deutsches forschungsnetz

DFN-AAI

Der Foliensatz

Wolfgang Pempe (pempe@dfn.de)

Föderierte Identitäten, AAI und Web-SSO

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

User Id: `lmuster`
Passwd: ••••••

Online Shop XY

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

Datenbankanbieter YZ

User Id: `lm1970`
Passwd: ••••••

Verlag WX

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**
  - DFN-Verein schließt Verträge mit allen teilnehmenden Einrichtungen und Dienstanbietern

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.)

DFN-AAI - Entwicklung

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, ndsIDM, sciebo, hessenbox, …

E-Research – CLARIN, DARIAH, ELIXIR, MII …

Internat. Forschungscommunities (→ eduGAIN)

Bibliotheksnutzer*Innen

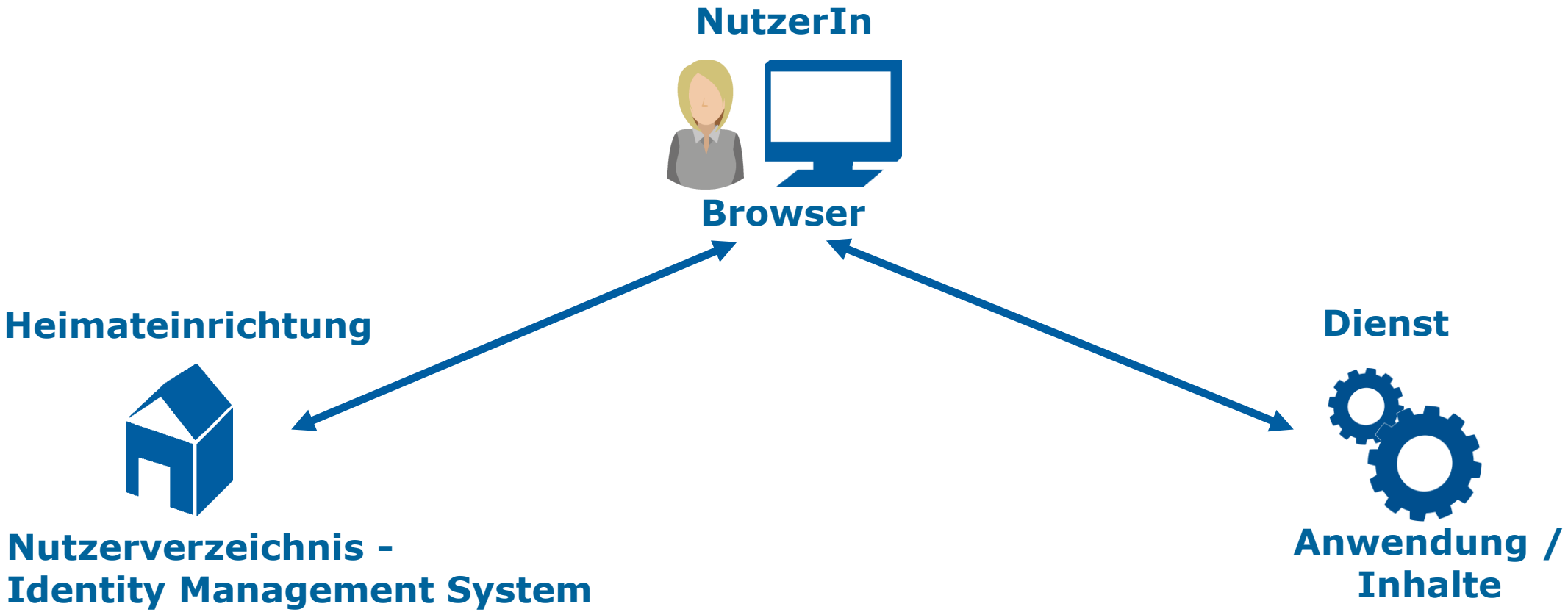
Studierende, Lehrpersonal

Forschende

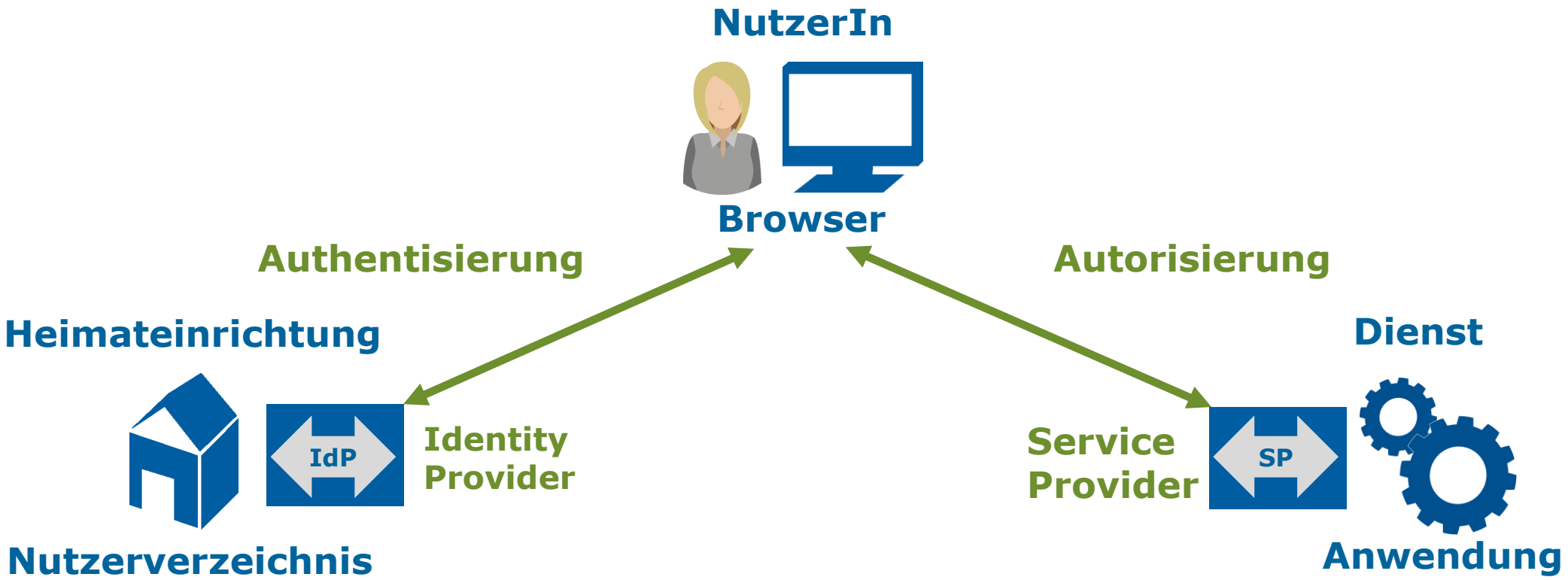
Beispiele aus dem DFN-Umfeld

- Konferenzdienste, DFNconf: https://www.conf.dfn.de/ (Räume verwalten)
- DFN Mailsupport: https://portal.mailsupport.dfn.de/ (Konfiguration)
- eduroam Konfigurationsassistent https://cat.eduroam.org (Betreiber: GÉANT)
- eduVPN (Pilotbetrieb) https://www.eduvpn.org
- Diverse Sync-and-Share Dienste
  https://www.dfn.de/dfn-cloud/syncshare-dienste/
- Liste der über die DFN-AAI verfügbaren Dienste unter
  https://tools.aai.dfn.de/entities/

