Attribute Release

Technical and Legal Issues

Contractual Matters

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

DARIAH/DASISH AAI Workshop,
17/18 October 2013, Cologne

Overview

Attribute Release

- Technical Issues
- Legal Issues
- CoC and other Solutions, supporting Measures

Contractual Matters

- AAI Contracts

Attribute Release – Technical Issues

The Standard Situation

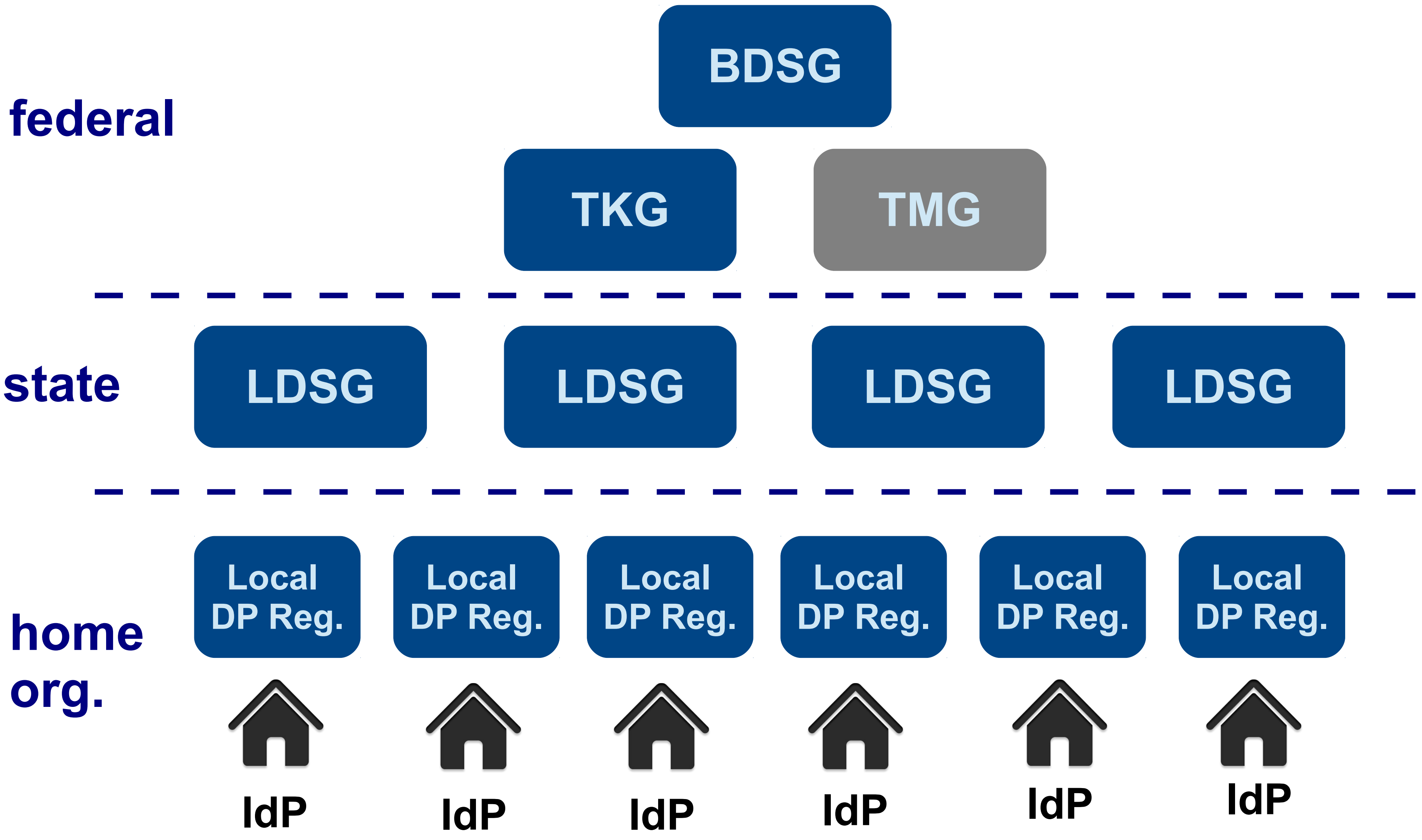
- Operationial IdP, running for a long time
- 10.000+ users
- One Attribute Filter Policy per SP
- Configuration requires restart of servlet container (not necessarily, but quite often)

→ **How to set up a new Attribute Filter Policy?**

→ **What happens if something goes wrong?**

Attribute Release – Legal Issues (1)

Data Protection in Germany…



federal

BDSG

TKG

TMG

state

LDSG

LDSG

LDSG

LDSG

home org.

