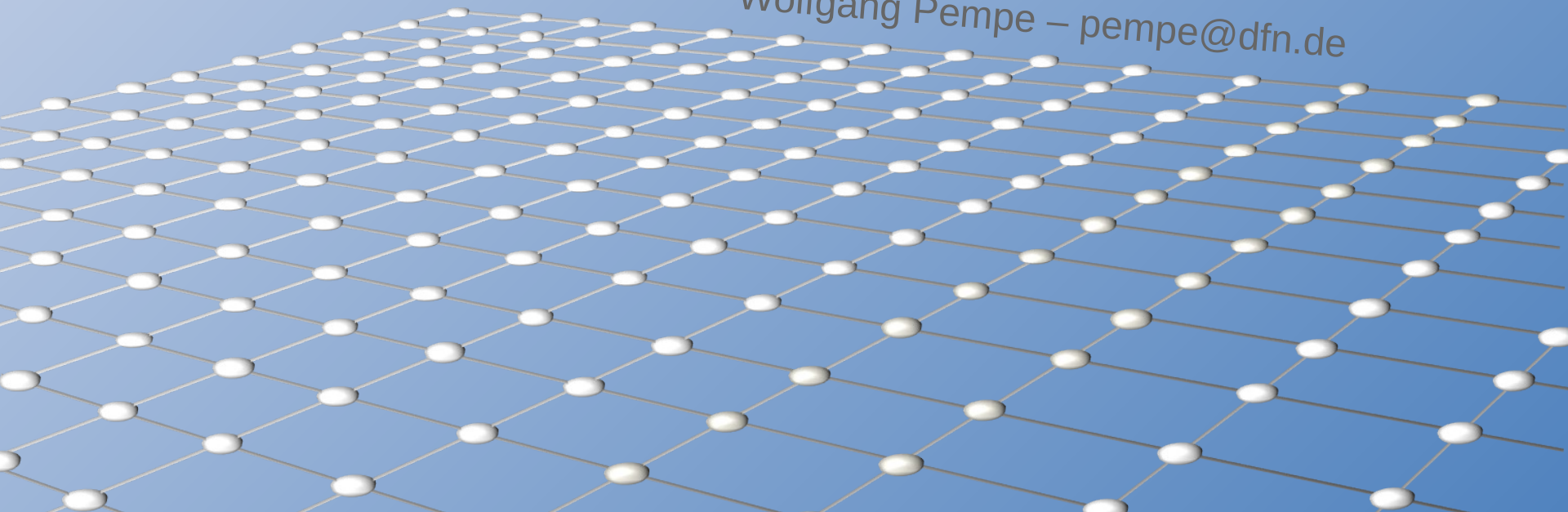
DFN
Deutsches Forschungsnetz

FIM – Organisational Issues at the NREN Level

FIM Meeting June 21/22, 2012
MPI for Psycholinguistics, Nijmegen

Wolfgang Pempe – pempe@dfn.de



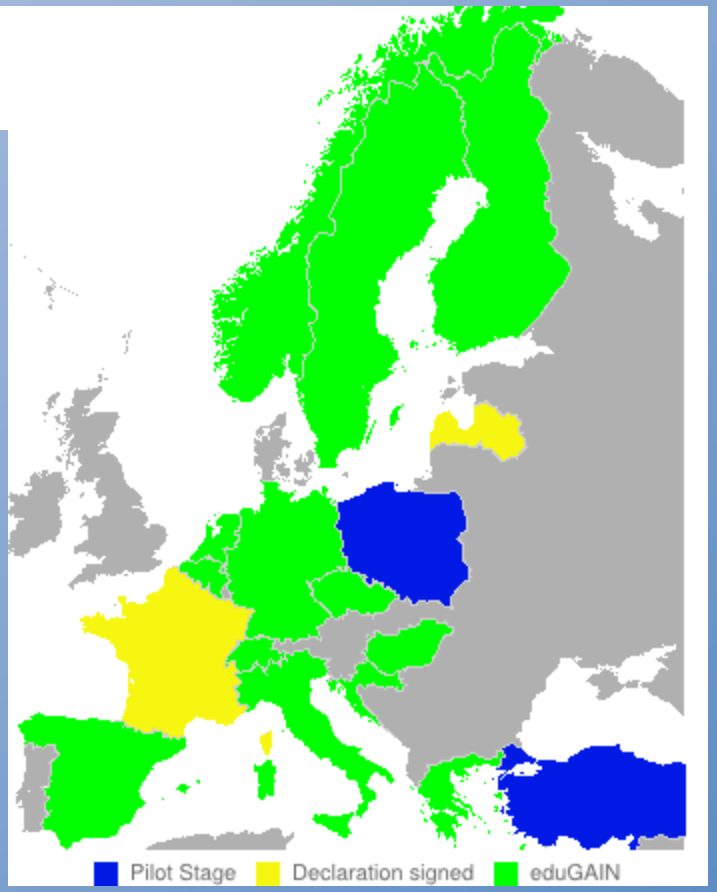
Selected Issues

- Interfederation
- Attributes
  - Release
  - Management
- Enhancing the Level of Trust: Entity Attributes

Interfederation / eduGAIN

(http://www.edugain.org)

- Developed in the context of GÉANT2 (JRA5, as eduroam)
- AAI / SSO across federations and political borders
- Focus on research + education
- Not restricted on European Federations
- DFN participating
- Already productive (~ 90 entities)

