Identity Management und Shibboleth: Ein Überblick

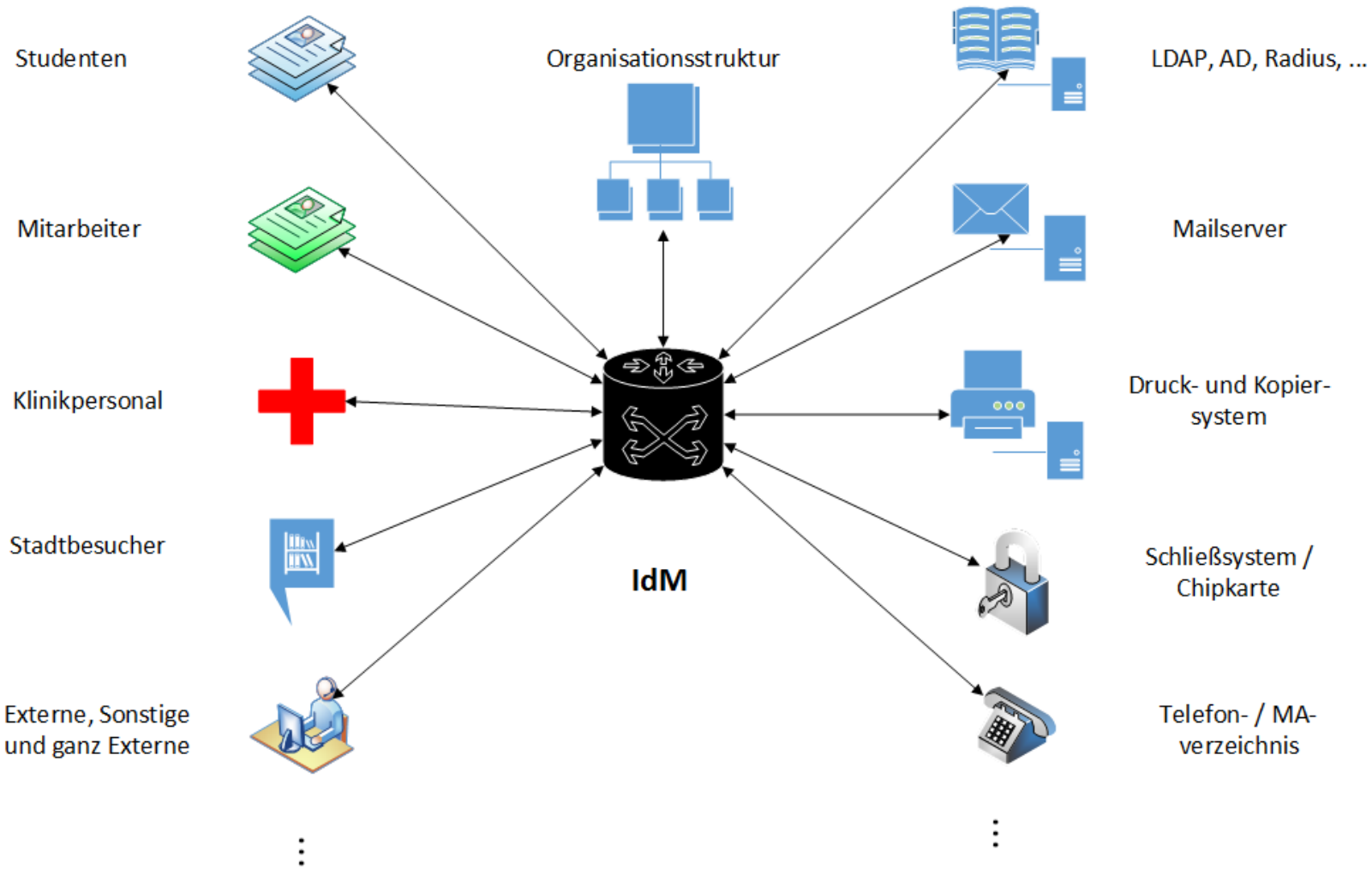
Thorsten Michels

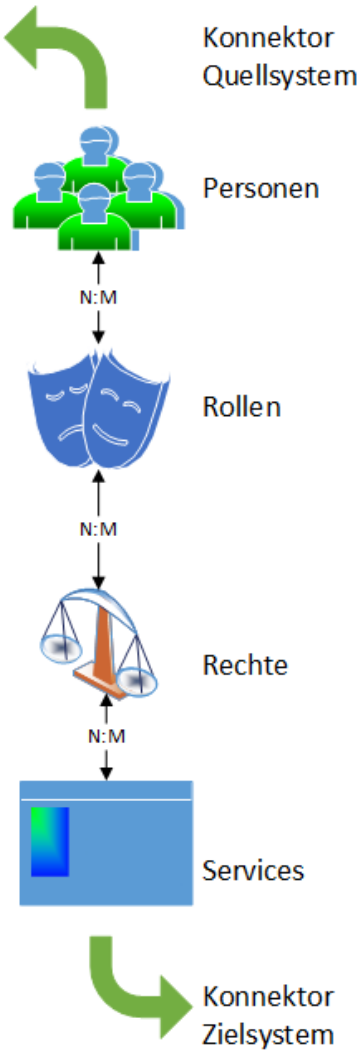
RHRK

26. März 2019

Identity- (und Access-) Management:

Die richtigen Personen haben zur richtigen Zeit den richtigen Zugriff auf die richtigen Ressourcen.

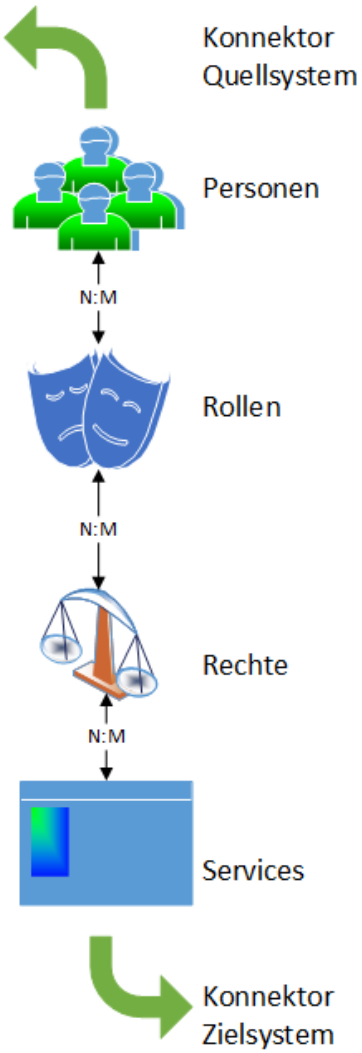

Studenten
Mitarbeiter
Klinikpersonal
Stadtbesucher
Externe, Sonstige und ganz Externe
Organisationsstruktur
IdM
LDAP, AD, Radius, ...
Mailserver
Druck- und Kopier-system
Schließsystem / Chipkarte
Telefon- / MA-verzeichnis



Personen: Identitäten
Wie identifiziert man eigentlich eine Person?

