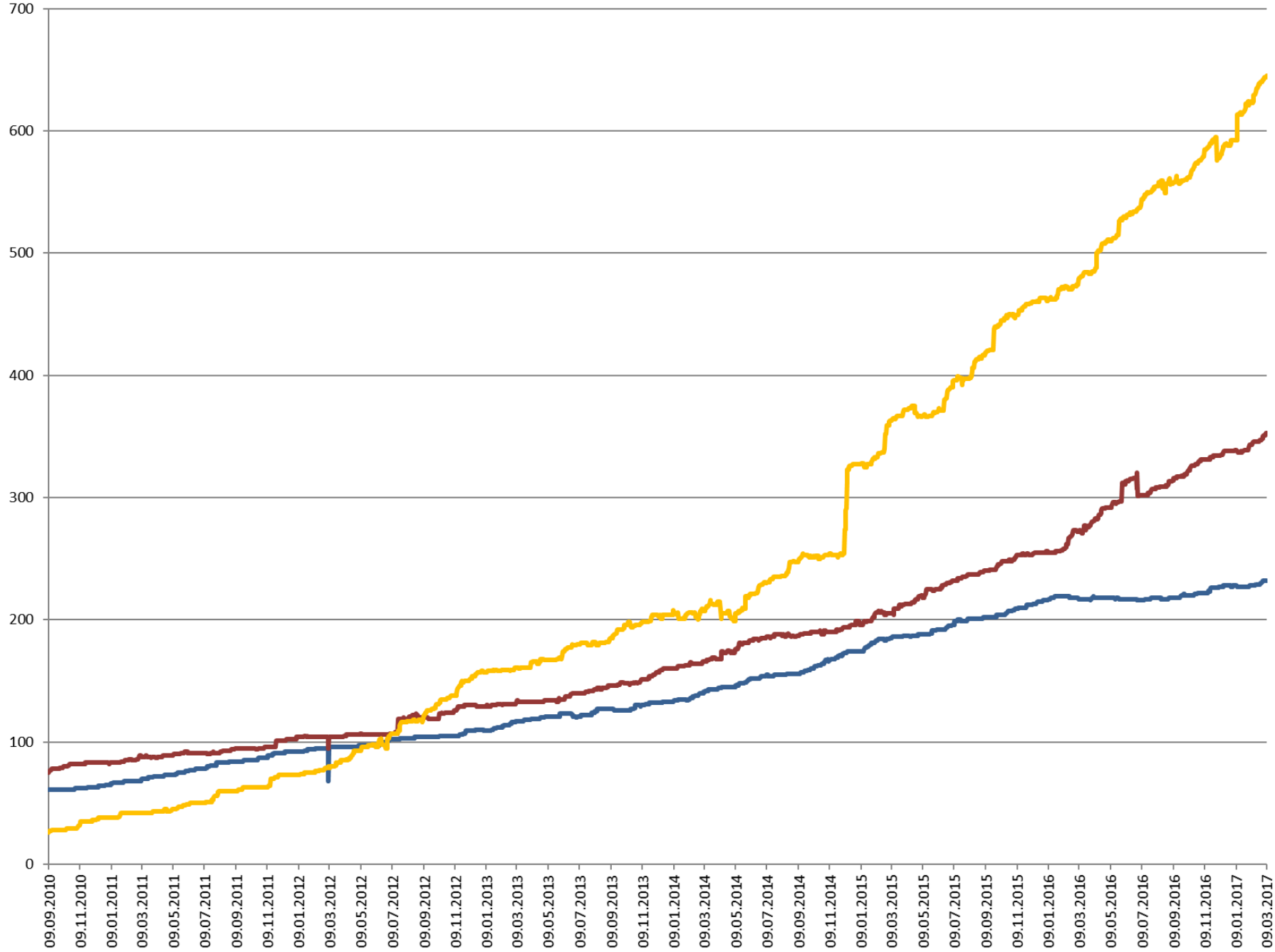
Neues aus der DFN-AAI

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

66. DFN-Betriebstagung,
21./22. März 2017, Berlin

DFN-AAI – aktuelle Zahlen



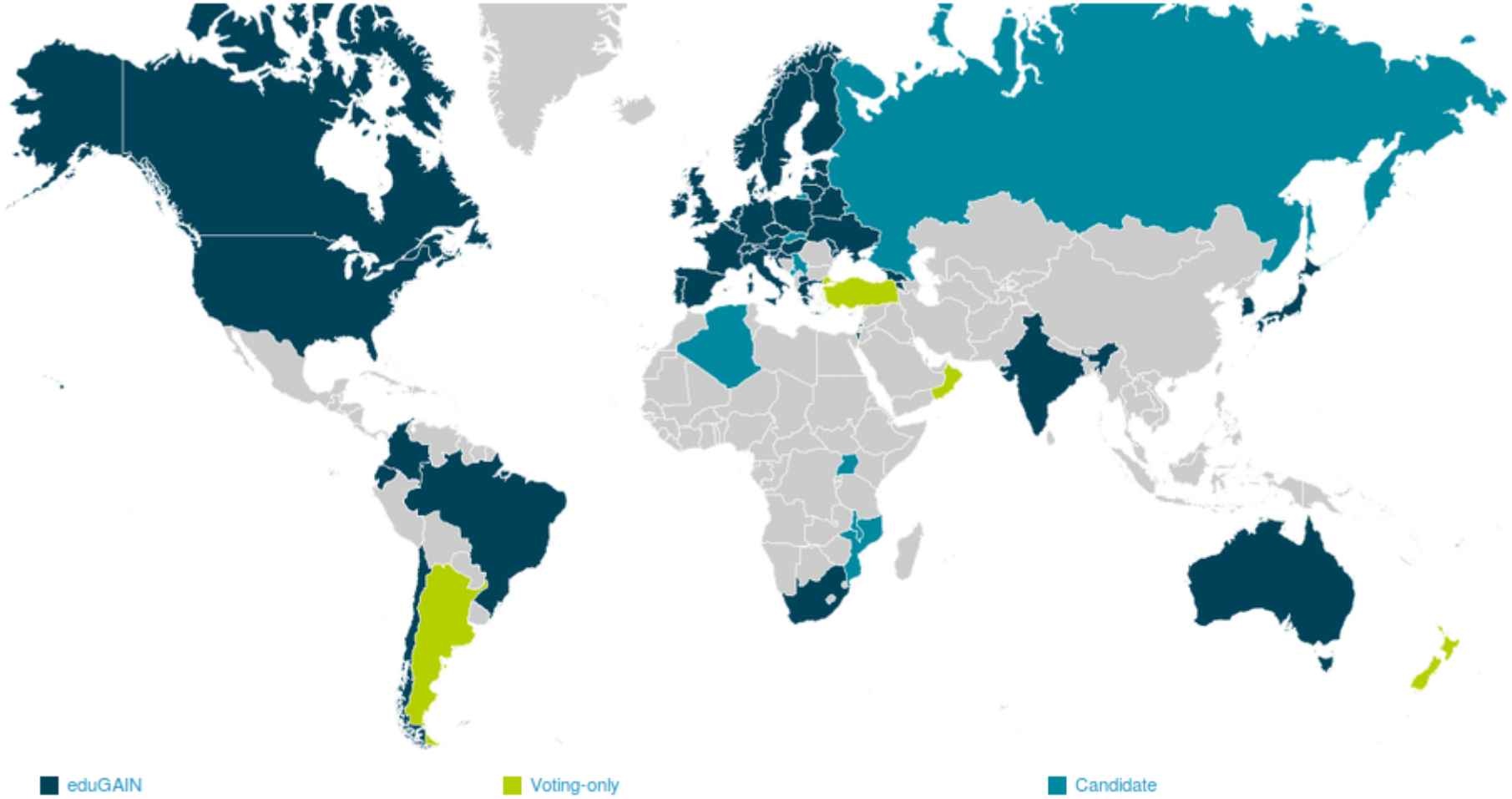
Stand:
9.3.2017

IdP: 232

SP: 353

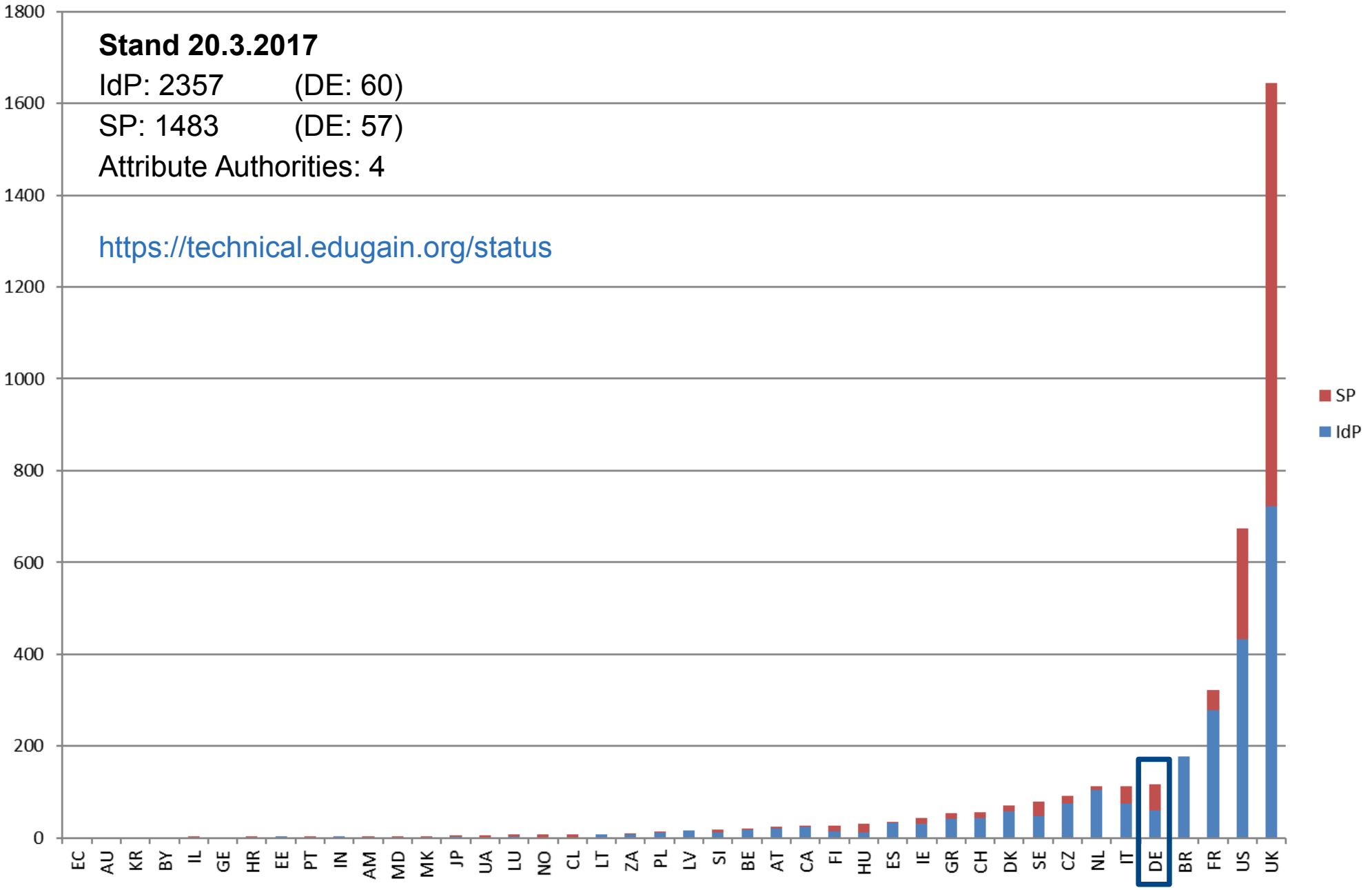
lokale SP: 645

Interfederation / eduGAIN



Quelle: http://www.edugain.org/technical/status

Beteiligung an eduGAIN



Metadaten-Signatur und DFN-PKI G2

- Wurzelzertifikat „Deutsche Telekom Root CA 2“ der ersten Generation läuft im Juli 2019 ab
- Umstellung der DFN-PKI auf ein neues Wurzelzertifikat und eine neue Zertifizierungshierarchie
- DFN-AAI: Zertifikatkette zur Validierung der Signatur der DFN-AAI Föderationsmetadaten
  → Zertifikat zur Signaturvalidierung aus neuer Hierarchie