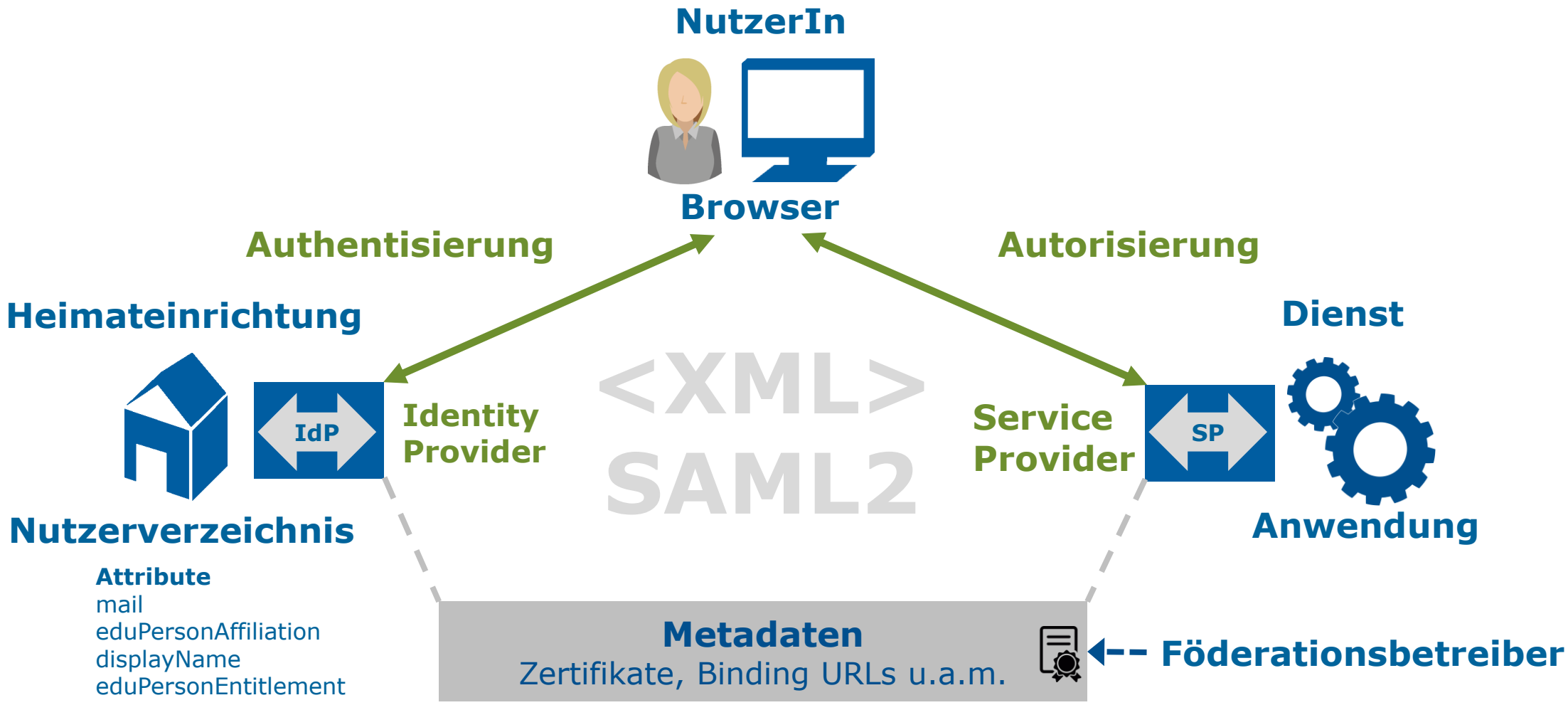
Web-SSO = Dreiecksbeziehung



Dreiecksbeziehung im Detail

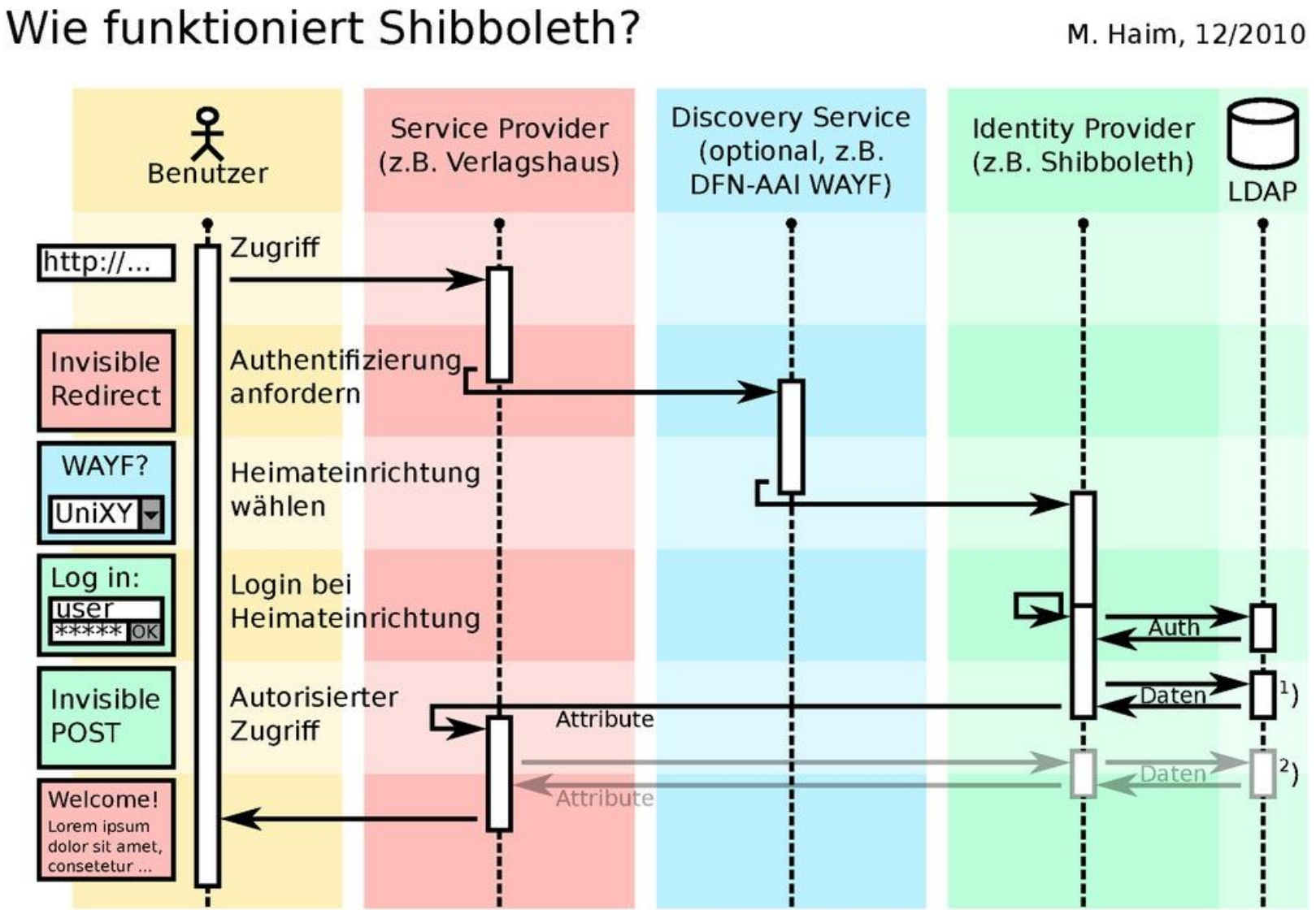


Lingua franca: SAML (bzw. SAML2)