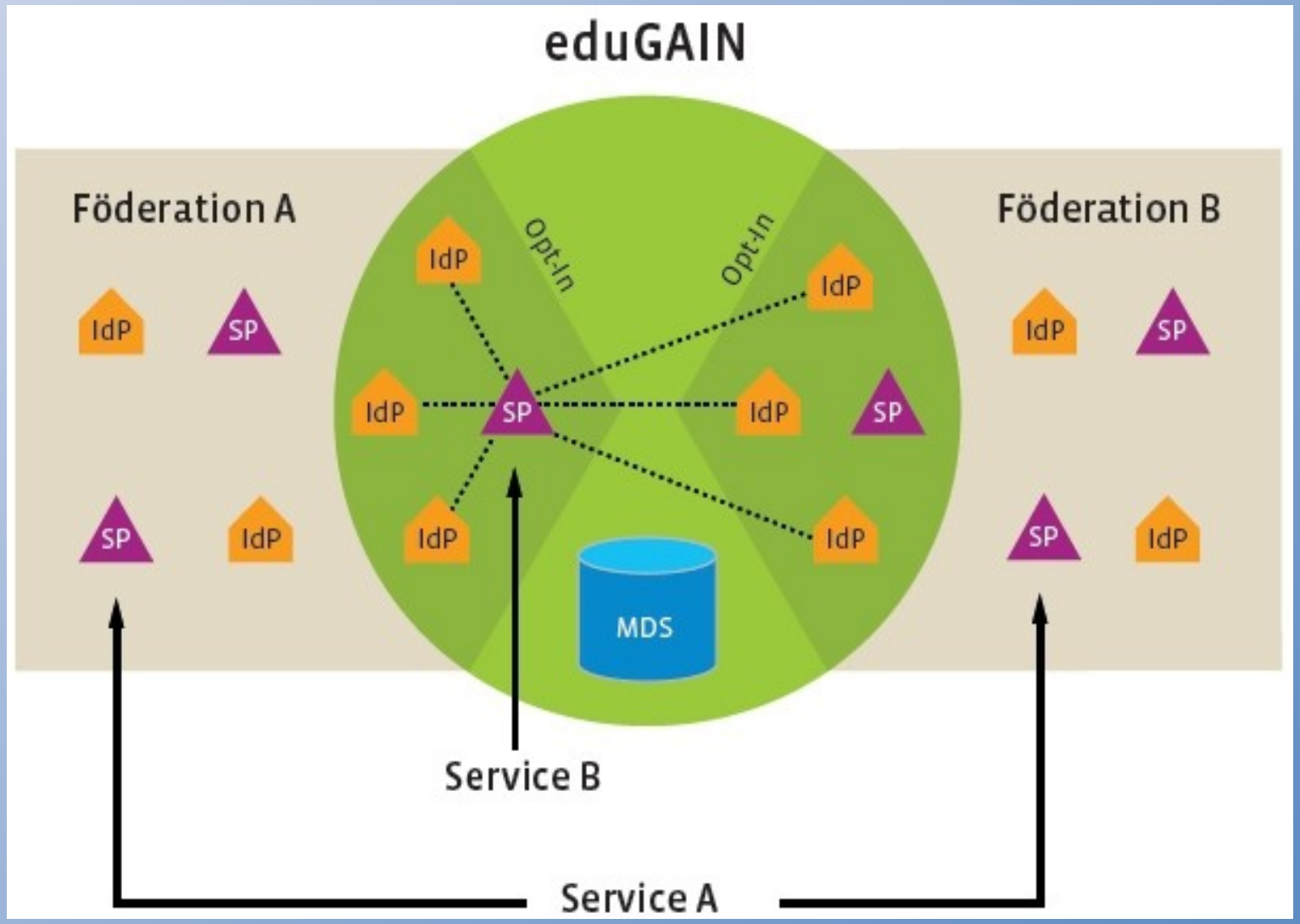


Source: http://www.edugain.org/technical