deutsches forschungsnetz

Dienste in der DFN-AAI – Datenschutzaspekte

HÜF 09.002 Datenschutz-Erfahrungsaustausch II | 6. Juni 2019

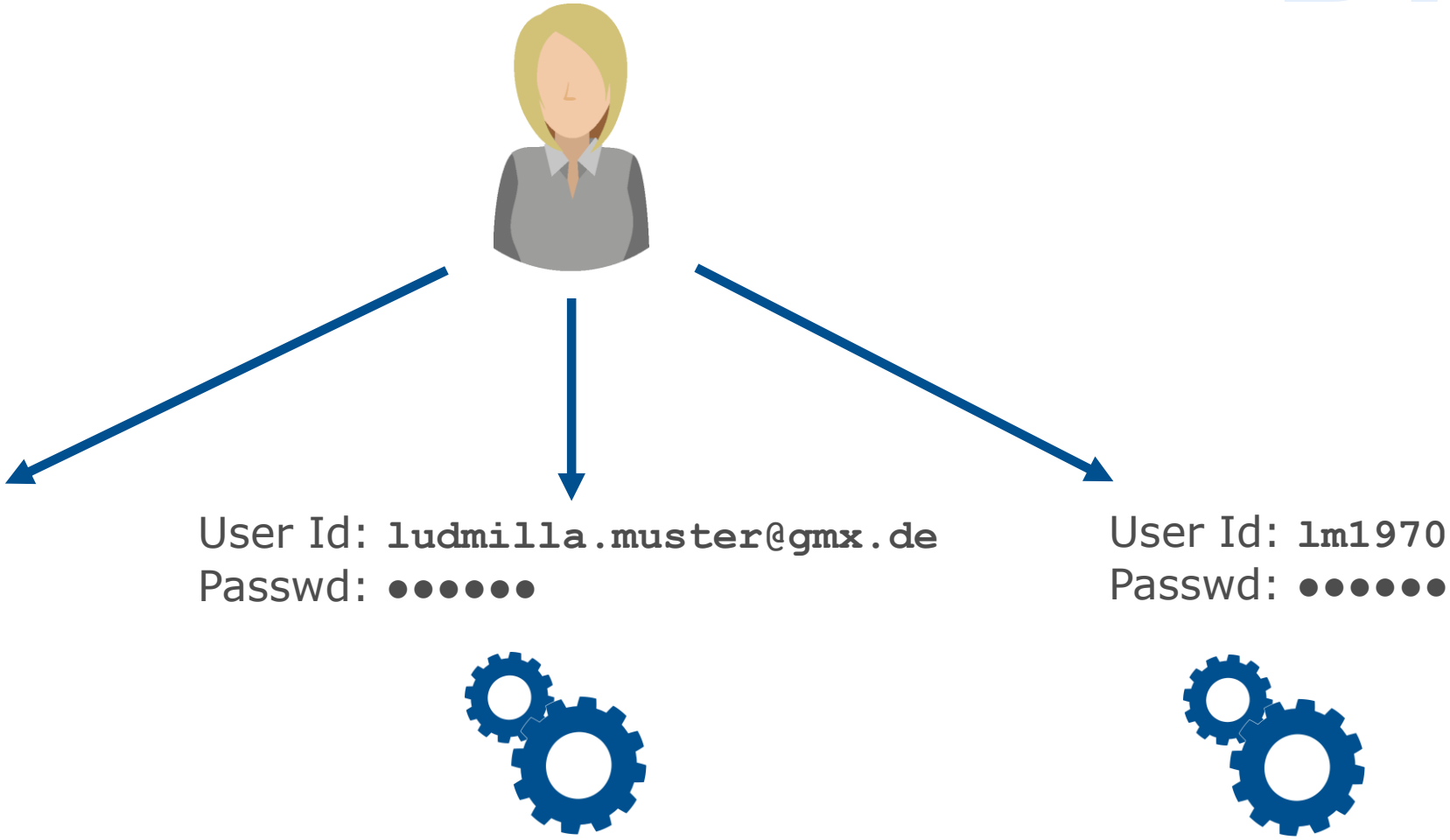
Wolfgang Pempe (pempe@dfn.de)

Einführung und Überblick DFN-AAI

Begriffsbestimmung

- **AAI** = **A**uthentication and **A**uthorization **I**nfrastructure
- AAI bildet den technischen und organisatorischen Rahmen für föderiertes Identity Management
- **Föderiertes Identity Management:**
  - Austausch von Identitätsdaten über Dienst- und Organisationsgrenzen hinweg
  - Keine dienstspezifischen Identitäten
  - Eine Identitätsquelle als führendes System
- Voraussetzung für (Web-)SSO, (Web) **S**ingle **S**ign-**O**n
  - Einmal anmelden für 1..n Dienste, für die man zugriffsberechtigt ist

Dienstspezifische Identitäten



Föderierte Identität

User Id: `lmuster`
Passwd: ••••••

Heimateinrichtung

Online Shop XY

Datenbankanbieter YZ

Verlag WX

Föderation

- Eine AAI kann lokal oder auch einrichtungsübergreifend betrieben werden
- Im letztgenannten Fall bedarf es einer zentralen Instanz, die als AAI-Betreiber die Einhaltung der technischen und rechtlichen Rahmenbedingungen sicherstellt und auf diese Weise ein Vertrauensverhältnis etabliert
- Dies ist in der Regel eine sog. Identity Federation, bzw. einfach „Föderation“
- Eine solche Föderation ist z.B. die **DFN-AAI**

Worum geht es in der (DFN-)AAI?

