– Nur für den internen Gebrauch bestimmt –

Freie Universität Berlin

FUDIS-Shibboleth-Antrag

Antrag auf Nutzung des Produktes *FUDIS-Shibboleth* durch den zentralen Dienst FUDIS (FU Directory and Identity Service) der ZEDAT

Fassung: Februar 2009
Version 1.1

Inhalt

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 Attributauswahl

Nach einer erfolgreichen Authentifizierung können Attribute übermittelt werden. In jedem Fall werden die Benutzerkontoattribute uid, accountId, eduPersonPrincipalName übertragen. Zusätzlich können noch die nachfolgenden Attribute übertragen werden. Bitte kreuzen Sie die benötigten Attribute an. Im Anhang finden Sie eine Beschreibung zu den Attributen.

- cn
- displayName
- mail
- scopedPersonIdentifier
- eduPersonAffiliation
- eduPersonPrimaryAffiliation
- eduPersonScopedAffiliation

Verwendungszweck:

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 (employee)**

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

❍ **Studierende (student)**

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

❍ **Lehrende (faculty)**

Genaue Spezifikation: *(z.B. Lehrende des FB Geowissenschaften)*	
Begründung:	

❍ **Alumni (alum)**

Genaue Spezifikation:	
Begründung:	

❍ **Sonstige (affiliate)**

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.

Alumni sind die Ehemaligen der Hochschule.

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

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 genannten Regelungen für den Benutzernamen gelten auch für sämtliche anderen Attribute, die von FUDIS an die teilnehmenden Systeme übertragen werden.
- 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. (Bei dem Produkt FUDIS-Shibboleth erfolgt die Eingabe des Passwortes direkt an dem Authentifizierungsserver.)
- 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 Verwendungszwecks 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

I. Anhang – Beschreibung der FUDIS-Shibboleth-Attribute

Attribute zum Benutzerkonto

Attributname	uid
Werte	einer
Beschreibung	Name des Benutzerkontos ohne Angabe des Realms
Erlaubte Werte/Syntax	Länge: 3-8 Zeichen Erlaubte Zeichen: a-z und 0-9 Das erste Zeichen darf keine Zahl sein
Beispiel	hmuster

Attributname	accountId
Werte	mehrere
Beschreibung	Eindeutige IDs für den Account. Die ID bleibt nach der Umbennung der uid erhalten.
Erlaubte Werte/Syntax	{<typ>}<id>@zedat.fu-berlin.de <typ> := UNIX-UIDNUMBER | WINDOWS-SSID <id> := beliebiger String
Beispiel	{UNIX-UIDNUMBER}10838@zedat.fu-berlin.de

Attributname	eduPersonPrincipalName
Werte	einer
Beschreibung	Name des Benutzerkontos mit Angabe des Realms
Erlaubte Werte/Syntax	<uid>@zedat.fu-berlin.de
Beispiel	hmuster@zedat.fu-berlin.de

Attribute zur Person

Attributname	cn
Werte	einer
Beschreibung	Vollständiger Name ohne Titel zu einer Person, der innerhalb einer Organisationseinheit eindeutig ist.
Erlaubte Werte/Syntax	Directory String nach RFC 4517
Beispiel	Max von Mustermann Klaus Müller (2)

Attributname	displayName
Werte	einer
Beschreibung	Name zu einer Person, der bei einer Anwendung angezeigt werden soll. Dieser kann aus verschiedenen Gründen vom tatsächlichen Namen abweichen
Erlaubte Werte/Syntax	Directory String nach RFC 4517
Beispiel	M. Mustermann (für Melanie Mustermann) Bono (Künstlername für Paul Hewson)

Attributname	mail
Werte	mehrere
Beschreibung	E-Mail-Adresse
Erlaubte Werte/Syntax	siehe RFC822
Beispiel	m.melanie@fu-berlin.de hmuster@zedat.fu-berlin.de

Attributname	scopedPersonIdentifier
Werte	mehrere
Beschreibung	Schlüssel, unter dem die Person in den jeweiligen System geführt wird.
Erlaubte Werte/Syntax	<key>@<system>[.obsolete] <key> := beliebiger String <system> := beliebiger String Für Schlüssel, die durch andere Schlüssel in dem jeweiligen System ersetzt wurden, und daher obsolet sind, wird .obsolete angehängt.
Beispiel	010838@staff.fu-berlin.de (für Personalnr) 1234567@student.fu-berlin.de (für Matrikelnummer)

Rolleninformationen zum Benutzerkonto/zur Person bezogen auf die Organistaion

Attributname	eduPersonAffiliation
Werte	mehrere
Beschreibung	Grobe Organisationsrolle innerhalb der Hochschule
Erlaubte Werte/Syntax	faculty: Mitglied des Lehrkörpers student: Studierende staff: Mitarbeiter, die nicht zum Lehrkörper gehören employee: faculty, staff und sonstige Angestellte alum: Alumni member: faculty, staff, student affiliate: Partner der Organisation wie Gasthörer, Gastdozenten, Dienst-leister
Beispiel	staff

Attributname	eduPersonPrimaryAffiliation
Werte	einer
Beschreibung	Primäre Grobe Organisationsrolle innerhalb der Hochschule
Erlaubte Werte/Syntax	ein Wert aus eduPersonAffiliation
Beispiel	staff

Attributname	eduPersonScopedAffiliation
Werte	mehrere
Beschreibung	Grobe Organisationsrolle mit Angabe der Organisation
Erlaubte Werte/Syntax	<eduPersonAffiliation>@zedat.fu-berlin.de
Beispiel	staff@zedat.fu-berlin.de