- Vorname, Nachname, andere Namensbestandteile
- Geburtsdatum und -ort
- MatrikelNummer, PersonalNummer, . . .

Person als eine Form von Objekten im IdM:
OUs, Gruppen, Rollen, Zielsystemaccounts, . . . ?



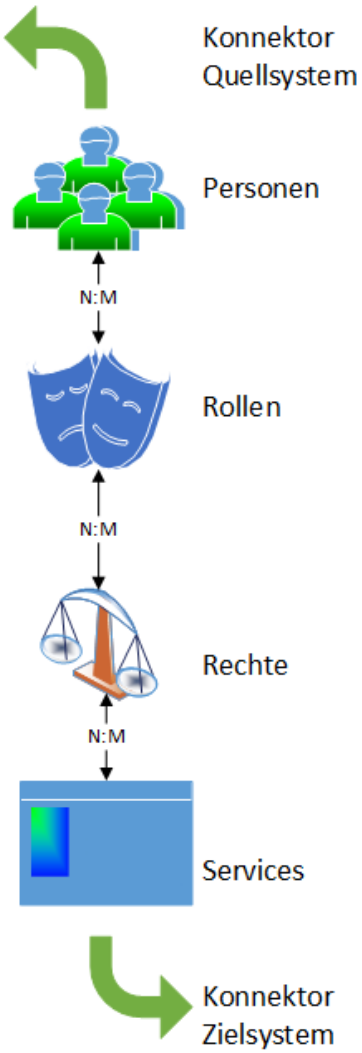
Rollen:

Professoren, (nicht)wiss. Mitarbeiter, Studenten, Promotionsstudenten, externe Doktoranden, Stipendiaten, Hiwis, nicht immatrikulierte Hiwis, Azubis, FSJ, FÖJ, Bufdi, Praktikanten, Gasthörer, Lehrbeauftragte, Privatdozenten, Honorarprofessoren, Gastdozenten, Vertretungsprofessoren, Gastwissenschaftler, Rentner, Mitarbeiter und Studenten von anderen Hochschulen, Alumni, Mitarbeiter von An-Instituten, Servicetechniker, Forschungspartner, Akkreditoren, Ehrensenatoren, Klinikpersonal, Kooperationspartner, Studentenwerk, Landesprüfungsamt, GmbHs und Vereine der Hochschule, abgeordnete Lehrer, Personen mit Werkvertrag,

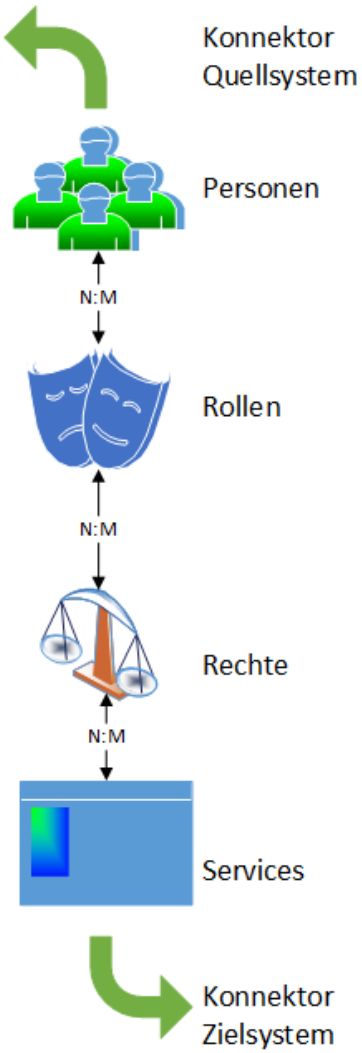
. . .

Susan Something nasty's happening tonight. I'm hoping he can tell me what it is, but he's got to be able to think straight first.
Mustrum Ridcully And you brought him *here*?

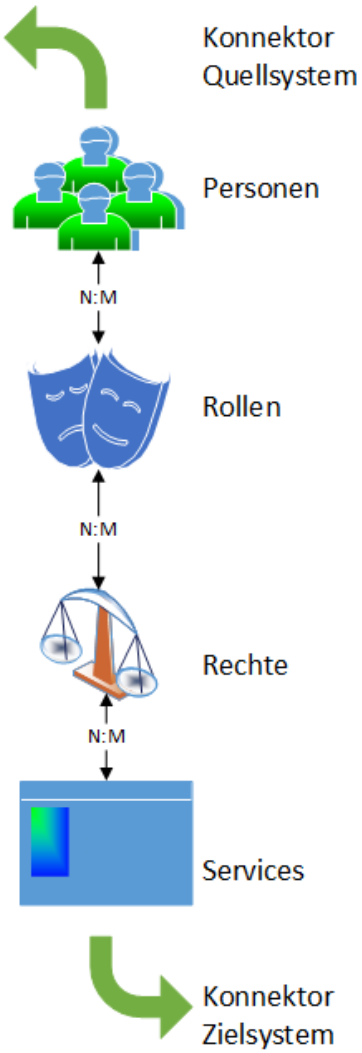
Terry Pratchett, *Hogfather*



Rollen:
OU-Leiter, Präsident, Gremienmitglieder, Prüfungsausschuß,
Mitglied des Fachbereichs X, Studiert X,
Dekan/Geschäftsführer von X,
Weiblich,
Projektbeteiligte,
studentische und andere Gruppen,
Stellvertreter, ...



