bwIDM Attributspezifikation

bwIDM Projektteam

31. Juli 2013

Dokument	bwIDM Attributspezifikation
Version	1.0
Letzte Änderung	31.07.2013
Status	FINAL

Inhaltsverzeichnis

1 Einleitung

Eine Aufgabe der bwIDM-Föderation ist es, eine gemeinsame Authentifizierungs- und Authorisierungsinfrastruktur für die Hochschulen und andere wissenschaftliche Einrichtungen, im Geschäftsbereich des Ministeriums für Wissenschaft Forschung und Kunst (MWK), im Land Baden-Württemberg, zur Verfügung zu stellen. Dies dient dazu, dass Endnutzer der einzelnen Einrichtungen standortübergreifende Ressourcen transparent innerhalb ihres lokalen Kontextes nutzen können. Vereinfacht bedeutet dies, dass innerhalb der Föderation ein Nutzer einer Einrichtung auf eine Ressource einer anderen Einrichtung mit seinen lokalen Zugangsdaten zugreifen kann.

Die technische Realisierung basiert auf der, von der Internet2 entwickelten, Authentifizierungs- und Authorisierungssoftware Shibboleth[1], deren Einsatz sich in vielen ähnlich aufgebauten Föderationen bewährt hat.

Ziel dieses Dokumentes ist es, die Standardattribute zu definieren die, zum Zweck der Authorisierung und Anwendungsunterstützung, zwischen der Organisation des Endnutzers (Heimatorganisation) und des Ressourcenanbieters ausgetauscht werden. Als Basis für diese Attributspezifikation dienen die von der Internet2 entwickelte Objektklasse *eduPerson*[2] und die im RFC2798 spezifizierte Objektklasse *inetOrgPerson*[3].

2 Verwendung der Attributspezifikation

2.1 Heimatorganisation

Wie in der Federation Access Policy beschrieben umfasst diese Attributspezifikation den sogenannten Kernsatz an Attributen innerhalb der bwIDM-Föderation. Dies bedeutet, dass jede Heimatorganisation, die Mitglied der Föderation ist, die hier beschrieben Attribute über die ihr angehörigen Endbenutzer liefern können MUSS. Dazu müssen die in den lokalen Identitätsmanagementsystemen vorhandenen Attribute auf die hier beschrieben Attribute abgebildet werden. Die für die jeweiligen Services freizugebenden Attribute können den jeweiligen Service Access Policies der Anbieter entnommen werden.

Zusätzlich zu dem hier spezifiziertem Kernsatz, kann die Übermittlung weiterer Attribute für die Verwendung einzelner Services nötig sein. Die Spezifikation dieser weiteren Attribute obliegt den Service Anbietern und kann der Service Access Policy des jeweiligen Dienstes entnommen werden.

2.2 Service Provider

Die in diesem Dokument beschriebenen Attribute (Kernsatz) können von jeder Heimatorganisation der bwIDM-Föderation bereitgestellt werden. Nicht alle hier veröffentlichten Attribute werden immer benötigt, es gilt das Prinzip der Datensparsamkeit. Aufgabe des Service Providers ist es, die von ihm zur Erbringung

[1] `http://shibboleth.net/`
[2] `http://middleware.internet2.edu/eduperson/`
[3] `http://tools.ietf.org/html/rfc2798`

seiner Dienstleistung benötigten Attribute im Rahmen der Service Access Policy zu veröffentlichen.

Sollte der definierte Kernsatz für die Erbringung des Services nicht ausreichend sein, wird es dem Anbieter freigestellt einen ergänzenden Attributsatz zu definieren. Dabei wird empfohlen sich an dem unter 2.3 vorgestellten Template zu orientieren. Dabei sollte der Anbieter wenn möglich auf die gleichen Objektklassen (eduPerson, inetOrgPerson) zurückgreifen.