/status.php

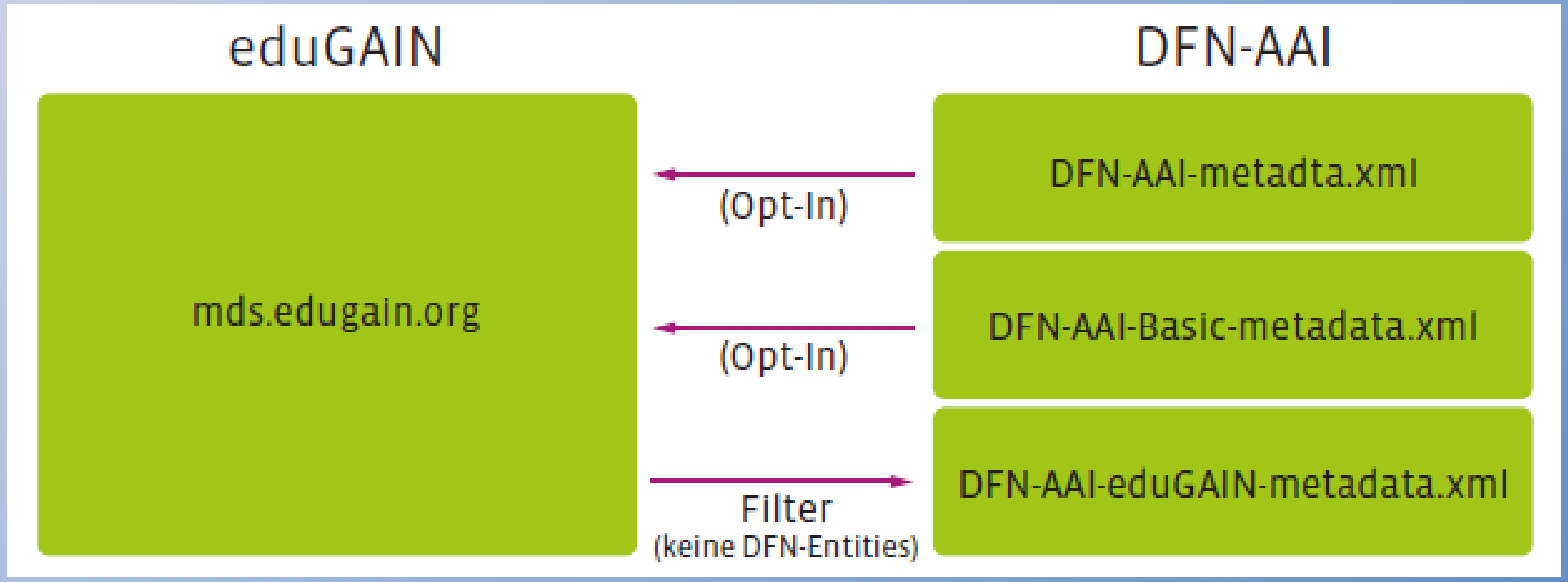
eduGAIN – how does it work?