Rechte:
Lesen (in beschränkten Bereichen?), Ändern, Neuanlegen, Löschen,
Entdecken, Suchen, Vergleichen (Authentifizierung), Ausführen



Services:

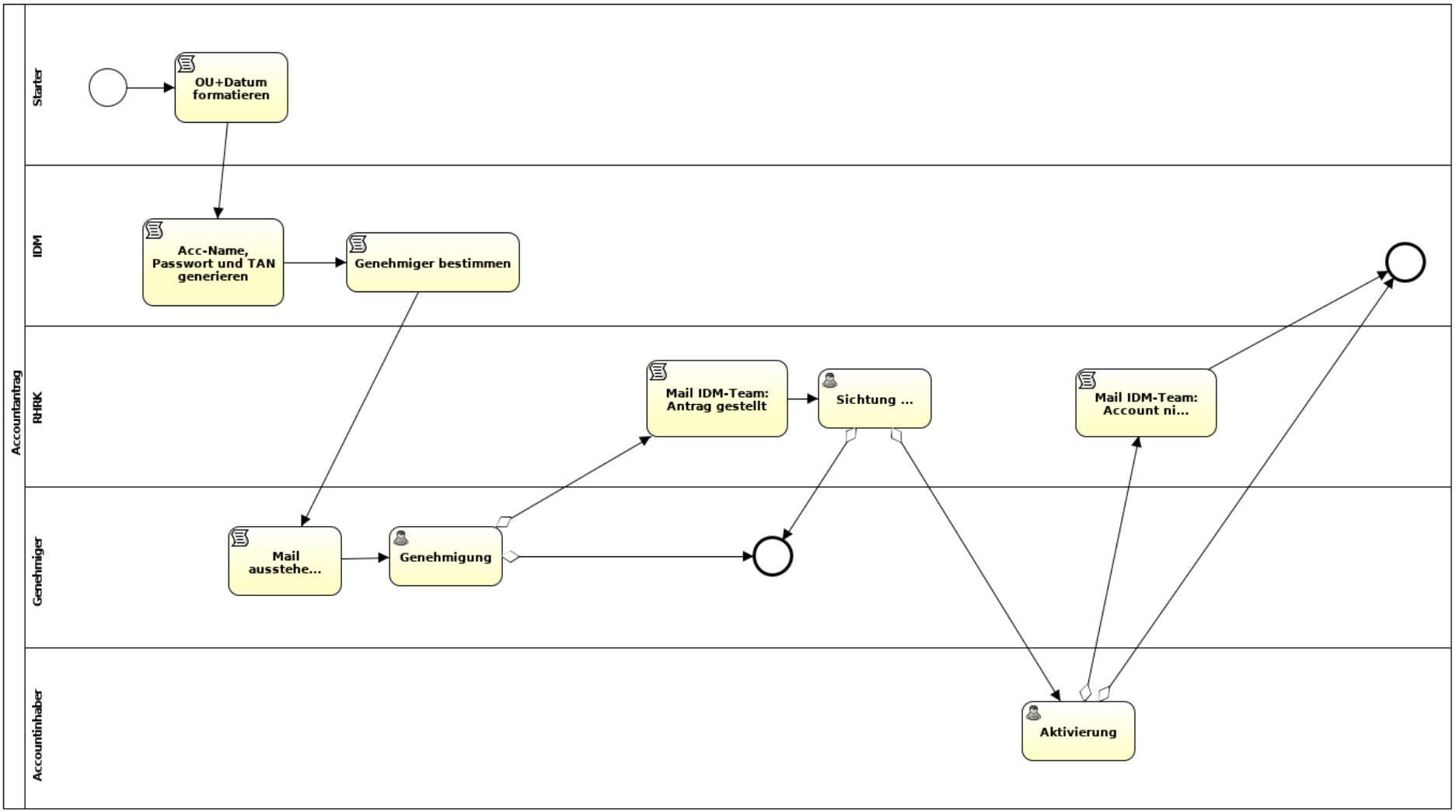
- Account-/ Attributtransformationen
- Reconciliation: Vergleich von Soll- und Ist-Zustand; lokale / verwaiste Accounts
- Admin-/ Manageraccount

→ Kooperation mit Zielsystemadmins!

Prozesse: am Beispiel „Accountlöschung“

- Wenn die Befristung ausläuft: Warnmail an den Benutzer verschicken.
- 14 Tage später: Account sperren.
- Einen Monat danach: Account löschen
  (und Löschprozesse auf den Zielsystemen auslösen).
- Maßnahmen, um aus dem Prozeß auch wieder auszusteigen.

Prozesse:


Accountantrag
Starter
IDM
RHRK
Genehmiger
Accountinhaber
OU+Datum formatieren
Acc-Name, Passwort und TAN generieren
Genehmiger bestimmen
Mail IDM-Team: Antrag gestellt
Sichtung ...
Mail IDM-Team: Account ni...
Mail ausstehe...
Genehmigung
Aktivierung

Prozesse: Typische „Hauptkriegsschauplätze“:

- Woher kommen die Daten?
- Welche Daten / Attribute kommen?
- Wann und wie oft kommen die Daten?
- Wie zuverlässig sind Aktualität und Qualität der Daten?
- Wer stößt unregelmäßige Änderungen (z. B. Versetzungen) an?
- Wer genehmigt oder bestätigt das jeweils?

Weitere Themen:

- Reporting und Audit
- Identity Matching
- IDs: ORCID, Edu-ID, Ausweise
- Gruppenverwaltung
- Userselfservice
- Passwortmanagement
- Authentifizierungsarten
- Föderierte Dienste
- SingleSignOn

Shibboleth.

