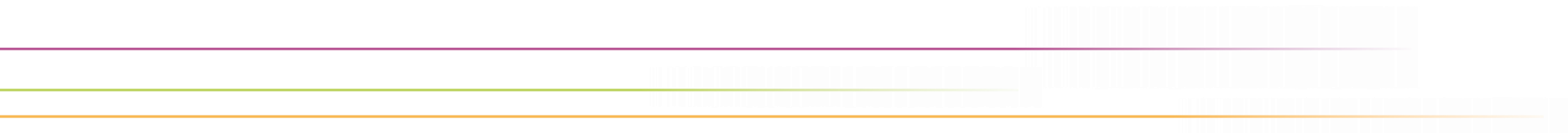


deutsches forschungsnetz

DEN

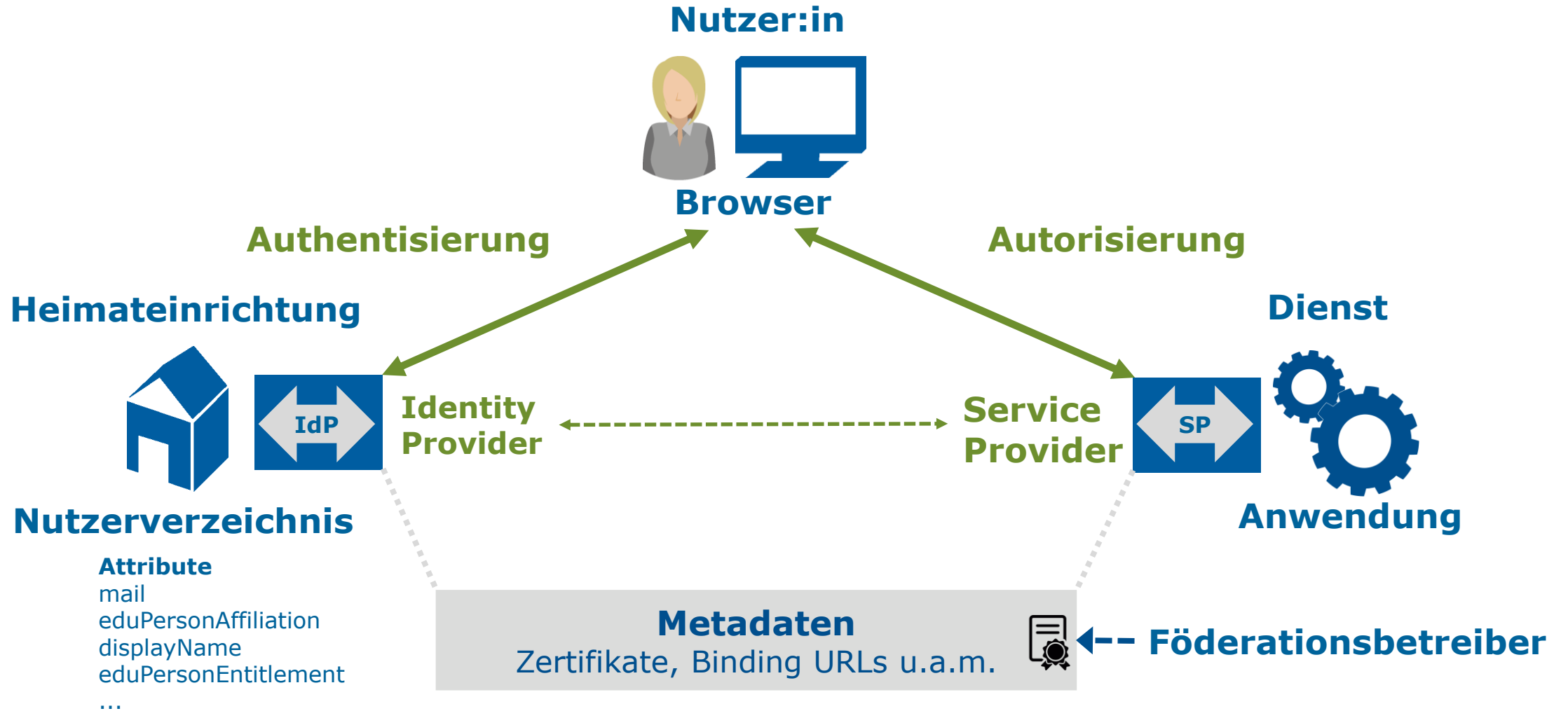


AAI und Datenschutz

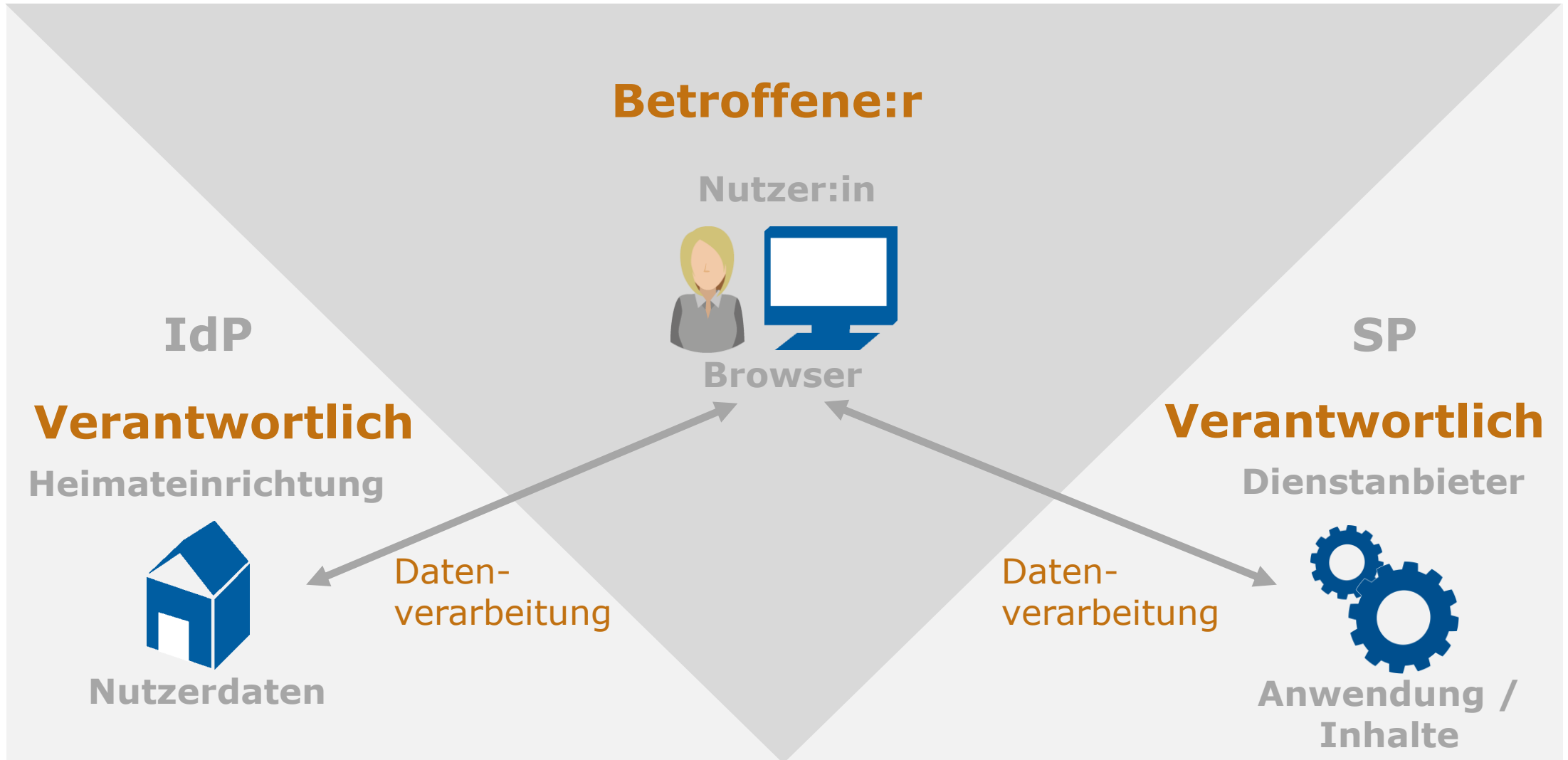
77. DFN-Betriebstagung | Forum AAI | 18. Oktober 2022

Wolfgang Pempe (pempe@dfn.de)

Wie funktioniert eine Föderation?



Siehe auch: <https://shibboleth.atlassian.net/wiki/spaces/CONCEPT/overview>



- ▶ Mesh-Föderation -> kein zentraler Knoten, über den Daten fließen
- ▶ Organisiert die Vertrauensbasis, nicht die Verkehrswege
- ▶ Verarbeitet keine Daten von Endnutzer(inne)n
- ▶ Beauftragt Teilnehmer grundsätzlich *nicht* mit der Verarbeitung personenbezogener Daten
- ▶ Weist Teilnehmer per Vertrag darauf hin, dass Lizenz- und Datenschutzfragen bilateral zwischen Einrichtungen und Diensteanbietern geregelt werden müssen

Siehe auch unter https://doku.tid.dfn.de/de:aai:datenschutz_rolle

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 bzw. Freigabe der 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

