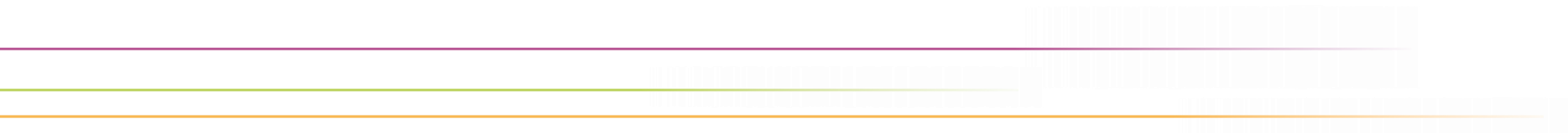


DEN
deutsches forschungsnetz



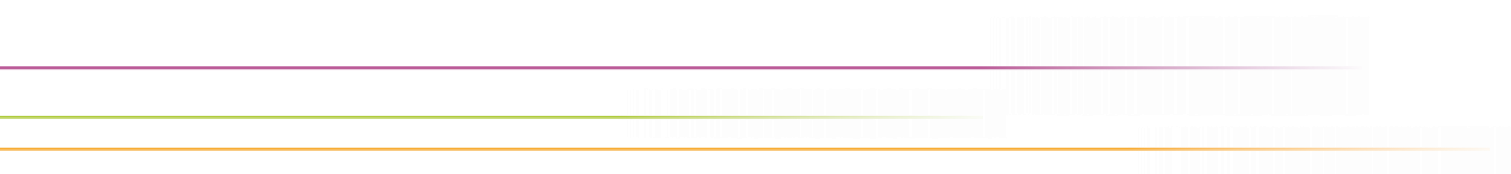


User Consent mit Shibboleth IdP 4.1.x

DFN-AAI Workshop Februar 2022 | 7. Februar 2022

Wolfgang Pempe (pempe@dfn.de)

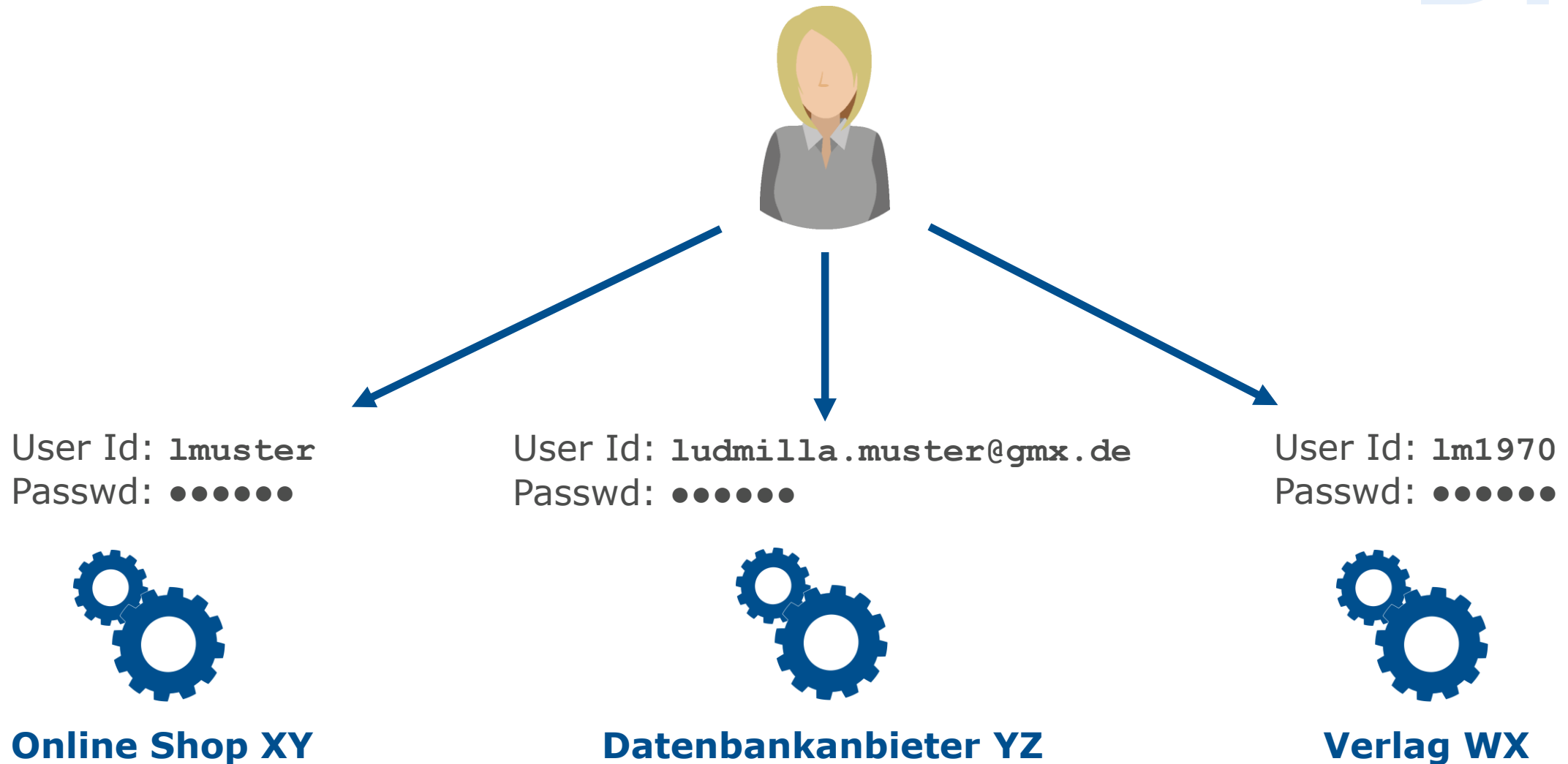
Steffen Hofmann (steffen.hofmann@fu-berlin.de)