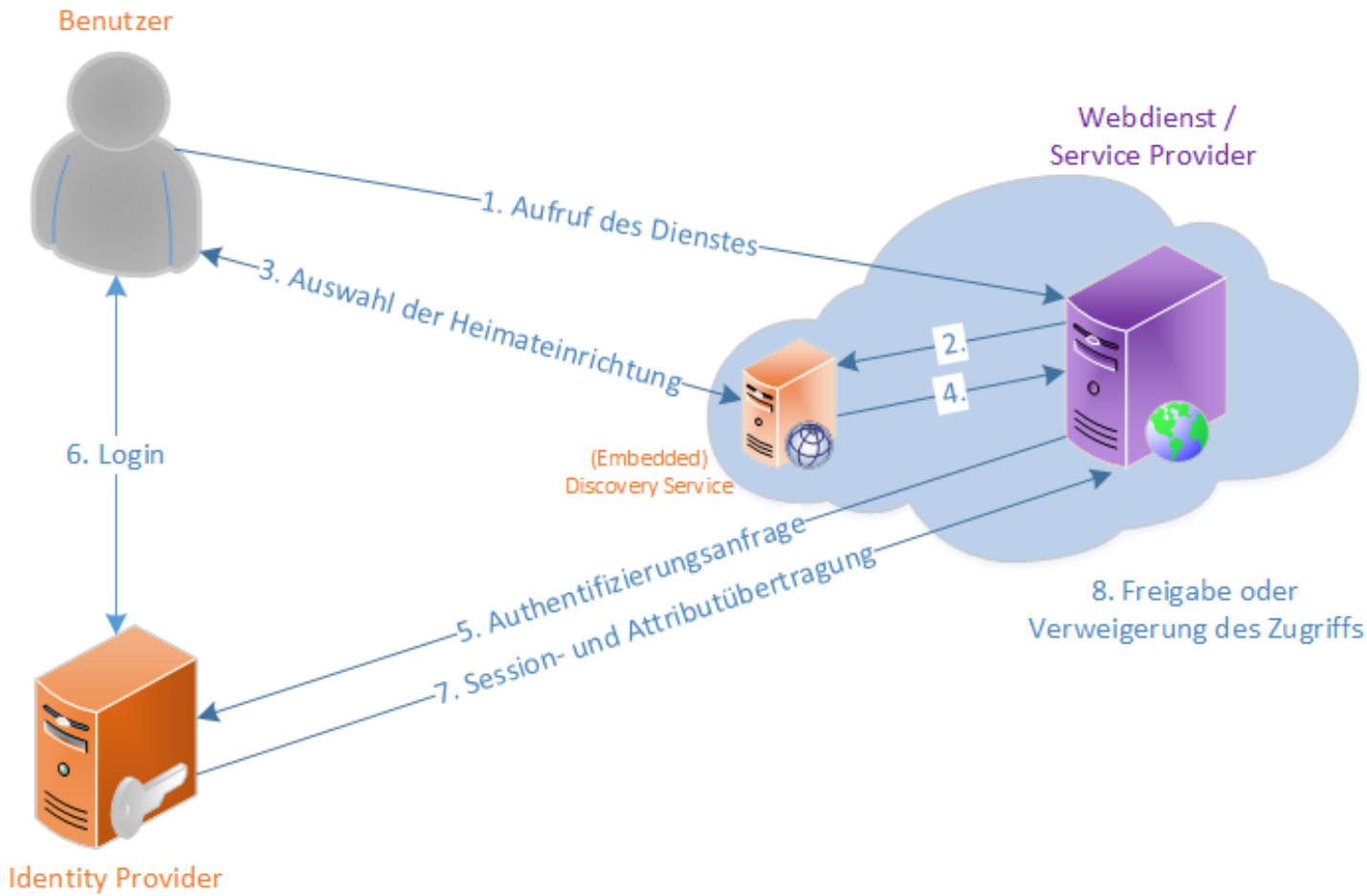
OpenSource Software zum Single Sign-on
(vor allem, aber nicht nur) für Webanwendungen
implementiert SAML (Security Assertion Markup Language)

INTERNET2®

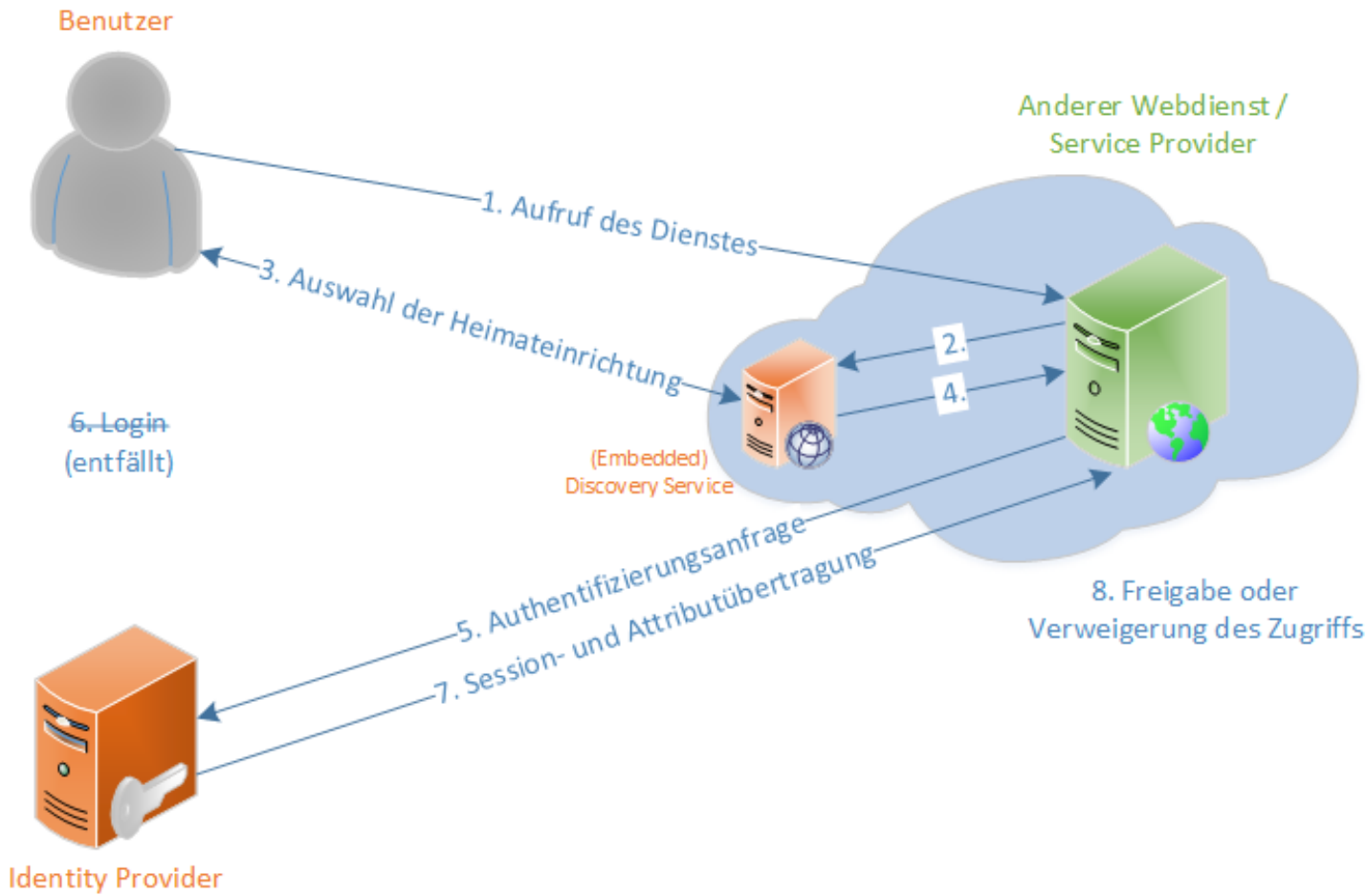
entwickelt von der Internet2-Initiative (`www.internet2.edu`),
unterstützt von einem internationalen Konsortium (DFN u. a.)