- Zugriff auf **Dienste** via
  - Web-SSO
  - (Non-Web-SSO)
- Technisch: **Metadaten**
- Organisatorisch: **Vertrauen**
- **Zusammenarbeit** lokal, aber v.a. auch über Einrichtungs- und ggf. Föderations-Grenzen hinweg
- Datenschutz bzw. **Datensparsamkeit:** Nutzername + Passwort werden nicht an Dienste übertragen (u.a.m.)

Dienste und Nutzergruppen

2007 → heute

„Content Provider" (Verlage, Datenbanken) – Springer, Elsevier, etc.

Verteilung lizenzierter Software – Microsoft Dreamspark, Kivuto, etc.

E-Learning – Moodle, Bildungsportal Sachsen, VHB, etc.

Speicher-, Kommunikationsdienste – Gigamove, WebConf …

Landesdienste – bwIDM, SaxID, sciebo, hessenbox, …

E-Research – CLARIN, DARIAH, ELIXIR …

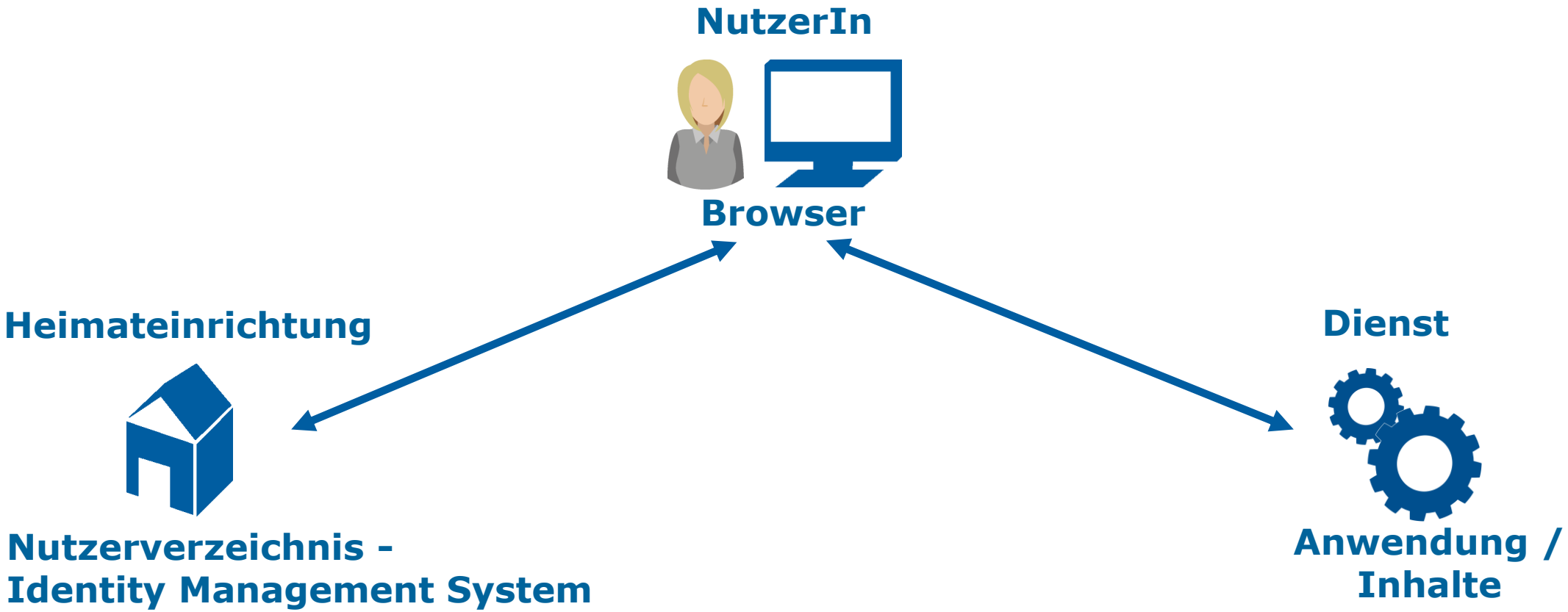
Internat. Forschungscommunities (→ eduGAIN)