Der Kontext:

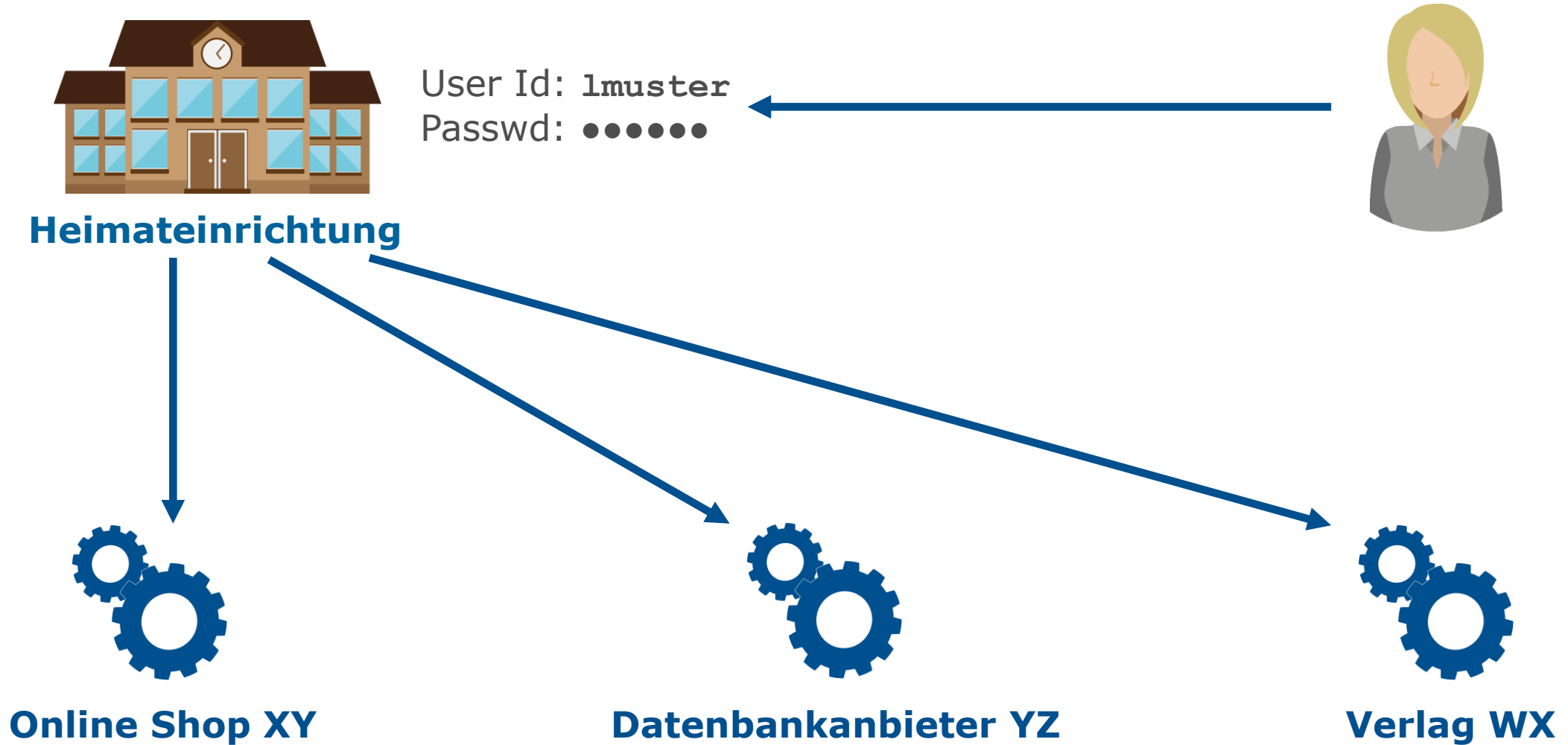
AAI, föderierte Identitäten, Web-SSO

Dienstspezifische Identitäten



Föderierte Identität

DFN

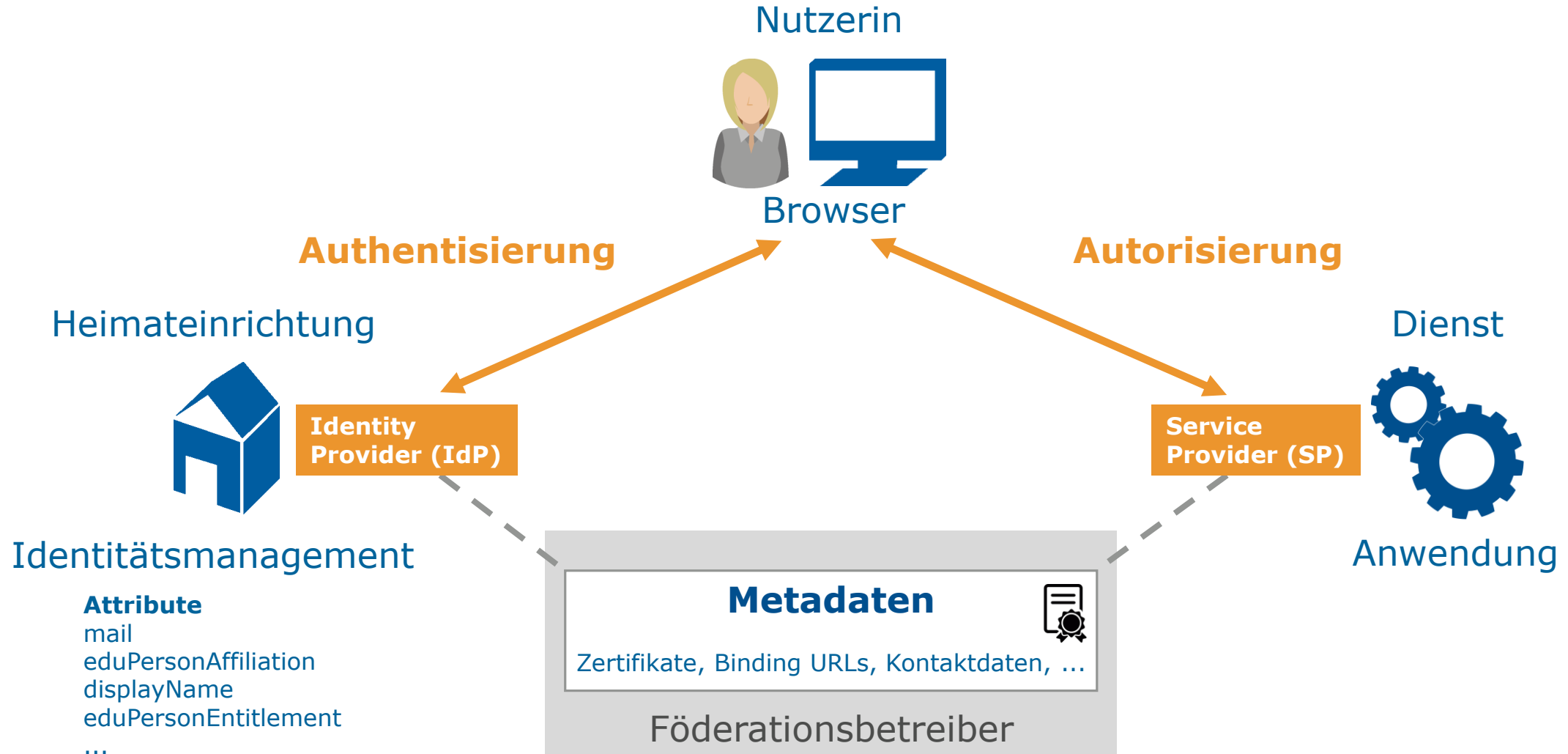


Begriffsbestimmung

- ▶ AAI = **A**uthentication and **A**uthorization **I**nfrastructure
 - ▶ Bildet den technischen und organisatorischen Rahmen für föderiertes Identitätsmanagement
- ▶ Föderiertes Identitätsmanagement
 - ▶ Austausch von Identitätsdaten über Dienst- und Organisationsgrenzen hinweg
 - ▶ Vermeidung von dienstspezifischen Identitäten und Username/Password
 - ▶ erfordert eine Identitätsquelle als führendes System
- ▶ AAI ermöglicht **S**ingle **S**ign-**O**n (SSO)
 - ▶ einmal anmelden für mehrere Dienste, für die man zugriffsberechtigt ist
 - ▶ üblicherweise auf Web-Anwendungen beschränkt, Erweiterungen jedoch möglich