- Metadata Service (aggregation, validation, signing, redistribution, etc.)
- Metadata Profile (SAML2)
- Set of Policies
- How to participate?
  - **Federations** have to join eduGAIN
  - Entities registered with one of these federations can “opt-in”
  - . . . are added to the metadata set the home federation provides to eduGAIN
  - . . . have to implement the eduGAIN metadata the home federation redistributes to its users

Register once + connect to everywhere



Metadata Flows



eduGAIN – Issues

- Technically quite homogeneous, but . . .
- Policies of the participating federations are rather different
- Levels of Assurance?
- Certificate Policies?
- Data Protection?

  → GÉANT Data Protection Code of Conduct

  https://refeds.terena.org/index.php/Data_protection_coc

Attributes

Release and Management

Data Protection / Privacy Issues

- From the juridical point of view, at least in Germany, the situation is slightly confusing:
  - 'Bundesdatenschutzgesetz' (BDSG)
  - 'Telemediengesetz'
  - 'Telekommunikationsgesetz'
  - The several federal laws ('Landesdatenschutzgesetze')
  - And of course the local (home organisation's) data protection guidelines...
- IdP operators are often afraid of releasing anything to anyone

Steps to tackle this problem

- Convince our Home Organisations to
  - Define their decision-making process(es)
  - Identify responsibilities
  - Provide these information to the Federation
  - (we're planning to extend our MD administration accordingly)
  - Install user consent modules like uApprove
- Help to ensure legal certainty (e.g. legal opinions)
- Do everything to reduce technical efforts, e.g. by providing pre-defined Attribute Filter Policies
- If nothing else helps: Conclude a contract (SP ↔ IdP or as general agreement within a RI)

