Hochschule Bremerhaven

ALFRED-WEGENER-INSTITUT
HELMHOLTZ-ZENTRUM FÜR POLAR- UND MEERESFORSCHUNG

Einbettung einer lokalen Software eines Föderationsmitgliedes zur Bereitstellung in einem Föderationsumfeld (DFN-AAI)

Bachelorarbeit im Studiengang Informatik

Fabian Mangels <fabian@mangels.it>

Bremerhaven, 20.02.2019

Gliederung

1. Einleitung
2. Grundlagen
3. Vorhandene Komponenten
4. Praktische Umsetzung
5. Fazit und Ausblick

Einleitung

Herausforderungen

- Zunehmende Menge an digitalen Forschungsdaten – viele sogar einzigartig
- Bedarf an Rechenleistung steigt
- Daten- und Informationsaustausch in einem internationalen Forschungsumfeld

- Lösung: International vernetzte Forschungsdateninfrastruktur

- Helmholtz-Datenföderation (HDF)
- Deutsches Forschungsnetz (DFN)
- Vertrauensvolle Infrastruktur bzw. Föderation – DFN-AAI
- Föderatives Identitätsmanagement (FIM)

Herausforderungen

- Zunehmende Menge an digitalen Forschungsdaten – viele sogar einzigartig
- Bedarf an Rechenleistung steigt
- Daten- und Informationsaustausch in einem internationalen Forschungsumfeld

- Lösung: International vernetzte Forschungsdateninfrastruktur

- Helmholtz-Datenföderation (HDF)
- Deutsches Forschungsnetz (DFN)
- Vertrauensvolle Infrastruktur bzw. Föderation – DFN-AAI
- Föderatives Identitätsmanagement (FIM)

Szenario

- Bereitstellung einer lokalen Ressource in einer Föderation (DFN-AAI)
- „Benötigte Komponente“ wurde im Zuge der Ausarbeitung erstellt
- *SP-IdP-Proxy* als Einstiegspunkt für den Fremdnutzer

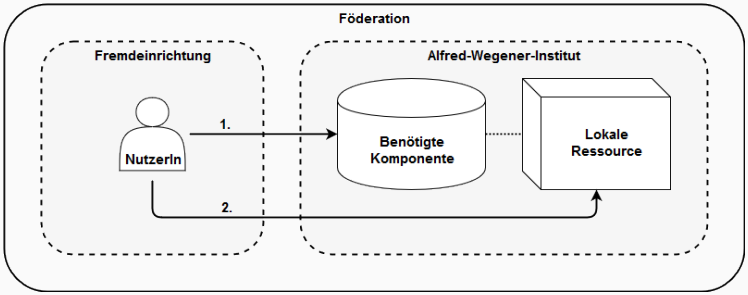


Abbildung 1: Vereinfachter Überblick des Szenarios

Grundlagen

Identitätsmanagement (IdM)

„Identitätsmanagement liefert die notwendigen Grundlagen zu jedweder Form von personalisiertem und berechtigtem Zugriff auf schützenswerte Ressourcen, Dienste und Systeme und bildet somit einen elementaren Baustein des IT-Sicherheitsmanagements“ [JD08, S. 225].

Grundlegende Konzepte:

- Authentifizierung
- Autorisierung

Zentrale Bestandteile des IdMs:

- Digitale Identitäten einer Entität
- Identitätsspeicher
- Integration von Identitätsspeichern
- Identitätsmanagement-Prozesse

Identitätsmanagement (IdM)

„Identitätsmanagement liefert die notwendigen Grundlagen zu jedweder Form von personalisiertem und berechtigtem Zugriff auf schützenswerte Ressourcen, Dienste und Systeme und bildet somit einen elementaren Baustein des IT-Sicherheitsmanagements“ [JD08, S. 225].

Grundlegende Konzepte:

- Authentifizierung
- Autorisierung

Zentrale Bestandteile des IdMs:

- Digitale Identitäten einer Entität
- Identitätsspeicher
- Integration von Identitätsspeichern
- Identitätsmanagement-Prozesse

Identitätsmanagement (IdM)

„Identitätsmanagement liefert die notwendigen Grundlagen zu jedweder Form von personalisiertem und berechtigtem Zugriff auf schützenswerte Ressourcen, Dienste und Systeme und bildet somit einen elementaren Baustein des IT-Sicherheitsmanagements“ [JD08, S. 225].

Grundlegende Konzepte:

- Authentifizierung
- Autorisierung

Zentrale Bestandteile des IdMs:

- Digitale Identitäten einer Entität
- Identitätsspeicher
- Integration von Identitätsspeichern
- Identitätsmanagement-Prozesse

Identitätsverteilung

- Verwirklichung organisationsübergreifender Geschäftsprozesse
- Sicherer und vertrauensvoller Austausch von Daten und digitaler Identitäten

- Föderatives Identitätsmanagement (FIM)
  „Lokal authentifizieren, global autorisieren“ [ABB+18, vgl. S. 4f.].
  Kernkomponenten des verteilten Ansatzes:
  - Entität
  - Client
  - Identitätsanbieter (IdP)
  - Diensteanbieter (SP)
- *Single Sign-on*, *Single Log-out*
- Nutzerzentriertes Identitätsmanagement

Identitätsverteilung

- Verwirklichung organisationsübergreifender Geschäftsprozesse
- Sicherer und vertrauensvoller Austausch von Daten und digitaler Identitäten

- Föderatives Identitätsmanagement (FIM)
  „Lokal authentifizieren, global autorisieren“ [ABB+18, vgl. S. 4f.].
  Kernkomponenten des verteilten Ansatzes:
  - Entität
  - Client
  - Identitätsanbieter (IdP)
  - Diensteanbieter (SP)
- *Single Sign-on*, *Single Log-out*
- Nutzerzentriertes Identitätsmanagement

Identitätsverteilung

- Verwirklichung organisationsübergreifender Geschäftsprozesse
- Sicherer und vertrauensvoller Austausch von Daten und digitaler Identitäten

- Föderatives Identitätsmanagement (FIM)
  „Lokal authentifizieren, global autorisieren“ [ABB+18, vgl. S. 4f.].
  Kernkomponenten des verteilten Ansatzes:
  - Entität
  - Client
  - Identitätsanbieter (IdP)
  - Diensteanbieter (SP)
- *Single Sign-on*, *Single Log-out*
- Nutzerzentriertes Identitätsmanagement

Vorhandene Komponenten

- *Security Assertion and Markup Language*
- Transport von Authentifikations- und Autorisierungsinformationen im browserbasierten Umfeld
- XML-Standard, der von OASIS im Mai 2002 spezifiziert wurde
- Bestandteile des XML-*Frameworks*:
  - *Assertions* – Authentisierungs-, Autorisierungs- oder Attributaussagen
  - *Protocols* – Anfrage- und Antwortprotokolle für die Übermittlung der Assertions
  - *Bindings* – Abbildung des SAML-Protokolls auf Nachrichten- und Kommunikationsprotokolle
  - *Profiles* – Zusammenspiel von *Assertions*, *Protocols* und *Bindings* (Randbedingungen)