Wortherkunft:
hebräisch „Ähre“
alttestamentarisch
Buch der Richter

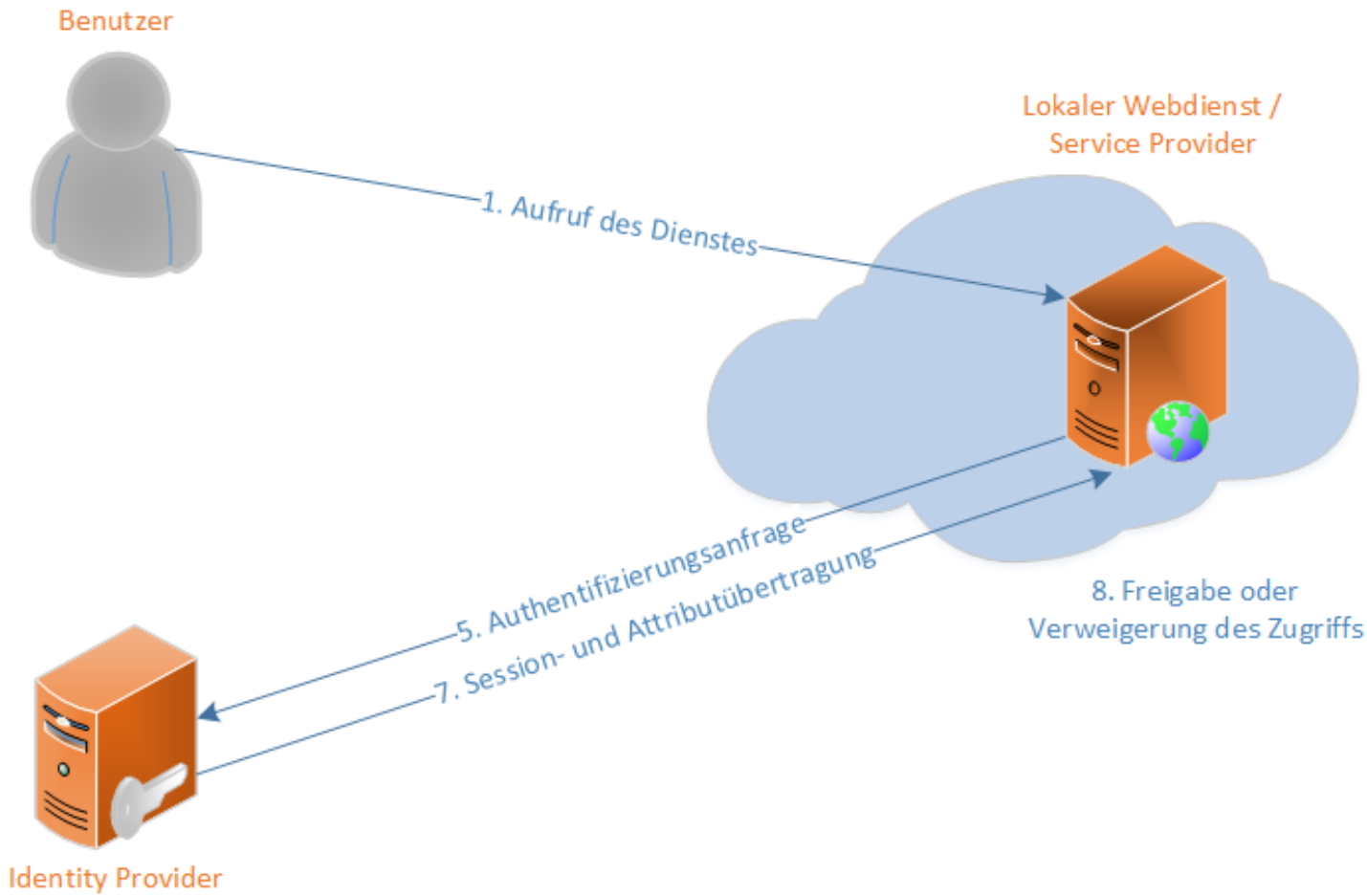
Ablauf


Benutzer
Webdienst /
Service Provider
1. Aufruf des Dienstes
3. Auswahl der Heimateinrichtung
2.
4.
(Embedded)
Discovery Service
6. Login
5. Authentifizierungsanfrage
7. Session- und Attributübertragung
8. Freigabe oder
Verweigerung des Zugriffs
Identity Provider

Ablauf – Single Sign-on



Ablauf


Benutzer
Lokaler Webdienst / Service Provider
1. Aufruf des Dienstes
5. Authentifizierungsanfrage
7. Session- und Attributübertragung
8. Freigabe oder Verweigerung des Zugriffs
Identity Provider

Drei typische Anwendungsfälle:

Beispielanwendung	Identifizierungsart	Attribut	Attributwert
eLearning Plattform	Identität	principalName	muster@uni-kl.de
Online Videothek	Pseudonym	persistentId	12Zw8wtuuFQt
Verlag	Gruppenmitgliedschaft	scopedAffiliation	member@uni-kl.de

persistent / pairwise / targeted ID: ist unterschiedlich pro Benutzer **und** SP, bleibt aber gleich über Sessions hinweg.

Wichtig: Autorisierung führt der SP durch!

Attribute

Schema	**Attribut**	**Wert**
inetOrgPerson	givenName	Frank
	sn	Stein
	uid	stein
	ou	Biologie
	displayName	Dr. Frank N. Stein
	mail	stein@bio.uni-kl.de, frank.stein@bio.uni-kl.de

Attribute

Schema	Attribut	Wert
eduPerson	eduPersonPrincipalName	stein@uni-kl.de
	eduPersonAffiliation	member
		employee, faculty, staff,
		student, affiliate, library-walk-in
	eduPersonScopedAffiliation	member@uni-kl.de
	eduPersonEntitlement	urn:mace:dir:entitlement:common-lib-terms
		http://rarp-kl.de/entitlement/hpc

Attribute

Schema	**Attribut**	**Wert**
SCHAC	schacDateOfBirth	18180101
	schacPersonalUniqueCode	urn:schac:personalUniqueCode:de:↵ uni-kl.de:Matrikelnummer:123456
dfnEduPerson	dfnEduPersonCostCenter	ABC/123
	dfnEduPersonStudyBranch1	01
AD	memberOf	...