- ▶ föderiertes Identitätsmanagement erfordert zentrale Instanz: Föderationsbetreiber
 - ▶ definiert die organisatorischen, technischen und rechtlichen Rahmenbedingungen
 - ▶ stellt deren Einhaltung sicher
 - ▶ etabliert auf diese Weise das Vertrauensverhältnis innerhalb der Föderation
- ▶ DFN-Verein ist Betreiber der einrichtungsübergreifenden Föderation DFN-AAI
 - ▶ Zielgruppe: Hochschulen und Forschungseinrichtungen
 - ▶ hält Dienstvereinbarungen mit über 390 Einrichtungen aus der Wissenschaft
 - ▶ hält über 200 Dienstvereinbarungen mit Dienst Anbietern außerhalb der Wissenschaft
- ▶ Konzept der Föderation erlaubt Hierarchien (Interföderation eduGAIN, Subföderationen)

Wie funktioniert eine Föderation?



- ▶ **Föderationsbetreiber**

DFN-Verein

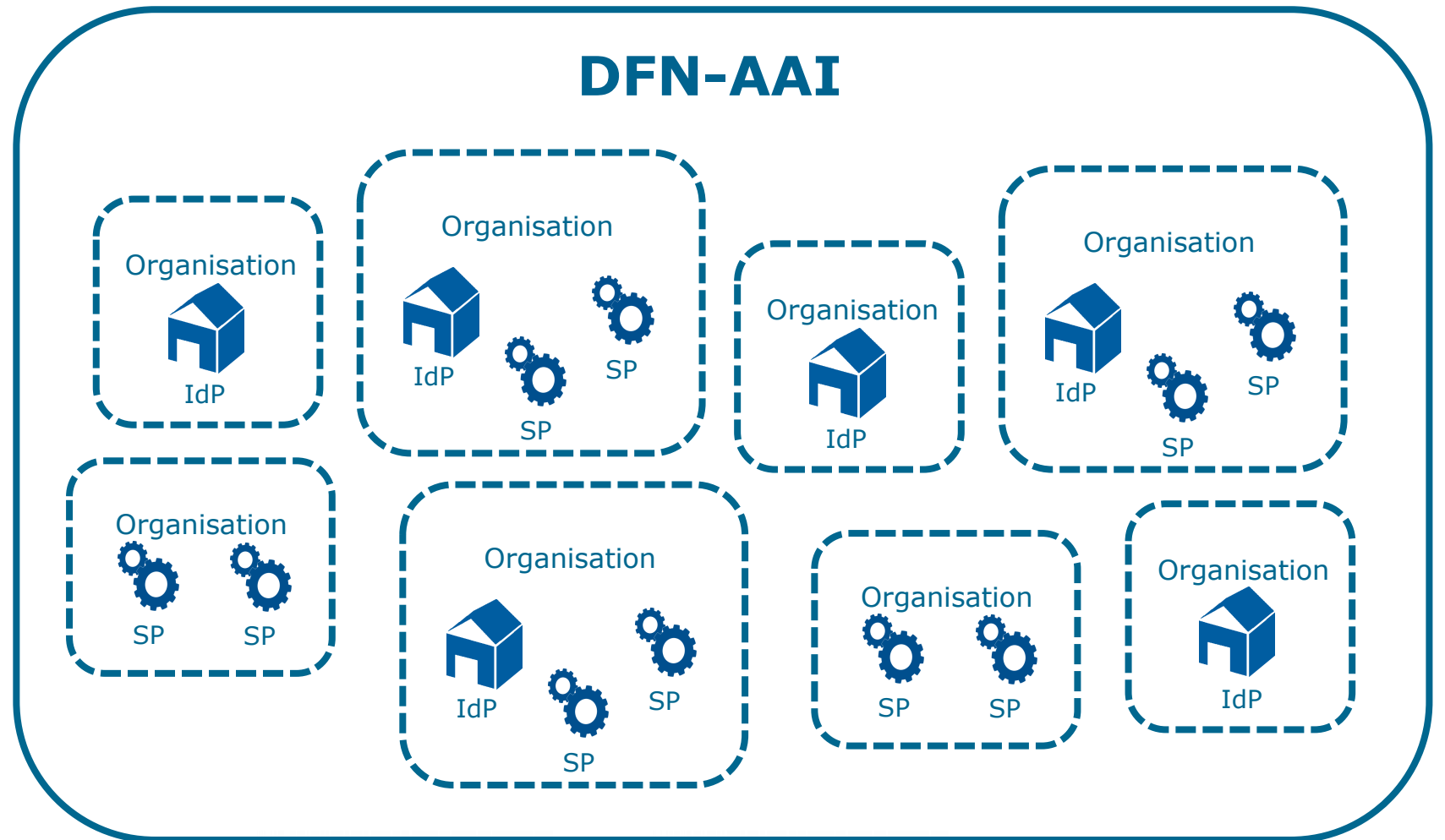
- ▶ **Vertrauen**

Verträge mit allen Teilnehmern, Policies, Levels of Assurance

- ▶ **Technik**

Metadatenverwaltung und -Signierung

Aktuell ca. 350 teilnehmende Einrichtungen und 675 Dienste (zzgl. ~1300 lokale SP)