- *Security Assertion and Markup Language*
- Transport von Authentifikations- und Autorisierungsinformationen im browserbasierten Umfeld
- XML-Standard, der von OASIS im Mai 2002 spezifiziert wurde
- Bestandteile des XML-*Frameworks*:
  - *Assertions* – Authentisierungs-, Autorisierungs- oder Attributaussagen
  - *Protocols* – Anfrage- und Antwortprotokolle für die Übermittlung der Assertions
  - *Bindings* – Abbildung des SAML-Protokolls auf Nachrichten- und Kommunikationsprotokolle
  - *Profiles* – Zusammenspiel von *Assertions*, *Protocols* und *Bindings* (Randbedingungen)

```
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="cn" Name="urn:oid:2.5.4.3" NameFormat="
    urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue>Fabian Mangels</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue>fabian.mangels@awi.de</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="sn" Name="urn:oid:2.5.4.4" NameFormat="
    urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue>Mangels</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Listing 1: SAML-*Assertion – AttributeStatement*

- *Lightweight Directory Access Protocol*
- Protokoll um mit Verzeichnisdiensten (Identitätsspeicher) zu operieren
- Internetstandard, wird von der IETF fortlaufend weiterentwickelt
- RFC 4510, 4511

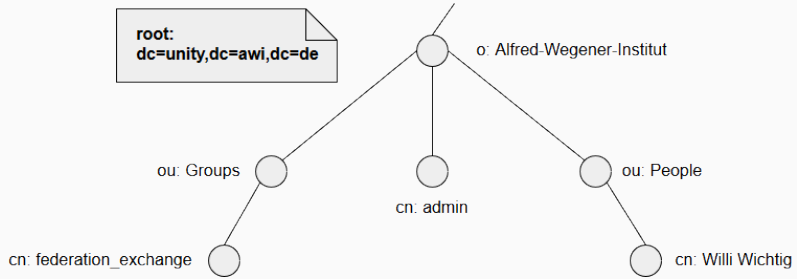


Abbildung 2: Verwendeter LDAP-Namensraum (DIT)

- *Authentication and Authorization Infrastructure*
- Infrastruktur für Attributaustausch und Identitätsfeststellungen jener Entität
- DFN-Verein als Föderationsbetreiber
- Aktive Teilnahme erfordert mind. einen IdP und die Einhaltung der *Policies* (Verlässlichkeitsklassen)
- *Shibboleth* als IdP / SP
- Vetrauen durch signierte Metadaten an zentraler Stelle

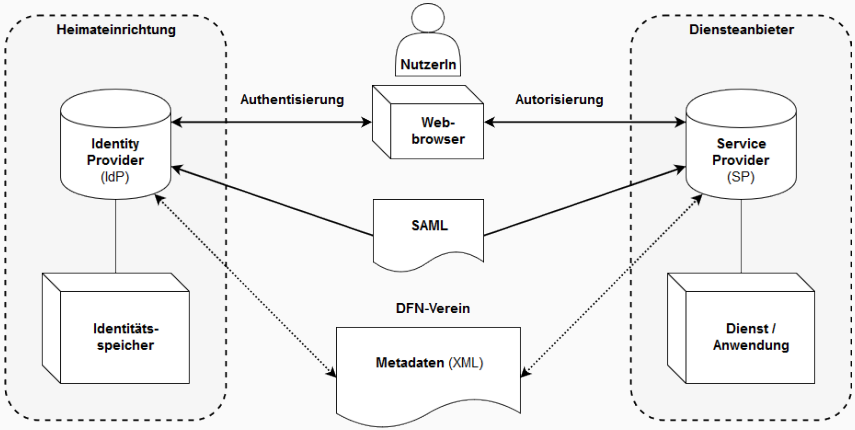


Abbildung 3: Grundlegende SSO-Interaktion in der DFN-AAI [Pem18b, vgl. S. 11]

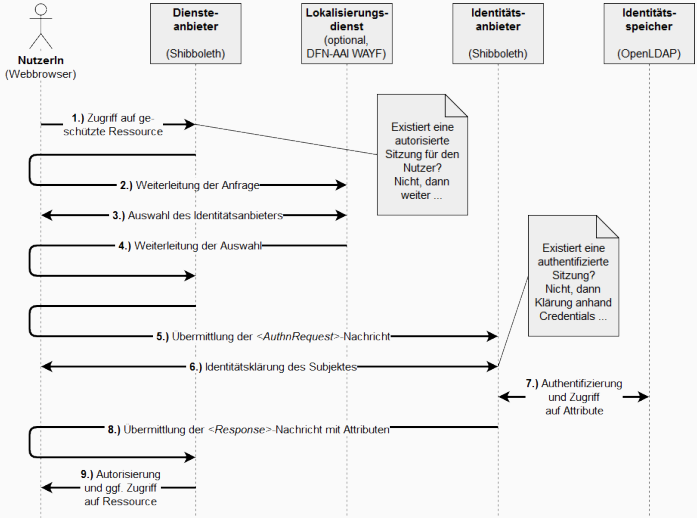


Abbildung 4: SAML 2.0 — *Single Sign-on* [HCH+05, WC08, vgl. S. 15, S. 8]

Shibboleth

- *Open Source*-Software
- IdP / SP im SAML-Kontext
- Entwicklung erfolgt durch das *Internet2*-Projekt und OASIS seit 2000
- *Shibboleth* als Synonym für SAML-basiertes Web-SSO
- Bereitstellung von Attributen, Identifizierung des Nutzers, Autorisierung am SP

1. Produktivföderation (*Advanced*) + *eduGAIN*:
   `https://shib-idp.awi.de/idp/shibboleth`
2. Testföderation:
   `https://shib-idp2.awi.de/idp/shibboleth`

Shibboleth

- *Open Source*-Software
- IdP / SP im SAML-Kontext
- Entwicklung erfolgt durch das *Internet2*-Projekt und OASIS seit 2000
- *Shibboleth* als Synonym für SAML-basiertes Web-SSO
- Bereitstellung von Attributen, Identifizierung des Nutzers, Autorisierung am SP

1. Produktivföderation (*Advanced*) + *eduGAIN*:
   `https://shib-idp.awi.de/idp/shibboleth`
2. Testföderation:
   `https://shib-idp2.awi.de/idp/shibboleth`

Unity IdM

- *Open Source*-Software
- Vielseitige Identitätsmanagementlösung
- In *Java* geschrieben
- Verwendet einen *Jetty* HTTP-Server und standardmäßig die DB *H2*
- Unterstützt viele verschiedene Authentifizierungsprotokolle
- Ermöglicht „einfache“ Integration in ein bestehendes IdM
- Verwendung im Szenario als *SP-IdP-Proxy*:
  - Admin-Endpunkt
  - Nutzerprofil-Endpunkt
  - RESTful API-Endpunkt
  - SAML-Authentifizierungscontroller

Unity IdM

- *Open Source*-Software
- Vielseitige Identitätsmanagementlösung
- In *Java* geschrieben
- Verwendet einen *Jetty* HTTP-Server und standardmäßig die DB *H2*
- Unterstützt viele verschiedene Authentifizierungsprotokolle
- Ermöglicht „einfache“ Integration in ein bestehendes IdM
- Verwendung im Szenario als *SP-IdP-Proxy*:
  - Admin-Endpunkt
  - Nutzerprofil-Endpunkt
  - RESTful API-Endpunkt
  - SAML-Authentifizierungscontroller

OpenLDAP

- *Open Source*-Software
- Referenzimplementierung des LDAP (RFC 4511)
- Entwicklung durch die *OpenLDAP Foundation*
- In der Programmiersprache *C* geschrieben
- Eigenständiger LDAP-Server bzw. -Daemon – *slapd*
- Diverse Bibliotheken und weitere nützliche Werkzeuge
- Agiert als Identitätsspeicher im Szenario

VMware vRealize Automation (vRA)

- Zentrale Plattform (*Marketplace*)
  - Anforderung von IT-Diensten durch Nutzer
  - Verwaltung von Cloud- bzw. IT-Ressourcen durch Administratoren
- *On-Demand*-Dienste
- Kommerzielle SW des US-amerikanischen Unternehmens *VMware*
- Bereitstellung im Umfeld der DFN-AAI-Föderation
- Anmeldung an der Plattform durch Nutzer aus dem erwähnten LDAP-Verzeichnisdienst

Praktische Umsetzung

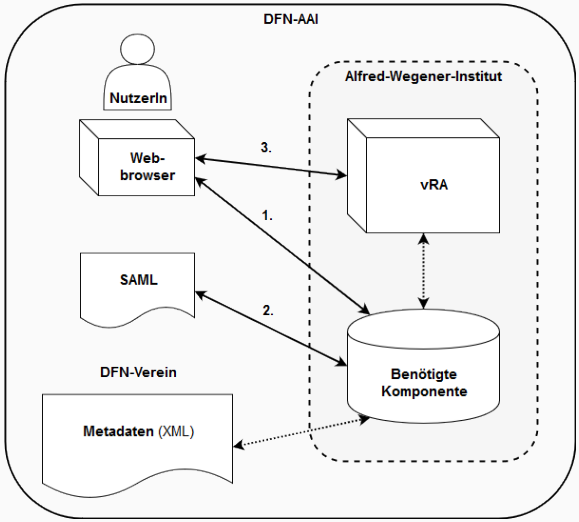


Abbildung 5: Kontextdiagramm des betrachteten Szenarios

Überblick der Umsetzung ii

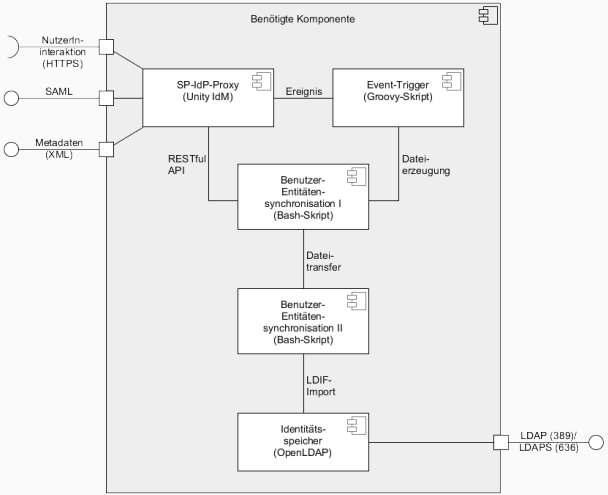


Abbildung 6: Bausteinsicht der benötigten Komponente