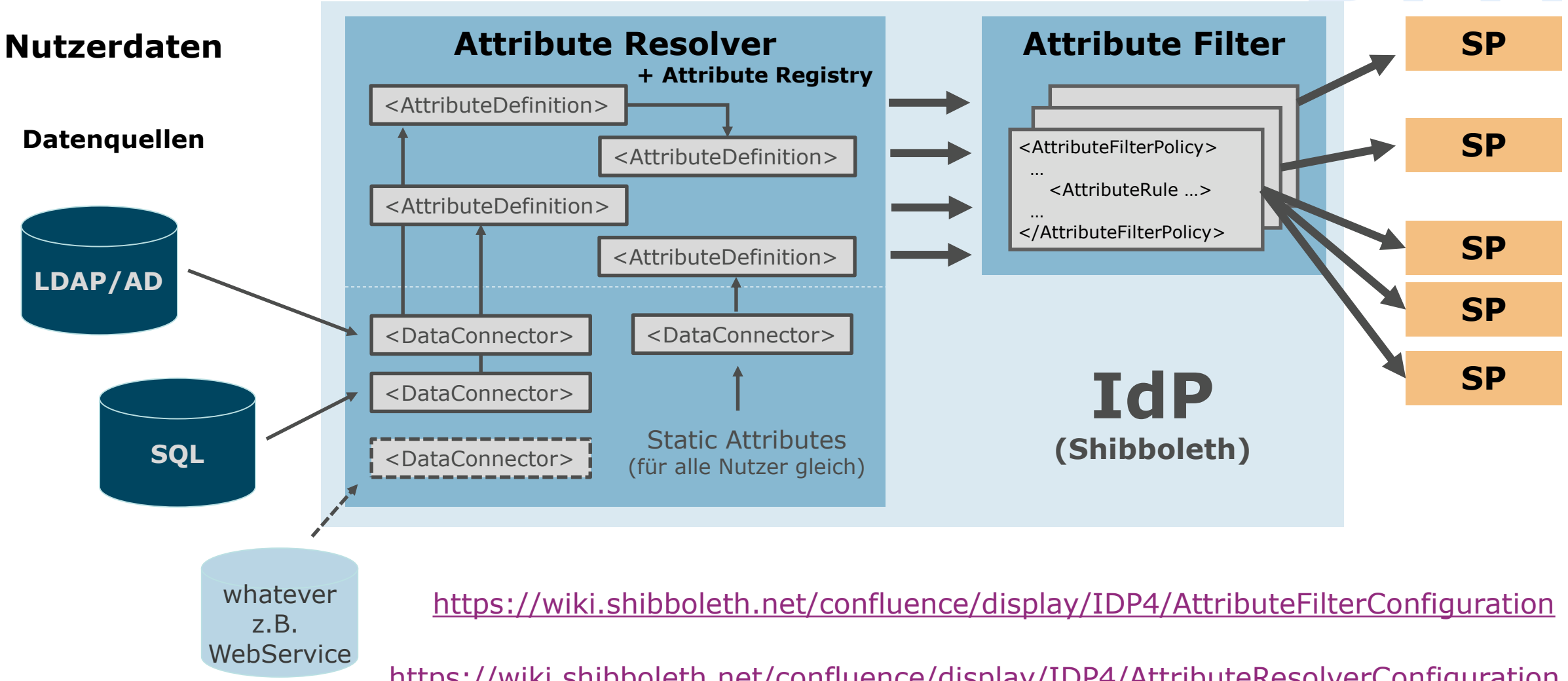
Siehe auch: https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

Kommunikation im Detail



Quelle: Manuel Haim, Uni Marburg

Der Weg der Attribute



https://wiki.shibboleth.net/confluence/display/IDP4/AttributeFilterConfiguration

https://wiki.shibboleth.net/confluence/display/IDP4/AttributeResolverConfiguration

SAML

- 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

SAML Metadaten

- Standardisiertes XML-Format (→ SAML)
- Enthalten alle Informationen, die für eine Kommunikation zwischen den beteiligten Entities (IdPs, SPs, Attribute Authorities) benötigt werden
- Eindeutiger Identifier: **entity ID**
- Datentyp: anyURI
  - (z.B. https://idp.dfn.de/idp/shibboleth)
  - Muss nicht auf eine Web-Ressource verweisen (Best Practice: IdP/SP-Metadaten), also auch nicht notwendigerweise dem Hostnamen der jeweiligen Entity entsprechen
  - Allerdings sollte die jeweilige Einrichtung auch die Rechte an der betreffenden Domain besitzen
- Einführung und Überblick unter https://www.oasis-open.org/committees/download.php/51890/SAML%20MD%20simplified%20overview.pdf

Typen von Entities

IdP = Identity Provider

- Liefert Informationen (Assertions) über Nutzer an SPs
  - Authentifizierung erfolgreich
  - Attribute (weitere Angaben, dienen der Autorisierung am SP sowie der Identifizierung des Nutzers / der Nutzerin bzw. der Personalisierung des betreffenden Dienstes)

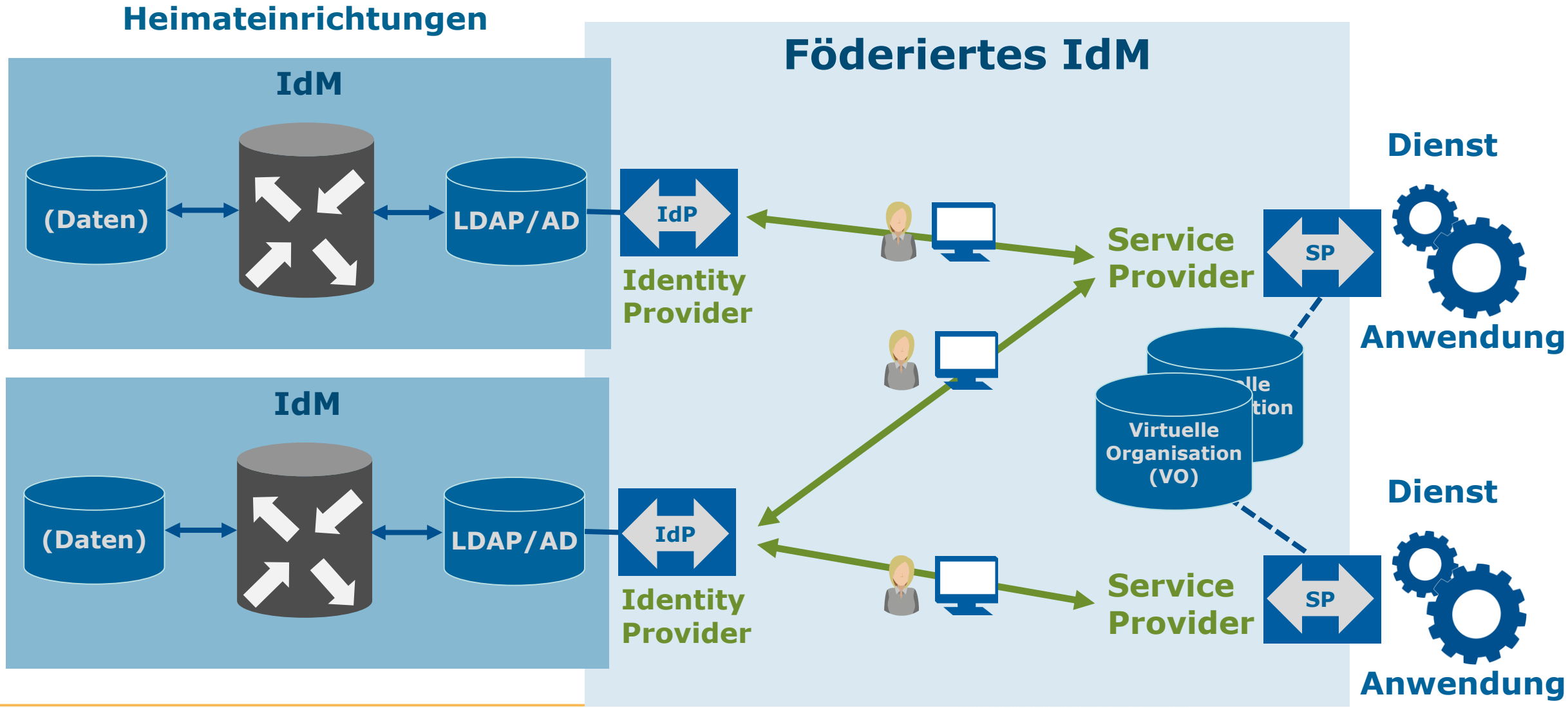
Attribute Authority

- „Abgespeckter IdP", liefert nur Attribute
- Direkter Zugriff seitens SP anhand einer Name ID (oder eines Äquivalents)

