Speicherung und Ausspähen von Benutzernamen und Passwörtern beim Nutzer des Produktes möglich	Verschlüsselte Verbindung	Bewertung der Sicherheitsanforderung an das Produkt nutzende System
LDAP-Data	●	-[1)]	-	-	●	-	●	hoch
LDAP-Data-Anonymous	●	-	-	-	●	-	-	sehr hoch
Flatfile-Data	●	-[1)]	-	-	●	-	●	hoch
LDAP-AuthN	-	●	-	-	-	●	●	sehr hoch
Shib-AuthN	-	●	-	-	-	-	●	hoch
LDAP-AuthZ	-	-[1)]	●	-	●	-	●	nor-mal
LDAP-AuthN&Data	●	●	-	-	●	●	●	sehr hoch
LDAP-AuthZ&Data	●	-[1)]	●	-	●	-	●	hoch
Shib-AuthN&AuthZ&Data	●	●	●	●	●	-	●	hoch

[1)] Authentifizierung erfolgt ausschließlich für einen Funktionsbenutzer.