```
<MetadataProvider id="LocalMetadata" xsi:type="FilesystemMetadataProvider"
    metadataFile="%{idp.home}/metadata/local-unitysrv1.xml"/>
```

Listing 2: Eintragung der lokalen Metadatendatei im *Shibboleth* IdP

```
<AttributeFilterPolicy id="unity">
  <PolicyRequirementRule xsi:type="OR">
    <Rule xsi:type="Requester" value="https://unitysrv1.awi.de" />
  </PolicyRequirementRule>
  <AttributeRule attributeID="mail" permitAny="true" />
  <AttributeRule attributeID="surname" permitAny="true" />
  <AttributeRule attributeID="givenName" permitAny="true" />
  <AttributeRule attributeID="commonName" permitAny="true" />
  <AttributeRule attributeID="displayName" permitAny="true" />
</AttributeFilterPolicy>
```

Listing 3: Angewandte Filterrichtlinie im *Shibboleth* IdP

```
<MetadataProvider id="LocalMetadata" xsi:type="FilesystemMetadataProvider"
    metadataFile="%{idp.home}/metadata/local-unitysrv1.xml"/>
```

Listing 2: Eintragung der lokalen Metadatendatei im *Shibboleth* IdP

```
<AttributeFilterPolicy id="unity">
  <PolicyRequirementRule xsi:type="OR">
    <Rule xsi:type="Requester" value="https://unitysrv1.awi.de" />
  </PolicyRequirementRule>
  <AttributeRule attributeID="mail" permitAny="true" />
  <AttributeRule attributeID="surname" permitAny="true" />
  <AttributeRule attributeID="givenName" permitAny="true" />
  <AttributeRule attributeID="commonName" permitAny="true" />
  <AttributeRule attributeID="displayName" permitAny="true" />
</AttributeFilterPolicy>
```

Listing 3: Angewandte Filterrichtlinie im *Shibboleth* IdP

```
# (Issuer field). This should be unique URI which identifies the server.
unity.saml.requester.requesterEntityId=https://unitysrv1.awi.de