SP = Service Provider

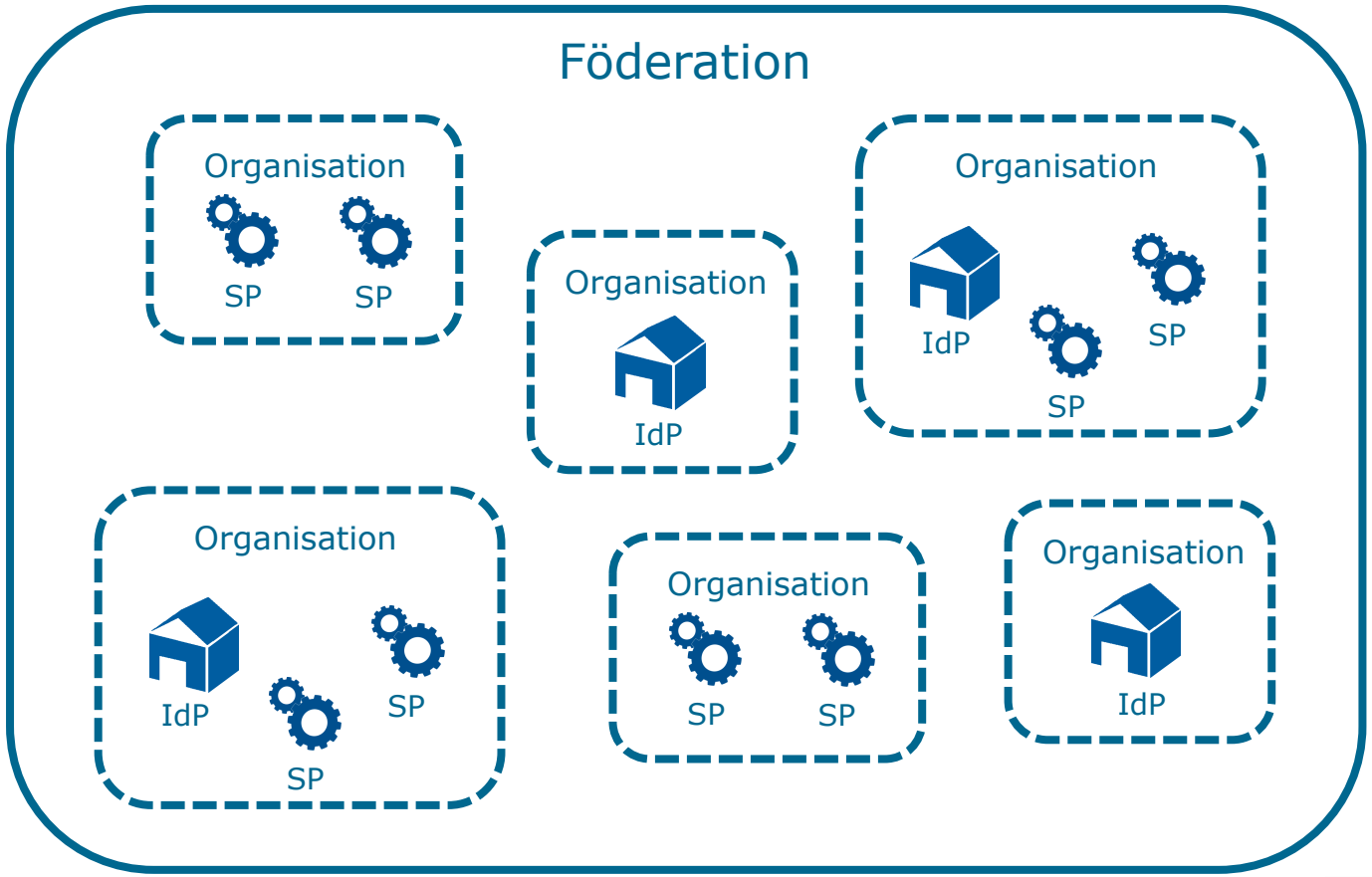
- Schützt Ressourcen
- Wertet Assertions aus und reicht Attribute an die dahinterliegende(n) Anwendunge(n) weiter

Das große Bild…



Föderationen

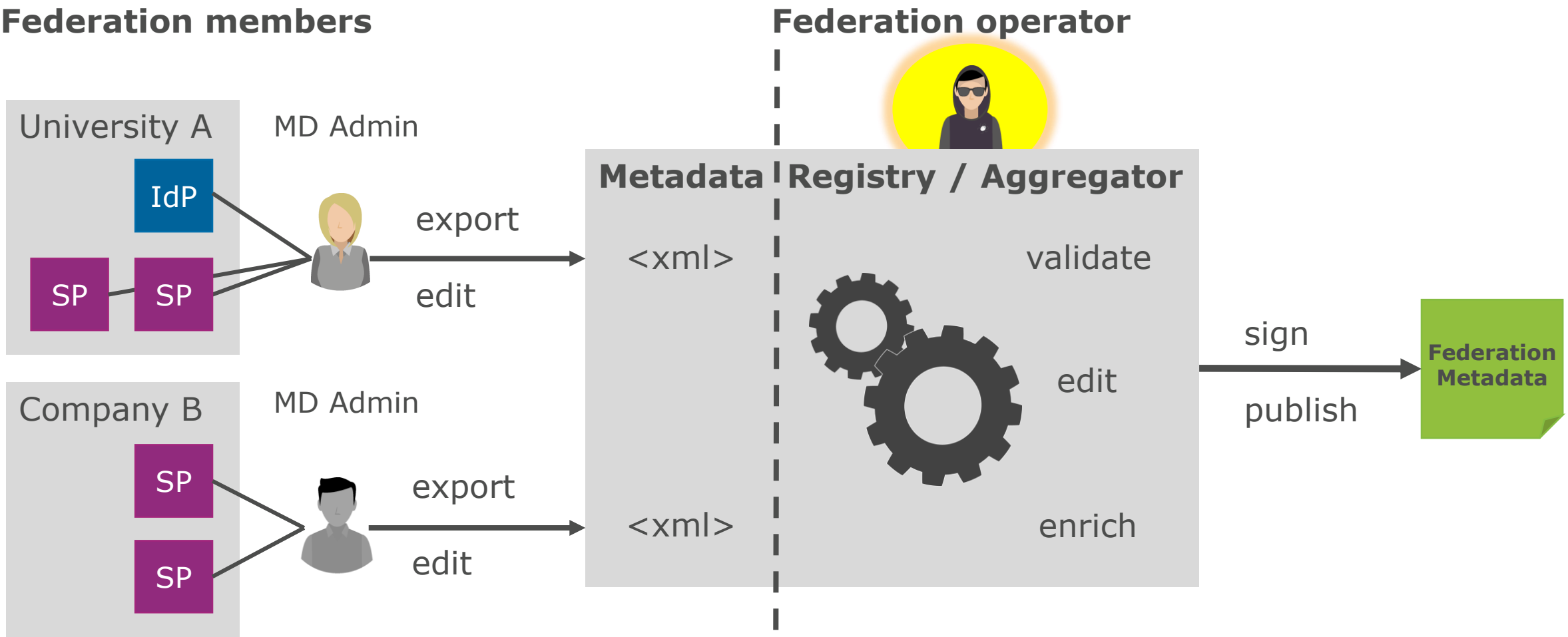
z.B. DFN-AAI



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 und Dienstanbietern
  - Metadatenverwaltung
    - Zertifikatprüfung und –überwachung (u.a.m.)
    - Signierte Metadaten