Datenschutzaspekte

Disclaimer

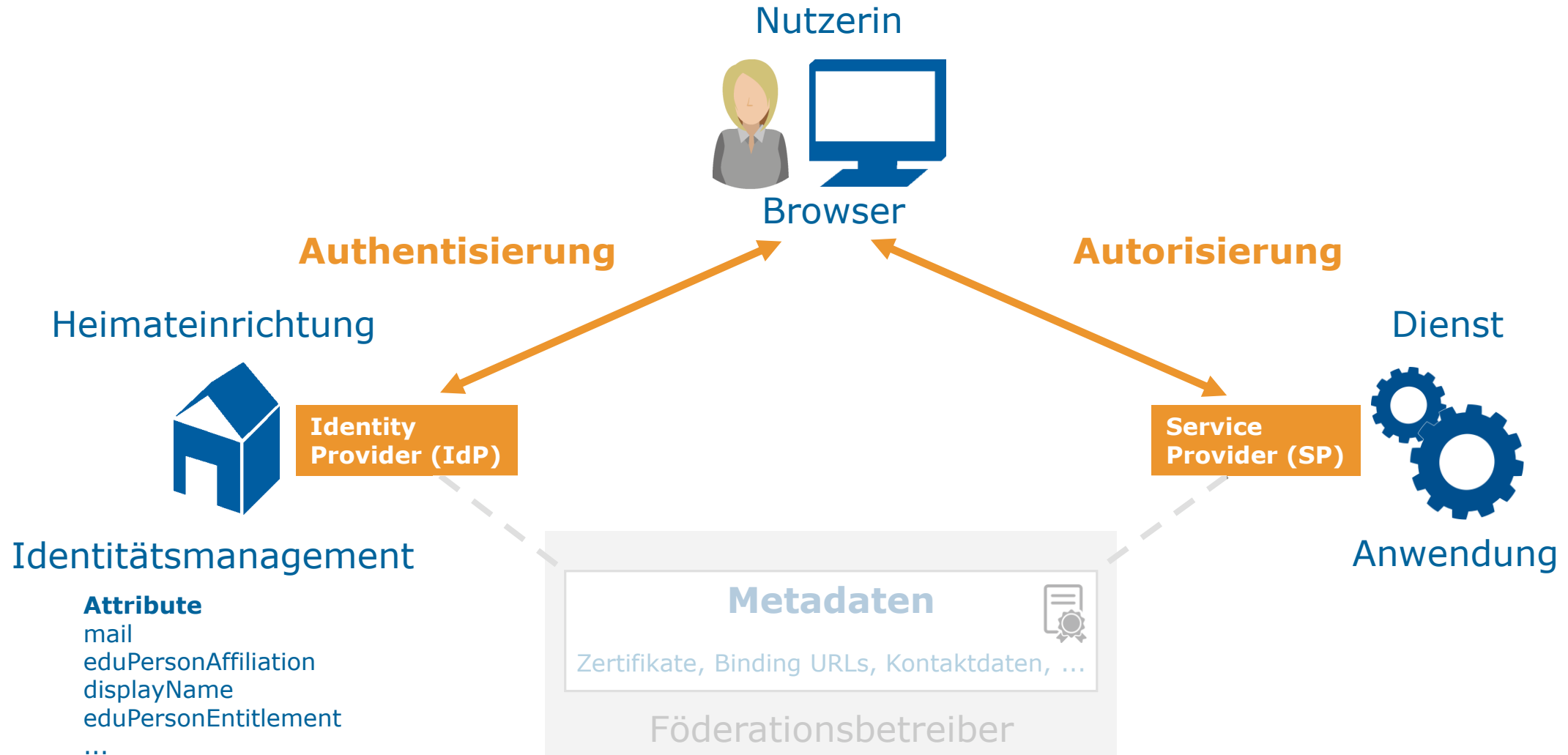
Bitte beachten:

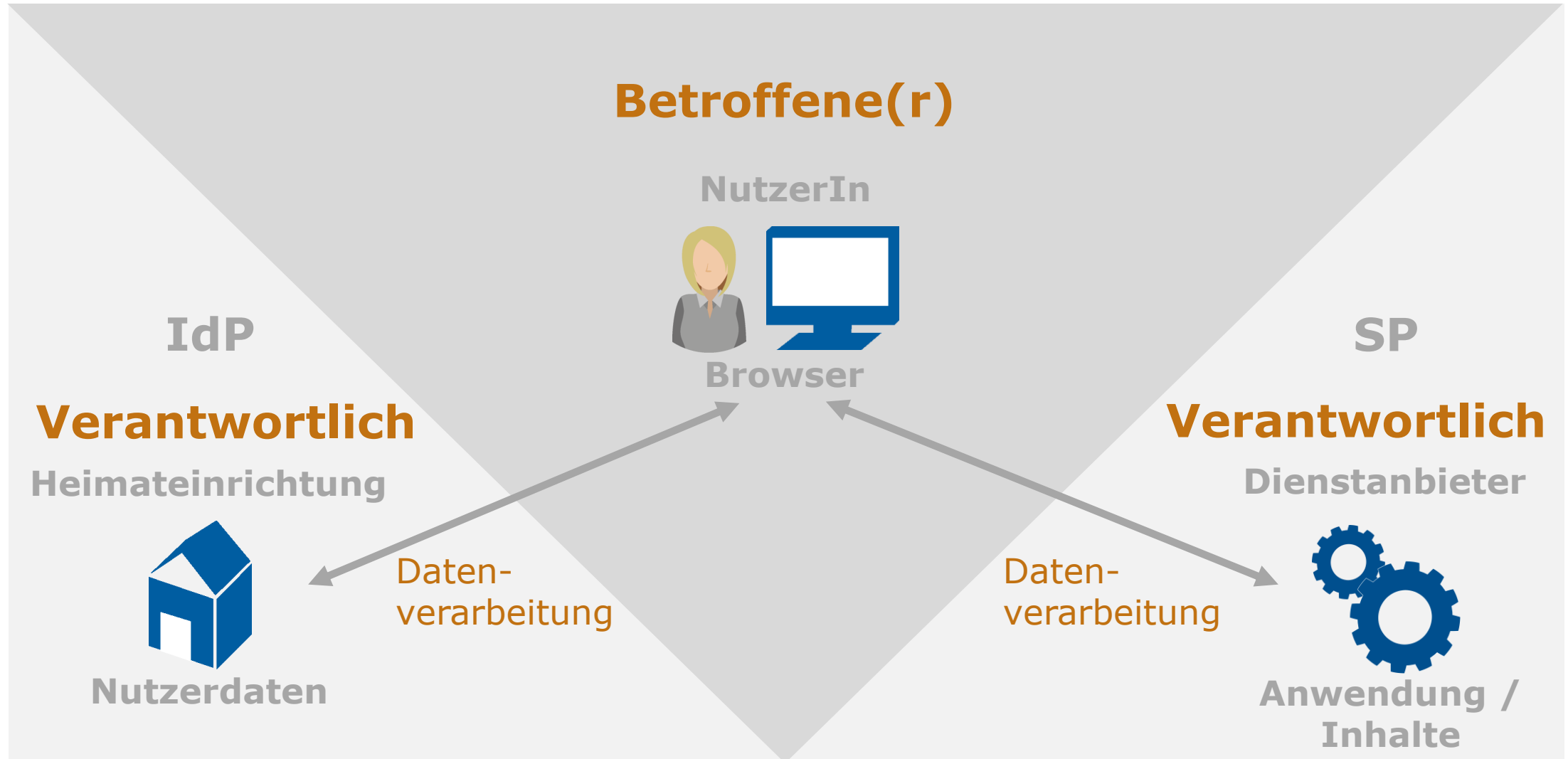
- ▶ Im folgenden werden keine rechtsverbindlichen Aussagen getroffen!
- ▶ Bei den hier beschriebenen Empfehlungen handelt es sich um unverbindliche Vorschläge. Der DFN-Verein übernimmt keine Verantwortung für etwaige juristische Streitfälle, die sich aus diesen Beispielen oder daraus abgeleiteten Konfigurationen ergeben!
- ▶ Konsultieren Sie bitte vor der Inbetriebnahme der skizzierten Lösungen in jedem Fall die für Datenschutzfragen zuständige Stelle bei Ihnen im Hause!

Rechtliche Aspekte

- ▶ Juristische Rahmenbedingungen
 - ▶ EU-Datenschutzgrundverordnung (DSGVO)
 - ▶ Bundesdatenschutzgesetz (BDSG)
 - ▶ Landesdatenschutzgesetze
 - ▶ ggf. einrichtungsinterne Richtlinien
- ▶ Siehe auch FAQ-Seite im Wiki:
https://doku.tid.dfn.de/de:aai:datenschutz_faq
- ▶ Forschungsstelle Recht im DFN:
[Datenschutzrechtliche Analyse des AAI-Verfahrens](#)

Wir erinnern uns...