#Federation metadata configured trusted IdPs:
unity.saml.requester.metadataSource.federation.url=http://www.aai.dfn.de/fileadmin
    /metadata/dfn-aai-test-metadata.xml
unity.saml.requester.metadataSource.federation.perMetadataTranslationProfile=sys:
    samlShib
```

Listing 4: Einstellungen des SAML-Authentifizierungscontrollers [UT16]

- Grundeinstellungen an SW
- Weitere Konfigurationen an den benötigten Endpunkten

ID	KDF	SALT (#Zeichen)	HASH (#Zeichen)
	DES (Data Encryption Standard)	2	11
1	MD5 (Message Digest 5)	≤ 16	22
5	SHA-256 (seit glibc 2.7)	≤ 16	43
6	SHA-512 (seit glibc 2.7)	≤ 16	86

Tabelle 1: Unterstützte KDFs in der *crypt(3)*-Funktion [Lin18]

- userPassword: {CRYPT}$**ID**$rounds=**X**$**SALT**$**HASH**
- Dabei gilt: **ID** $\in$ {1,5,6}, 1000 $\leq$ **X** $\leq$ 999999999,
  SALT, **HASH** $\in$ {[a-z]*,[A-Z]*,[0-9]*,[.]*,[/]*}

ID	KDF	SALT (#Zeichen)	HASH (#Zeichen)
	DES (Data Encryption Standard)	2	11
1	MD5 (Message Digest 5)	≤ 16	22
5	SHA-256 (seit glibc 2.7)	≤ 16	43
6	SHA-512 (seit glibc 2.7)	≤ 16	86

Tabelle 1: Unterstützte KDFs in der *crypt(3)*-Funktion [Lin18]

- userPassword: {CRYPT}$**ID**$rounds=**X**$**SALT**$**HASH**
- Dabei gilt: **ID** $\in$ {1,5,6}, 1000 $\leq$ **X** $\leq$ 999999999,
  SALT, **HASH** $\in$ {[a-z]*,[A-Z]*,[0-9]*,[.]*,[/]*}

- Apache-Library „commons-codec-1.11.jar“
- „org.apache.commons.codec.digest.Crypt“

```
private String[] crypt(String password, CryptParams params) {
  String saltCrypt = genSaltCrypt(params.getSaltLength());
  String crypt = Crypt.crypt(password,
  "$" + params.getIdHashingAlgorithm() + "$rounds=" + params.getRounds() + "$" +
    saltCrypt);
  return crypt.split("\\$");
}
```

Listing 5: *Java* – Erzeugung eines *crypt(3)*-Passworthashes

Vorarbeiten – Hashverfahren iii

```
private Random random = new SecureRandom();
private static final String B64T = "./0123456789
    ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz";

private String genSaltCrypt(final int num) {
  final StringBuilder saltString = new StringBuilder();
    for (int i = 1; i <= num; i++) {
      saltString.append(B64T.charAt(random.nextInt(B64T.length())));
    }
  return saltString.toString();
}
```

Listing 6: *Java* – Erzeugung eines *crypt(3)-Salts*

```java
private static final int CRYPT_HASH_POS = 4;

private boolean verifyCrypt(PasswordInfo stored, String password) {
  CryptParams params = new CryptParams(stored.getMethodParams());
  String crypt = Crypt.crypt(password, "$" + params.getIdHashingAlgorithm() + "
    $rounds=" + params.getRounds()
  + "$" + new String(stored.getSalt(), StandardCharsets.UTF_8));
  String[] cryptParts = crypt.split("\\$");
  byte[] testedHash = cryptParts[CRYPT_HASH_POS].getBytes(StandardCharsets.UTF_8);
  return Arrays.areEqual(testedHash, stored.getHash());
}
```

Listing 7: *Java* – Verifikation eines *crypt(3)*-Passworts

Überblick der Umsetzung ii

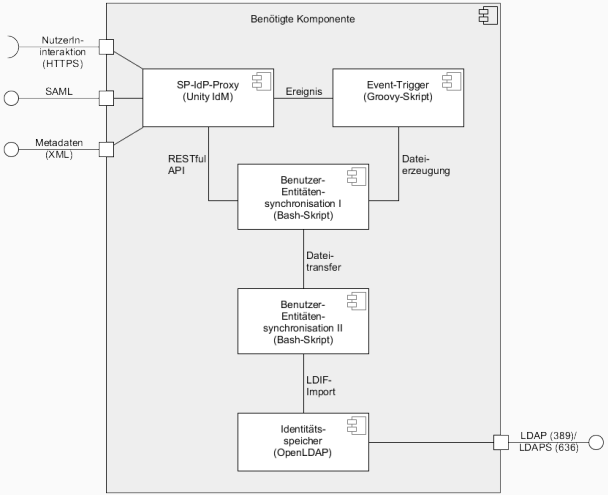


Abbildung 6: Bausteinsicht der benötigten Komponente

Implementierung

- Zwei *Bash*-Skripte auf zwei separaten VMs (flexibel)
- *Properties*-Dateien, Variablen- und Methodennutzung
- Kommunikation über verschlüsselten Transportkanal (SSH, SCP, HTTPS)
- Sichtbarkeit von Passwörtern
- Protokollierung
- *init*-Skripte für beide Prozesse („*/etc/init.d/*“)
- Eigene Systembenutzer zur Ausführung
- Verschlüsselung der LDIF-Dateien via *One-time Password* (OTP) – „*openssl*“

Implementierung – Benutzer-Entitätensynchronisation I

```
unityServer.core.enableLowLevelEvents=true
unityServer.core.script.n.file=${CONF}/scripts/myGroovy_basicEvents.groovy
unityServer.core.script.n.trigger=methodInvocation.submitEnquiryResponse
```

Listing 8: Aktivierung der „*Low Level Events*“ in *Unity IdM* [UT18]

- entityId_<entityId>_methodInvocation.submitEnquiryResponse_<timestamp>.unity
- entityId_<entityId>_methodInvocation.setEntityCredential_<timestamp>.unity
- entityId_<entityId>_methodInvocation.removeEntity_<timestamp>.unity
- entityId_<entityId>_methodInvocation.createAttribute_<attributeName>_<timestamp>.unity
- entityId_<entityId>_methodInvocation.setAttribute_<attributeName>_<timestamp>.unity
- entityId_<entityId>_methodInvocation.removeAttribute_<attributeName>_<timestamp>.unity

Implementierung – Benutzer-Entitätensynchronisation I

```
unityServer.core.enableLowLevelEvents=true
unityServer.core.script.n.file=${CONF}/scripts/myGroovy_basicEvents.groovy
unityServer.core.script.n.trigger=methodInvocation.submitEnquiryResponse
```

Listing 8: Aktivierung der „*Low Level Events*“ in *Unity IdM* [UT18]

- entityId_<entityId>_methodInvocation.submitEnquiryResponse_<timestamp>.unity
- entityId_<entityId>_methodInvocation.setEntityCredential_<timestamp>.unity
- entityId_<entityId>_methodInvocation.removeEntity_<timestamp>.unity
- entityId_<entityId>_methodInvocation.createAttribute_<attributeName>_<timestamp>.unity
- entityId_<entityId>_methodInvocation.setAttribute_<attributeName>_<timestamp>.unity
- entityId_<entityId>_methodInvocation.removeAttribute_<attributeName>_<timestamp>.unity

Implementierung – Benutzer-Entitätensynchronisation I

```
1 inotifywait -mq -e create -e attrib --format %f $MONITORING_DIR | while read FILE
```

Listing 9: Überwachung eines Verzeichnisses mit „*inotifywait*“