Metadata Aggregation and Management



Föderation(en) + Metadaten in der DFN-AAI

- Organisatorisch handelt es sich bei der DFN-AAI zwar um eine Identity Federation, die aber **mehrere** Metadatensätze verwaltet und zur Verfügung stellt (Liste unter https://doku.tid.dfn.de/de:metadata)

Föderationen

Typ	Aktivierung	Name	Status	Kommentar
Produktion: DFN-AAI	◉	DFN-AAI	zugelassen	
	○	DFN-AAI-Basic		
	○	keine		
	☐	lokale Metadaten		
Produktion: Interföderation	☐	eduGAIN		
Test	☑	DFN-AAI-Test	zugelassen	

schreiben | schreiben & zurück | **abbrechen**

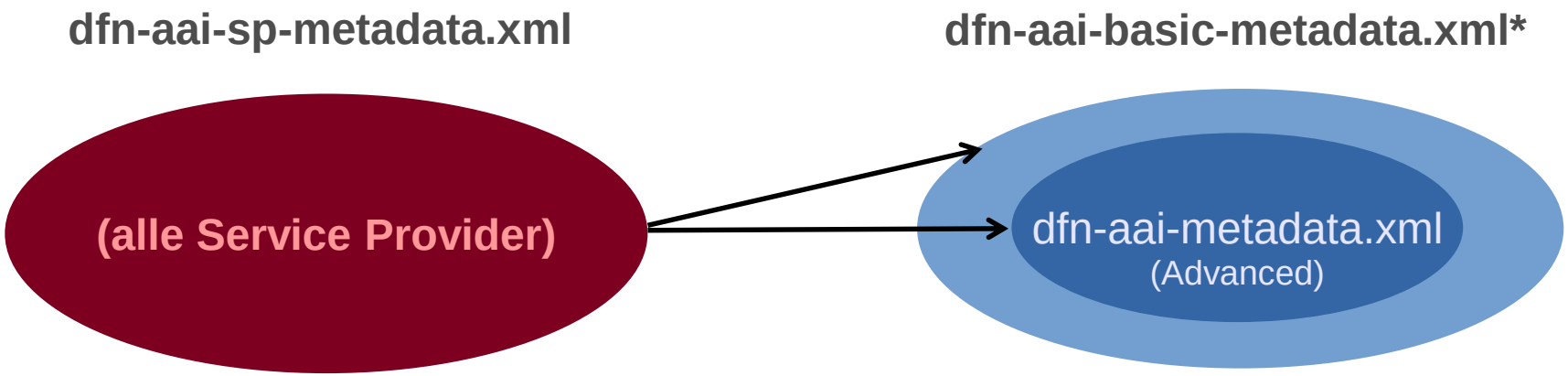
Verlässlichkeitsklassen in der DFN-AAI (1)

Verlässlichkeits-klasse	Identifizierung durch Heimateinrichtung	Verfahren zum Ausweis einer Identität	Datenhaltung und Prozesse zur Pflege der Identitäten
n.a. / Test	Verfahren freigestellt	Verfahren freigestellt	Verfahren freigestellt
Basic	Rückantwort von eindeutiger Adresse (E-Mail, Tel.-Nr., Postanschrift, etc.)	Anhand eindeutig zuzuordnender digitalen Adresse	Verpflichtung bzgl. Aktualität innerhalb von 3 Monaten
Advanced	pers. Vorsprechen gegenüber Vertrauens-instanz unter Vorlage amtlicher Dokumente (alternativ: Post-Ident, eID/nPA). Die an den Hochschulen etablierten Einschreibungs- und Einstellungsprozesse werden als gleichwertig akzeptiert	pers. Account bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Verpflichtung bzgl. Aktualität innerhalb von 2 Wochen

Vgl. https://doku.tid.dfn.de/de:degrees_of_reliance

Verlässlichkeitsklassen in der DFN-AAI (2)

Technische Umsetzung: getrennte Metadatensätze



* enthält **alle** IdP

	IdP / AA	SP
Advanced	`dfn-aai-sp-metadata.xml`	`dfn-aai-metadata.xml`
Basic	`dfn-aai-sp-metadata.xml`	–
Advanced + Basic	–	`dfn-aai-basic-metadata.xml`
eduGAIN	`dfn-aai-edugain+sp-metadata.xml`	`dfn-aai-edugain+idp-metadata.xml`
Lokale Metadaten	`dfn-aai-local-999-metadata.xml*`	`dfn-aai-local-999-metadata.xml*`

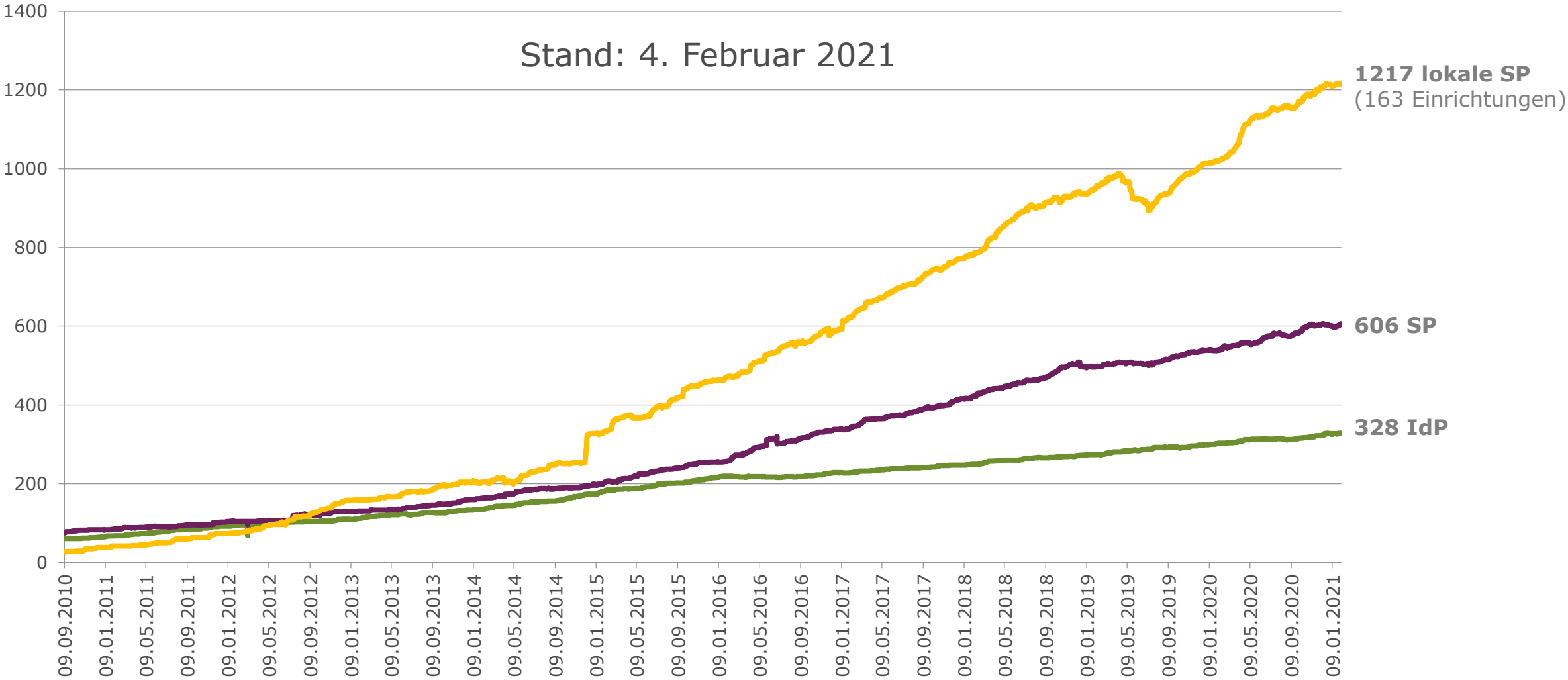
https://doku.tid.dfn.de/de:production

* „999“ wird durch einrichtungs-spezifische Nummer ersetzt

Lokale Metadaten (= Mini-Föderation)

