Peter Gietz, DAASI International GmbH
Jochen Lienhard, Universität Freiburg
Siegfried Makedanz, Alfred Wegener Institut
Bernd Oberknapp, Universität Freiburg
Hans Pfeiffenberger, Alfred Wegener Institut
Jürgen Rauschenbach, DFN-Verein
Ato Ruppert, Universität Freiburg
Renate Schroeder, DFN-Verein

DFN-AAI
Technische und organisatorische Voraussetzungen
- Attribute -

1 Einleitung

Das Projekt DFN-AAI hat das Ziel, eine gemeinsame Authentifizierungs- und Autorisierungsinfrastruktur für Anbieter von Ressourcen (Anbieter) und Nutzer dieser Ressourcen (Anwender) zur Verfügung zu stellen. Als Software wird die im Internet2 entwickelte Open Source Software Shibboleth eingesetzt. Shibboleth hat sich als auf der Verwendung von Attributen basierte Authentifizierungs- und Autorisierungssoftware bestens bewährt und wird in einer wachsenden Zahl von Forschungsnetzen eingesetzt.

Ziel dieses Papiers ist es, die Standard-Attribute zu beschreiben, die zum Zweck der Autorisierung zwischen Anwender und Anbieter ausgetauscht werden können. Des Weiteren werden Attribute beschrieben, die eine anwendungsunterstützende Bedeutung haben und die, eine institutionelle Bestätigung vorausgesetzt, ebenfalls durch Shibboleth übermittelt werden können. Grundlage für die Beschreibung der Attribute ist die von Internet2 entwickelte Objektklasse *eduPerson*, die zusammen mit der Standardobjektklasse *inetOrgPerson* verwendet wird.

Nicht alle hier beschriebenen Attribute werden immer benötigt, es gilt das Prinzip der Datensparsamkeit. Shibboleth bietet die Möglichkeit, einen Autorisierungsvorgang ohne Weitergabe personenbezogener Daten durchzuführen. Durch die Implementierung eines Attributfreigabeverfahrens, zum Beispiel mit ShARPE/Autograph, können Nutzer in Eigenverantwortung die Attribute auswählen, die zu ihrer Person freigegeben werden sollen.

2 Übersicht über obligatorische und empfohlene Attribute

Die hier vorliegende Tabelle beschreibt die zum Austausch zwischen Anwender und Anbieter vorgesehenen Attribute. Vorhandene Attribute in den Identity Management Systemen oder vertrauenswürdigen Nutzerverwaltungen der Anwender müssen eindeutig auf die hier beschriebenen Attribute abgebildet werden können. Dazu sei auf das Werkzeug ShARPE (siehe Anhang) verwiesen, das in die Version 2 von Shibboleth integriert sein wird.

Die Liste der hier beschriebenen Attribute kann nicht von vornherein als vollständig betrachtet werden, weitere Anwendungen und Anforderungen der Anbieter können eine Erweiterung notwendig machen.

Ohne die als **obligatorisch** eingestuften Attribute können viele Anwendungen nicht oder nur sehr eingeschränkt genutzt werden, entsprechend sollte jedes Identity Management System diese Attribute (durch eine Abbildung der vorhandenen Attribute) liefern können. Die als **empfohlen** eingestuften Attribute werden für einzelne Anwendungen bzw. bestimmte Funktionalitäten in den Anwendungen benötigt. Kann ein Identity Management System diese Attribute nicht liefern, können die Anwendungen nur eingeschränkt genutzt

werden. Beispiele für die Verwendung der Attribute sind in Kapitel 3 in der Beschreibung der Attribute unter Verwendungszweck aufgeführt.

