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

User Id: `lmuster`
Passwd: ••••••

User Id: `ludmilla.muster@gmx.de`
Passwd: ••••••

User Id: `lm1970`
Passwd: ••••••

Online Shop XY

Datenbankanbieter YZ

Verlag WX

Föderierte Identität

User Id: `lmuster`
Passwd: ••••••

Heimateinrichtung

Online Shop XY

Datenbankanbieter YZ

Verlag WX

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

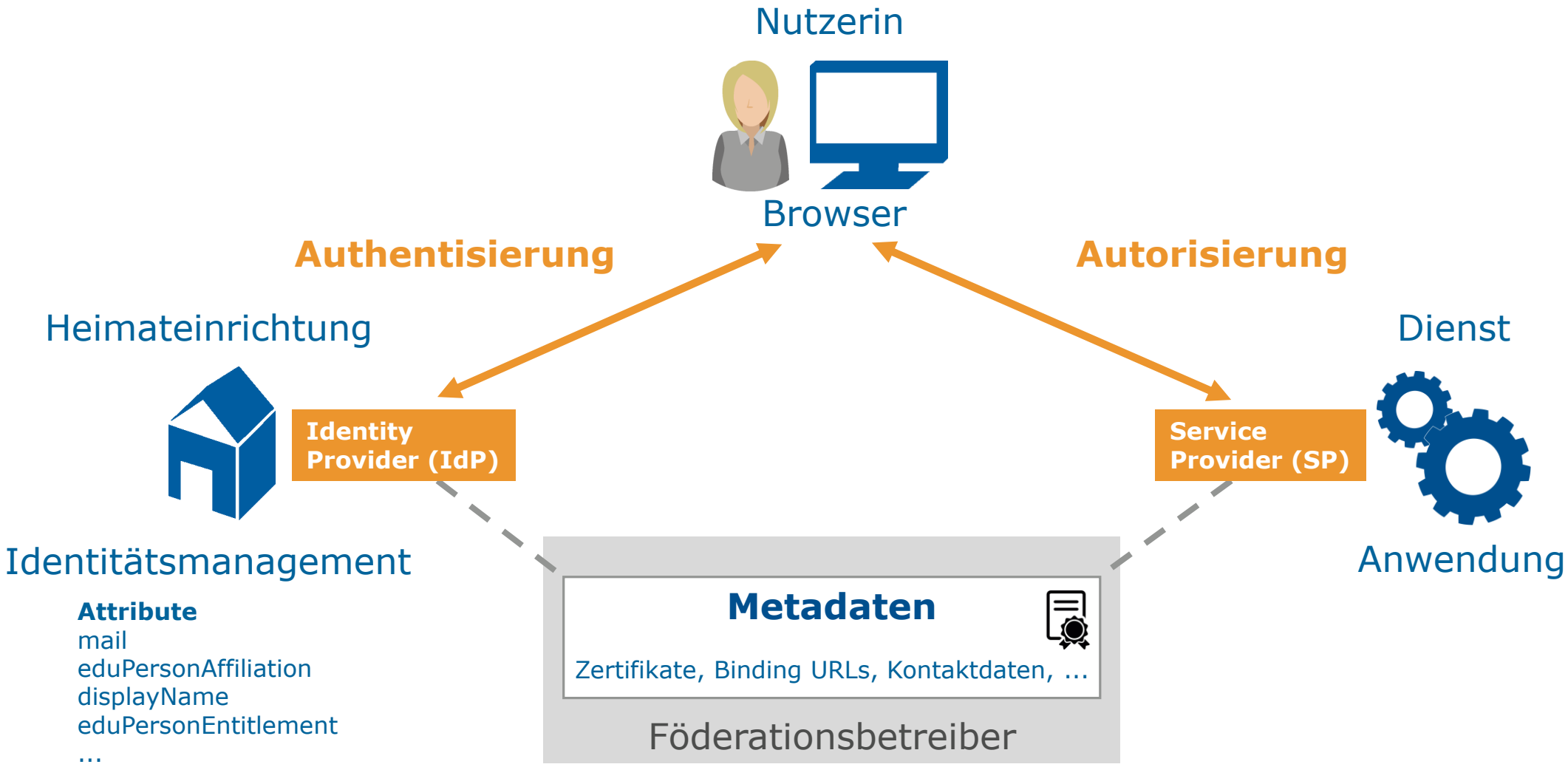
Föderation

- 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 Dienstanbietern außerhalb der Wissenschaft