2.3 Attributbeispiel

Name	Der Name des Attributs
DFN	ob das Attribut identisch zur DFN Definition ist
Beschreibung	Eine kurze Beschreibung des Attributs
Vokabular	Eine Liste von erlaubten Werten
Verwendung	Verwendung des Attributes (wenn zutreffend)
Referenz	optionale Referenz zu einem Standard auf dem das Attribut basiert
OID	`Object Identifier`
LDAP Syntax	Der LDAP Syntax des Attributes
# an Werten	Einfach- oder Mehrfachwert
Beispiel	`Beispielwert im LDIF Format`

3 Attributdefinitionen

3.1 Principal Name

Name	eduPersonPrincipalName
DFN	identisch
Beschreibung	Ein Identifikator für eine Person mit Scope. Er wird mit "user@scope" repräsentiert, wobei "user" ein namensbasierter Identifikator für eine Person und "scope" die Domain (meist DNS registriert) beschreibt. Jeder Wert von "scope" definiert einen Namensraum, innerhalb dessen der Identifikator eindeutig sein muss.
Vokabular	nicht zutreffend
Verwendung	Der eduPersonPrincipalName wird als weltweit eindeutiger Loginname benutzt. Zudem wird er oft (intern) in Anwendungen verwendet, wenn der Benutzer eindeutig identifiziert werden soll und ein Pseudonym hierfür nicht genügt.
Referenz	eduPerson[4]
OID	`1.3.6.1.4.1.5923.1.1.1.6`
LDAP Syntax	Directory String
# an Werten	einer
Beispiel	`lawrence.tester@uni-konstanz.de`

[4] `http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#eduPersonPrincipalName`

3.1.1 Anmerkungen

Im Gegensatz zum Attribut 'mail' (siehe 3.2) muss es sich nicht um eine funktionierende und dieser Person zugeordnete Mail-Adresse handeln, auch wenn diese vom Syntax gleich ist.

3.2 E-Mail Adresse

Name	mail
DFN	identisch
Beschreibung	Beinhaltet die E-Mail Adresse der Person. Bevorzugte Adresse für das "To:'-Feld einer E-Mail die an diese Person gesendet werden soll.
Vokabular	entfällt
Verwendung	Kontaktierung des Benutzers, eindeutige ID zur Personalisierung
Referenz	inetOrgPerson[5], RFC2821[6]
OID	`0.9.2342.19200300.100.1.3`
LDAP Syntax	IA5 String (256)
# an Werten	mehrere (Empfehlung: einer)
Beispiel	`eva.musterfraz@uni-ulm.de`

3.2.1 Semantik

Der 'mail' (rfc822mailbox) Attributtyp beinhaltet die Internet Mail Adresse in Mailbox [RFC2821] Form.

3.2.2 Anmerkungen

Sollte eine Person mehrere Mail-Adressen besitzen, wird empfohlen nur eine E-Mail Adresse zu übermitteln. Hierbei sollte die E-Mail Adresse verwendet werden, die auch von der Heimatorganisation verwendet wird, um den Benutzer zu erreichen.

[5] `http://tools.ietf.org/html/rfc2798`
[6] `http://www.ietf.org/rfc/rfc2821.txt`

3.3 Vorname

Name	givenName
DFN	identisch
Beschreibung	Der Vorname einer Person
Vokabular	entfällt
Verwendung	Ansprache des Benutzers. Wird üblicherweise in Kombination mit surname verwendet.
Referenz	inetOrgPerson[7], definiert in RFC4519[8], eduPerson[9]
OID	`2.5.4.42`
LDAP Syntax	Directory String
# an Werten	einer (mehrere nach RFC4519, siehe Anmerkungen)
Beispiel	`Eva`

3.3.1 Semantik

Das givenName Attribut beinhaltet nach RFC4519 den Teil des Namens einer Person, der nicht der Nachname ist.

3.3.2 Anmerkungen

Innerhalb der bwIDM Föderation MÜSSEN Heimatorganisationen nur einen einzelnen Wert für dieses Attribut liefern. Es sollte der Vorname geliefert werden, der für die offizielle Kommunikation mit der Person verwendet wird.