Nr	Attribut	LDAP-Name des Attributs	aus Objektklasse				Klassifizierung	
			person	organizationalPerson	inetOrgPerson	eduPerson	*obligatorisch*	*empfohlen*
1	Name	cn (common name)	x					x
2	Nachname	sn (surname)	x				x	
3	Vorname	GivenName			x			x
4	Angezeigter Name	DisplayName			x			x
5	User ID	Uid			x			x
6	Zertifikat	userCertificate			x			x
7	Postadresse (Dienst)	postalAddress		x				x
8	Telefonnummer (Dienst)	telephoneNumber	x					x
9	E-Mailadresse (Dienst)	Mail			x		x	
10	Organisationsname	organisationName (o)		x				x
11	Organisationseinheit (OU) z.B. Abteilung	organisationalUnitName (ou)		x				x
12	DN der Organisation	eduPersonOrgDN				x		x
13	DN der Organisations-einheit	eduPersonOrgUnitDN				x		x
14	DN der wichtigsten OU	eduPersonPrimary-OrgUnitDN				x		x
15	Name in Form von Netz-ID	eduPersonPrincipal-Name				x	x	
16	Art d. Zugehörigrigkeit zur eigenen Organisation	eduPersonAffiliation				x		x
17	Hauptsächliche Art der Zugehörigkeit	eduPersonPrimary Affiliation				x		x
18	Art d. Zugehörigkeit plus Domain Namen	eduPersonScopedAffiliation				x	x	
19	Berechtigung	eduPersonEntitlement				x	x	
20	Eindeutiges Pseudonym f. Anbieter	eduPersonTargetedID				x	x	
21	Spitzname	eduPersonNickname						x

3 Definition der Attribute

3.0 Meta-Informationen und Schreibweisen für Attribute

Beschreibung	Kurze Beschreibung des Attributs
aus Objektklasse	Standard-LDAP-Objektklasse, in der das Attribut ursprünglich definiert wurde
Semantik	Bedeutung des Attributs
LDAP Syntax	LDAP-Syntax des Attributs (RFC 2252). Die Syntax wird in Stringform angegeben (nicht als OID). Eine Zahl in runden Klammer spezifiziert eine Maximallänge.
Anzahl der Werte	ein: Das Attribut darf nur einen Wert haben mehrere: Das Attribut kann beliebig viele Werte haben
erlaubte Werte	Kontrolliertes Vokabular: Liste der erlaubten Werte für das Attribut
Klassifizierung	obligatorisch/empfohlen (siehe Kapitel 2)
Beschreibung	Zusätzliche Informationen
Beispiel	Beispiel im LDIF Format (LDAP Data Interchange Format, RFC 2849)
Verwendungszweck	Beispiele für die (geplante) Verwendung der Attribute

Eine detaillierte Spezifikation der Attribute ist in der Beschreibung der zugehörigen Objektklasse zu finden (s Anhang).

3.1 Name (commonName, cn)

Beschreibung	Name eines Objekts, in der Objektklasse "person" Name einer natürlichen Person
aus Objektklasse	person
Semantik	X.500-Attribut in Übereinstimmung mit RFC 2256, das den vollen Namen einer Person beschreibt, in der Regel als „<Vorname>blank <Nachname>“
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Wird häufig als Attribut verwendet, das dem gesamten Eintrag den Namen gibt (namensgebendes Attribut). Da der Personenname oft nicht eindeutig ist, eignen sich andere Attribute besser zur Namensgebung, z.B. uid oder eduPersonPrincipleName.
Beispiel	Beispiel1: cn: Karl-Peter Gietz cn: Peter Gietz
Verwendungszweck	Nicht verfälschbare Anzeige des Namens, z.B. wissenschaftliche Journale mit öffentlicher Diskussion / nichtanonymer Peer-Review

3.2 Nachname (surName, sn)

Beschreibung	Nachname oder Familienname

aus Objektklasse	person
Semantik	X.500-Attribut in Übereinstimmung mit RFC 2256, das den Nachnamen einer Person beschreibt
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	obligatorisch
Bemerkungen	Für die DFN-AAI sollte der Anwender nur einen Wert bereit stellen und zwar den Nachnamen, der für die offizielle Kommunikation mit der Person genutzt wird.
Beispiel	Beispiel1: sn: Rösler-Laß Beispiel2: sn: Rauschenbach
Verwendungszweck	E-Learning: Zuordnung von Personen zu Lerngruppen im E-Learningsystem, zum Beispiel durch Tutoren. Wird üblicherweise in Kombination mit givenName verwendet.