Attribute

Sprechen Sie mit Ihrem örtlichen IdP-Admin darüber, welche Attribute zur Verfügung stehen und was bzw. wen sie bei Ihnen beinhalten!

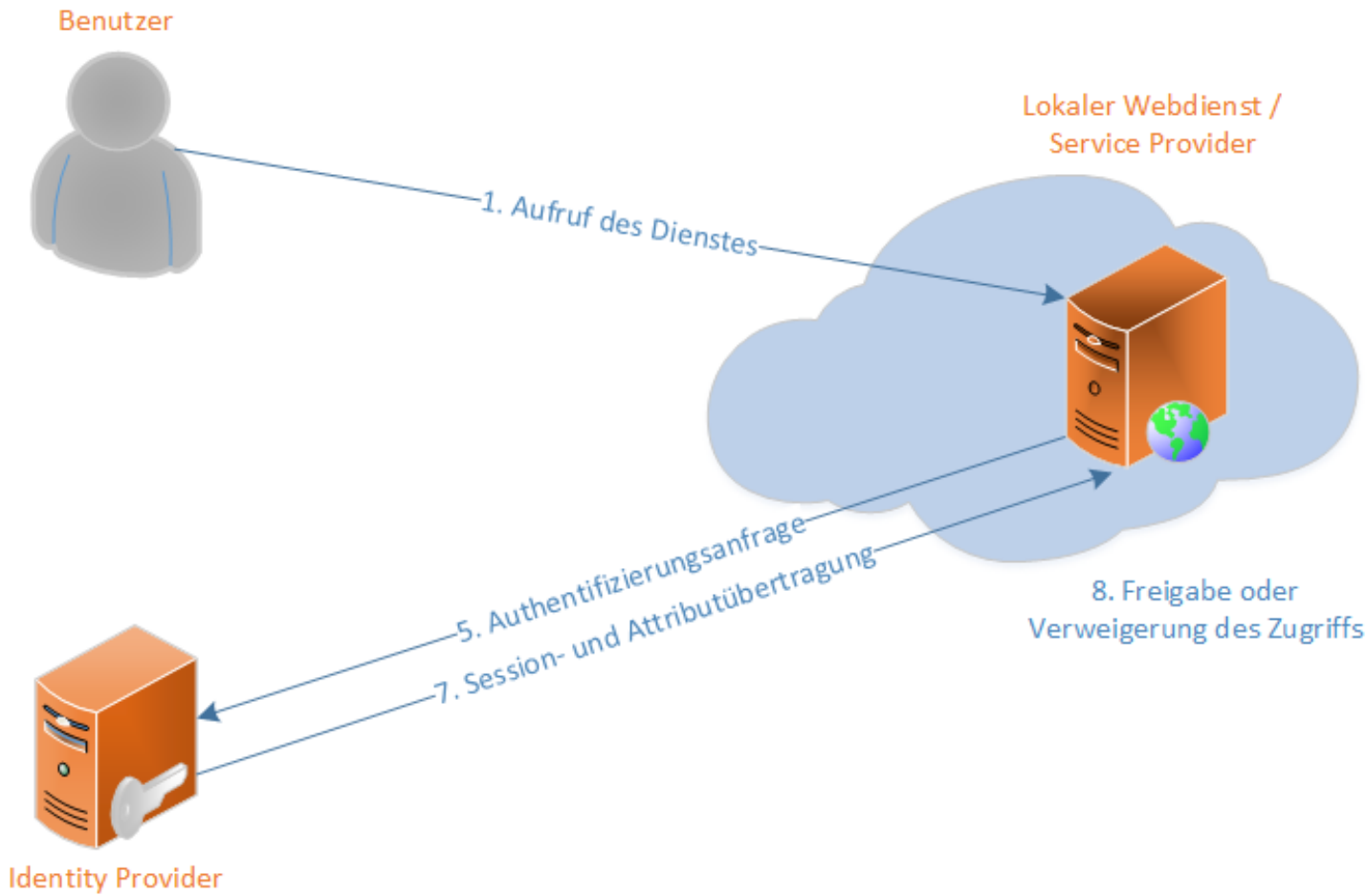
Vorteile für den Benutzer

- Keine Vielzahl von Accounts und Passwörtern
- Single Sign-on
- Phishing wird erschwert
- bei Verlagsangeboten u. ä.: keine Registrierung nötig, stattdessen anonyme/pseudonyme Nutzung
- standortunabhängig: keine VPN-Installation nötig, Webbrowser (oder SOAP-fähige Applikation) reicht $\Rightarrow$ geräteunabhängig
- Datenschutz: Benutzer wird zu übertragenen Attributen informiert und kann/muß ggfs. zustimmen
- Einbinden weiterer Authentifizierungsarten möglich: 2FA, X509, Kerberos, IP-Bereich

