Name	Datum	Version	Zusammenfassung der Änderungen
Petra Berg	19.06.2019	1	HU-Daten Shibboleth IdP / HU Föderation
Petra Berg	14.02.2020	2	Ergänzungen zu Attributen und SP Checkliste
Petra Berg	19.10.2020	3	IdP Zertifikat RollOver Vorbereitung
Petra Berg	27.11.2020	4	IdP Zertifikat RollOver Abschluss
Petra Berg	14.10.2022	5	Änderungen der Zertifikat Eigenschaften

1 Shibboleth Infrastruktur der HU

An der Humboldt-Universität wird ein Shibboleth IdP betrieben. Dieser ist in folgenden Föderationen registriert:

- DFN AAI (Advanced)
- eduGAIN
- HU intern

Für die Authentifizierung interner Dienste ist die HU interne Föderation implementiert. Die Shibboleth Authentifizierung sollte für alle neuen Web-Dienste der HU genutzt werden.

1.1 HU Föderation

In der HU-Föderation befindet sich der Shibboleth IdP der HU und ServiceProvider HU interner Dienste.

Die Kommunikationsbasis stellen die Metadaten dar, die mit einer Gültigkeit von 4 Wochen 2 mal pro Woche generiert werden. Die Glaubwürdigkeit wird durch die Signatur mit dem IdP Zertifikat hergestellt.

Die Benötigten URLs ab Oktober 2020 sind:

- HU-Metadaten: http://shib-idp.cms.hu-berlin.de/shibboleth/HU-metadata-g2.xml
- IdP Zertifikat: https://shib-idp.cms.hu-berlin.de/shibboleth/shib-idp-g2.pem

1.2 HU Shibboleth Identity Provider

Der IdP der HU besitzt die entityID: „https://shib-idp.cms.hu-berlin.de/idp/shibboleth".

Es wird das Protokoll SAML 2.0 unterstützt.

Grundsätzlich gibt der IdP transiente NameId's auf Authentifizierungsanfragen zurück. Das heißt für jede Session wird ein neuer Identifyer generiert. Eine eventuelle Wiedererkennung des Nutzers muss über Attribute sicher gestellt werden.

NameIDFormat: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Zur eindeutigen Identifizierung und Autorisierung von Nutzern können verschiedene Attribute übertragen werden. Die Attribute werden dem IdP vom HU Identitätsmanagement System – HU-IAM bereit gestellt. Die Attribute, die unterstützt werden folgen den vom DFN empfohlenen Attributen der Objektklassen person, InetOrgPerson, eduPerson und SCHAC. Eine genaue

Auflistung der Attribute und deren Wertebereich befindet sich in Anhang A.

Vor der Übertragung an den anfragenden Dienst werden alle Attribute, mit Ausnahme des Dienst abhängigen Pseudonyms, dem Nutzer zur Zustimmung/Kenntnisnahme präsentiert. Dabei hat der Nutzer die Möglichkeit, Attribute, die in den Metadaten nicht als ‚required' gekennzeichnet sind, von der Übertragung auszuschließen.

1.3 Voraussetzungen für Service Provider der HU internen Föderation

1.3.1 Zertifikat

Jeder Service Provider benutzt Zertifikate für die Kommunikation in zwei verschiedenen Protokollen. Das eine Protokoll betrifft die Web-Kommunikation über HTTPS und das zweite Protokoll ist die SAML Kommunikation. Während für die Web Kommunikation über den Browser nur von einer öffentlichen CA signierte Zertifikate benutzt werden können, kann die Trust-Beziehung für das SAML Zertifikat auch über einen anderen Weg hergestellt werden, daher sind an diesen Stellen auch selbstsignierte Zertifikate möglich, die jedoch keine längere Laufzeit als 39 Monate haben sollten.

Die Validierung eines selbstsignierten Zertifikats kann durch eine mit einem persönlichen Zertifikat signierte EMail an den Shibboleth Administrator (shibadmin@hu-berlin.de) erfolgen.

1.3.2 EntityID

Die EntityID ist eine eindeutige Identifikation des SP und wird meist als URL in der Form http:// + Hostname + App_Name + /shibboleth generiert.