3.4 Nachname

Name	surname (sn)
DFN	identisch
Beschreibung	Nachname, Familienname der Person
Vokabular	entfällt
Verwendung	Ansprache des Benutzers. Wird üblicherweise in Kombination mit givenName verwendet.
Referenz	inetOrgPerson[10], RFC4519[11], eduPerson[12]
OID	`2.5.4.4`
LDAP Syntax	Directory String
# an Werten	einer (mehrere nach RFC4519, siehe Anmerkungen)
Beispiel	Musterfrau

3.4.1 Semantik

Dies ist das X.500-Attribut (RFC2256), das den Familiennamen einer Person beinhaltet.

[7] `http://tools.ietf.org/html/rfc2798`
[8] `http://tools.ietf.org/html/rfc4519`
[9] `http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#givenName`
[10] `http://tools.ietf.org/html/rfc2798`
[11] `http://tools.ietf.org/html/rfc4519`
[12] `http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#sn`

3.4.2 Anmerkungen

Innerhalb von bwIDM MÜSSEN Heimatorganisationen nur einen einzelnen Wert für dieses Attribut liefern. Es sollte der Nachname geliefert werden, der für die offizielle Kommunikation mit der Person verwendet wird.

3.5 Zugehörigkeit (Affiliation)

Name	eduPersonScopedAffiliation
DFN	identisch
Beschreibung	Der Wert besteht aus einem linken und einem rechten Teil getrennt durch ein '@' Zeichen. Der linke Teil spezifiziert eine Zugehörigkeit zu einer weitgefassten Kategorie wie z.B. Student, Alumni... Er beinhaltet einen Wert aus dem unten definierten Vokabular. Der rechte Teil definiert die Organisationseinheit innerhalb der die Person der Kategorie zugehört. Diese entspricht den in der EPPN (siehe 3.1) auf der rechten Seite verwendeten Werten.
Vokabular	**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 **library-walk-in** Mitarbeiter, die sich (physikalisch) in der Bibliothek befinden Das Attribut bleibt leer, sollte keine der Kategorien auf die Person zutreffen.
Verwendung	Festlegung von Berechtigungen anhand des Status des Benutzers.
Referenz	eduPerson[13]
OID	`1.3.6.1.4.1.5923.1.1.1.9`
LDAP Syntax	Directory String
# an Werten	mehrere
Beispiel	• `student@kit.edu` • `member@uni-ulm.de`

[13] `http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#eduPersonScopedAffiliation`

3.5.1 Semantik

Ein Wert von "x@y" wird als Zusicherung verstanden, das die Person die Zugehörigkeit "x" zur Organisation (security domain) "y" hat. So ist eine Person mit dem Wert "student@kit.edu" ein Student am KIT.

3.5.2 Anmerkungen

Wird dazu verwendet den Nutzerkreis auf bestimmte Nutzergruppen einzuschränken oder um unterschiedliche Funktionalität je Benutzergruppe anzubieten.

3.6 Berechtigung (Entitlement)

Name	eduPersonEntitlement
DFN	identisch
Beschreibung	URI (entweder URL oder URN), der Berechtigungen der Person für speziellen Ressourcen anzeigt.
Vokabular	nur URIs (URL oder URN)
Verwendung	Das Attribut wird in vielen Anwendungen verwendet, um Benutzern spezielle Rechte zuzuweisen oder den Zugriff auf die Anwendung auf ausgewählte Benutzer zu beschränken.
Referenz	eduPerson[14], RFC4512[15]
OID	`1.3.6.1.4.1.5923.1.1.1.7`
LDAP Syntax	Directory String
# an Werten	mehrere
Beispiel	• `urn:mace:dir:entitlement:common-lib-terms` • `http://bwidm.de/entitlement/bwUniCluster`

3.6.1 Semantik

Berechtigung, auf eine bestimmte Ressource zuzugreifen zu können.