Bibliotheksnutzer*Innen

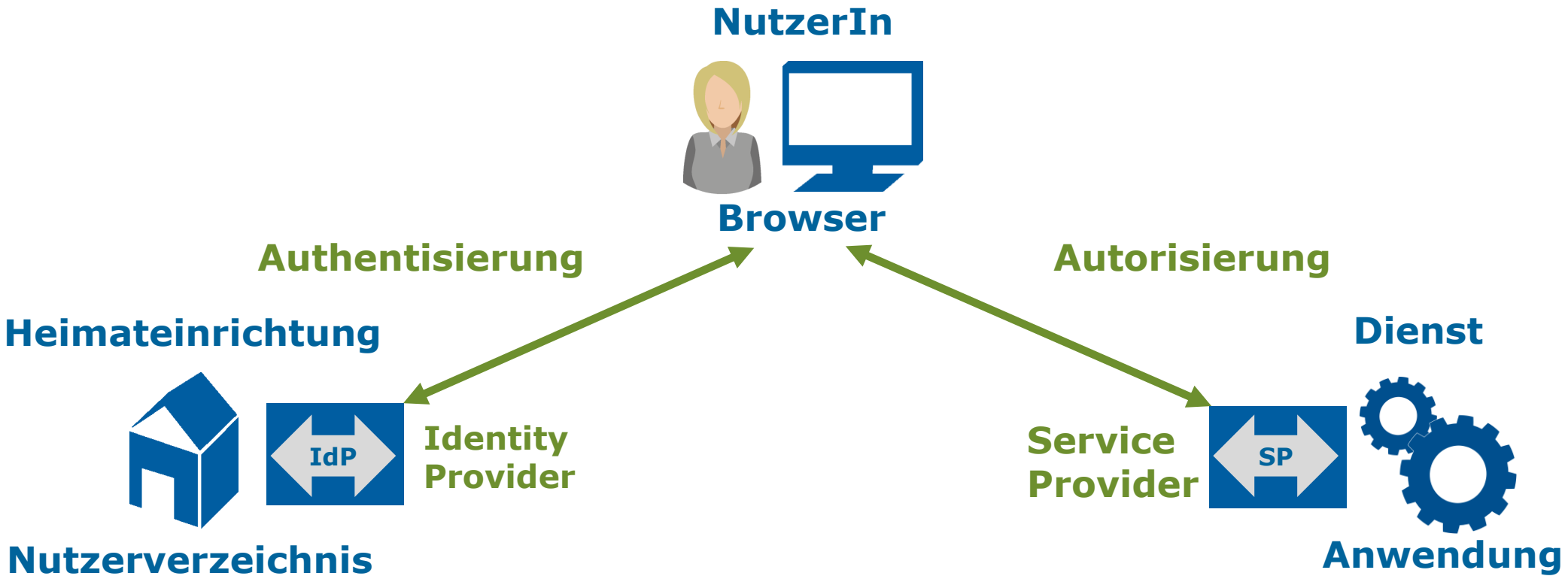
Studierende, Lehrpersonal

Forschende

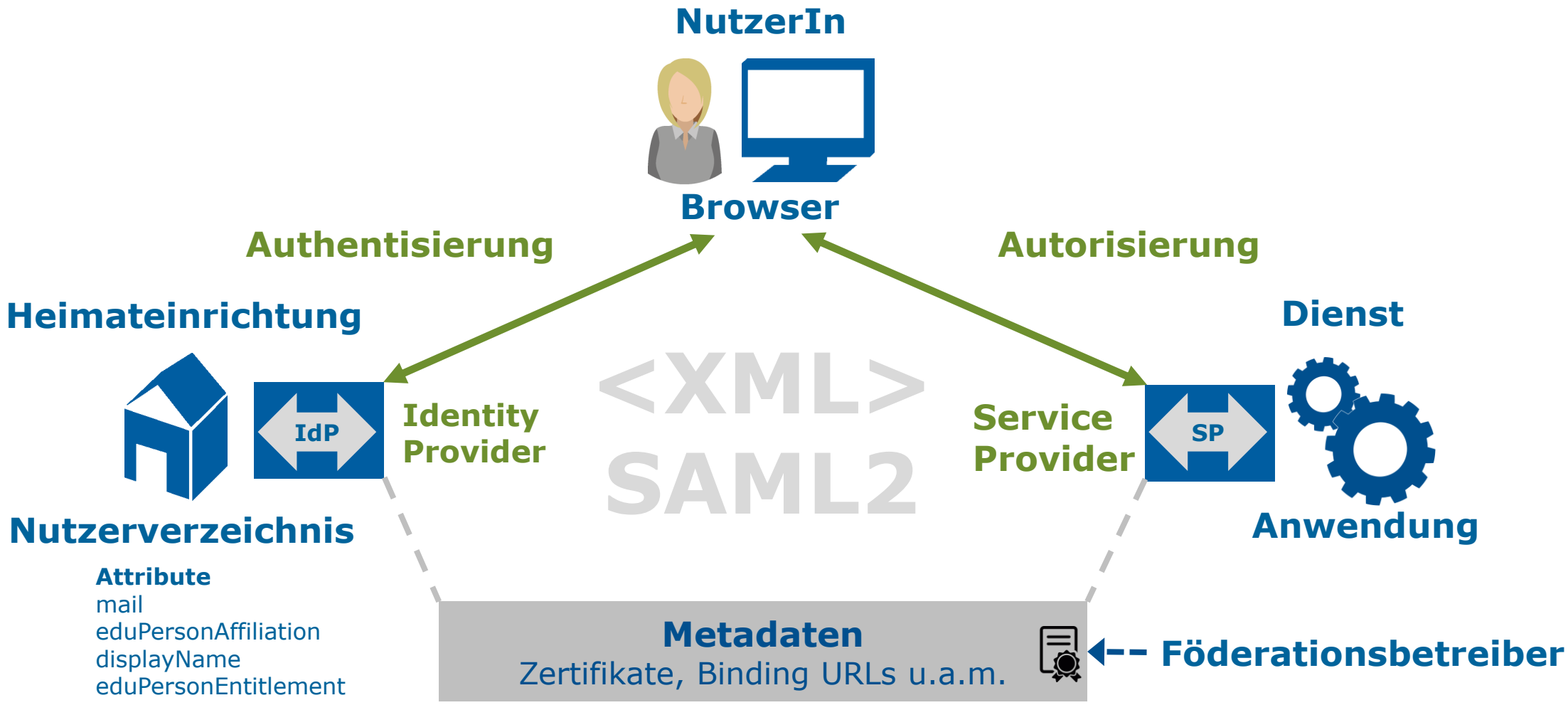
Web-SSO = Dreiecksbeziehung



Dreiecksbeziehung im Detail



Lingua franca: SAML (bzw. SAML2)



Siehe auch: https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

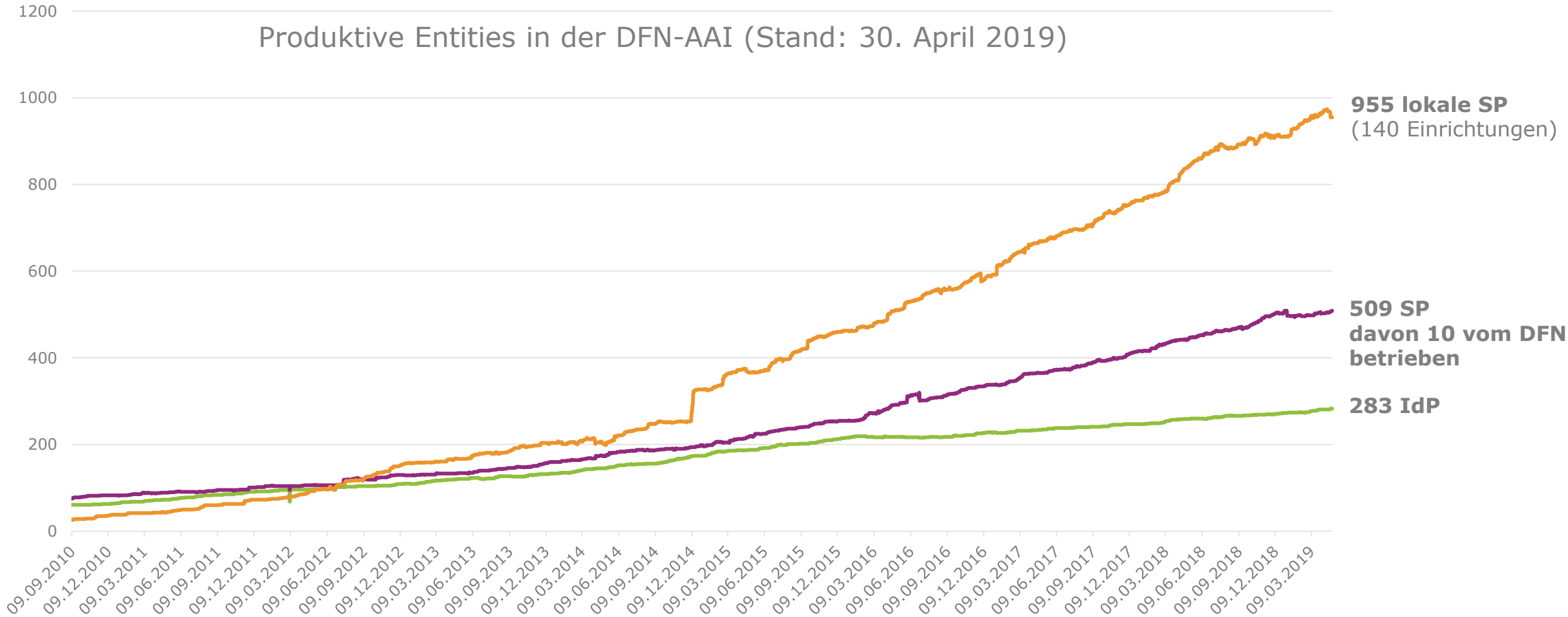
SAML und SAML Metadaten

- Steht für: **S**ecurity **A**ssertion **M**arkup **L**anguage
- XML-Framework (offener Standard bei OASIS), das aus mehreren Spezifikationen besteht
- Die wichtigsten Komponenten:
  - **Metadata**
  - **Assertions** + Protocols
  - Bindings
  - Profiles
- **Metadaten** enthalten alle Informationen, die für eine sichere Kommunikation zwischen den beteiligten Entities (IdPs, SPs) benötigt werden

