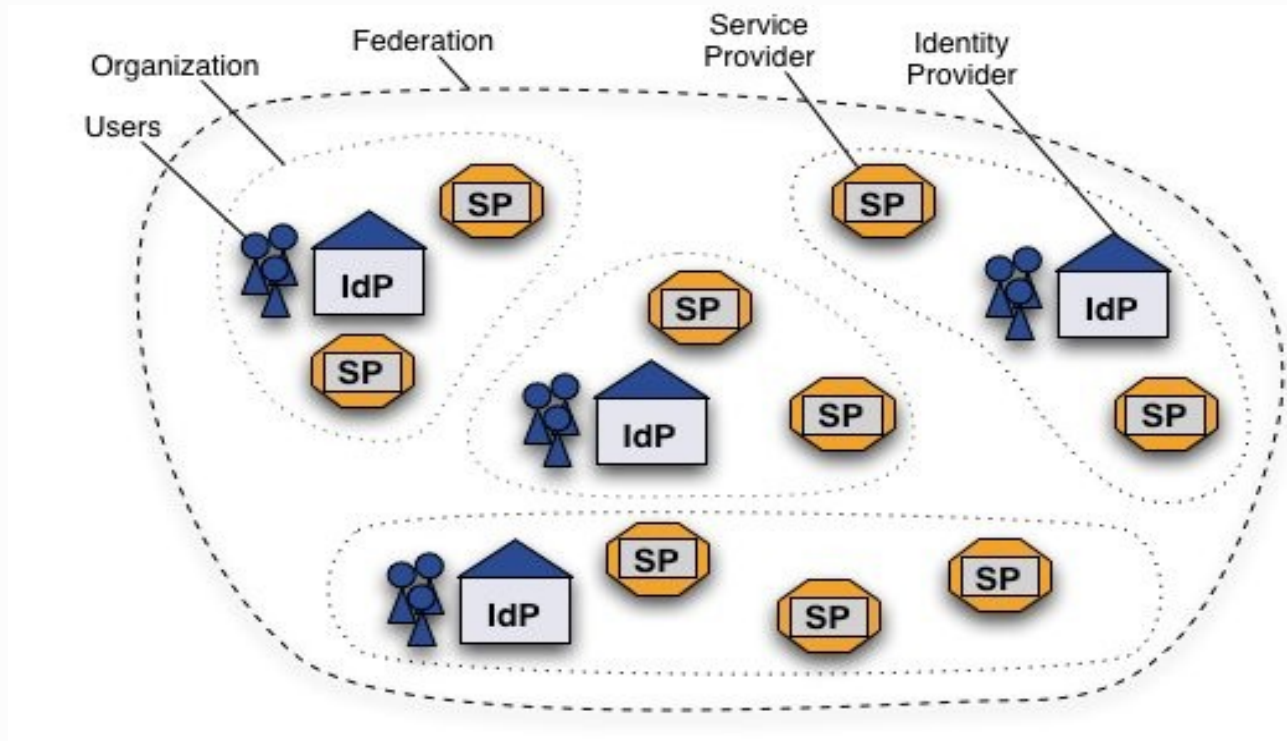


Intra- und Inter-Föderation mit der DFN-AAI

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

ZKI Arbeitskreis Verzeichnisdienste
Frühjahrstreffen 5./6. März 2013, Rostock



(Quelle: <http://www.switch.ch/aai/about/federation/>)

Auf Softwareebene gibt es keine Föderationen, sondern nur Metadaten.
Aber ohne Föderationen gäbe es keine verlässlichen Metadaten!