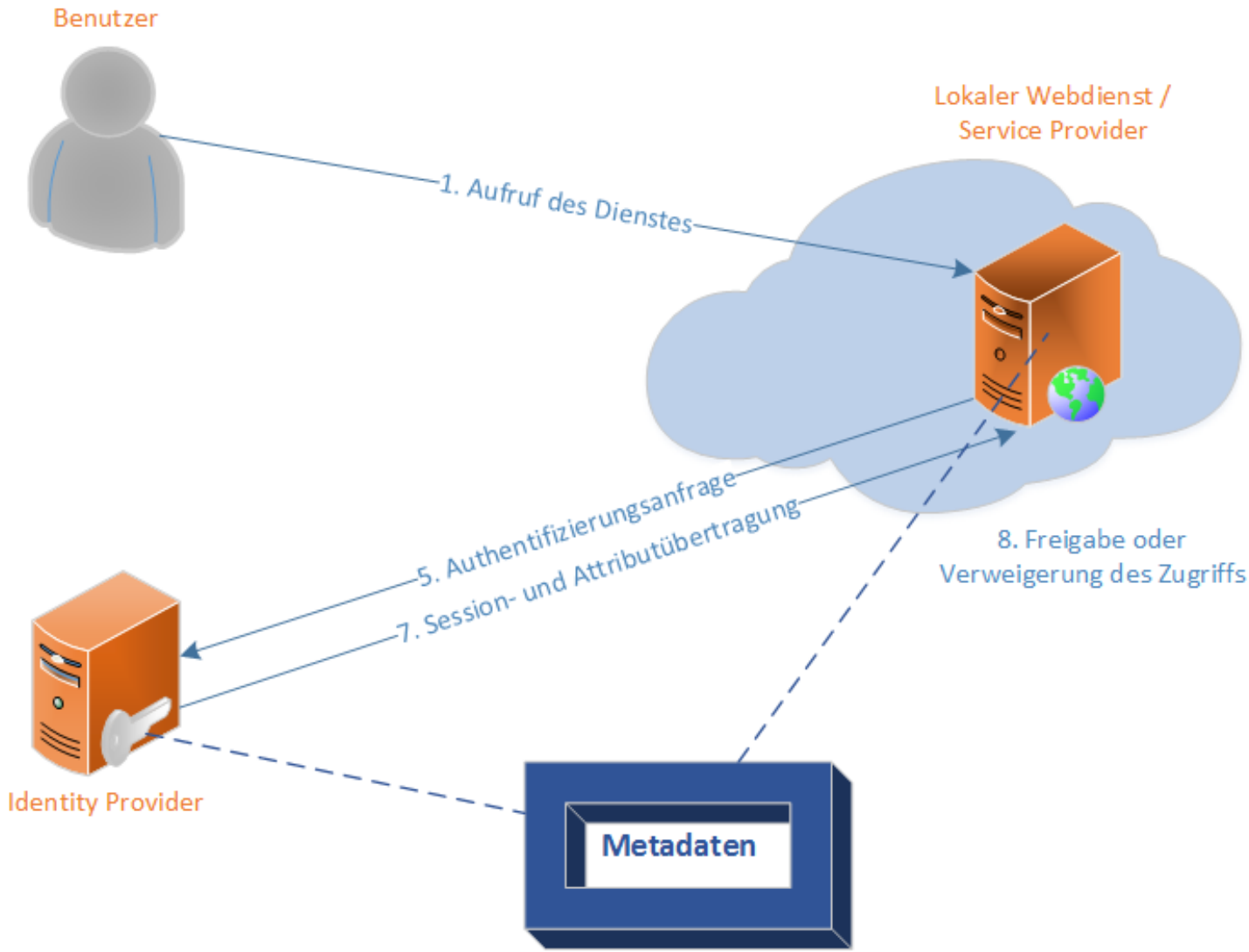
Vorteile für Dienstanbieter

- nutzt bewährte Software und etablierte Standards (SAML, SOAP, TLS, XML)
- keine eigene Accountverwaltung (oder Pflege von IP-Listen) nötig
- kein Rücksetzen von vergessenen Passwörtern
- Passwörter tauchen nicht mal flüchtig im Anwendungssystem auf
- auch anonyme/pseudonyme Nutzung möglich (Umfragen)
- vergleichsweise geringer Aufwand bei der Integration in die eigene Webanwendung
- einfache Nutzung über Einrichtungsgrenzen hinweg möglich
- automatische Übertragung von Attributen zur Autorisierung: Korrektheit durch Föderationsvertrag gesichert

Nochmal: Bestandteile



Nochmal: Bestandteile



Föderation – AAI

DFN betreibt die Föderation
(AAI: Authentifikations- und Autorisierungs-Infrastruktur)
und deren Metadatenverwaltung: das „Adreßbuch“ der Föderation:

- rechtlich: Schaffung eines Vertrauensverhältnisses zwischen den Teilnehmern
- organisatorisch: Verwaltung der Ansprechpartner
- technisch: gegenseitiges Bekanntmachen von Zertifikaten und URLs

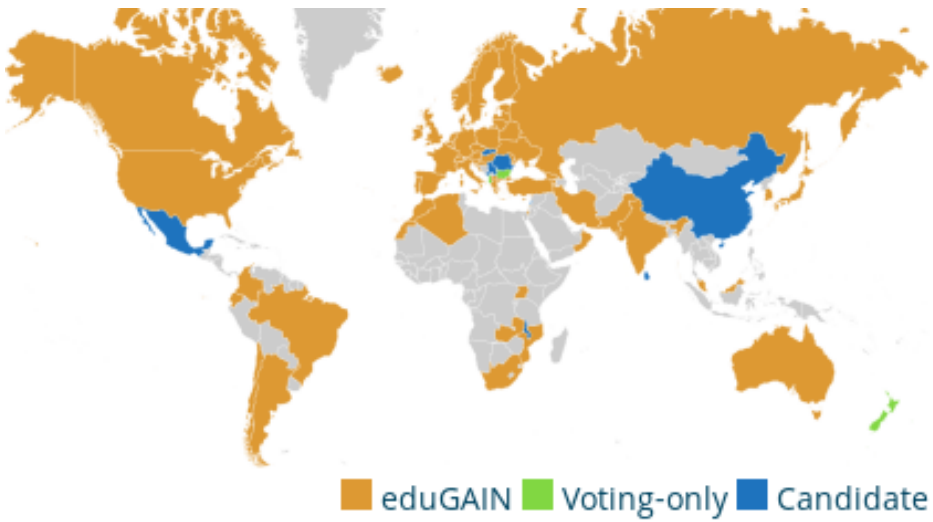
Teilnehmer verpflichten sich zur Einhaltung von Spielregeln:

- Datenqualität des IdM
- standardisierte Attributschemata
- Datenschutz und Datensparsamkeit

Incident Response (SIRTFI: Security Incident Response Trust Framework for Federated Identity)

Föderationen

- DFN: 2 Verläßlichkeitsklassen + Testföderation
- Lokale Föderation einer Hochschule
- Regionale Föderation: RARP, bwIdm
- Staatenübergreifend: edugain



~~Nachteile~~ Potentielle Probleme

- Single Point of Failure
- Passwort muß entsprechend geschützt werden.
- Vertraglich zugesicherte Qualität des IdM muß auch eingehalten werden.
- Neues Konzept: Föderation/Metadaten, SSO-Konsequenzen
- Einarbeitungszeit und Konfigurationsarbeit für Admins
  (wird durch die sehr gute Community wieder wettgemacht).