Metadaten und Föderation

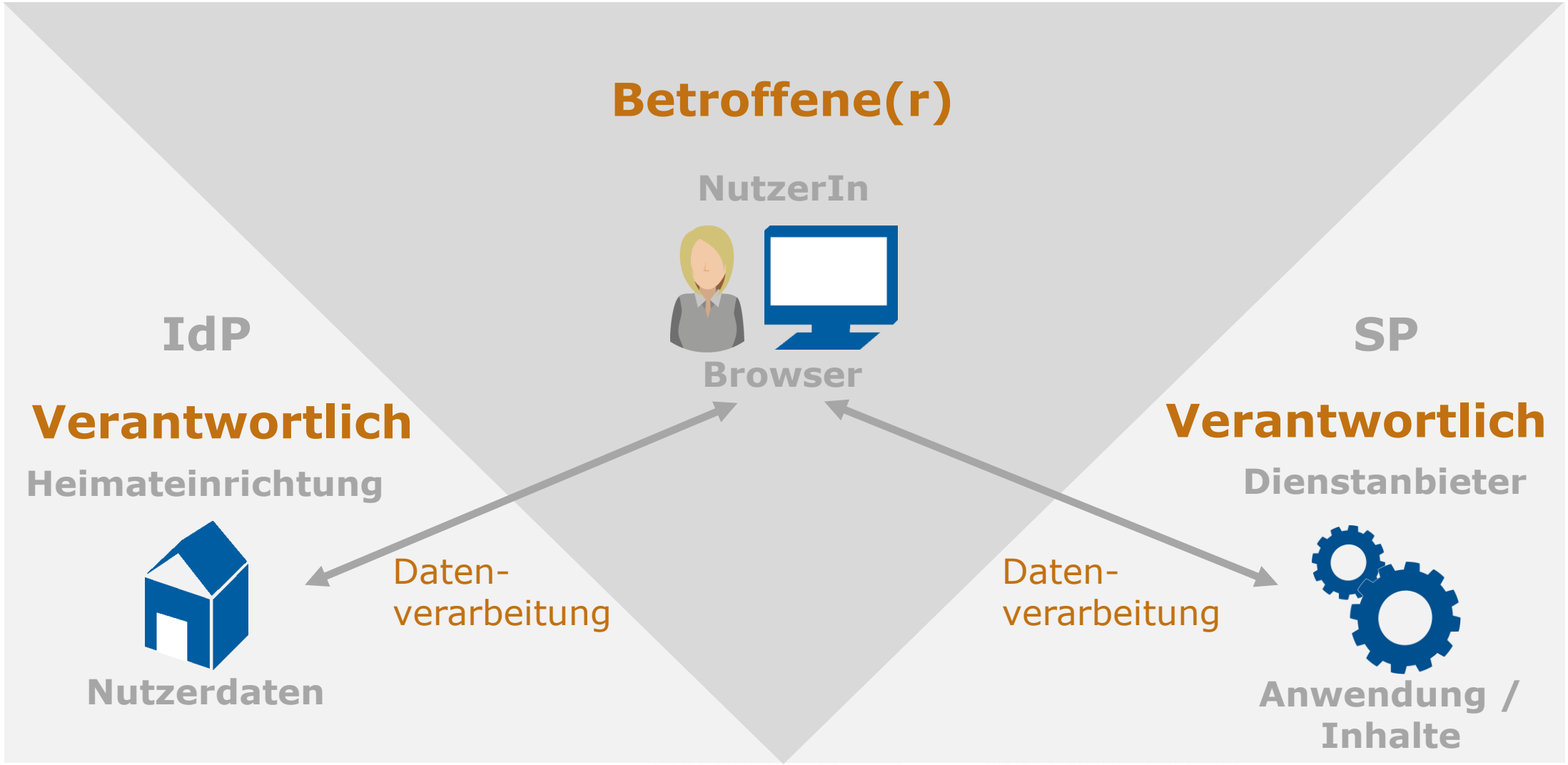
- Das **technische** Rückgrat einer Föderation stellen die Metadaten dar:
  Nur wenn auf beiden Seiten (IdP, SP) die Metadaten des jeweiligen Kommunikationspartners bekannt sind (und ihnen vertraut wird!), funktioniert die Kommunikation!
- Der **DFN** als Föderationsbetreiber schafft das notwendige **Vertrauensverhältnis**:
  - Verträge mit allen Teilnehmern
  - Metadatenverwaltung
    - Zertifikatprüfung und –überwachung (u.a.m.)
    - Signierte Metadaten