3.6.2 Anmerkungen

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 Heimatorganisationen abgesprochen werden!

[14] `http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#eduPersonEntitlement`
[15] `http://www.ietf.org/rfc/rfc4512.txt`

3.7 uid

Name	uid
DFN	identisch
Beschreibung	Eindeutiger Identifikator einer Person innerhalb einer Organisation.
Vokabular	Alphanummerisch
Verwendung	Wird zusammen mit dem Organisationskürzel zur eindeutigen Identifikation einer Person verwendet sollte der EPPN nicht anwendbar sein.
# an Werten	einer
Beispiel	• `abc234` • `hmeier`

3.7.1 Semantik

Die uid ist innerhalb der Organisation ein eindeutiger Identifier für eine Person.

3.7.2 Anmerkungen

Die uid wird zusammen mit dem Organisationskürzel als eindeutiger Identifier für eine Person innerhalb der Föderation verwendet. Die Kombination aus Organisationskürzel und uid wird immer dann verwendet, wenn die EPPN nicht eingesetzt werden kann, z.B. wenn eine Zeichenbeschränkung vorliegt. Sollte eine Verwendung der EPPN technisch möglich sein, sollte diese vorgezogen werden.

3.8 Organisationskürzel

Name	http://bwidm.de/bwidmOrgId
Beschreibung	Ein eindeutiges zweistelliges Kürzel für die Organisation.
Vokabular	Zweistellig, [a-z], alle vergebenen Kürzel
Verwendung	Wird zur eindeutigen Identifikation der Organisation, als Ersatz für den Domainnamen, verwendet.
# an Werten	einer
Beispiel	• `fr` • `ul`

3.8.1 Semantik

Das Organisationskürzel ist innerhalb der bwIDM-Föderation ein eindeutiger Identifikator für die Organisation der Person.

3.8.2 Anmerkungen

Das Organisationskürzel wird jeder Organisation, die der bwIDM-Föderation beitritt, einmalig zugewiesen. Danach wird sie als statisches Attribut ausgeliefert.

4 Sonstige Attribute

4.1 Persistenter Name Identifier

Name	IdPPersistentNameIdentifier
Beschreibung	Die persistente ID ist ein anonymer, persistenter Identifier für eine Person. Die ID wird beim ersten Zugriff einer Person auf einen Service vom Identity Provider generiert und gespeichert. Bei weiteren Zugriffen der Person auf den Service wird die persistent ID wieder bereitgestellt.
Verwendung	Die persistent ID eignet sich dazu, service-lokale Benutzerkonten selbst dann noch einer Person zuordnen zu können, wenn sich deren eduPersonPrincipalName einmal ändern sollte, z.B. durch Namensänderung, Heirat usw.
Referenz	shibboleth[16], DFN[17]
# an Werten	einer
Beispiel	`https://idp-test.uni-konstanz.de/idp2/shibboleth!` `https://bwidm-sp01.uni-konstanz.de/sp!NH/AJuow/` `mvpQztOrAiDJUGoXew=`

4.1.1 Semantik

Die persistent ID hat die Form eines Triplets mit dem Format <Name für die Quelle des Identifiers>!<Name für den beabsichtigten Empfänger des Identifiers>!<anonymisierter identifier für den Principal>. Sie ist also für die Kombination aus Person-Identity Provider-Service Provider eindeutig.

4.1.2 Anmerkungen

Im Gegensatz zu den anderen in diesem Dokument vorgestellten Attributen wird die persistent ID nicht im lokalen IDM für eine Person vorgehalten, sondern vom shibboleth Identity Provider nach Bedarf generiert. Dieses Attribut stellt somit eine Anforderung an die technische Realisierung des Identity Providers und nicht an die lokale Datenhaltung.

[16] `https://wiki.shibboleth.net/confluence/display/SHIB2/IdPPersistentNameIdentifier`

[17] `https://www.aai.dfn.de/dokumentation/identity-provider/konfiguration/persistenter-name-identifier/`