```
1 curl -s -k --netrc-file $CONF_DIR/.netrc -X PUT -H "Content-Type: application/json
    " -d "{\"values\":[\"$uid\"],\"name\": \"userName\",\"groupPath\": \"/\"}" "
    https://unitysrv1.awi.de/rest-admin/v1/entity/$entityId/attribute"

3 curl -s -k --netrc-file $CONF_DIR/.netrc "https://unitysrv1.awi.de/rest-admin/v1/
    entity/$entityId/attributes" | sed -e 's/\\//g' -e 's/"{/{/g' -e 's/}"/}/g' >
    ${WORK_DIR}/$FILE.tmp
```

Listing 10: HTTP-Anfragen an die *RESTful API* mit „*curl*“

```
1 inotifywait -mq -e create -e attrib --format %f $MONITORING_DIR | while read FILE
```

Listing 9: Überwachung eines Verzeichnisses mit „*inotifywait*“

```
1 curl -s -k --netrc-file $CONF_DIR/.netrc -X PUT -H "Content-Type: application/json
    " -d "{\"values\":[\"$uid\"],\"name\": \"userName\",\"groupPath\": \"/\"}" "
    https://unitysrv1.awi.de/rest-admin/v1/entity/$entityId/attribute"

3 curl -s -k --netrc-file $CONF_DIR/.netrc "https://unitysrv1.awi.de/rest-admin/v1/
    entity/$entityId/attributes" | sed -e 's/\\//g' -e 's/"{/{/g' -e 's/}"/}/g' >
    ${WORK_DIR}/$FILE.tmp
```

Listing 10: HTTP-Anfragen an die *RESTful API* mit „*curl*“

```
result=$(cat ${WORK_DIR}/$FILE.tmp | jq -c '.[] | select(.["name"] == "surname") |
    .["values"][0]' | sed 's/"//g')
```

Listing 11: „*surname*“ – Parsen der JSON-Datei mit „*jq*“

```
writeInLdif "dn:" "uid=$uid,ou=People,dc=unity,dc=awi,dc=de"
writeInLdif "changetype:" "modify"
writeInLdif "replace:" "userPassword"
passwdHash=$(getJsonValue "hash")
passwdSalt=$(getJsonValue "salt")
writeInLdif "userPassword:" '{CRYPT}$5$rounds=5000$'$passwdSalt'$'$passwdHash
```

Listing 12: LDIF-Erstellung aufgrund neuer *Credentials* einer Entität

```
result=$(cat ${WORK_DIR}/$FILE.tmp | jq -c '.[] | select(.["name"] == "surname") |
    .["values"][0]' | sed 's/"//g')
```

Listing 11: „*surname*“ – Parsen der JSON-Datei mit „*jq*“

```
writeInLdif "dn:" "uid=$uid,ou=People,dc=unity,dc=awi,dc=de"
writeInLdif "changetype:" "modify"
writeInLdif "replace:" "userPassword"
passwdHash=$(getJsonValue "hash")
passwdSalt=$(getJsonValue "salt")
writeInLdif "userPassword:" '{CRYPT}$5$rounds=5000$'$passwdSalt'$'$passwdHash
```

Listing 12: LDIF-Erstellung aufgrund neuer *Credentials* einer Entität

```
openssl rand -base64 -out ${WORK_DIR}/$FILE.otp 128

openssl enc -aes-256-cbc -salt -in ${WORK_DIR}/$FILE.ldif -out ${WORK_DIR}/$FILE.
    ldif.enc -pass file:${WORK_DIR}/$FILE.otp

openssl rsautl -encrypt -inkey ${CONF_DIR}/public_key.pem -pubin -in ${WORK_DIR}/
    $FILE.otp -out ${WORK_DIR}/$FILE.otp.enc
```

Listing 13: Verschlüsselung der zu übertragenden Dateien mit „*openssl*“ [OT18]

```
scp ${WORK_DIR}/$FILE.otp.enc openldap:~/work/.
scp ${WORK_DIR}/$FILE.ldif.enc openldap:~/monitoring/.
```

Listing 14: Übertragung der kryptographischen Dateien mit „*scp*“

```
openssl rand -base64 -out ${WORK_DIR}/$FILE.otp 128

openssl enc -aes-256-cbc -salt -in ${WORK_DIR}/$FILE.ldif -out ${WORK_DIR}/$FILE.
    ldif.enc -pass file:${WORK_DIR}/$FILE.otp

openssl rsautl -encrypt -inkey ${CONF_DIR}/public_key.pem -pubin -in ${WORK_DIR}/
    $FILE.otp -out ${WORK_DIR}/$FILE.otp.enc
```

Listing 13: Verschlüsselung der zu übertragenden Dateien mit „*openssl*“ [OT18]

```
scp ${WORK_DIR}/$FILE.otp.enc openldap:~/work/.
scp ${WORK_DIR}/$FILE.ldif.enc openldap:~/monitoring/.
```

Listing 14: Übertragung der kryptographischen Dateien mit „*scp*“

```
openssl rsautl -decrypt -inkey ${CONF_DIR}/private_key.pem -in ${WORK_DIR}/$FILE.
    otp.enc -out ${WORK_DIR}/$FILE.otp

openssl enc -d -aes-256-cbc -in ${WORK_DIR}/$FILE.ldif.enc -out ${WORK_DIR}/$FILE.
    ldif -pass file:${WORK_DIR}/$FILE.otp
```

Listing 15: Entschlüsselung der empfangenen Dateien mit „*openssl*“ [OT18]

```
ldapmodify -x -D cn=admin,dc=unity,dc=awi,dc=de -y $CONF_DIR/.passwd -f $WORK_DIR/
    $FILE.ldif
```

Listing 16: Ausführung von „*ldapmodify*“

```
openssl rsautl -decrypt -inkey ${CONF_DIR}/private_key.pem -in ${WORK_DIR}/$FILE.
    otp.enc -out ${WORK_DIR}/$FILE.otp

openssl enc -d -aes-256-cbc -in ${WORK_DIR}/$FILE.ldif.enc -out ${WORK_DIR}/$FILE.
    ldif -pass file:${WORK_DIR}/$FILE.otp
```

Listing 15: Entschlüsselung der empfangenen Dateien mit „*openssl*“ [OT18]