Aktuelle Zahlen DFN-AAI



Datenschutzaspekte AAI

Datenschutz – Rollen

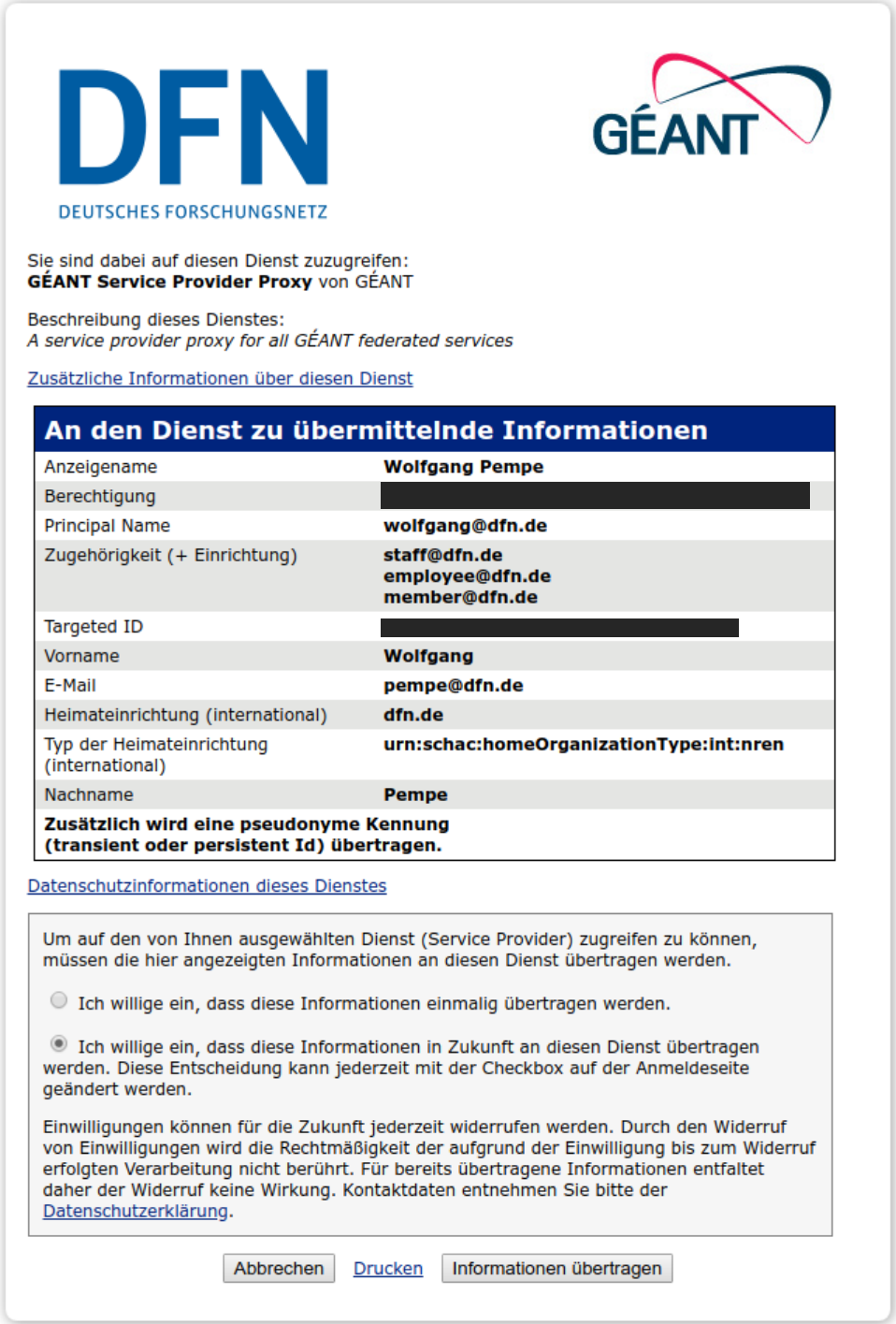


IdP-Betreiber

- Im AAI-Kontext werden Nutzerdaten auf folgende Weisen verarbeitet:
  - Authentifizierung des Nutzers / der Nutzerin (üblicherweise Username + Passwort)
  - Ggf. Attributfreigabe an den anfragenden SP (Redirect über Browser)
- Aktuelle IdP-Software wie Shibboleth bietet Möglichkeit zur Information und Einwilligung (und ggf. Widerspruch) der Endnutzer*innen
  - Datenschutzerklärung und ggf. Nutzungsbedingungen des IdP
  - Anzeige von Informationen zum SP inkl. Datenschutzerklärung (kommen aus Föderationsmetadaten)
  - Anzeige der zur Nutzung des Dienstes/SP erforderlichen Attribute
  - Einwilligung zur Freigabe/Übertragung der Attribute
  - Dokumentation der Einwilligung