1.3.3 Metadaten

Die Metadaten zum SP müssen neben den Standards wie EntityDescriptor und SPSSODescriptor folgende zusätzlichen Informationen enthalten:

- UI Extensions: DisplayName, Description, Logo (URL), InformationURL
- SingleLogoutService
- AssertionConsumerService (für mindestens ein Binding)
- AttributeConsumingService: Aufzählung der benötigten und optionalen Attribute
- ContactPerson: technisch und administrativ

1.3.4 Attribute

Die vom SP Angeforderten Attribute sollten eine Teilmenge der in Anhang A aufgeführten Attribute sein. Handelt es sich um personenbezogene Daten, muss es eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten geben, die meist in Form eines Sicherheitskonzeptes dokumentiert ist. Für die Einrichtung der Attributfreigabe auf Seite des IdP ist zumindest ein Verweis auf die Rechtmäßigkeit der Datenverarbeitung nötig.

Sollte der Dienst weitere oder andere Daten als die in der Attributliste aufgeführten benötigen, so ist das mit dem Shibboleth-Administrator zu klären.

1.3.5 Checkliste für ServiceProvider der HU Föderation

1. Implementieren eines Shibboleth ServiceProviders

2. Einrichten eines Zertifikats für die Authentifizierung
   (kann dem Server-Zertifikat entsprechen)
3. Definition der geforderten Attribute (siehe Attributliste) aufgeteilt in
   ‚requiered = true‘ - notwendig und
   ‚requiered = false‘ - freiwillig
4. Einbinden der IdP Metadaten (siehe oben)
5. ggf. Einrichten eines WAYF / Discovery Services für weitere Föderationen zur Auswahl der Heimateinrichtung
6. Erzeugen der Metadaten für den SP und an shibadmin@hu-berlin.de schicken.
7. Implementieren der Autorisierung der Nutzer (Zugriffsberechtigungen)
8. Test

2 Anhang A

Attribute	Name	Typ	Schema	#	Wert / Werte
email	urn:oid:0.9.2342.19200300.100.1.3	String	InetOrgPerson	M	Liste von E-Mail Adressen
cn	urn:oid:2.5.4.3	String	person	M	Vollständiger Personenname
gn	urn:oid:2.5.4.42	String	InetOrgPerson	M	Liste der Vornamen
displayName	urn:oid:2.16.840.1.113730.3.1.241	String	InetOrgPerson	S	Anzeigename einer Person
o	urn:oid:2.5.4.10	String	InetOrgPerson	M	Name der Organisation, der die Person angehört
department Number	urn:oid:2.16.840.1.113730.3.1.2	String	InetOrgPerson	S	OKZ der Person
labeledURI	urn:oid:1.3.6.1.4.1.250.1.57	String	InetOrgPerson	M	Liste interner ID's (FIS, UB, ...)
eduPerson Affiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	String	eduPerson	M	Liste der Zugehörigkeiten: member, student, staff, faculty, professor, employee
eduPerson Entitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	String	eduPerson	M	Liste von Berechtigungen (Rollen)
eduPerson PrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Scoped String	eduPerson	S	Nutzername mit Einrichtungsscope (@hu-berlin.de)
eduPerson ScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	Scoped String	eduPerson	M	Liste der Zugehörigkeiten mit Einrichtungsscope
eduPerson TargetedId	urn:oid:0.9.2342.19200300.100.1.1	String	eduPerson	S	Dienstabhängiger eindeutiger Pseudonym des Nutzers
schacHome Organization	urn:oid:1.3.6.1.4.1.25178.1.2.9	String	SCHAC	S	hu-berlin.de
schacHome OrganizationType	urn:oid:1.3.6.1.4.1.25178.1.2.10	String	SCHAC	M	Einrichtungstypen nach SCHAC Schema
schacPersonal UniqueCode	urn:oid:1.3.6.1.4.1.25178.1.2.14	String	SCHAC	M	Persönliche, eindeutige Codes
schacDateOf Birth	urn:oid:1.3.6.1.4.1.25178.1.2.3	String	SCHAC	S	Geburtsdatum (JJJJMMTT)