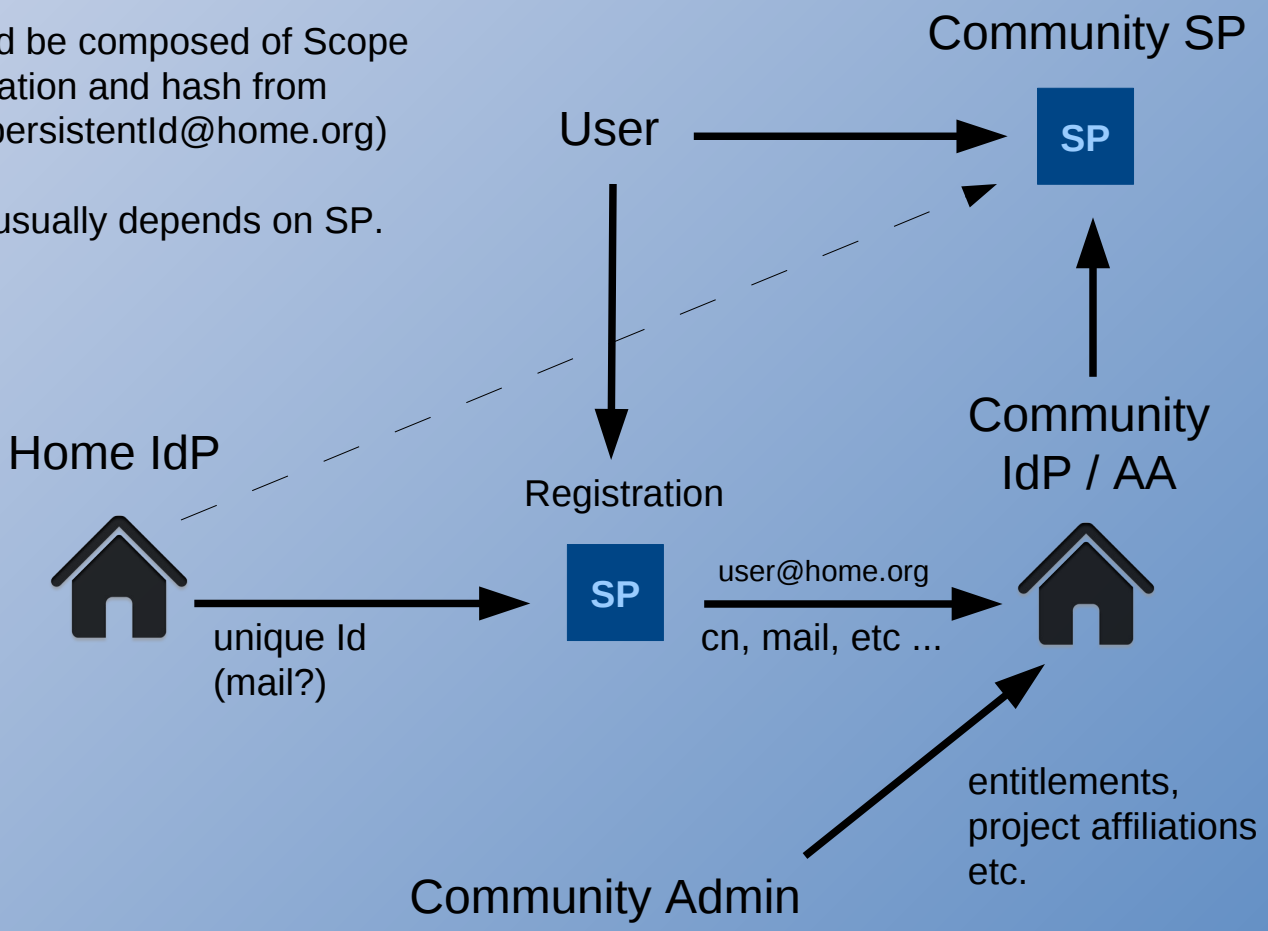
FIM paper: Attribute delegation to the research community

- Use Home Organisations' IdPs for AuthN only?
- Maintain community-managed Attribute Authority?
- That's the way it should work (IMHO) …
- But:
  - How to map identities between the instances in a trustworthy and reliable way? How to prevent e.g. a student to fake his professor's identity?
  - ➔ 'Home IdP' has to provide a uniqe identifier (perhaps persistentId – or better mail?)
  - What about 'homeless' people? (→ VHO?)
- … and who will operate + maintain such an IdP?

Community-managed Attribute Authority

Could Unique Id be composed of Scope from sopedAffilation and hash from persistentId? (persistentId@home.org)

Difficult, value usually depends on SP. (→ SP proxy?)



Entity Attributes

```
<mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="http://id.incommon.org/attribute/entity/category">
    <saml:AttributeValue>
       http://id.incommon.org/category/research-and-scholarship
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

(Example: InCommon's Research and Scholarship category)

Entity Attributes (1)

- Recent requirement:
  - How to make sure that only 'authorized' IdPs are able to access some particular SPs?
- Pass the necessary information with the metadata by implementing the 'SAML V2.0 Metadata Extension for Entity Attributes' with our Metadata Administration
- Can be used for a broad range of purposes – entitlement of whole Home Organisations, metadata / attribute filter, building virtual federations, …
- Well documented example is InCommon's *Research and Scholarship Category*

Entity Attributes (2)

- How to prevent misuse?
  - A malevolent SP/IdP administrator could set such an attribute ad libitum ...
- In our specific case we decided to implement a mechanism to apply for such attributes:
  - The attribute has to be confirmed by one of the federation operators after checking back with an authorized project member
- Implementation will take place within the next 3 months.
- Suggestions for further use cases?

DFN
Deutsches Forschungsnetz

Thank you for your attention.

—

Any questions, comments?