- Einrichtungs-spezifischer Metadatensatz, in dem interne SPs sowie der jeweilige IdP registriert sind
- Metadaten werden stündlich neu generiert und signiert, bei Bedarf Zugriff nur für bestimmte IP-Bereiche
- Validierung der Metadaten, automatische Zertifikat-Checks
- Lohnt sich vor allem für Einrichtungen mit vielen lokalen SPs (z.B. FU Berlin über hundert SPs)
- Angebot wird derzeit (4.2.2021) von 163 Einrichtungen mit insgesamt 1217 SPs genutzt
- Doku: https://doku.tid.dfn.de/de:metadata_local

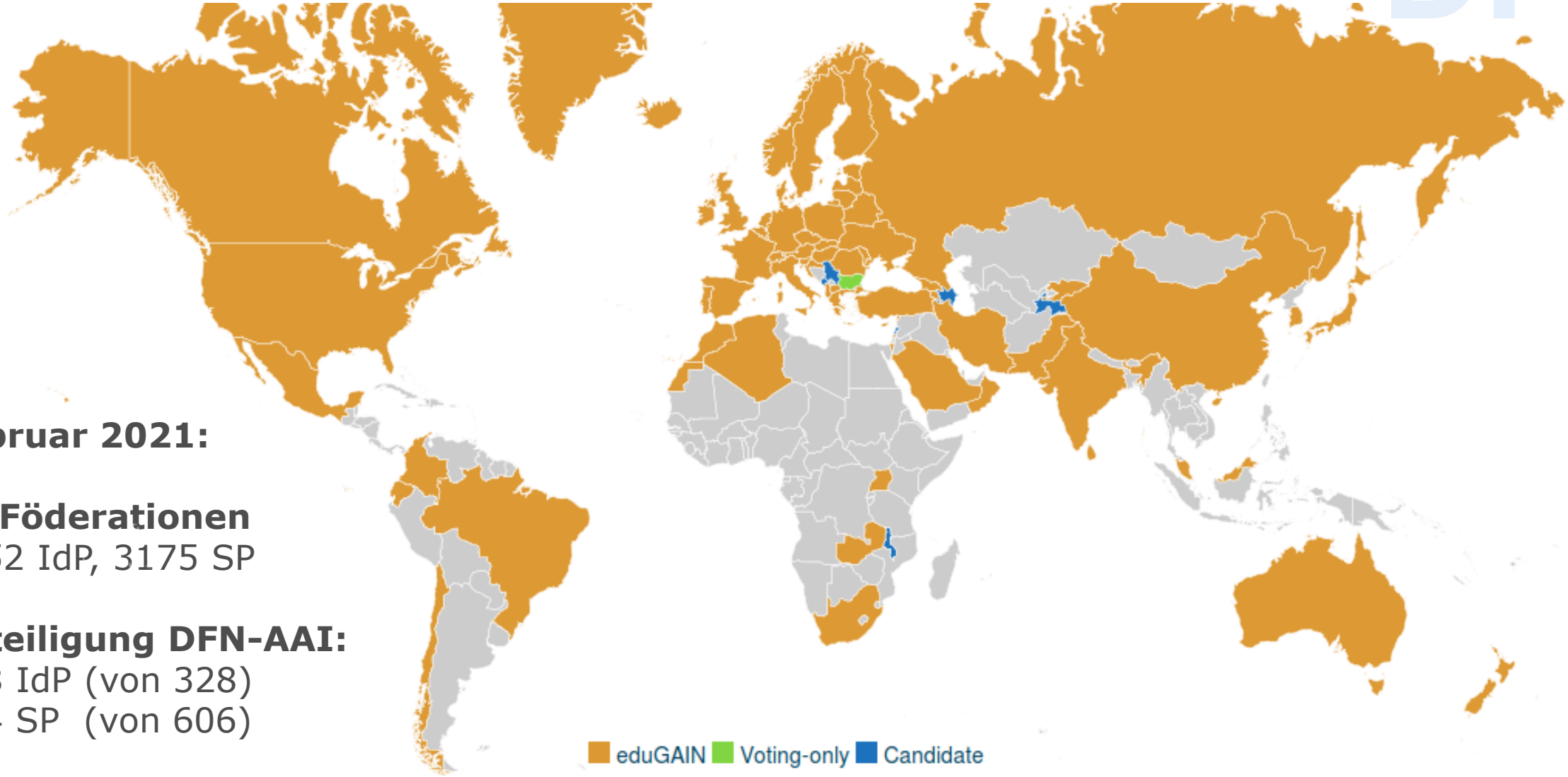
Aktuelle Zahlen DFN-AAI



eduGAIN

- Föderationsübergreifende AAI
- Betrieben von GÉANT, seit Ende 2011 im Produktivbetrieb
- Aggregation der Metadaten der teilnehmenden Föderationen („Upstream Metadata“)
- Teilnehmende Föderationen verteilen diese Metadaten intern („Downstream Metadata“)
- Upstream Metadata: Opt-in vs. Opt-out; DFN-AAI verfolgt eine Opt-in Policy, d.h. Teilnahme nur auf expliziten Wunsch
- Keine Vertragsbeziehungen zwischen DFN und IdP/SP anderer Föderationen(!)

eduGAIN – beteiligte Föderationen



Februar 2021:

71 Föderationen
4152 IdP, 3175 SP

Beteiligung DFN-AAI:
248 IdP (von 328)
144 SP (von 606)

Discovery

Discovery Service

- Auch bekannt als **WAYF**, „**W**here **A**re **Y**ou **F**rom“
- Dient der Browser-gestützten Einrichtungsauswahl für den/die Endnutzer(in)
- Stellt Verbindung zwischen SP und IdP her
- Varianten:
  - Zentraler Discovery Service
  - (z.B. von Föderation betrieben)
  - Embedded Discovery Service (am SP)
  - WAYFless URLs
- DFN-AAI Wiki: https://doku.tid.dfn.de/de:discovery

Beispiel zentraler Discovery Service

- Vom DFN betrieben
- Stündlich neu generiert
- DFN-AAI (”Advanced”)
- DFN-AAI-Basic
- DFN-AAI-Basic+eduGAIN
- DFN-AAI-Test
- ...

Embedded Discovery Service (EDS)

- Nutzerfreundlich, da nur IdPs gelistet, die tatsächlich für den Dienst relevant sind
- Wird lokal am SP anhand der eingelesenen Metadaten konfiguriert
- Filterfunktion: Blacklist / Whitelist
- Üblicherweise JavaScript Anwendung
- Beispiele
  - SWITCH EDS: https://www.switch.ch/aai/guides/discovery/embedded-wayf/
  - Shibboleth EDS: https://doku.tid.dfn.de/de:shibeds
- Best Practice Empfehlungen: NISO ESPReSSO, REFEDS Discovery Guide; aktuell: RA21 Initiative

WAYFless URLs

- URL, der beim betreffenden SP direkt einen *Authentication Request* zu einem bestimmten IdP auslöst
- IdP und SP sind hart verdrahtet
- Sehr nutzerfreundlich, da Einrichtungsauswahl entfällt
- Muss angepasst werden, wenn sich der betreffende URL des SP ändert!
- Wird nicht von allen SPs unterstützt
- Beispiel:
  https://doku.tid.dfn.de/Shibboleth.sso/Login?entityID=https://idp.dfn.de/idp/shibboleth
- Siehe auch unter https://doku.tid.dfn.de/de:shibwayfless