3.3 Vorname (givenName)

Beschreibung	Vorname einer Person
aus Objektklasse	inetOrgPerson
Semantik	Nach RFC 2256: Das Attribut Vorname ist für den Teil des Namens gedacht, der nicht Nachname oder mittlerer Name ist
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Für die DFN-AAI sollte der Anwender nur einen Wert bereitstellen.
Beispiel	Beispiel1: givenName: Barbara Beispiel2: givenName: Jan
Verwendungszweck	E-Learning: Zuordnung von Personen zu Lerngruppen im E-Learningsystem, zum Beispiel durch Tutoren. Wird üblicherweise in Kombination mit sn (surName) verwendet.

3.4 Angezeigter Name (displayName)

Beschreibung	Angezeigter Name einer Person
aus Objektklasse	inetOrgPerson
Semantik	Nach RFC 2798 wird dieses Attribut genutzt, um nur einen vollen Namen darzustellen. Das Attribut diplayName wird benötigt, da commonName ein multi-value-Attribut ist.
LDAP Syntax	DirectoryString
Anzahl der Werte	ein
erlaubte Werte	entfällt

Klassifizierung	empfohlen
Bemerkungen	Aus dem multi-value Attribut commonName wird ein Wert für den displayName gewählt. In der Regel der Name einer Person, unter dem sie allgemein bekannt ist.
Beispiel	Beispiel1: displayName: Peter Gietz Beispiel2: displayName: Ato Ruppert
Verwendungszweck	Da das Attribut einwertig ist und den üblichen Namen einer Person enthält, eignet es sich für anwendungsunterstützende Zwecke besser als cn (s. a. commonName)

3.5 User ID (uid)

Beschreibung	Login-ID
aus Objektklasse	inetOrgPerson
Semantik	Spezifiziert einen Login Namen für ein System
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Muss innerhalb der Organisation eindeutig sein. Eignet sich dann auch als namensgebendes Attribut
Beispiel	Beispiel1: uid: Abc234 Beispiel2: uid: hmeier
Verwendungszweck	E-Learning: Personalisierung der Anwendungen.

3.6 Nutzer-Zertifikat (userCertificate)

Beschreibung	Zertifikat eines Nutzers
aus Objektklasse	inetOrgPerson
Semantik	Enthält ein X.509-Zertifikat, das einen öffentlichen Schlüssel mit Identitätsdaten in Zusammenhang bringt. Findet Verwendung im Rahmen einer PKI
LDAP Syntax	Certificate
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Muss beim Transport als binary gekennzeichnet werden.
Beispiel	Beispiel1: userCertificate; binary: MIIF8DCCCBNigAwIBAg.....
Verwendungszweck	Speicherung von Zertifikaten

3.7 Postadresse (postalAddress)

Beschreibung	dienstliche Postadresse
aus Objektklasse	organizationalPerson
Semantik	Das Attribut postalAddress enthält die notwendigen Informationen für die Auslieferung einer Postsendung. Es darf aus maximal 6 durch "$" voneinander getrennten Zeilen à 30 Zeichen bestehen.
LDAP Syntax	PostalAddress
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	
Beispiel	Beispiel1: postalAddress: DFN-Verein$Stresemannstr.78$ 10963 Berlin
Verwendungszweck	Postalische Lieferadresse, die ein Anbieter zur Auslieferung einer Ware benötigt