```
ldapmodify -x -D cn=admin,dc=unity,dc=awi,dc=de -y $CONF_DIR/.passwd -f $WORK_DIR/
    $FILE.ldif
```

Listing 16: Ausführung von „*ldapmodify*“

Fazit und Ausblick

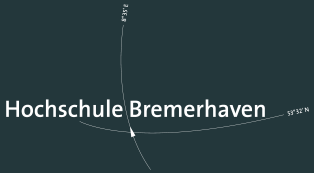
Fazit

- Verteiltes FIM als logische Weiterentwicklung
- IdP als zentrale Schnittstelle des IdM der Heimateinrichtung (Authentifizierung)
- Autorisierung erfolgt vermehrt an einem *SP-IdP-Proxy*
- Lokale Referenz (Benutzerkonto) wird gebraucht – kein „wirkliches“ SSO
- Funktionstüchtige Umsetzung im Testumfeld

Ausblick

- Kleinere Verbesserungen / Maßnahmen, weitere Tests
- Größere Probleme:
  1. Laufzeit eines lokalen Kontos (*Session-Timeout*)
  2. Gruppenberechtigungen (*eduPerson*, *Policies*)
- Nutzung des zentralen *SP-IdP-Proxys* im HDF-Umfeld
- Verbesserungen durch *OpenID Connect* (OIDC) in der DFN-AAI?

Vielen Dank für Ihre Aufmerksamkeit!



Einbettung einer lokalen Software eines Föderationsmitgliedes zur Bereitstellung in einem Föderationsumfeld (DFN-AAI)

Bachelorarbeit im Studiengang Informatik

Fabian Mangels <fabian@mangels.it>
Bremerhaven, 20.02.2019

Anhang

Alfred-Wegener-Institut (AWI)

- Deutsche Forschungseinrichtung in der Polar- und Meeresforschung
- Hauptsitz in Bremerhaven
- > 1000 Mitarbeiter
- Außenstellen: Potsdam, Helgoland und Sylt
- Fachbereiche: Geo-, Bio- und Klimawissenschaften
- Leistungsfähige Infrastruktur: Stationen in der Arktis und Antarktis, Schiffe und Flugzeuge
- Rechenzentrum

Abbildung 7: AWI Campus Bremerhaven [AT18]

Alfred-Wegener-Institut (AWI)

- Deutsche Forschungseinrichtung in der Polar- und Meeresforschung
- Hauptsitz in Bremerhaven
- > 1000 Mitarbeiter
- Außenstellen: Potsdam, Helgoland und Sylt
- Fachbereiche: Geo-, Bio- und Klimawissenschaften
- Leistungsfähige Infrastruktur: Stationen in der Arktis und Antarktis, Schiffe und Flugzeuge
- Rechenzentrum

Abbildung 7: AWI Campus Bremerhaven [AT18]

Objektklasse	Zuständigkeit
top (abstrakt)	Alle Einträge gehören zur abstrakten Objektklasse „*top*“.
organizationalUnit (strukturell)	Definiert die Basis eines Eintrags, der eine Organisationseinheit darstellt.
organizationalPerson (strukturell)	Grundlage für einen Eintrag, der eine Person in Bezug auf eine Organisation repräsentiert.