Local DP Reg.

Local DP Reg.

Local DP Reg.

Local DP Reg.

Local DP Reg.

Local DP Reg.

IdP

IdP

IdP

IdP

IdP

IdP

Attribute Release – Legal Issues (2)

… is not that easy

- Complex hierarchy of laws and regulations
- Different legal conditions depending on location of IdP (federal state and even Home Organization)
- IdP operator has to consult the local DPO

→ **IdP operators are reluctant to release personal data (in some cases, DPOs may be uncertain, too)**

Attribute Release – Solutions (1)

Supporting Measures (by Fed Op)

- Improve & extend online documentation (Shibboleth IdP)
  - How to configure attribute filter as reloadable resource → server.xml
    (no interaction with servlet container necessary)
  - More examples of Attribute Filter Policies
  - Usage of opaque identifiers
    (eduPersonUniqueId [draft] vs. ePPN)
- Implementation of CoC with metadata registry (done)
- Promote CoC (scheduled for the next weeks with CLARIN)
- Promote / encourage implementation of user consent modules, esp. uApprove (comply with §4 BDSG)

Attribute Release – Solutions (1)

Supporting Measures (by SP Op)

- Promote Services
    - The more popular a service becomes + the bigger the user community (like SSH), the more IdP Ops are willing to release personal data (e.g. to GigaMove)
- Implementation of CoC → next slides
- Facilitate attribute release technically by supporting a small and unified attribute profile, for instance the CoC profile or CLARIAH *Call for Action on Federated Identity*
- Declaration of required attributes in metadata

Attribute Release – Solutions (3)

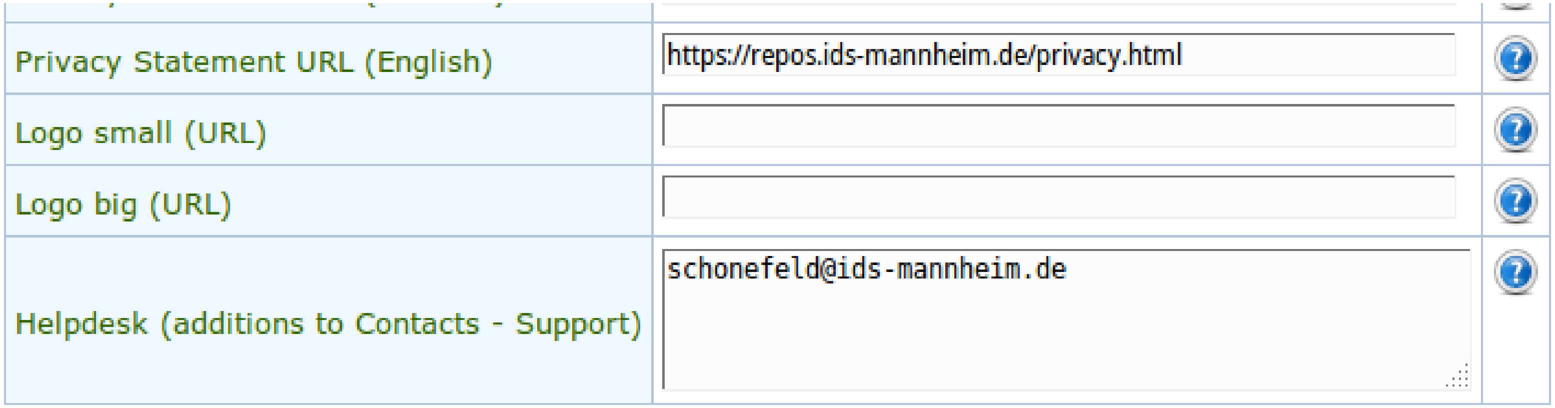
Code of Conduct for Service Providers

(GÉANT Data Protection Code of Conduct for Service Providers in EU/EEA)