IdP – User Consent Modul

- Anzeige der zu übertragenden Daten
- Ggf. Informationen zur Rechtsgrundlage, aufgrund derer die Datenübertragung erfolgt
- Ggf. Hinweis auf Widerspruchsrecht
- Anzeige von Informationen zum empfangenden SP (aus den Metadaten)
  - Name, Beschreibung
  - URL/Link zu weiteren Informationen
  - URL zur Datenschutzerklärung



IdP – Datenübertragung

Forschungsstelle Recht im DFN:

- Rechtsgrundlage ist in den meisten Fällen Art. 6.1 lit. a) DSGVO
- Bei hochschulinternen Diensten (IdP- und SP-Betreiber i.d.R. identisch) kann auch Art, 6.1 lit. e) oder f) zum Tragen kommen (dann Hinweis auf Widerspruchsrecht gem. Art. 21)
- In manchen Fällen auch Art. 88 in Verbindung mit § 26 BDSG (kein Widerspruchsrecht)

Entsprechend ist das User Consent Modul anzupassen, technische Umsetzung: https://doku.tid.dfn.de/de:shibidp3consent_dsgvo

Wichtig: Zweck der Datenübertragung ist die Anmeldung und Nutzung des ausgewählten Dienstes (SP). Die Datenverarbeitung durch den Dienstanbieter (SP-Betreiber) bleibt davon unberührt!

SP-Betreiber

- Eigener Verantwortlicher im Sinne der EU-DSGVO, sofern nicht mit IdP-Betreiber identisch (d.h. nicht die selbe juristische Person)
- Direkte Rechtsbeziehung zu Endnutzer(in)
- Tatbestand der Auftragsverarbeitung innerhalb der DFN-AAI **i.d.R.** nicht gegeben (wenige Ausnahmen); Szenario eher innerhalb lokaler, d.h. hochschulinterner Föderationen oder auf Landesebene denkbar
- Eigene Dienst-/SP-spezifische Datenschutzerklärung obligatorisch
- Als Rechtsgrundlage der Datenverarbeitung wird häufig Art. 6.1 lit. f) angenommen. Letztendlich abhängig vom Einzelfall.

Gemeinsame Verantwortung? (Art. 26)

- Bei der vom DFN-Verein betriebenen Föderation DFN-AAI handelt es sich um keine technische Infrastruktur (im Gegensatz zu Facebook o.ä.), IdP und SP kommunizieren direkt miteinander bzw. über den Browser des Nutzers (DFN schafft lediglich das Vertrauensverhältnis)
- I.d.R. Getrennte Verarbeitung und getrennte Verantwortlichkeiten
  - IdP: Freigabe von Nutzerdaten (auf Anforderung des Nutzers / der Nutzerin)
  - SP: Verarbeitung von Nutzerdaten zur Erbringung des Dienstes
- Zweck und Mittel (modulo Übertragungsprotokoll) der Verarbeitung werden getrennt festgelegt
- Derzeit ca. 300 IdP und ca. 500 SP (327 Betreiber): Skalierung?

Fazit

- Die Struktur der DFN-AAI sorgt für eine klare klare Trennung von Verantwortlichkeiten
- Im Standardfall (Datenübertragung via SAML) keine gemeinsame Verantwortung und keine Auftragsverarbeitung
- Beurteilung, welcher Sachverhalt vorliegt, muss im Einzelfall erfolgen …
  - … insbesondere dann, wenn nur Teilaspekte eines Dienstes über die AAI bedient werden (z.B. DFN Mailsupport, PVP NRW)
  - … und spezielle vertragliche Regelungen zwischen Dienstanbieter und Heimateinrichtung bestehen