3.8 Telefonnummer (telephoneNumber)

Beschreibung	Dienstliche Telefonnummer
aus Objektklasse	person
Semantik	Dienstliche Telefonnummer einer Person. Die Telefonnummer muss dem internationalen Format entsprechen: Landesvorwahl + Ortsvorwahl ohne Null + Teilnehmernummer
LDAP Syntax	TelephoneNumber
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	
Beispiel	Beispiel1: telephoneNumber: +49 30 88429923
Verwendungszweck	

3.9 E-Mailadresse (mail)

Beschreibung	Dienstliche E-Mailadresse
aus Objektklasse	inetOrgPerson
Semantik	RFC 1274: Das Attribut mail spezifiziert eine elektronische Mailbox nach dem Standard RFC822
LDAP Syntax	IA5String (256)
Anzahl der Werte	mehrere
erlaubte Werte	entfällt

Klassifizierung	obligatorisch
Bemerkungen	Zur Erfüllung bestimmter Dienste (z.B. Notification Service) wird der Anbieter die Weitergabe dieses Attributs verlangen.
Beispiel	Beispiel1: mail: kaehler@dfn.de Beispiel2: mail: Hans.Maier@awi.de
Verwendungszweck	E-Learning: (automatische) Benachrichtigungen, zum Beispiel in Foren, Ordnern oder durch Tutoren. Bibliotheken: (automatisches) Verschicken von Informationen, zum Beispiel neue Ergebnisse für eine in der Anwendung hinterlegte Recherche (Alert-Dienst). Alle Anwendungen: Kann als eindeutige ID zur Personalisierung verwendet werden.

3.10 Organisationsname (organizationName, o)

Beschreibung	Name der Organisation bzw. Institution, der eine Person angehört
aus Objektklasse	inetOrgPerson
Semantik	Abbildung des Organisationsnamen im Personeneintrag
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	
Beispiel	Beispiel1: o: Christian-Abrecht Universität Kiel o: Universität Kiel
Verwendungszweck	Zusammen mit dem commonName oder displayName zu dem unter 3.1 geschilderten Zweck der De-Anonymisierung

3.11 Organisationseinheitsname (organizationalUnit, ou)

Beschreibung	Name einer Organisationseinheit
aus Objektklasse	organizationalPerson
Semantik	Name einer Organisationseinheit (Abteilung, Fachbereich) im Personeneintrag
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	
Beispiel	Beispiel1: ou: Fachbereich Mathematik
Verwendungszweck	E-Learning: Beschränkung des Zugangs zu Kursen aus urheberrechtlichen oder administrativen Gründen.

3.12 DN der Organisation (eduPersonOrgDN)

Beschreibung	Der DN (distinguished name) des Directoryeintrags, der die Organisation der Person repräsentiert
aus Objektklasse	eduPerson
Semantik	Der Directoryeintrag, auf den der DN weist, sollte ein Eintrag der in X.521 definierten Objektklasse "organization" sein.
LDAP Syntax	DN
Anzahl der Werte	ein
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Mit Hilfe des DN kann eine effiziente Suche durchgeführt werden, um mehr über die Organisation herauszufinden, der die Person angehört. commonName, surname und eduPersonOrgDN sind die drei Attribute, die zu den "core"-Attributen von eduPerson gehören.
Beispiel	Beispiel1: eduPersonOrgDn: o=Universität Würzburg, c=de Beispiel2: eduPersonOrgDn: dc=uni-tuebingen, dc= de
Verwendungszweck	