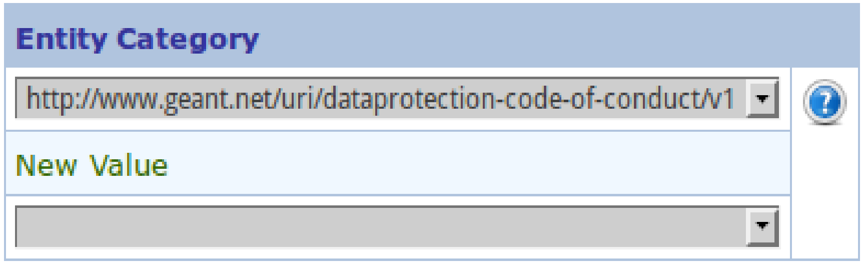
- SP declares conformance with EU Data Protection Directive both in a
  - human readable (PrivacyStatementURL) and
  - machine readable (Entity Category) way
- (almost) fixed maximum set of attributes, actually required attributes have to be documented in metadata
- Federation Op has to make sure that those requirements are met
- Ideally only one Attribute Filter Policy required to release attributes to a group of SPs

Attribute Release – Solutions (4)

CoC Entity Category



Privacy Statement URL (English)	https://repos.ids-mannheim.de/privacy.html
Logo small (URL)	
Logo big (URL)	
Helpdesk (additions to Contacts - Support)	schonefeld@ids-mannheim.de



Entity Category

http://www.geant.net/uri/dataprotection-code-of-conduct/v1
New Value

(DFN-AAI metadata administration tool)

Attribute Release – Solutions (5)

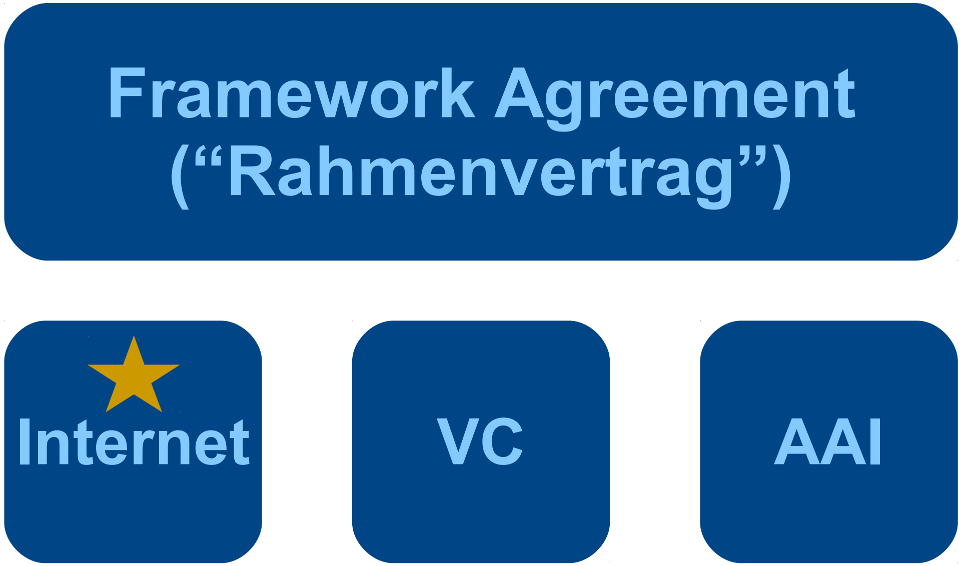
Does the Code of Conduct make sense?

- “Only” summarizes existing law / regulations
  (BTW: DFN-AAI SP contract binds SP to German and EU DP law)
- But still helpful:
- Confidence-building measure: IdP operators are no lawyers – and CoC makes it clearly visible that SP really cares for data protection
- Technically effective way to release attributes via Entity Category-based Attribute Filter Policy
- CoC-compliant entities are monitored by eduGAIN and participating federations, e.g. if the Privacy Statement URL is being removed in the DFN-AAI metadata registry, the Entity Category is automatically being removed, too → no attribute release

AAI Contracts

DFN Contractual Framework

Services for R&E Institutions


Framework Agreement
("Rahmenvertrag")

Internet

VC

AAI

and more ...

**Service Agreements
("Dienstvereinbarungen")**

For users of DFN Internet, all other services are free.