- Konzept der Föderation erlaubt Hierarchien (Interföderation eduGAIN, Subföderationen)

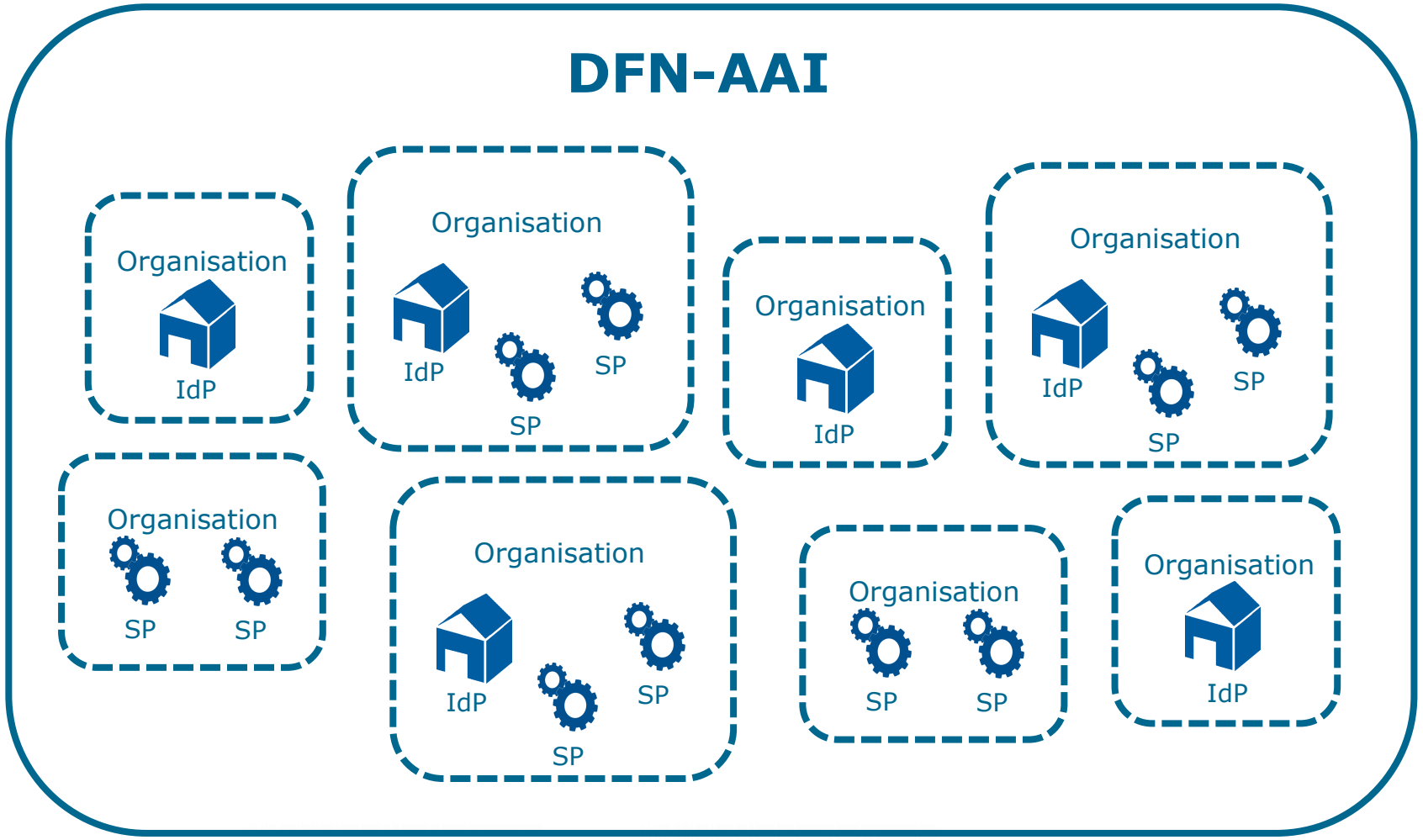
Wie funktioniert eine Föderation?