IdP-Betreiber

- ▶ Im AAI-Kontext werden Nutzendendaten 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** (Nachweispflicht, Art. 7.1 → IdP Log)

IdP - Authentisierung

- ▶ Credentials der Heimateinrichtung
- ▶ Attributfreigaben widerrufen bzw. erneute Anzeige der Attribute
- ▶ Sofern in Metadaten vorhanden, können MDUI-Elemente des SP angezeigt werden
- ▶ Nutzungs-/Datenschutzbestimmungen für den IdP können verlinkt werden



Anmelden bei DFN-AAI Attribute Viewer

Benutzername

test-dsgvo

Passwort

.....

Anmeldung nicht speichern

Hier können Sie die an Dienst zu übermittelnden Informationen einsehen, die entweder aufgrund einer von Ihnen erteilten Einwilligung oder einer anderen gesetzlichen Grundlage übermittelt werden. Liegt eine Einwilligung von Ihnen vor, kann sie durch Anklicken der Checkbox für die Zukunft widerrufen werden.

Anmelden

- > [Passwort vergessen?](#)
- > [Kontakt IT Support](#)
- > [Einwilligungserklärung](#)
- > [Datenschutz](#)

Hinweis: Zum Logout schließen Sie den Browser, damit keine anderen Personen unter Ihrer Benutzerkennung weiterarbeiten können. (Eine zentrale Abmeldung ist nicht immer möglich und nicht alle Dienste bieten ein Logout an.)



DFN-AAI Attribute Viewer (Test-SP3)

IdP – User Consent Modul (1)

- ▶ Aktivierung und Konfiguration des Moduls im Wiki dokumentiert:
<https://doku.tid.dfn.de/de:shibidp:config-tou>
- ▶ **Terms of Use**
 - ▶ ... müssen bei der ersten Anmeldung bestätigt werden (sofern aktiv)
 - ▶ ... sowie bei jeder Änderung des Wortlauts
 - ▶ Info bzgl. Bestätigung kann in IdP-seitiger Datenbank abgelegt werden, Zeitraum ist konfigurierbar
 - ▶ ... und wird außerdem geloggt

DFN

DEUTSCHES FORSCHUNGSNETZ

Einwilligungserklärung

Die hier aufgerufene Seite ist der Identity Provider (IdP) **[der Hochschule XYZ]**. Der IdP dient der gesicherten Anmeldung an Diensten, sogenannten Service Providern (SP), die über die DFN-AAI verfügbar sind. Hierzu ist der IdP mit dem Nutzerverzeichnis **[der Hochschule XYZ]** verbunden.

Die Authentifizierungs- und Autorisierungs-Infrastruktur DFN-AAI wird vom DFN-Verein verwaltet. Er schafft das notwendige Vertrauensverhältnis und den organisatorisch-technischen Rahmen für den Austausch von Benutzerinformationen zwischen Einrichtungen (IdP) und Diensteanbietern (SP-Betreibern) in der DFN-AAI.

Im Rahmen des Anmeldevorgangs führt der IdP zunächst eine Authentifizierung der NutzerInnen durch. Dies geschieht in der Regel über die Eingabe der Nutzerkennung und eines Passworts. Die Überprüfung Ihrer Anmeldedaten erfolgt immer am IdP **[der Hochschule XYZ]**. Diese Anmeldedaten werden nicht an einen SP übertragen. Anschließend werden die zur Nutzung des SP erforderlichen Angaben (sog. Attribute) an den betreffenden SP übertragen. Dies können zum Beispiel der Name, die E-Mail-Adresse oder die Gruppenzugehörigkeit innerhalb **[der Hochschule XYZ]** (Student, Mitarbeiter, ...) sein.

Um den Grundsatz der Datenminimierung umzusetzen, fordern viele SP anstelle von Klarnamen nur SP-spezifische, persistente pseudonyme Kennungen ein. Um dies umzusetzen, werden diese Kennungen im Rahmen des Anmeldevorgangs vom IdP generiert und dauerhaft gespeichert. Mit Aktivieren der Checkbox unter diesem Text willigen Sie in die Speicherung der hiermit verbundenen Informationen seitens des IdP ein. Sie können diese Einwilligung jederzeit durch eine Erklärung gegenüber dem Betreiber des IdP, mit einer E-Mail an xxx@xxx widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Weitere Informationen zum Datenschutz finden Sie in der [Datenschutzerklärung](#).