inetOrgPerson (unterstützend)	Erweiterung der Objektklasse „*organizationalPerson*“, um den heutigen Anforderungen der Bereitstellung von Internet- und Intranet-Verzeichnisdiensten gerecht zu werden.
eduPerson (unterstützend)	Unterstützt den Austausch zwischen Bildungs- und Forschungseinrichtungen mit vordefinierten Attributen über Personen.

Tabelle 2: Grundlegende LDAP-Objektklassen [Smi00, Zei06, Sci06, IT16, RFC 2798, RFC 4512, RFC 4519]

Operation	Erklärung
Bind	Beginn einer Sitzung.
Unbind	Beenden einer Sitzung.
Search	Suche nach Einträgen ab einer übergebenen Stelle, dem *Base DN*, im DIT.
Modify	Änderung eines Eintrags.
Add	Hinzufügen eines Eintrags an einer beliebigen Stelle im DIT.
Delete	Löschen eines Eintrags.
Compare	Vergleich eines Attributwertes mit einem spezifizierten Wert.

Tabelle 3: Zugriffsoperationen auf ein LDAP-Verzeichnis [JD08, vgl. S. 235]

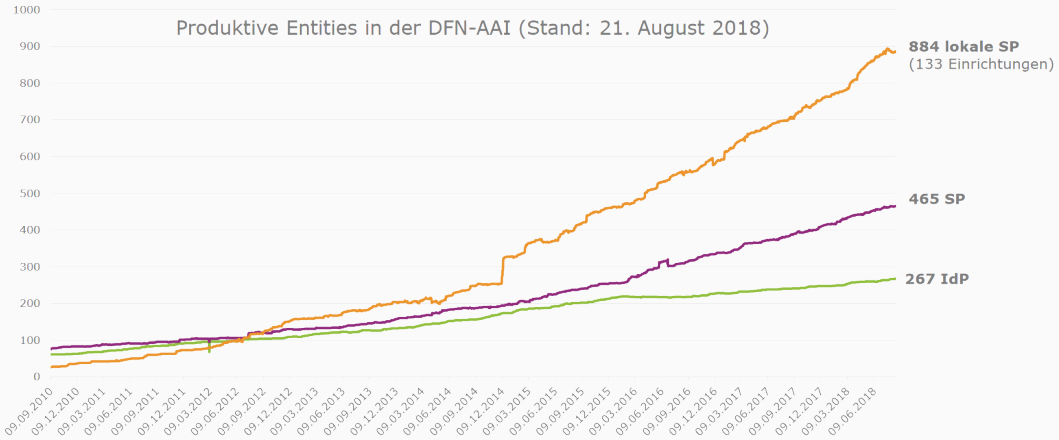


Abbildung 8: DFN-AAI – Produktive Entities [Pem18b, vgl. S. 35]

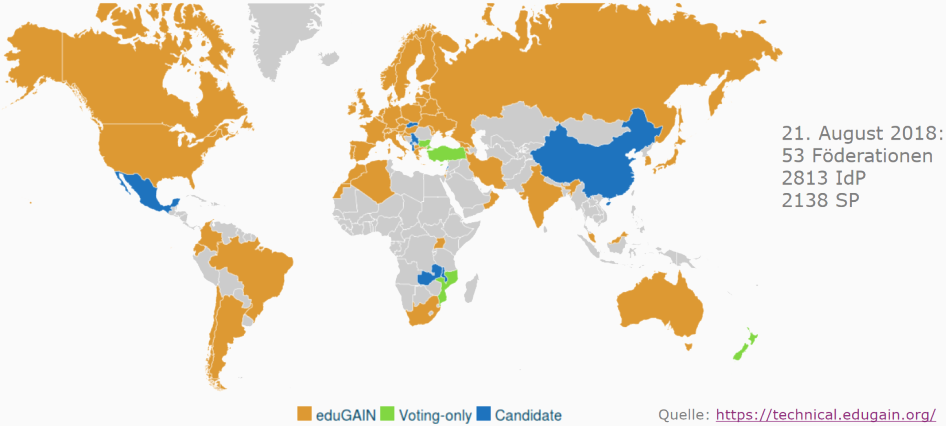


Abbildung 9: *eduGAIN* – beteiligte Föderationen [Pem18b, vgl. S. 37]

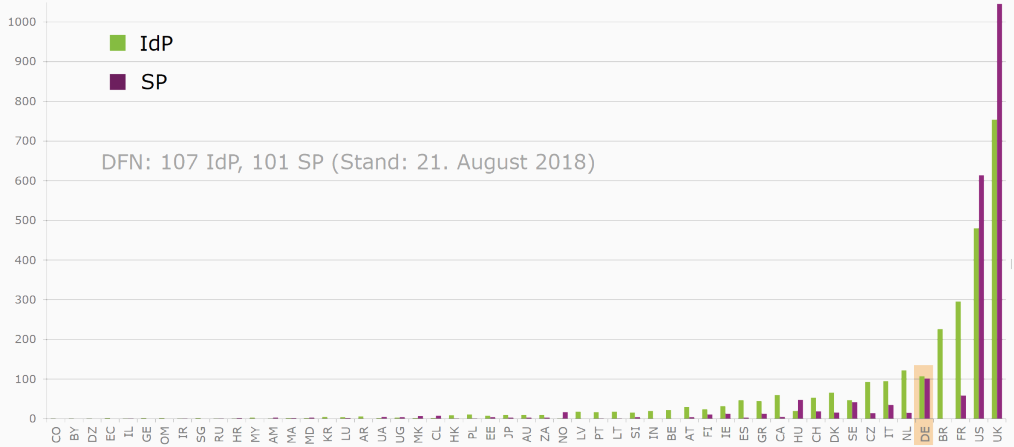


Abbildung 10: *eduGAIN* – Beteiligung je Föderation [Pem18b, S. 38]

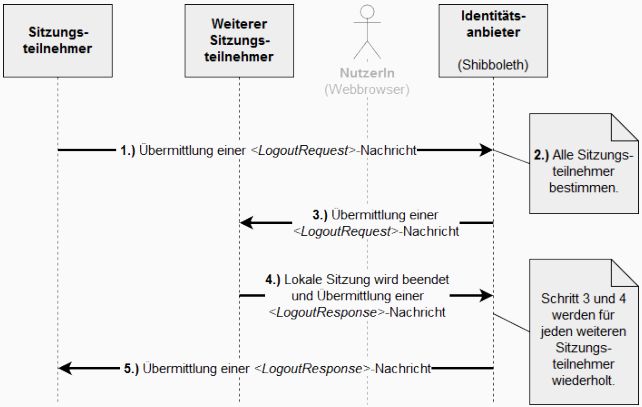


Abbildung 11: SAML 2.0 — *Single Log-out* [HCH+05, vgl. S. 33]

Verlässlichkeitsklasse	Identifizierung durch Heimateinrichtung	Verfahren zum Ausweis einer Identität	Datenhaltung und Prozesse zur Pflege der Identitäten
Test	Verfahren freigestellt.	Verfahren freigestellt.	Verfahren freigestellt.
Basic	Rückantwort von eindeutiger Adresse (E-Mail, Tel.-Nr., Postanschrift, etc.).	Anhand eindeutig zuzuordnender digitalen Adresse.	Verpflichtung bzgl. Aktualität innerhalb von 3 Monaten.
Advanced	Pers. Vorsprechen gegenüber Vertrauensinstanz unter Vorlage amtlicher Dokumente (alternativ: Post-Ident, eID / nPA). Die an den Hochschulen etablierten Einschreibungs- und Einstellungsprozesse werden als gleichwertig akzeptiert.	Pers. Account bzw. digitales Zertifikat (sichere Vergaberichtlinie).	Verpflichtung bzgl. Aktualität innerhalb von 2 Wochen.

Tabelle 4: Verlässlichkeitsklassen in der DFN-AAI [Pem18b, vgl. S. 31]

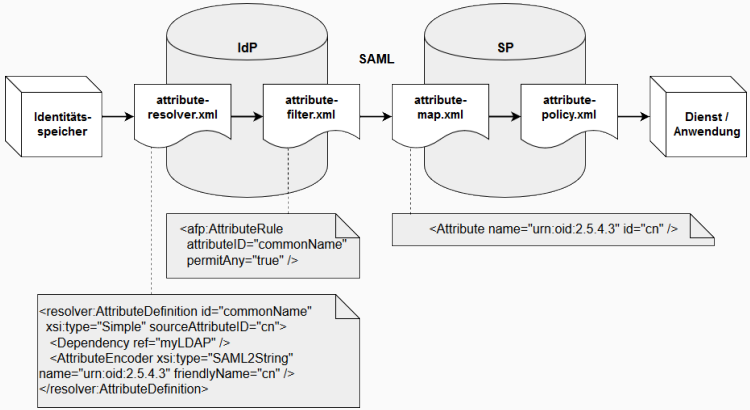


Abbildung 12: Attribut-Management in Shibboleth [Pem18a, vgl. S. 4]

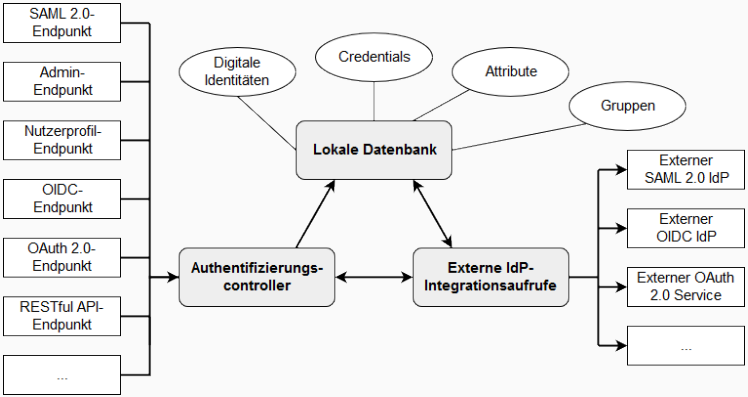


Abbildung 13: Systemaufbau von Unity IdM [UT18]