(Bernd Oberknapp, UB Freiburg,
http://aar.vascoda.de/doc/presentation/workshop-2006-10-10/AAR_20061010_Metadaten.pdf)

Anwendungsfall: bwIDM

- Siehe Vortrag Nussbaumer Oktober 2012 in Würzburg: "bwIDM Subföderation"
- Dienste (Service Provider) nur für teilnehmende Einrichtungen verfügbar
- Lösungsansätze:
 - ♦ Eigener Metadatensatz → aufwändig, skaliert nicht
 - ♦ Filter nach EntityIDs → bedarf permanenter Pflege
 - ♦ Entity Attribut: Entity Category → vielversprechend

Entity Categories – Überblick

- Attribute auf Entity-Ebene (oder höher)
- Sowohl Shibboleth IdP als auch SP (ab 2.5) unterstützen entsprechende Filterfunktionen
- Aufbau virtueller Föderationen
- Neue Aufgaben für Föderationsbetreiber:
Kontrolle, ob Attribute berechtigt vergeben werden
- Bereits produktiv bei InCommon eingesetzt
(Research & Scholarship Category – Attribut-Profil)

Umsetzung: Zutaten

- Eine Metadatenverwaltung, die die Vergabe von Entity Categories unterstützt
- Aktuelle Shibboleth-Software
 - ♦ SP 2.5.x
 - ♦ IdP 2.3.x
- Eine Föderation, die willens ist, die Vergabe dieser Attribute zu kontrollieren
- Eine zentral gepflegte Whitelist, die die IDs der teilnehmenden Entities enthält

Entity Category: bwidm-member

Entity-Kategorien

Neuer Wert

```
wolfgang@idphost0: /adm/services/aai/orgs/e15/idp/https_idp.dfn.de_idp_shibboleth 84x14
<EntityDescriptor entityID="https://idp.dfn.de/idp/shibboleth">
  <Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="http://macedir.org/entity-category">
        <saml:AttributeValue>http://aai.dfn.de/category/bwidm-member</saml:Attribu
teValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  <IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0 urn:oasis:
names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
```

Kontrolle seitens der Föderation

- Metadatenverwaltung: Kategorie nur auswählbar, wenn auch auf Whitelist vorhanden
- Nochmalige Überprüfung bei der stündlichen Metadaten-Generierung
- Kategorie wird automatisch gelöscht, wenn die betreffende EntityID nicht mehr gelistet ist
- Noch unklar, ob und in welchem Umfang solche Kontrollen für weitere Projekte leistbar sind...

SP – MetadataFilter

```
<MetadataProvider type="XML"
  uri="https://dev.aai.dfn.de/fileadmin/metadata/DFN-AAI-Test-metadata.xml"
  backingFilePath="/etc/shibboleth/metadata/DFN-AAI-Test-metadata-extensions.xml"
  reloadInterval="700">
  <MetadataFilter type="Whitelist" matcher="EntityAttributes">
    <saml:Attribute Name="http://macedir.org/entity-category"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue>http://aai.dfn.de/category/bwidm-member</saml:AttributeValue>
    </saml:Attribute>
  </MetadataFilter>
</MetadataProvider>
```


IdP – Attribute Filter Policy

```
<afp:AttributeFilterPolicy id="releaseBwAttributesToBwIdM">
  <afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://aai.dfn.de/category/bwidm-member" />

  <afp:AttributeRule attributeID="mail">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <afp:AttributeRule attributeID="sn">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>


  <!-- u.s.w. -->

</afp:AttributeFilterPolicy>
```

Vorsicht – Datenschutz!

- Grundsatz der Datensparsamkeit
- Keine Attributfreigabe nach dem Gießkannenprinzip (bei personenbezogenen Daten)
- In anderen Kontexten durchaus relevant
- SP sollten nur die Attribute übermittelt bekommen, die zur Erbringung des Dienstes notwendig sind
- Deklaration der Requested Attributes in den Metadaten
- Dynamische Attributfreigabe durch uApprove

<RequestedAttribute>

Attribute Consuming Service	
Name	eduPersonPrincipalName 
isRequired	true
benötigte Attribute hinzufügen	
Name	
isRequired	true

```
wolfgang@idphost0: ~ 91x7

<RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:mace:dir:attrib
ute-def:eduPersonPrincipalName" NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"
isRequired="true"></RequestedAttribute>
<RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1
.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="tru
e"></RequestedAttribute>
```