DFN-AAI

- **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

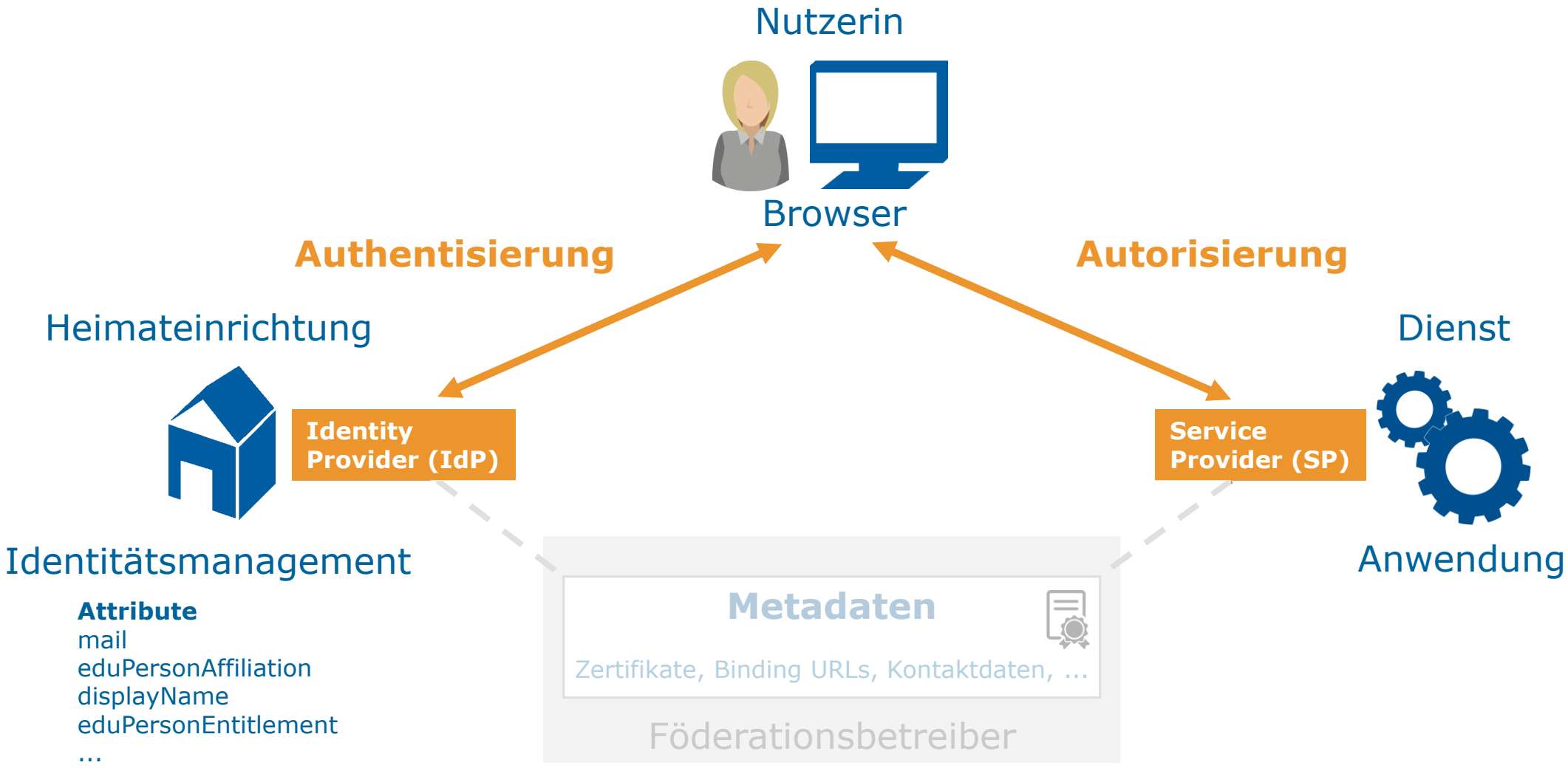
Bitte beachten:

- 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!