```
dn: cn=config
changetype: modify
add: olcPasswordHash
olcPasswordHash: {CRYPT}
-
add: olcPasswordCryptSaltFormat
olcPasswordCryptSaltFormat: $5$rounds=5000$%.16s
```

Listing 17: LDIF – Änderung des Standard-Passwortschemas

LDIF – create entity

```
dn: uid=awiFed2,ou=People,dc=unity,dc=awi,dc=de
changetype: add
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: awiFed2
loginShell: /bin/bash
homeDirectory: /home/awiFed2
gidNumber: 5000
uidNumber: 10002
description: uid=awiFed2,ou=People,dc=unity,dc=awi,dc=de
sn: Mangels
givenName: Fabian
cn: Fabian Mangels
displayName: Fabian Mangels
mail: fabian.mangels@awi.de
userPassword: {CRYPT}$5$rounds=5000$SVb/TG.2
    e9PnJLDJ$hsW4EChqtxFTb9clt6wAxN5P1azYKfo1ig.JgkoU4P.
```

Listing 18: entityId_2_methodInvocation.submitEnquiryResponse_1542024212.unity.ldif

```
dn: uid=awiFed2,ou=People,dc=unity,dc=awi,dc=de
changetype: delete
```

Listing 19: entityId_2_methodInvocation.removeEntity_1542024374.unity.ldif

```
dn: uid=awiFed2,ou=People,dc=unity,dc=awi,dc=de
changetype: modify
replace: userPassword
userPassword: {CRYPT}$5$rounds=5000$1xFqo/GHmt4QTkIm$zo7XVwNH3oVhPPq7aEA.
    miJ7LxWpwk3wYZa8oBH./N3
```

Listing 20: entityId_2_methodInvocation.setEntityCredential_1542024274.unity.ldif

LDIF – set attribute / remove attribute

```
dn: uid=awiFed2,ou=People,dc=unity,dc=awi,dc=de
changetype: modify
replace: mail
mail: fabian.mangels@awi.de
```

Listing 21: entityId_2_methodInvocation.setAttribute_email_1542024325.unity.ldif

```
dn: uid=awiFed2,ou=People,dc=unity,dc=awi,dc=de
changetype: modify
delete: mail
```

Listing 22: entityId_2_methodInvocation.removeAttribute_email_1542024343.unity.ldif

Atherton, Christopher J. ; Barton, Thomas ; Basney, Jim ; Broeder, Daan ; Costa, Alessandro ; Daalen, Mirjam V. ; Dyke, Stephanie ; Elbers, Willem ; Enell, Carl-Fredrik ; Fasanelli, Enrico Maria V. ; Fernandes, João ; Florio, Licia ; Gietz, Peter ; Groep, David L. ; Junker, Matthias B. ; Kanellopoulos, Christos ; Kelsey, David ; Kershaw, Philip ; Knapic, Cristina ; Kollegger, Thorsten ; Koranda, Scott ; Linden, Mikael ; Marinic, Filip ; Matyska, Ludek ; Nyrönen, Tommi H. ; Paetow, Stefan ; Paglione, Laura A D. ; Parlati, Sandra ; Phillips, Christopher ; Prochazka, Michal ; Rees, Nicholas ; Short, Hannah ; Stevanovic, Uros ; Tartakovsky, Michael ; Venekamp, Gerben ; Vitez, Tom ; Wartel, Romain ; Whalen, Christopher ; White, John ; Zwölf, Carlo M.:
Federated Identity Management For Research Collaborations.
In: *FIM4R* (2018), Juli.
http://dx.doi.org/10.5281/zenodo.1307551. –

DOI 10.5281/zenodo.1307551. –
abgerufen am 10.10.2018

AWI-Team:
AWI Bremerhaven.
https://www.awi.de/ueber-uns/standorte/bremerhaven.html.
Version: November 2018. –
abgerufen am 03.01.2019

Höllrigl, Thorsten:
***Informationskonsistenz im föderativen Identitätsmanagement: Modellierung und Mechanismen*, Karlsruher Institut für Technologie (KIT), Diss., 2011.**
http://dx.doi.org/10.5445/IR/1000022470. –
DOI 10.5445/IR/1000022470. –
abgerufen am 15.10.2018

Literaturverzeichnis iii

Hughes, John ; Cantor, Scott ; Hodges, Jeff ; Hirsch, Frederick ; Mishra, Prateek ; Philpott, Rob ; Maler, Eve:
Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 / OASIS.
Version: März 2005.
https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.
2005. –
techreport. –
abgerufen am 25.10.2018

Internet2-Team:
eduPerson Object Class Specification (201602) / Internet2.
Version: März 2016.
http:
//software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html.

2016. –
Forschungsbericht. –
abgerufen am 26.10.2018

Jochen Dinger, Hannes H.:
Netzwerk- und IT-Sicherheitsmanagement : eine Einführung.
Universitätsverlag Karlsruhe, Karlsruhe, 2008
https://publikationen.bibliothek.kit.edu/1000007400/142064. –
ISBN 978–3–86644–209–2. –
abgerufen am 06.10.2018

Linux Programmer's Manual:
crypt, crypt_r - password and data encryption.
man-page.
http://man7.org/linux/man-pages/man3/crypt.3.html.
Version: April 2018. –
abgerufen am 06.10.2018

Mangels, Fabian:
Einbettung einer lokalen Software eines Föderationsmitgliedes zur Bereitstellung in einem Föderationsumfeld (DFN-AAI).
http://epic.awi.de/48571/.
Version: December 2018


OpenSSL-Team:
openssl manpage – commands.
https://www.openssl.org/docs/man1.1.0/apps/.
Version: September 2018. –
abgerufen am 27.10.2018


Pempe, Wolfgang:
Attribute: Attribut-Schemata, -Generierung, -Übertragung und Verarbeitung am SP.
https://download.aai.dfn.de/ws/2018_fhdo/attributes.pdf.
Version: August 2018. –
abgerufen am 19.10.2018

Pempe, Wolfgang:
Grundlagen: AAI, Web-SSO, Metadaten und Föderationen.
https://download.aai.dfn.de/ws/2018_fhdo/grundlagen.pdf.
Version: August 2018. –
abgerufen am 19.10.2018

Sciberras, Andrew:
Lightweight Directory Access Protocol (LDAP): Schema for User Applications.
RFC 4519.
http://dx.doi.org/10.17487/RFC4519.
Version: Juni 2006 (Request for Comments). –
abgerufen am 21.10.2018


Smith, Mark C.:
Definition of the inetOrgPerson LDAP Object Class.
RFC 2798.
http://dx.doi.org/10.17487/RFC2798.
Version: April 2000 (Request for Comments). –
abgerufen am 21.10.2018


Unity-Team ; Unity (Hrsg.):
Unity SAML HowTo Manual.
Unity, April 2016.
http://www.unity-idm.eu/documentation/unity-1.9.0/saml-howto.html. –
abgerufen am 01.10.2018

Unity-Team ; Unity (Hrsg.):
Unity Manual.
Unity, August 2018.
http://www.unity-idm.eu/documentation/unity-2.6.2/manual.html. –
abgerufen am 01.10.2018

Widdowson, Rod ; Cantor, Scott:
Identity Provider Discovery Service Protocol and Profile / OASIS.
Version: März 2008.
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf.
2008. –
techreport. –
abgerufen am 25.10.2018


Zeilenga, Kurt:
Lightweight Directory Access Protocol (LDAP): Directory Information Models.
RFC 4512.
http://dx.doi.org/10.17487/RFC4512.
Version: Juni 2006 (Request for Comments). –
abgerufen am 21.10.2018