Dynamische Attributfreigabe

```
<afp:AttributeFilterPolicy id="releaseToCoC">
  <afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://www.edugain.org/dataprotection/coc-eu-01-draft" />

  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="ua:AttributeInMetadata" onlyIfRequired="true"/>
  </afp:AttributeRule>

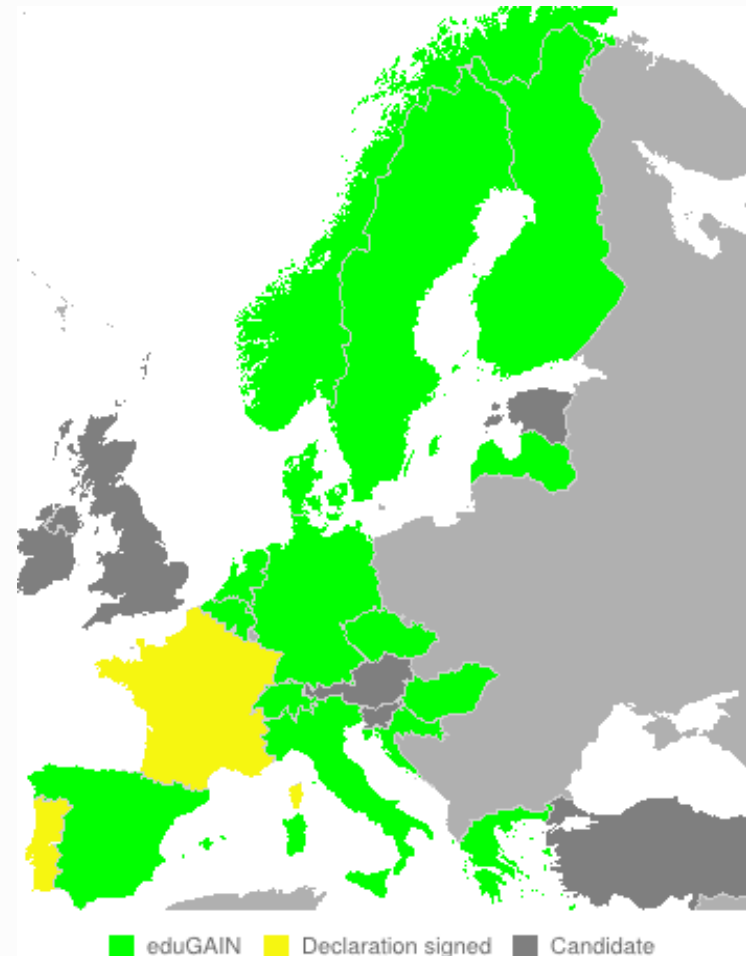
  <afp:AttributeRule attributeID="displayName">
    <afp:PermitValueRule xsi:type="ua:AttributeInMetadata" onlyIfRequired="true"/>
  </afp:AttributeRule>

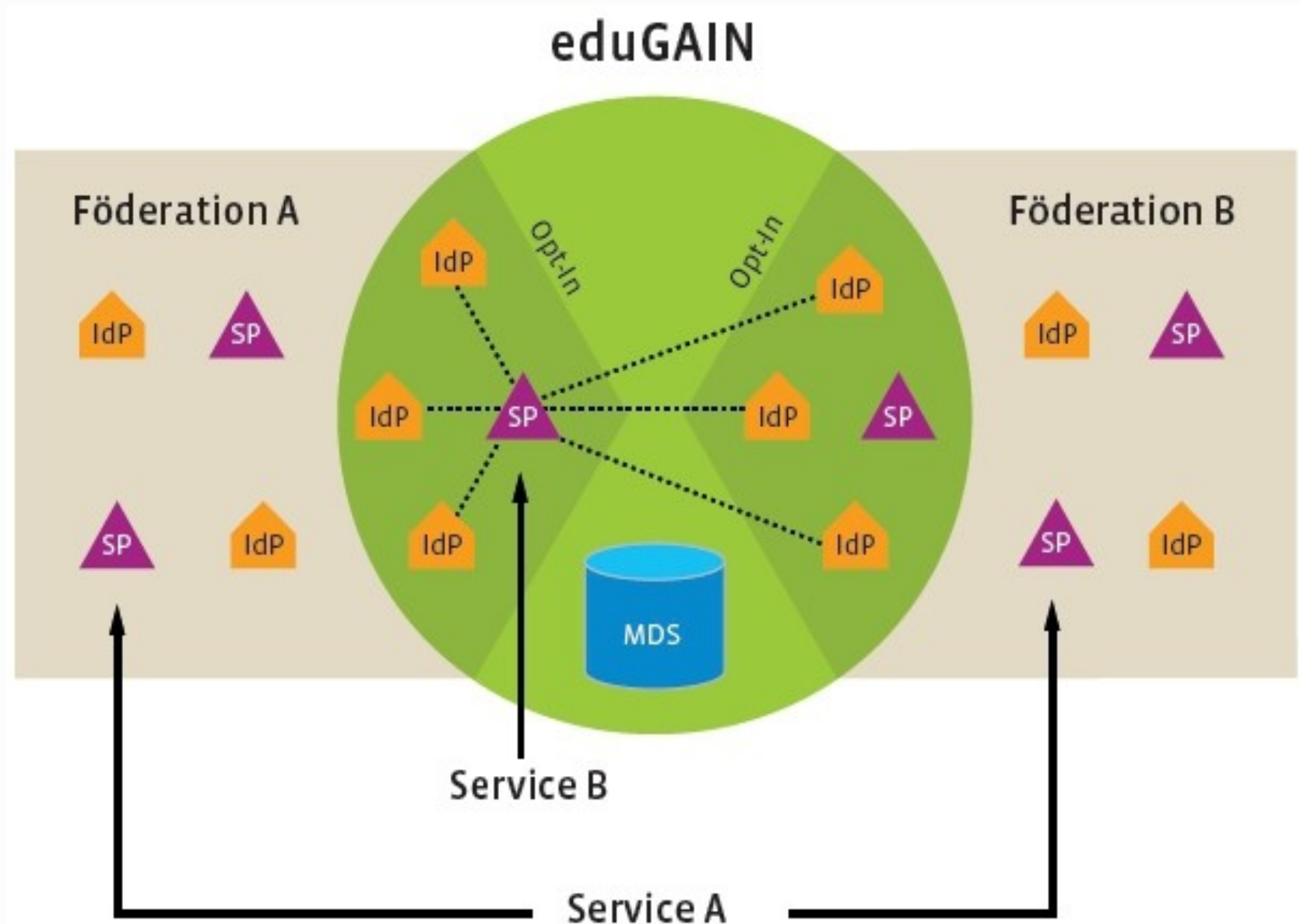
  <!-- u.s.w. -->

</afp:AttributeFilterPolicy>
```