Please note: AAI Service Providers are no "users"

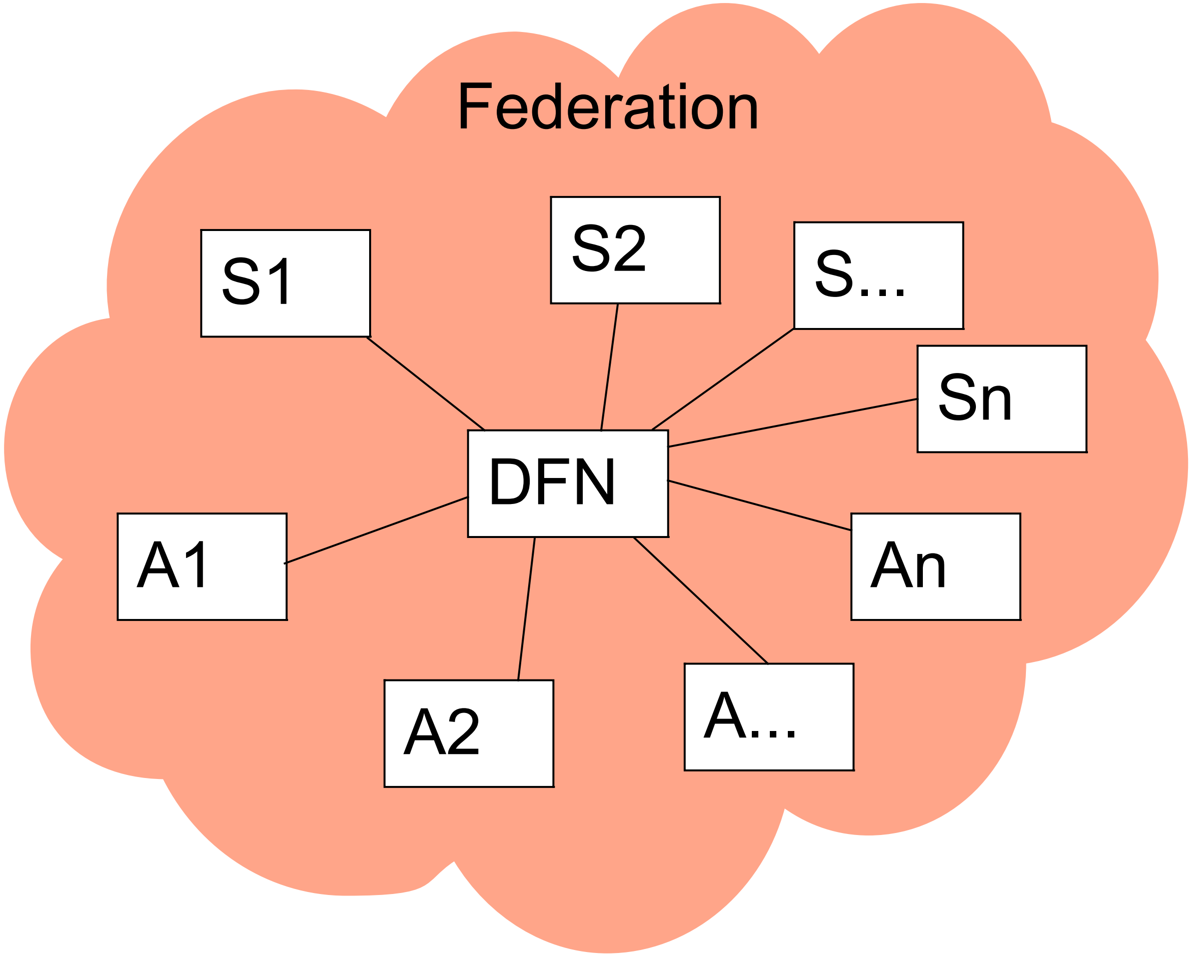
Services of the DFN-association

- Contracting of providers and users
- Operation of central technical services
- Development of new features or applications
- Organising international cooperation
- User support
- Provision of digital certificates (DFN-PKI)

- BUT: DFN is NOT involved in licence agreements related to information /content providers.

Central Contracting

The DFN-association is the central contractual partner for all participants of DFN-AAI.



IdP Contract

- The AAI-contract is an addition to other contracts between DFN and research institutions („just another piece of paper“).