Sie sind dabei auf diesen Dienst zuzugreifen:
GÉANT Service Provider Proxy von GÉANT

Beschreibung dieses Dienstes:
A service provider proxy for all GÉANT federated services

[Zusätzliche Informationen über diesen Dienst](#)

An den Dienst zu übermittelnde Informationen

Anzeigenname	Wolfgang Pempe
Berechtigung	[REDACTED]
Principal Name	wolfgang@dfn.de
Zugehörigkeit (+ Einrichtung)	staff@dfn.de employee@dfn.de member@dfn.de
Targeted ID	[REDACTED]
Vorname	Wolfgang
E-Mail	pempe@dfn.de
Heimatinrichtung (international)	dfn.de
Typ der Heimatinrichtung (international)	urn:schac:homeOrganizationType:int:nren
Nachname	Pempe

Zusätzlich wird eine pseudonyme Kennung (transient oder persistent Id) übertragen.

[Datenschutzinformationen dieses Dienstes](#)

Um auf den von Ihnen ausgewählten Dienst (Service Provider) zugreifen zu können, müssen die hier angezeigten Informationen an diesen Dienst übertragen werden.

- Ich willige ein, dass diese Informationen einmalig übertragen werden.
- Ich willige ein, dass diese Informationen in Zukunft an diesen Dienst übertragen werden. Diese Entscheidung kann jederzeit mit der Checkbox auf der Anmeldeseite geändert werden.

Einwilligungen können für die Zukunft jederzeit widerrufen werden. Durch den Widerruf von Einwilligungen wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Für bereits übertragene Informationen entfaltet daher der Widerruf keine Wirkung. Kontaktdaten entnehmen Sie bitte der [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:shibidp:config-consent-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)
 - ▶ In Einzelfällen auch AVV zwischen Heimateinrichtung und Dienstanbieter möglich
- ▶ Direkte Rechtsbeziehung zu Endnutzer(in)
- ▶ Eigene Dienst-/SP-spezifische Datenschutzerklärung obligatorisch
- ▶ Als Rechtsgrundlage der Datenverarbeitung wird häufig Art. 6.1 lit. f) angenommen. Letztendlich abhängig vom Einzelfall.

- ▶ Unterschiedliche Rechtsgrundlagen lassen sich technisch abbilden
 - ▶ Aber wer teilt uns diese mit?
Hochschulverwaltung, Fakultäten, Lehrbeauftragte, ...?
 - ▶ Existieren die hierfür erforderlichen Kommunikationskanäle? Wer kümmert sich darum?

- ▶ Bei Bedarf lassen sich die Rechtsgrundlagen auch für unterschiedliche Personengruppen abbilden, aber
 - ▶ ... was ist mit Personen, die mehreren Gruppen angehören?
 - ▶ ... ist die tatsächliche Granularität auch im IdM abgebildet bzw. abbildbar?
 - ▶ ... ist sich das Lehrpersonal, das die Nutzung bestimmter Online-Ressourcen obligatorisch macht, der datenschutzrechtliche Implikationen bewusst?

Vertrauensbildende Maßnahmen

Data Protection Code of Conduct for Service Providers in EU/EEA

- ▶ Selbstverpflichtungserklärung für SP-Betreiber
- ▶ Best Practices bzgl. Umgang mit personenbezogenen Daten in der AAI
- ▶ Metadaten-technisch über eine Entity Category modelliert
- ▶ Version 1 (GÉANT, 2013) auf Grundlage der europäischen Datenschutzrichtlinie 95/46/EG
- ▶ Version 2 (REFEDS, 28.3.2022) auf Grundlage der EU-DSGVO
 - ▶ Wird in der neuen Metadatenverwaltung unterstützt

Vielen Dank! Fragen? Kommentare?

DFN

► Kontakt

► Wolfgang Pempe

E-Mail: pempe@dfn.de

Tel.: +49-30-884299-308

Fax: +49-30-884299-370

Adresse:

DFN-Verein, Geschäftsstelle

Alexanderplatz 1

D-10178 Berlin



Referenzen

- ▶ DFN-AAI Wiki: <https://doku.tid.dfn.de/de:aai:dataprotection>
- ▶ Präsentation Forschungsstelle Recht im DFN (69. DFN-Betriebstagung):
 - ▶ [Datenschutzrechtliche Analyse des AAI-Verfahrens](#)
- ▶ GÉANT Data Protection Code of Conduct for Service Providers in EU/EEA
 - ▶ https://doku.tid.dfn.de/de:geant_coco
- ▶ REFEDS Data Protection Code of Conduct for Service Providers v.2 (GDPR):
 - ▶ <https://refeds.org/category/code-of-conduct>