Name	Date	Version	Summary of changes
Petra Berg	19.06.2019	1	HU-Data Shibboleth IdP / HU Federation
Petra Berg	14.02.2020	2	Supplements to attributes and SP check list
Petra Berg	19.10.2020	3	IdP Certificate roll over preparation
Petra Berg	27.11.2020	4	IdP Certificate roll over completion
Petra Berg	14.10.2022	5	Changes to the certificate properties
Petra Berg	09.11.2022	6	Translation into English

1 Shibboleth Infrastructure of HU

A Shibboleth IdP is operated at Humboldt University. This is registered in the following federations:

- DFN AAI (Advanced)
- eduGAIN
- HU internal

For the authentication of internal services the HU internal federation is implemented. Shibboleth authentication should be used for all new HU web based services.

1.1 HU Federation

The HU federation contains the Shibboleth IdP of the HU and ServiceProvider of HU internal services.

The communication basis is the metadata, which is generated twice a week with a validity of 4 weeks. The credibility is established by the signature with the IdP certificate.

The Required URLs as of October 2020 are:

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

1.2 HU Shibboleth Identity Provider

The IdP of the HU owns the entityID: „https://shib-idp.cms.hu-berlin.de/idp/shibboleth".

The SAML 2.0 protocol is supported.

Basically, the IdP returns transient NameId's on authentication requests. This means that a new identifier is generated for each session. A possible recognition of the user must be ensured via attributes.

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

Various attributes can be transmitted to uniquely identify and authorize users. The attributes are provided to the IdP by the HU Identity Management System - HU-IAM. The attributes that are supported follow the DFN recommended attributes of the object classes person, InetOrgPerson, eduPerson and SCHAC. A detailed list of the attributes and their value range can be found in Appendix A.

Before transmission to the requesting service, all attributes, with the exception of the service-dependent pseudonym, are presented to the user for approval/acceptance. The user has the option to exclude attributes that are not marked as 'required' in the metadata from the transmission.

1.3 Requirements for service providers of the HU internal federation

1.3.1 Certificate

Each service provider uses certificates for communication in two different protocols. One protocol is for web communication over HTTPS and the second protocol is for SAML communication. While only certificates signed by a public CA can be used for web communication via the browser, the trust relationship for the SAML certificate can also be established via another route, so self-signed certificates are also possible at these points, but they should not have a longer validity period than 39 months.

The validation of a self-signed certificate can be done by sending an email signed with a personal certificate to the Shibboleth Administrator (shibadmin@hu-berlin.de).

1.3.2 EntityID

The EntityID is a unique identifier of the SP and is usually generated as a URL in the form http:// + hostname + App_Name + /shibboleth.

1.3.3 Metadata

The metadata for the SP must contain the following additional information in addition to the standards such as EntityDescriptor and SPSSODescriptor:

- UI Extensions: DisplayName, Description, Logo (URL), InformationURL
- SingleLogoutService
- AssertionConsumerService (for at least one binding)
- AttributeConsumingService: enumeration of required and optional attributes
- ContactPerson: technical and administrative

1.3.4 Attributes

The attributes requested by the SP should be a subset of the attributes listed in Appendix A. If personal data is involved, there must be a legal basis for the processing of personal data, which is usually documented in the form of a security concept. To set up attribute sharing on the part of the IdP, at least a reference to the lawfulness of the data processing is necessary.

If the service requires additional or different data than those listed in the attribute list, this must be clarified with the Shibboleth administrator.

1.3.5 Checklist for ServiceProvider of HU Federation

1. Implementation of a Shibboleth ServiceProvider
2. Set up a certificate for authentication
   (can correspond to the server certificate)
3. Definition of requested Attributes (see attribute list) split in

‚requiered = true‛ - necessary and
‚requiered = false‛ - voluntary

4. Including the IdP metadata (see above)
5. If applicable, set up a WAYF / Discovery Service for additional federations to select the home organization.
6. Generate the metadata for the SP and send it to shibadmin@hu-berlin.de.
7. Implementing the authorization of users (access permissions)
8. Test

2 Appendix A

Attribute	Name	Typ	Schema	#	Wert / Werte
email	urn:oid:0.9.2342.19200300.100.1.3	String	InetOrgPerson	M	List of E-Mail addresses
cn	urn:oid:2.5.4.3	String	person	M	Full person name
gn	urn:oid:2.5.4.42	String	InetOrgPerson	M	List of given names
displayName	urn:oid:2.16.840.1.113730.3.1.241	String	InetOrgPerson	S	Display name of person
o	urn:oid:2.5.4.10	String	InetOrgPerson	M	Name of organization, which the person belongs to
department Number	urn:oid:2.16.840.1.113730.3.1.2	String	InetOrgPerson	S	For HU: OKZ of person
labeledURI	urn:oid:1.3.6.1.4.1.250.1.57	String	InetOrgPerson	M	List of internal ID's (FIS, UB, ...)
eduPerson Affiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	String	eduPerson	M	List of affiliations: member, student, staff, faculty, professor, employee
eduPerson Entitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	String	eduPerson	M	List of entitlements (roles)
eduPerson PrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Scoped String	eduPerson	S	User name with organization scope (@hu-berlin.de)
eduPerson ScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	Scoped String	eduPerson	M	List of affiliations with organization scope
eduPerson TargetedId	urn:oid:0.9.2342.19200300.100.1.1	String	eduPerson	S	Service-dependent unique pseudonym of the user
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	Organization type via SCHAC scheme
schacPersonal UniqueCode	urn:oid:1.3.6.1.4.1.25178.1.2.14	String	SCHAC	M	Personal, unique codes
schacDateOf Birth	urn:oid:1.3.6.1.4.1.25178.1.2.3	String	SCHAC	S	Birthdate (YYYYMMDD)