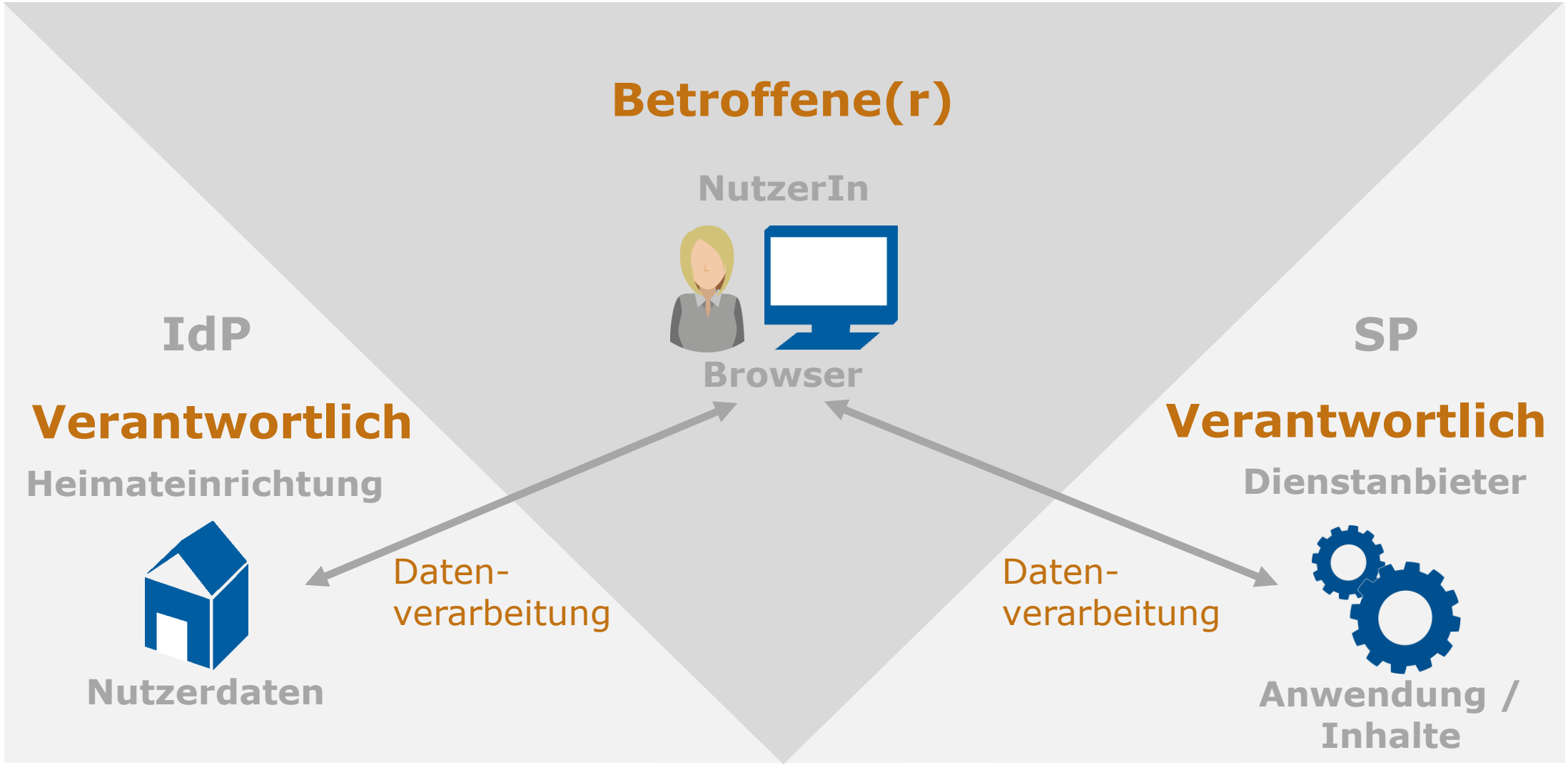
Rechtliche Aspekte

- 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…



Datenschutz – Rollen

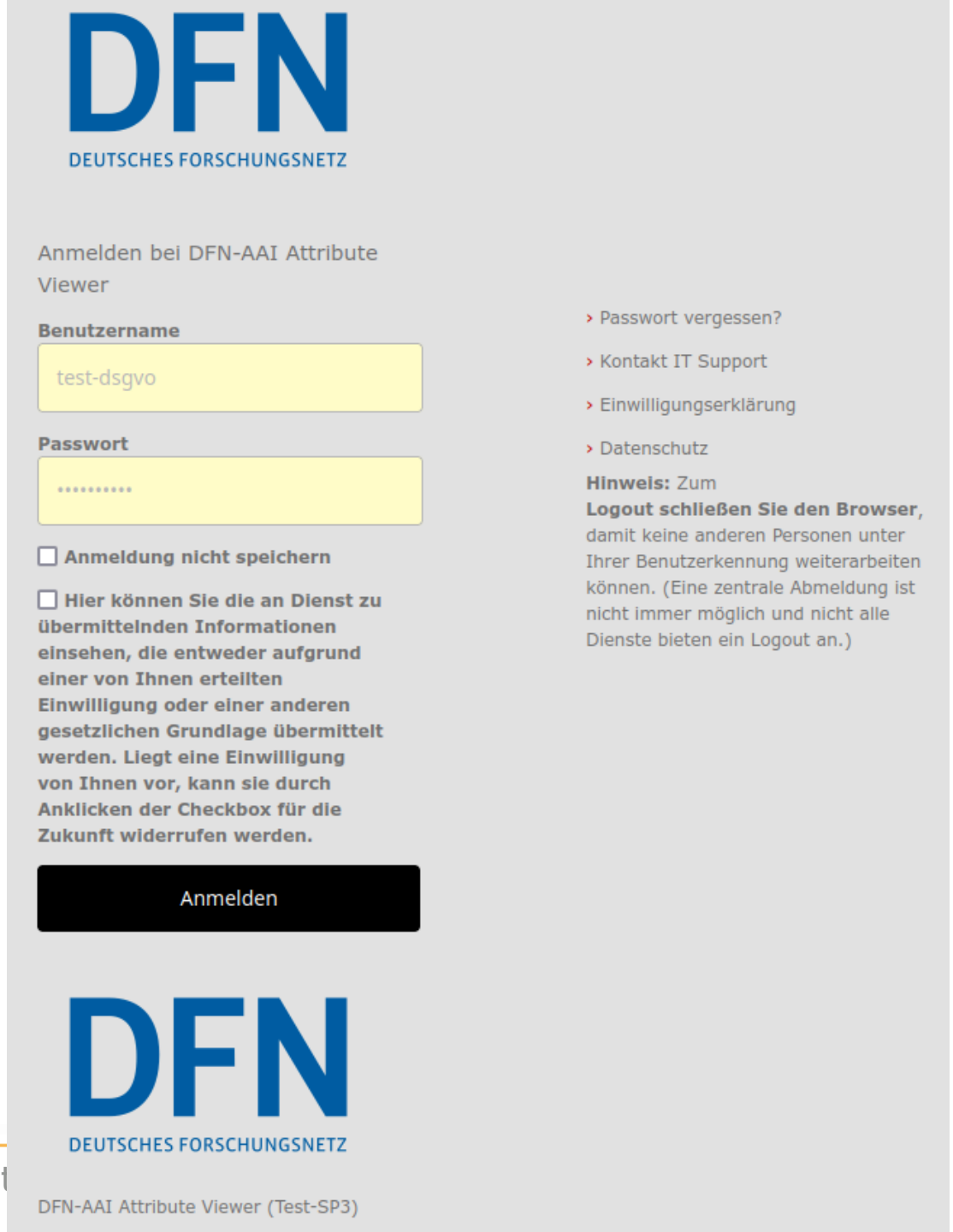