3.13 DN der Organisationseinheit (eduPersonOrgUnitDN)

Beschreibung	Der DN (distinguished name) des Directoryeintrags, der die Organisationseinheit der Person repräsentiert
aus Objektklasse	eduPerson
Semantik	Der Directoryeintrag, auf den der DN weist, sollte ein Eintrag der in X.521 definierten Objektklasse "organizationalUnit" sein.
LDAP Syntax	DN
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Mit Hilfe des DN kann eine effiziente Suche durchgeführt werden, um mehr über die Organisationseinheit herauszufinden, der die Person angehört. Zugehörigkeit zu einer OU kann für die Autorisierung ausgewertet werden.
Beispiel	Beispiel1: eduPersonOrgUnitDN: ou= FB Informatik, o=Universität Würzburg, c=de eduPersonOrgUnitDN: ou=FB Mathematik, o=Universität Würzburg, c=de
Verwendungszweck	Autorisierung auf der Ebene von Organisationseinheiten

3.14 DN der wichtigsten OU (eduPersonPrimaryOrgUnitDN)

Beschreibung	Der DN (distinguished name) des Directoryeintrags, der die wichtigste Organisationseinheit der Person repräsentiert
aus Objektklasse	eduPerson

Semantik	Der Directoryeintrag, auf den der DN weist, sollte ein Eintrag der in X.521 definierten Objektklasse "organizationalUnit" sein.
LDAP Syntax	DN
Anzahl der Werte	ein
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Wird eingesetzt zur Beschreibung des DN der wichtigsten Organisationseinheit, wenn eine Person mehreren Organisationseinheiten angehört. Weiteres s. 3.15
Beispiel	Beispiel1: eduPersonPrimaryOrgUnitDN: ou= FB Informatik, o=Universität Würzburg, c=de
Verwendungszweck	Eingeschränkte Autorisierung auf der Ebene von Organisationseinheiten

3.15 Name in Form einer Netz-ID (eduPersonPrincipalName)

Beschreibung	Netz-ID einer Person
aus Objektklasse	eduPerson
Semantik	Der Wert besteht aus einem linken und einem rechten Teil getennt durch @, z.B. user@uni-hannover.de, wobei der rechte Teil die (in der Regel im DNS registrierte) Domain und der linke Teil eine innerhalb der Domain eindeutige ID beschreibt.
LDAP Syntax	DirectoryString
Anzahl der Werte	ein
erlaubte Werte	entfällt
Klassifizierung	obligatorisch
Bemerkungen	Im Gegensatz zum Attribut mail (3.10) *muss* es sich nicht um eine funktionierende und dieser Person zugeordnete Mail-Adresse handeln. Auch wird man eher hier als an anderer Stelle eine persistente ID realisieren können – vorbehaltlich des Verkaufs der Domäne.
Beispiel	Beispiel1: eduPersonPrincipalName: ruppert@uni-freiburg.de Beispiel2: eduPersonPrincipalName: Hnsmr123@awi.de
Verwendungszweck	Der eduPersonPrincipalName wird häufig (intern) in Anwendungen verwendet, wenn der Benutzer eindeutig identifiziert werden muss und ein Pseudonym (siehe eduPersonTargetedID) hierfür nicht genügt, zum Beispiel beim schreibenden Zugriff auf Wikis, Foren oder Repositories.

3.16 Art der Zugehörigkeit zur eigenen Organisation (eduPersonAffiliation)

Beschreibung	Art der Zugehörigkeit zur eigenen Organisation
aus Objektklasse	eduPerson
Semantik	Spezifiziert verschiedene Kategorien für die Art der Zugehörigkeit einer Person zur Heimatorganisation

LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	faculty, student, staff, alum, member, affiliate, employee
Klassifizierung	empfohlen
Bemerkungen	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 Attribut bleibt leer, wenn alle Kategorien nicht passen In der eduPerson Spezifikation wird erwähnt, dass die Liste unvollständig ist Das Attribut eduPersonScopedAffiliation sollte diesem vorgezogen werden.
Beispiel	Beispiel1: eduPersonAffiliation: faculty eduPersonAffiliation: student
Verwendungszweck	Das Attribut wird je nach Anwendung mit oder ohne Scope verwendet, Beispiele siehe eduPersonScopedAffiliation. Autorisierung auf der Ebene von Zugehörigkeiten.