SP: Webserver-Konfiguration

Debian Paket `libapache2-mod-shib2`

```
<Location /alle>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  Require shib-session
</Location>

<Location /mitarb>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  Require shib-attr affiliation ~ ^staff@ ^employee@ ^faculty@
</Location>
```

Zertifikatsprofil „Shibboleth IdP SP“!

SP Konfiguration

Wichtigste Elemente in `/etc/shibboleth/shibboleth2.xml`:

```
<ApplicationDefaults
      entityID="https://sp.example.org/shibboleth"

<SSO  entityID="https://idp.example.org/idp/shibboleth">
<SSO  discoveryProtocol="SAMLDS"
       discoveryURL="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf"

<Handler  type="Status"  Location="/Status"
      acl="127.0.0.1  ::1  93.184.216.34" />

<MetadataProvider  type="XML"
      uri="https://www.aai.dfn.de/fileadmin/metadata/
        DFN-AAI-Local-000-metadata.xml"

<CredentialResolver  type="File"
      key="/etc/ssl/private/key.pem"
      certificate="/etc/ssl/localcerts/cert.pem" />
```

Ggfs. `attribute-map.xml` für zusätzliche Attribute

Angaben in Metadaten

Örtlicher Metadatenverwalter braucht Informationen über den SP:
Technische Details: Metadaten-Generator
Desweiteren:

- Displayname
- Beschreibung
- URL Informationsseite
- URL Datenschutzerklärung
- URL Logo
- Helpdesk
- Ansprechpartner: administrativ, technisch, support, security

Daten sieht der Benutzer auf UserConsent-Seite oder im Diensteverzeichnis.

Sessioninformationen

Sessionseite des SPs:

https://sp.example.org/Shibboleth.sso/Session

phpinfo():

Apache Environment

Variable	Value
Shib-Application-ID	default
Shib-Session-ID	_2c830cf829b52e8fedad86b5bde7b25e
Shib-Identity-Provider	https://idptest.rhrk.uni-kl.de/idp/shibboleth
Shib-Authentication-Instant	2019-03-14T14:20:14.865Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Session-Index	_c60b74eb416c1760dfe5e2bc39e4b177
affiliation	student@uni-kl.de;member@uni-kl.de
displayName	test stud
eduPersonTargetedId	https://idptest.rhrk.uni-kl.de/idp/shibboleth!https://sptest.rhrk.uni-kl.de/shibboleth!pySty8z4L797p3B8BrDgileoWn4=
entitlement	urn:mace:dir:entitlement:common-lib-terms
eppn	teststud@uni-kl.de
o	Technische Universitaet Kaiserslautern
persistent-id	https://idptest.rhrk.uni-kl.de/idp/shibboleth!https://sptest.rhrk.uni-kl.de/shibboleth!pySty8z4L797p3B8BrDgileoWn4=
schacPersonalUniqueCode	urn:schac:personalUniqueCode:de:uni-kl.de:Matrikelnummer:999998
unscoped-affiliation	member;student
HTTPS	on
SSL_TLS_SNI	sptest.rhrk.uni-kl.de
SSL_SERVER_S_DN_C	DE

Embedded Discovery Service

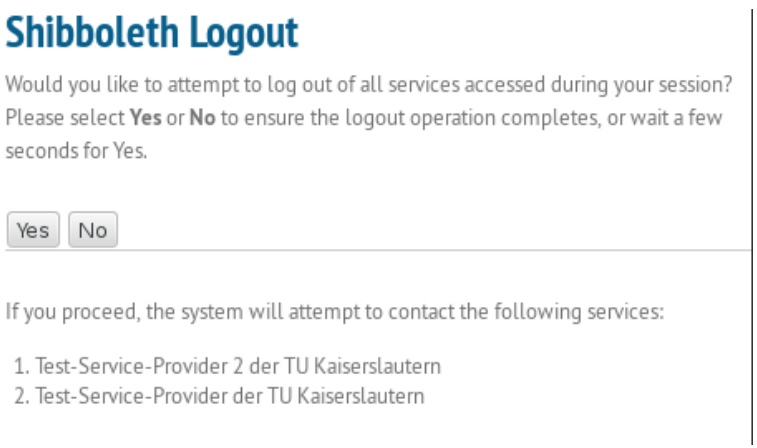
Kleines Paket aus Javascript- und CSS-Dateien zur Einrichtungsauswahl

Auswahlliste durch Metadatenfilterung (z.B. Whitelist, Entity-Category)
https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service

(Single-)Logout

Sessions: IdP, SP ↔ Anwendung, andere Anwendungen?

- SP- und Anwendungssession möglichst zusammenführen
- Logout vorsehen (Achtung: Automatisches Re-Login!)
- Logout erst in der Anwendung durchführen, dann Logout an SP weiterreichen: `https://sp.example.org/Shibboleth.sso/Logout`
- In der Lage sein, Logouts vom IdP entgegenzunehmen



`https://doku.tid.dfn.de/de:shibslo`

Zertifikatswechsel

- Zertifikat darf nicht einfach nur am Server und in der SP-Konfiguration ausgetauscht werden.
- Eintragen des neuen Zertifikats in der Metadatenverwaltung zum gegenseitigen Bekanntmachen.
- Mehrstufiger Prozeß:
  https://doku.tid.dfn.de/de:certificates#zertifikatstausch

Datenbereinigung

Wie werde ich die gesammelten Daten wieder los? (DSGVO!)
Woher weiß ich, wann ich einen Benutzer wieder löschen kann?
Auch dafür den IdP benutzen:

- https://doku.tid.dfn.de/de:shibidp3userdepro
- AAI-Forum auf der 70. DFN-Betriebstagung

Infoquellen

- DFN-AAI https://www.aai.dfn.de/
- DFN-AAI-Wiki https://doku.tid.dfn.de/de:dfnaai:start
  - Attribute https://doku.tid.dfn.de/de:attributes
  - Materialien aus Veranstaltungen https://doku.tid.dfn.de/de:shibidp3documents

  (Vielen Dank an alle, die etwas dazu beitragen!)
- Shibboleth-Consortium https://www.shibboleth.net/
- SP-Konfiguration:
  - DFN-Wiki https://doku.tid.dfn.de/de:shibsp
  - Switch https://www.switch.ch/aai/guides/sp/
  - Offizielles Wiki https://wiki.shibboleth.net/confluence/display/SP3/Home
- DFN-Diensteverzeichnis https://www.aai.dfn.de/verzeichnis/