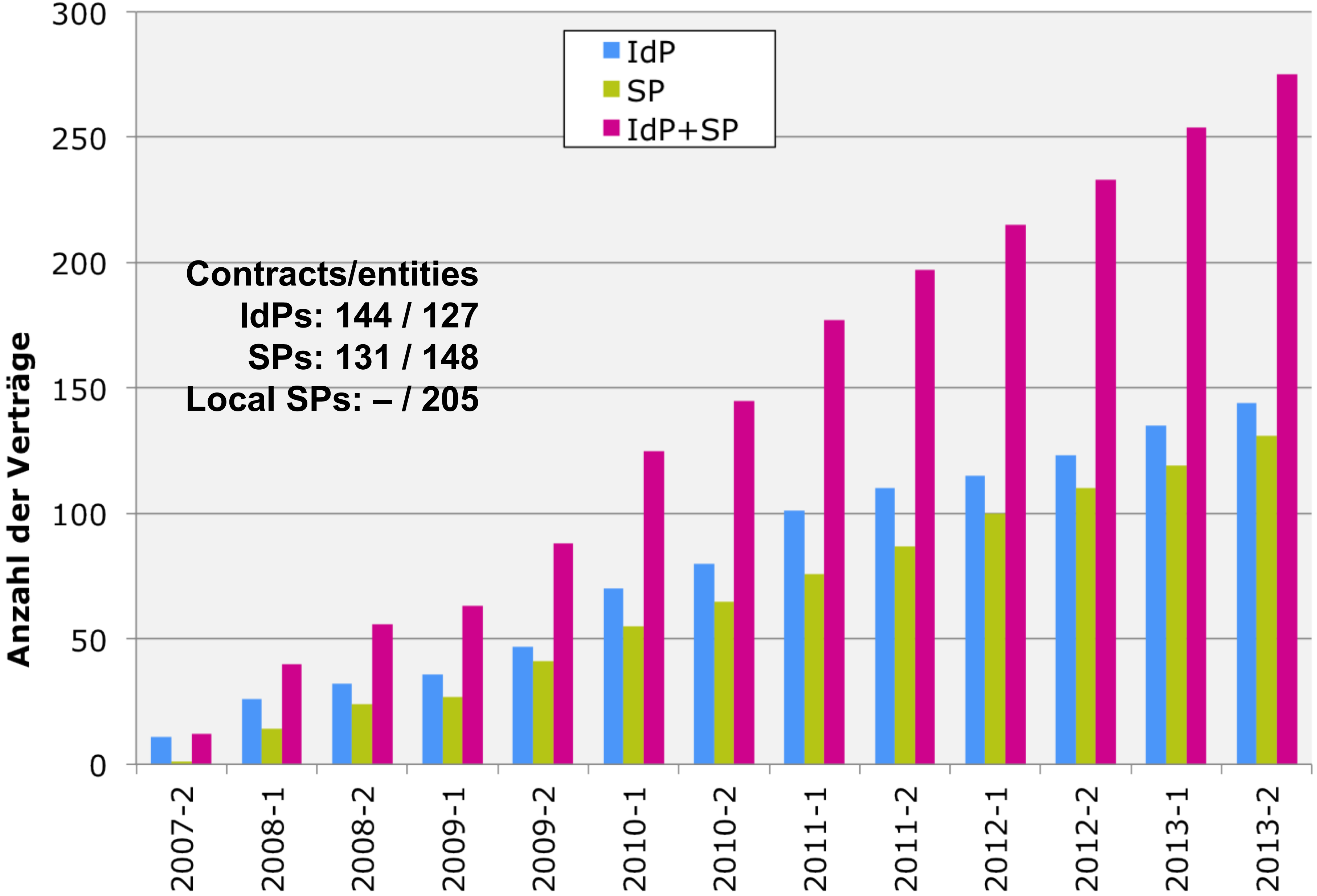
- Subjects of IdP agreement:
  - acceptance of der DFN federation policy
  - acceptance of attribute schemes
  - commitment to meet the demands on IdM systems („Verlässlichkeitsklassen“)
  - commitment (of DFN) to operate central technical services (Discovery-Service, usw.)
  - legal issues e.g. liability, termination, place of jurisdiction

- 144 IdP agreements signed

SP Contract

- Modification of the SWITCHaai Federation Partner Agreement
- Subjects of SP agreement:
  - acceptance of German law
  - acceptance of der DFN federation policy
  - acceptance of European data privacy laws
    (for US-American companies: Safe-Harbour)
  - legal issues e.g. liability, termination,
    place of jurisdiction
- Free of charge
- 131 SP agreements signed

Development of AAI contracts



Contracts/entities
IdPs: 144 / 127
SPs: 131 / 148
Local SPs: – / 205

Thanks for your attention!

Questions? Comments?

Contact

www: https://www.aai.dfn.de

email: hotline@aai.dfn.de, pempe@dfn.de