3.17 Hauptsächliche Art der Zugehörigkeit (eduPersonPrimaryAffiliation)

Beschreibung	Hauptsächliche Art der Zugehörigkeit
aus Objektklasse	eduPerson
Semantik	Spezifiziert verschiedene Kategorien für die hauptsächliche Art der Zugehörigkeit einer Person zur Heimatorganisation.
LDAP Syntax	DirectoryString
Anzahl der Werte	ein
erlaubte Werte	faculty, student, staff, alum, member, affiliate, employee
Klassifizierung	empfohlen
Bemerkungen	faculty: Mitglied des Lehrkörpers student: Studierende staff: Mitarbeiter, die nicht zum Lehrkörper gehören employee: faculty, employee, staff und sonstige Angestellte alum: Alumni affiliate: Partner der Organisation wie Gasthörer, Gastdozenten Attribut bleibt leer, wenn alle Kategorien nicht passen In der eduPerson Spezifikation wird erwähnt, dass die Liste sicher unvollständig ist
Beispiel	Beispiel1: eduPersonPrimaryAffiliation: faculty
Verwendungszweck	Eingeschränkte Autorisierung auf der Ebene von Zugehörigkeiten.

3.18 Art der Zugehörigkeit plus Domain Namen (eduPersonScopedAffiliation)

Beschreibung	Art der Zugehörigkeit der Person zur eigenen Organisation ergänzt um die zugehörige Domain
aus Objektklasse	eduPerson
Semantik	Der Wert besteht aus einem linken und einem rechten Teil getennt duch @ Der linke Teil spezifiziert verschiedene Kategorien für die Art der Zugehörigkeit einer Person zu einer (Heimat-)Organisation oder genauer einer Organisationseinheit, die der rechte Teil dann spezifiziert (Security Domain).
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	Für den linken Teil: faculty, student, staff, alum, member, affiliate, employee Der rechte Teil spezifiziert die Domain zu der die Beziehung besteht.
Klassifizierung	obligatorisch
Bemerkungen	Für die linke Seite gilt: 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, Dienstleister. Attribut bleibt leer, wenn alle Kategorien nicht passen Die rechte Seite beschreibt die Domain, zu der die Person gehört s. 3.17 eduPersonPrincipleName
Beispiel	Beispiel1: Bsp.1: eduPersonScopedAffiliation: faculty@uni-hannover.de Bsp.2: eduPersonScopedAffiliation: member@geo.uni-bremen.de
Verwendungszweck	E-Learning: Festlegung von Berechtigungen anhand des Status des Benutzers. Bibliotheken: Wird von einigen Anbietern verwendet, um den Zugriff auf lizenzpflichtige Inhalte zu kontrollieren (insbesondere bei älteren Implementierungen, bei neueren Implementierungen wird meistens eduPersonEntitlement verwendet, s. nächster Abschnitt). Einige Anbieter planen, das Attribut zu verwenden, um je nach Benutzergruppe unterschiedliche Funktionalität anzubieten (zum Beispiel bestimmte Funktionen nur für faculty und staff). Ermöglicht eine Einschränkung der Wahrscheinlichkeit leichtfertiger Nutzung teurer Ressourcen. (Z.B.: AWI erlaubt allen Mitgliedern des Fachbereichs Geowissenschaften Zugriff auf sein Tera-Byte-Archiv – und erwartet von seinen Kooperationspartnern in diesem Fachbereich die Korrektur von falschem oder auch nur unzweckmäßigem Verhalten.)