Ablehnen

Ich willige in die Speicherung der o.g. Informationen ein

IdP – User Consent Modul (2)

Attribute Release

- ▶ Anzeige der zu übertragenden Daten
- ▶ 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	urn:mace:rediris.es:entitlement:wiki:tfemc2
Principal Name	wolfgang@dfn.de
Zugehörigkeit (+ Einrichtung)	staff@dfn.de employee@dfn.de member@dfn.de
Targeted ID	m25QVsGCIEFwPJOHWozhg5R5pxk=
Vorname	Wolfgang
E-Mail	pempe@dfn.de
Heimateinrichtung (international)	dfn.de
Typ der Heimateinrichtung (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)
- ▶ 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 (Ausnahme: Auftragsverarbeitung)
- ▶ 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 gegeben
- ▶ Eigene Dienst-/SP-spezifische Datenschutzerklärung obligatorisch
- ▶ Als Rechtsgrundlage der Datenverarbeitung wird häufig Art. 6.1 lit. f) „berechtigtes Interesse“ angenommen. Letztendlich abhängig vom Einzelfall.

Fazit für DFN-AAI

- ▶ Die Struktur der DFN-AAI sorgt für eine klare klare Trennung von Verantwortlichkeiten
- ▶ Im Standardfall (Datenübertragung via SAML) keine gemeinsame Verantwortung (Art. 26) und keine Auftragsverarbeitung (Art. 28)
- ▶ 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

Attributübertragung:

Anpassung User Consent Modul für
unterschiedliche Rechtsgrundlagen

Empfehlungen für IdP-Betreiber

- ▶ Forschungsstelle Recht im DFN:

[Datenschutzrechtliche Analyse des AAI-Verfahrens](#) (2018)

- ▶ Lösungsmodell 1:

Ausschließlich Einwilligung als Rechtsgrundlage (Art. 6 Abs. 1 lit. a DSGVO)

- ▶ Lösungsmodell 2: Differenzierung

- ▶ „Notwendige Dienste“ – Beschäftigungsverhältnis (Art. 88 mit § 26 BDSG)
- ▶ „Nützliche Dienste“ – berechtigtes Interesse der Einrichtung (Art. 6 Abs. 1 lit. f oder e, letzteres in Verb. mit spezieller Erlaubnisnorm)
- ▶ „Sonstige Dienste“ – Einwilligung, s.o.

Lösungsmodell 2

- ▶ Was muss am Shibboleth IdP getan werden, um Lösungsmodell 2 technisch umzusetzen?
 - ▶ **Information** der Nutzenden über Zweck und Rechtsgrundlage der Verarbeitung
 - ▶ Abhängig von Rechtsgrundlage die betreffenden **Interaktionsmöglichkeiten** realisieren (Einwilligung, Widerspruch, Abbruch)
 - ▶ **Dokumentation** des Vorgangs (Nachweispflicht, Schreiben ins Log)
- ▶ Bisheriger Ansatz mit Shib IdP 3.x und 4.0.x
 - ▶ Parallel zum **Attribute Release Interceptor Flow** zwei weitere Flows definieren: **Attribute Info** („nützliche Dienste“) und **Attribute Must** („Notwendige Dienste“)
 - ▶ Flows werden über zentral definierte Activation Conditions angesteuert, abhängig vom anfragenden SP und ggf. weiteren Bedingungen wie z.B. Gruppenzugehörigkeit

Lösungsansatz für Shib IdP 4.1.x

- ▶ Der bestehende Lösungsansatz für Shib IdP 3.x und 4.0.x lässt sich für Shib IdP 4.1.x nur mit unverhältnismäßig hohem Aufwand anwenden
- ▶ Die Unterscheidung der Rechtsgrundlagen für die jeweilige Attributfreigabe bzw. –Übertragung wird über ein **IdP-internes Attribut** transportiert
- ▶ Abhängig vom Attributwert können im User Consent Modul die jeweils zutreffenden **Informationen** angezeigt und **Interaktionsmöglichkeiten** für die Nutzenden angeboten werden
- ▶ Abhängig vom Attributwert kann die jeweilige Rechtsgrundlage im Consent Audit Log **dokumentiert** werden → Nachweispflicht

Praktische Umsetzung

- ▶ Gemeinsame Sichtung der Doku im Wiki:
<https://doku.tid.dfn.de/de:shibidp:config-consent-dsgvo>
- ▶ Kurze Demo mit Test-Instanzen des DFN

Vielen Dank! Haben Sie noch Fragen?

DFN

► Kontakt

► Wolfgang Pempe

E-Mail: pempe@dfn.de

Telefon: +49 30 884299-380

Fax: +49 30 884299-370

Anschrift:

DFN-Verein, Geschäftsstelle

Alexanderplatz1

10178 Berlin

► Steffen Hofmann

E-Mail: steffen.hofmann@fu-berlin.de

Telefon: +49 30 838 56031

Fax: +49 30 838 456031

Anschrift:

Freie Universität Berlin

ZEDAT, Identity Management and Media (IM)

Fabeckstr. 32

14195 Berlin