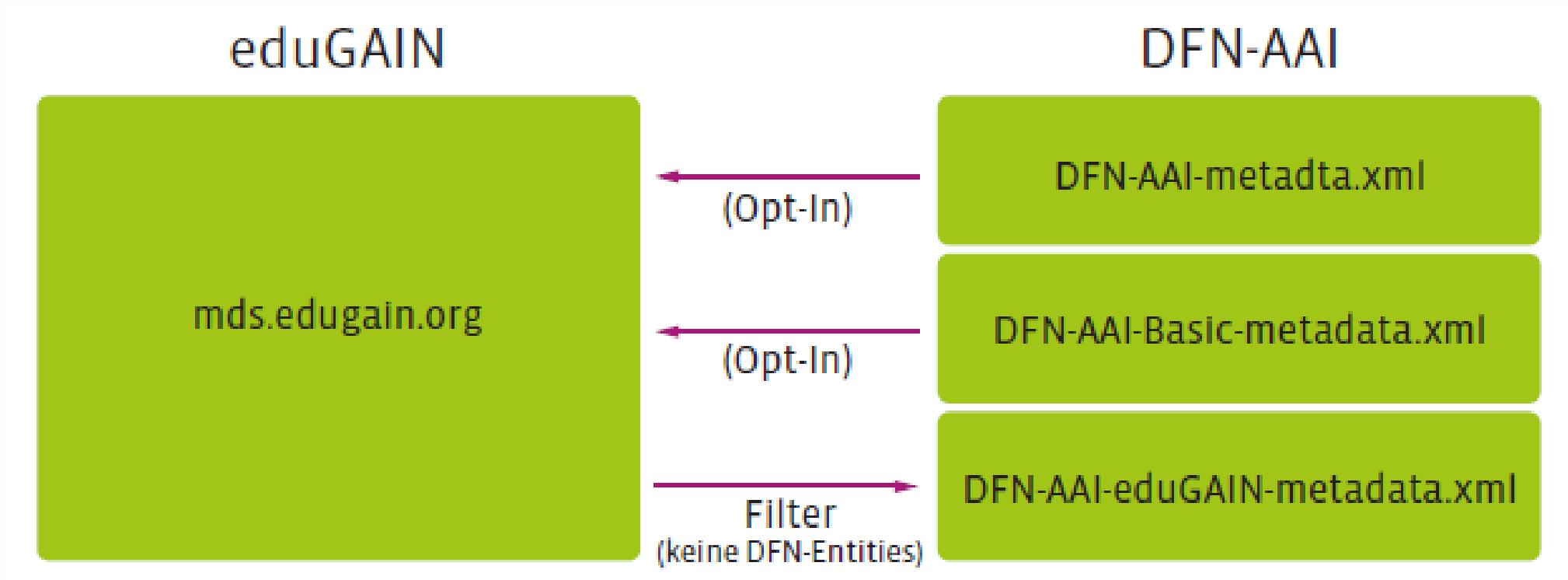


- Im Rahmen von GÉANT2 entwickelt (JRA5, wie eduroam)
- AAI / SSO über Föderations- und Ländergrenzen hinweg
- Fokus auf Bildung + Forschung
- Nicht auf Europa beschränkt
- DFN mit eigenen Metadaten beteiligt
- Derzeit über 130 Provider registriert






Metadaten-Management



"Opt-In" via Metadatenverwaltung

Föderationen					
Typ	Aktivierung	Name	Status	Kommentar	
Produktion: DFN-AAI	<input type="radio"/>	DFN-AAI			
	<input checked="" type="radio"/>	DFN-AAI-Basic + DFN-AAI	zugelassen		
	<input type="radio"/>	keine			
	<input type="radio"/>	lokale Metadaten			
Produktion: Interföderation	<input checked="" type="checkbox"/>	eduGAIN	zugelassen		
Test	<input type="checkbox"/>	DFN-AAI-Test			

Voraussetzungen:

- SAML2-fähig / -Unterstützung
- Entity ist in der Produktivföderation der DFN-AAI registriert

eduGAIN – offene Punkte

- Bislang kein offizielles Verzeichnis der registrierten Provider → welche Dienste sind verfügbar?
- Verlässlichkeitsklassen / Levels of Assurance?
- Datenschutz?
→ GÉANT Data Protection Code of Conduct
- Noch fehlen Frankreich, Österreich und UK
→ wichtig z.B. für ESFRI-Projekte
- Mehrfachregistrierungen

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

Kontakt

Portal: <https://www.aai.dfn.de>

EMail: hotline@aai.dfn.de

Tel.: +49 711 63314 215