3.19 Berechtigung (eduPersonEntitlement)

Beschreibung	URI (entweder URL oder URN), das Rechte der Person an speziellen Ressourcen anzeigt

aus Objektklasse	eduPerson
Semantik	Berechtigung auf bestimmte Ressourcen zuzugreifen
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	nur URIs
Klassifizierung	obligatorisch
Bemerkungen	Generelles Attribut zur Spezifikation der Berechtigungen einer Person. Die Heimateinrichtung vergibt z.B. in Abhängigkeit eines Vertrages mit einem Anbieter Werte für dieses Attribut an ausgewählte Personen (Studenten oder Mitarbeiter oder eine Auswahl von Mitarbeitern), die sich darüber autorisieren. Die Bedeutung der Attributwerte muss entweder auf Föderationsebene oder föderationsübergreifend festgelegt oder direkt zwischen Anbietern und Anwendern abgesprochen werden!
Beispiel	Beispiel1: eduPersonEntitlement: http://sp.de/aai/resources/bibl12 Beispiel2: eduPersonEntitlement: urn:mace:dir:entitlement:common-lib-terms
Verwendungszweck	Bibliotheken: Wichtigstes Attribut für den Bibliotheksbereich, wird von vielen Anbietern verwendet, um den Zugang zu lizenzpflichtigen Inhalten zu kontrollieren. MACE hat für den Fall einer typischen Campuslizenz, wie sie von den meisten Anbietern angeboten wird, den Attributwert urn:mace:dir:entitlement:common-lib-terms definiert (siehe http://middleware.internet2.edu/urn-mace/urn-mace-dir-entitlement.html). Es ist geplant, für weitere Lizenztypen entsprechende Attributwerte zu definieren. Allgemein: Das Attribut wird in vielen Anwendungen verwendet, um Benutzern spezielle Rechte (zum Beispiel Schreibrechte oder Administrationsrechte) zuzuweisen oder den Zugriff auf die Anwendung auf ausgewählte Benutzer zu beschränken (sofern die Nutzung anonym erfolgen kann, ansonsten wird eher eduPersonPrincipalName verwendet).

3.20 Eindeutiges Pseudonym (eduPersonTargetedID)

Beschreibung	Pseudonym für eine Person
aus Objektklasse	eduPerson
Semantik	Ein eindeutiges dauerhaftes Pseudonym einer Person für einen speziellen Anbieter
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	
Klassifizierung	obligatorisch

Bemerkungen	Der Anbieter erkennt unter dem Pseudonym eine bestimmte Person, ohne dass die Identität der Person preisgegeben wird. Der Wert kann z.B. ein anonymisierter, unumkehrbarer Wert (Hash) aus der ID des IdP, der ID des SP und der ID des Nutzers sein.
Beispiel	Beispiel1: eduPersonTargetedID: e530e2c54a4e490f
Verwendungszweck	Allgemein: Funktionalitäten wie zum Beispiel die Personalisierung einer Anwendung, für die die Anwendung den Benutzer wiedererkennen können muss, für die aber die Identität des Benutzers nicht bekannt sein muss. Bibliotheken: Viele Anbieter planen eine Personalisierung ihrer Angebote auf Basis der eduPersonTargetedID zu implementieren.

3.21 Spitzname (eduPersonNickname)

Beschreibung	Spitzname einer Person
aus Objektklasse	eduPerson
Semantik	Informeller Name oder Spitzname, unter dem die Person bekannt ist
LDAP Syntax	DirectoryString
Anzahl der Werte	mehrere
erlaubte Werte	entfällt
Klassifizierung	empfohlen
Bemerkungen	Attributwert wird von der Person selbst bestimmt
Beispiel	Beispiel1: eduPersonNickname: Gerti
Verwendungszweck	

Anhang:

ShARPE/Autograph	Shibboleth Attribute Release Policy Editor: http://mams.melcoe.mq.edu.au/wiki/display/MAMS/Shibbleth+Attribute+Release+Policy+Editor+(ShARPE)

Objektklassenspezifikation

- eduPerson	EduPerson Object Class Specification (Internet2): http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html
- inetOrgPerson	s. RFC 2798
- organizationalPerson	s. RFC 4519
- person	s. RFC 4519