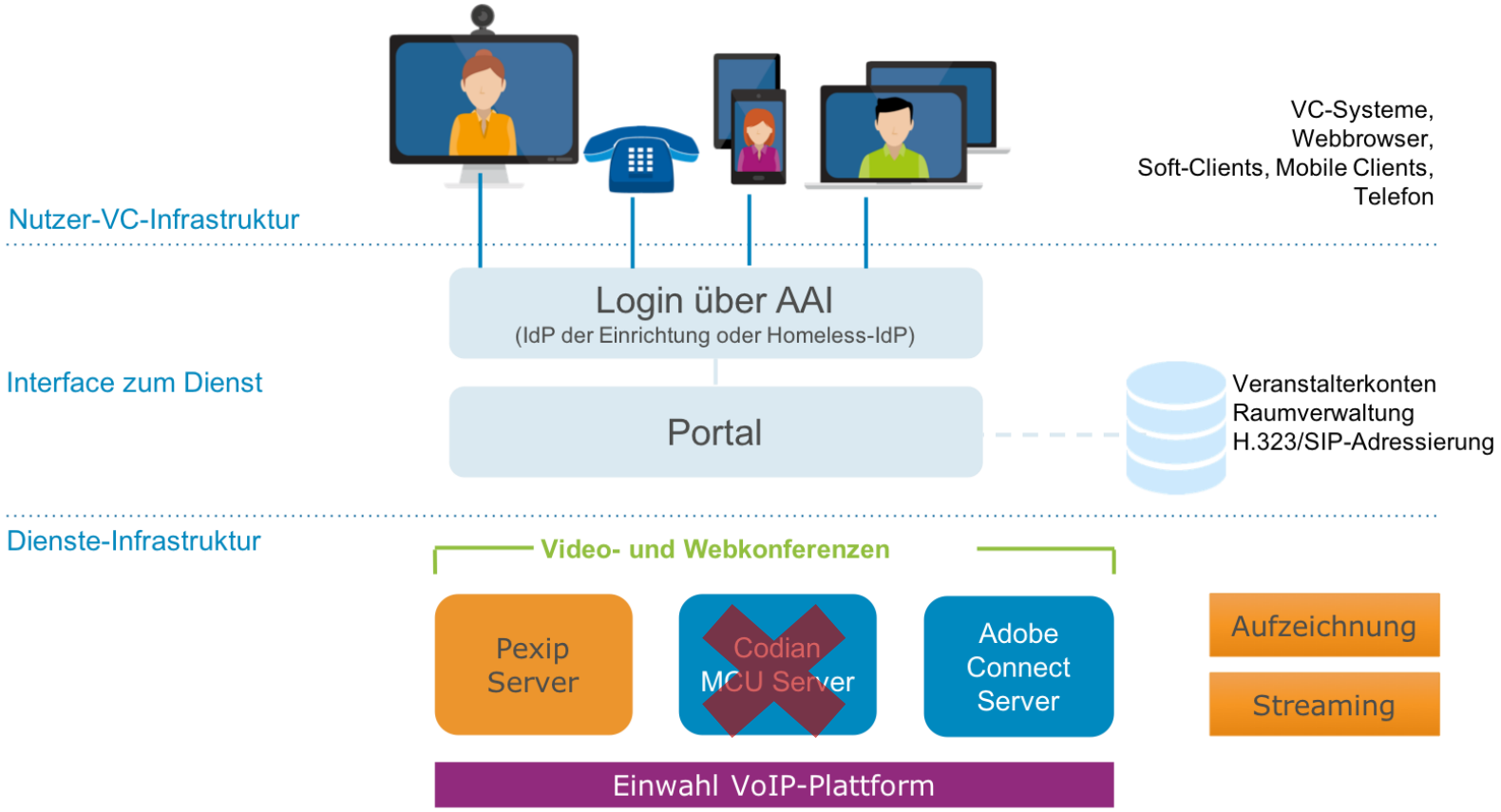
Betrachtungen zu DFN-Diensten

DFN Terminplaner

- Terminplaner Version 3 (veraltet) als SP in der DFN-AAI registriert
- Versionen 1 bis 3 (Foodle) zum Jahresende 2019 abgekündigt
- Aktuelle Version 4 (kein AAI-Dienst!) erfordert von Autoren manuelle Eingabe einer E-Mail-Adresse
- Keine Auftragsverarbeitung (Gutachten der FS Recht):
  - Dienst richtet sich ausschließlich an Endnutzer*innen
  - Keine Beauftragung seitens der Hochschulen
  - Rechtbeziehung nur zwischen DFN-Verein und Endnutzer*innen
- Version 4: Pers. Registrierung der Autoren aufgrund Art. 6.1 lit. b)
- Datenschutzerklärung: https://www.dfn.de/datenschutz-terminplaner/

DFNconf (1)

- (Tele-)Kommunikationsplattform, die mehrere Module umfasst



DFNconf (2)

- Zwei Module, die datenschutzrechtlich relevant sind (Codian ist abgekündigt)
  - Videokonferenzen (Pexip)
  - Webkonferenzen (Adobe Connect) für E-Learning
- Meeting-Veranstalter: Registrierung + Anmeldung über DFN-AAI
- Meeting-Teilnehmer: weitgehend anonyme Nutzung (IP-Adresse, Cookies, …)
- Spezialität Webkonferenzen:
  - Aufzeichnung → Veranstalter muss Einwilligung der Teilnehmer einholen
  - Hochladen von Dokumenten (Schulungsunterlagen) durch Veranstalter
  - API für Anbindung an LMS-Systeme (Moodle u.a.)
- https://www.conf.dfn.de/datenschutz/

Vielen Dank! Fragen? Kommentare?

- Kontakt

E-Mail: pempe@dfn.de
Tel.: +49-30-884299-308
Fax: +49-30-884299-370

Adresse:
DFN-Verein, Geschäftsstelle
Alexanderplatz 1
D-10178 Berlin

Informationsquellen

- SAML:

  https://www.oasis-open.org/standards#samlv2.0

  https://wiki.oasis-open.org/security

- Datenübermittlung durch IdP der Heimateinrichtung:

  M. Mörike, A. Strobel (Forschungsstelle Recht im DFN), Datenschutzrechtliche Analyse das AAI-Verfahrens (Präsentation)

- DFN-AAI Wiki:

  https://doku.tid.dfn.de/de:dfnaai:start,

- Verzeichnis(se) der Teilnehmer: https://www.aai.dfn.de/verzeichnis/