Teilnahme

Rollen in der DFN-AAI

- Föderationsbetreiber (DFN-Verein)
  - Verträge mit allen teilnehmenden Einrichtungen und Dienstanbietern
  - Metadatenverwaltung und -Signierung, Metadatenverwaltungsnutzerverwaltung
- Teilnehmer (IdP/AA → Dienstvereinbarung, SP → SP Agreement)
  - Vertrag: administrativer AP, technischer AP (beide in Vertrags-DB)
  - Metadata-Admin (in Vertrags-DB)
- Entity (IdP/AA/SP) – Kontakte in Metadaten:
  - Support
  - Administrativ
  - Technisch
  - Security

International (eduGAIN) in etwa parallele Strukturen

IR Koordination:
eduGAIN Security Team
abuse@edugain.org

Verträge für die Teilnahme an der DFN-AAI

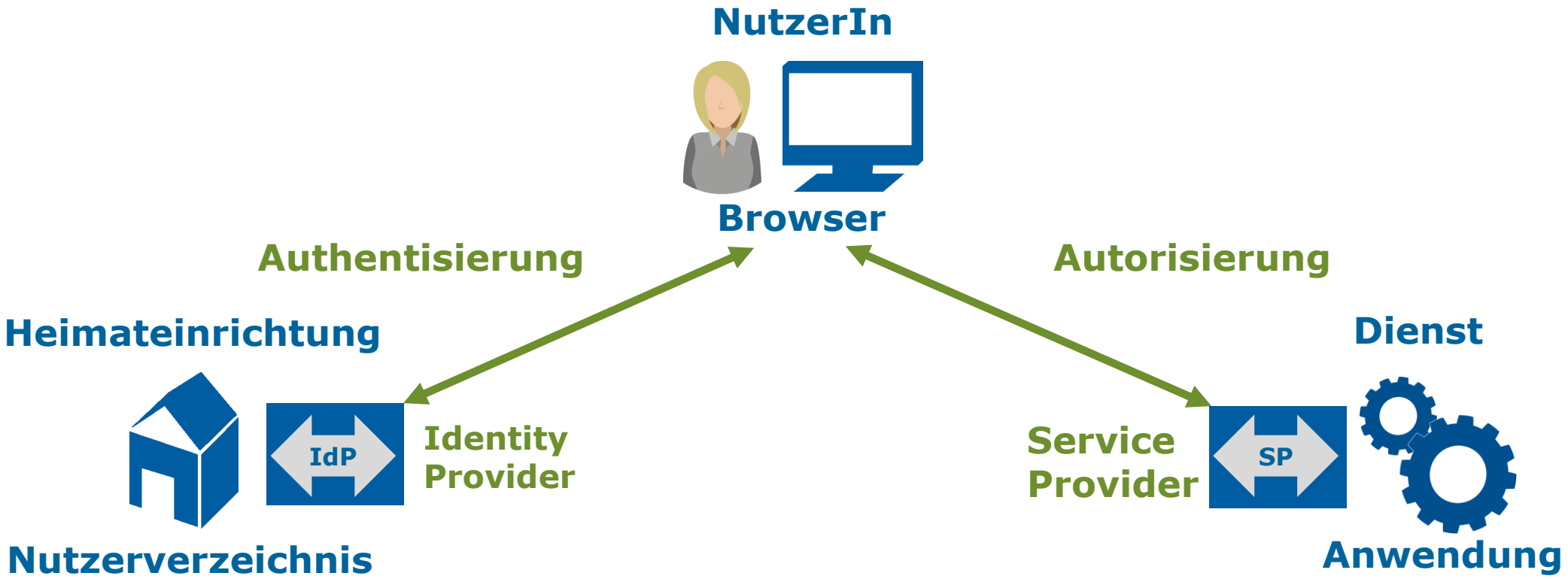
- Unterschiedliche Vertragstypen, abhängig von Rolle
  - Identity Provider (IdP) – Heimateinrichtungen (Hochschulen, Forschungseinrichtungen,…)
  - Service Provider (SP) – kommerzielle und nicht-kommerzielle Dienstanbieter, aber auch Heimateinrichtungen
- Heimateinrichtungen: DFN-AAI ist ein Mehrwertdienst (DFNInternet ab I02), erforderlich sind Rahmenvertrag *und* Dienstvereinbarung
  - Dienstvereinbarung beinhaltet SP-Option
- Dienstanbieter: SP-Agreement (englisch) – keine sonstigen Voraussetzungen

Teilnahme technisch

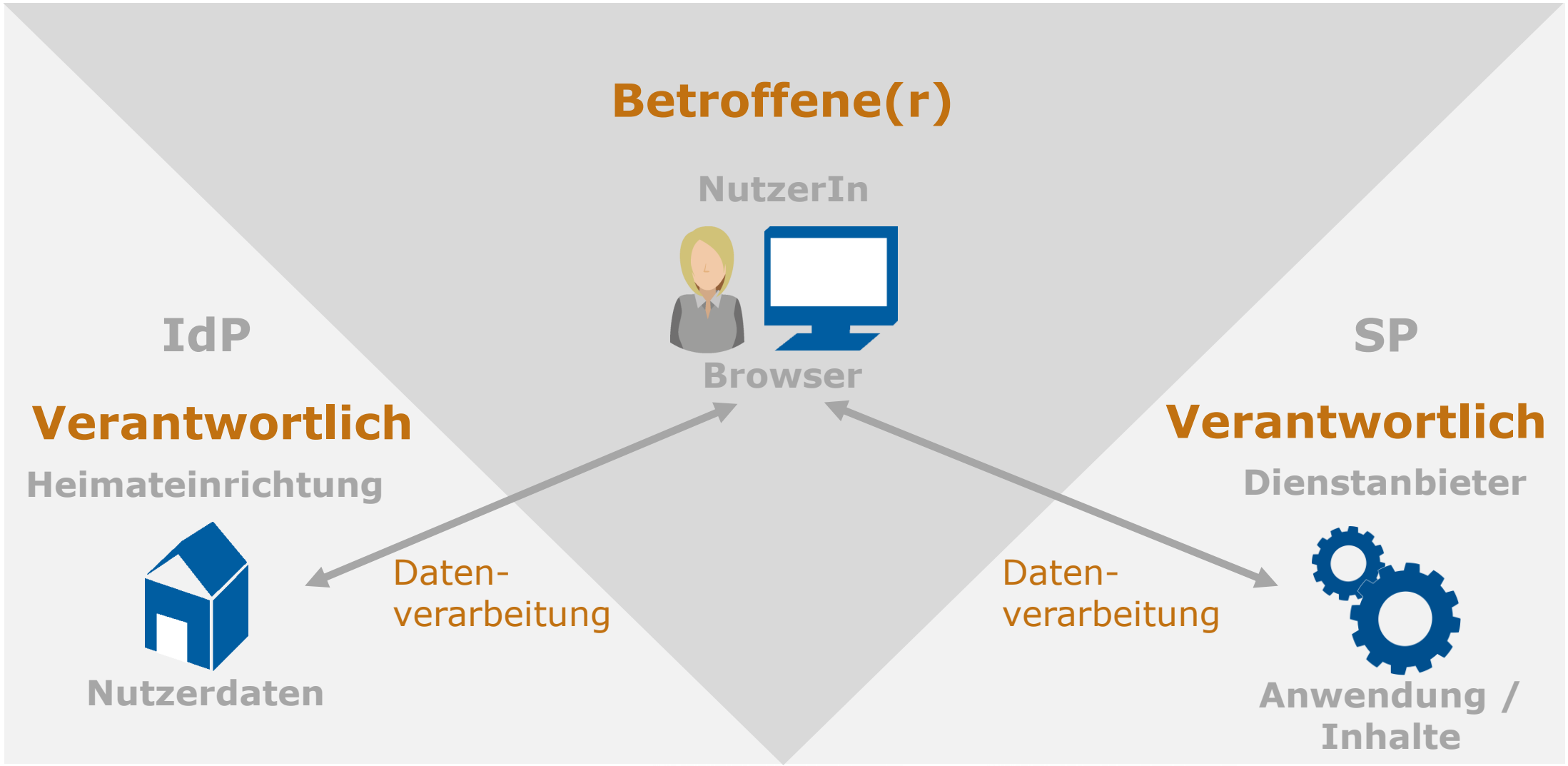
- Identity Provider (IdP) wird von oder im Auftrag der teilnehmenden Heimateinrichtung betrieben
  - Üblicherweise **eine** produktive Instanz
  - Shibboleth IdP ist gut dokumentiert
  - DFN-AAI Team bietet Support und Schulungen
- Service Provider (SP) wird von oder im Auftrag der teilnehmenden Einrichtung oder einer anderen Organisation (Dienstanbieter) betrieben
  - 1..n Instanzen
  - Shibboleth SP ist gut dokumentiert
  - DFN-AAI Team bietet Support (und Schulungen)