IdP-Betreiber

- 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



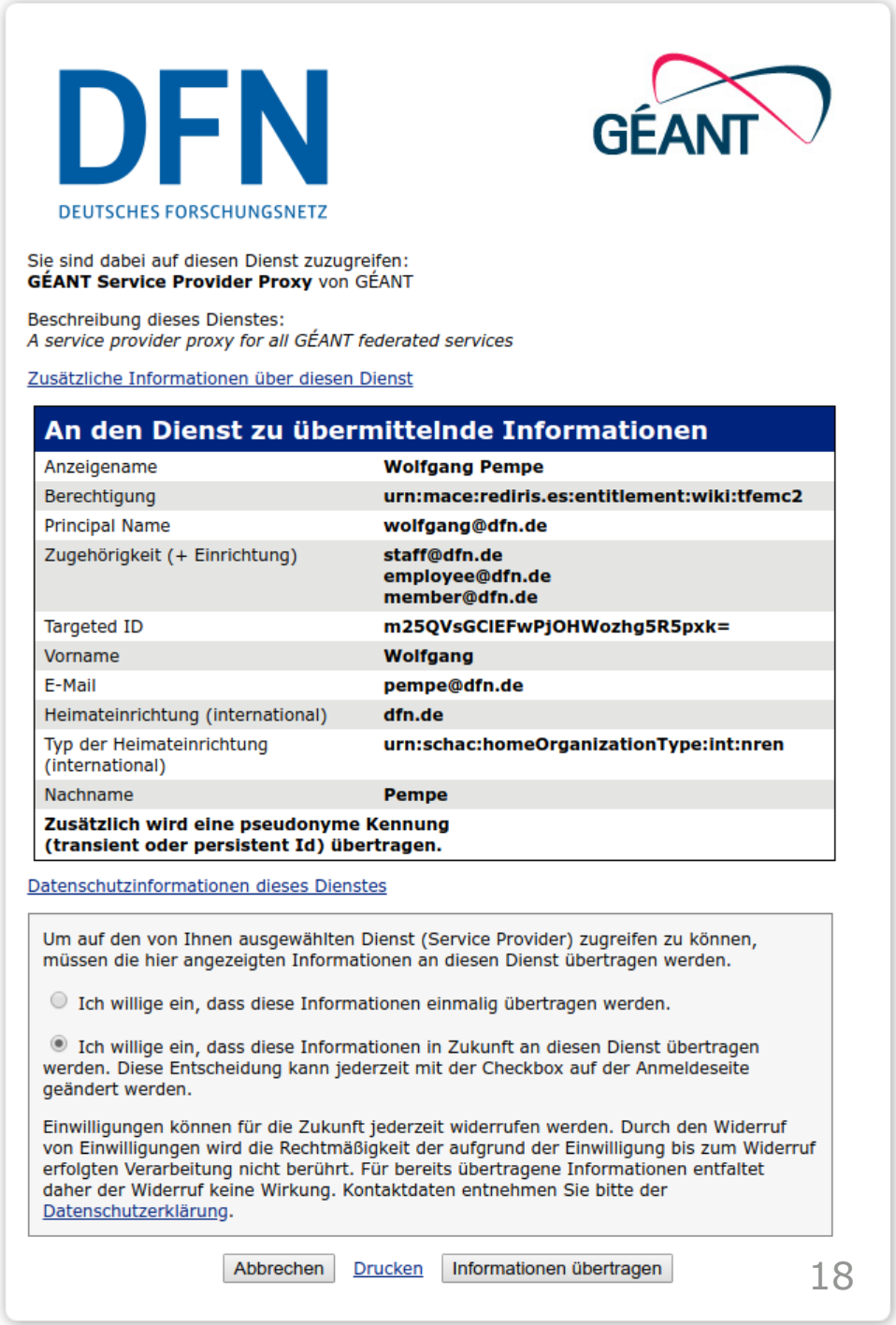
IdP – User Consent Modul (1)

- 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

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



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?

- 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