Datenschutzaspekte AAI

Wir erinnern uns…



Datenschutz – Rollen

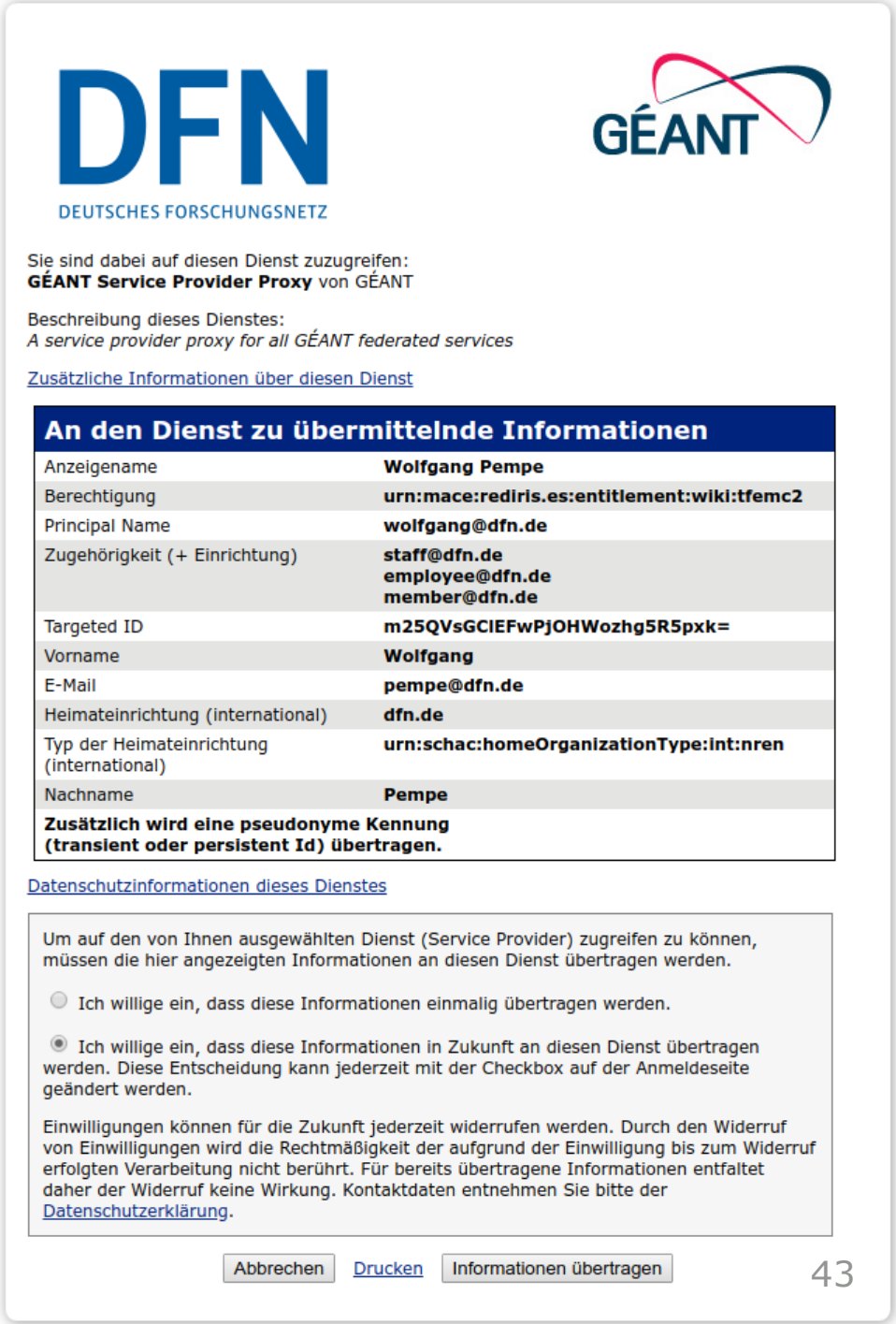


IdP-Betreiber

- 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 (4.2.2021) 328 IdP und 606 SP (374 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

Sonstiges

Shibboleth

- … ist der Name eines Software-Projekts: Identity Provider (Java) und Service Provider (Apache Modul, C++)
- Ursprünglich von Internet2 entwickelt, erstes Release 2003
- Bezeichnung geht zurück auf Bibel: Richter 12,5-6 (illustrierte Version, The Brick Testament)
- Weiterentwicklung wird seit 2013 vom Shibboleth Consortium getragen (über 50 Mitglieder)
- Aktuell 9 Entwickler beschäftigt

Aktivitäten und Kooperationen national

- Mitarbeit im ZKI Arbeitskreis Identity und Access Management
- ZKI Arbeitsgruppe edu-ID
- DFN-Betriebstagung: AAI-Forum
- Gemeinsam mit FU Berlin: seit 2015 jährlicher Shibboleth Workshop, nächster Termin: KW 8 (virtuell)
- Auf Anfrage Schulungsveranstaltungen für regionale Nutzerschaft
- Organisation und Moderation von Ad-hoc-Arbeitsgruppen

Aktivitäten und Kooperationen international

- DFN-Verein ist eduGAIN-Mitglied der ersten Stunde
- GÉANT Project (GN4-3): Beteiligung in WP5, „Trust & Identity“
- EOSC Future: Task 7.3 (AAI), Linked Third Party über GÉANT, Start demnächst
- AARC2 - Authentication and Authorisation for Research and Collaboration
  - Anforderungen der Research Communities erheben und Lösungen erarbeiten (Projektende April 2019)
- Mitgliedschaft im Shibboleth Consortium (seit 2014)
  - Wolfgang Pempe (DFN-Verein) ist als einer von zwei gewählten *Members*‘ *Representatives* Mitglied des Consortium Boards

Planungen für die nähere Zukunft

- Verlässlichkeitsklassen / Levels of Assurance nicht mehr nur über verschiedene Metadatensätze modellieren, sondern über Attribute (eduPersonAssurance) und Authentication Context Classes
  - Übernahme des REFEDS Assurance Framework https://refeds.org/assurance
  - Ermöglicht LoAs per Identität / Login-Vorgang
- Unterstützung für OpenID Connect, http://openid.net/connect/
- Konzept „AAIplus“ zur Sicherung der Zukunftsfähigkeit der DFN-AAI

Vielen Dank! Fragen? Kommentare?

- Kontakt

Wolfgang Pempe, Teamleiter DFN-AAI

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

- DFN-AAI Wiki:

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

- Verzeichnis(se) der Teilnehmer: https://tools.aai.dfn.de/entities/

- Shibboleth Wiki: https://wiki.shibboleth.net