- Neue URLs zum Download der Metadaten mit G2-Signatur, Doku unter https://wiki.aai.dfn.de/de:metadata
- Konfigurationsbeispiele im DFN-AAI Wiki sind bereits angepasst
- Metadaten mit G1-Signatur sind weiterhin verfügbar
- **Mit der Umstellung bitte nicht bis Juli 2019 warten!**

Incident Response - Sirtfi

- **S**ecurity **I**ncident **R**esponse **T**rust Framework for **F**ederated **I**dentity
- Treibende Kräfte: FIM4R, Teilchenphysik (insbes. CERN) u.a.m.
- IdP-/SP-/AA-Betreiber sichern zu, sich bei sicherheits-kritischen Vorfällen zeitnah gegenseitig zu informieren (Incident Response)
- Weitere Aspekte:
  - Betriebssicherheit (Operational Security)
  - Logging relevanter Informationen (Traceability)
  - Nutzungsbedingungen / Acceptable Use Policy
- https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

Sirtfi – Umsetzung auf Föderationsebene

- **Metadaten:** Entity Attribut + Security Contact

- Derzeit von 12 Föderationen unterstützt
- Nächste Schritte:
  - AARC/GÉANT: Self-Assessment Tool
  - DFN-AAI: Regelmäßige Kontrolle, ob Kontaktdaten aktuell sind
  - DP Code of Conduct 2 (in Arbeit): Voraussetzung für SPs

Metadatenverwaltung

- Oktober 2016: OpenSSL-Update auf www.aai.dfn.de sorgt für fehlerhafte Föderationsmetadaten
  → mehrstündige Beeinträchtigung der DFN-AAI :-(
- Schnell repariert, aber IdPs/SPs laden die Metadaten i.d.R. nur alle 2-3 Stunden neu . . .
- Überarbeitung der Metadatenverwaltung
  → zusätzliche Sicherheitsmechanismen
- Weitere Validierungsschritte, die ggf. zum Abbruch führen
  - Vergleich Dateigröße vorher – nachher
  - Anzahl der gelöschten Entities
- Code Review der älteren Abschnitte des Programmcodes der Metadatenverwaltung (fortlaufend)

AAI-Forum - heute um 14:30

Themen:

- SaxID
- Shibboleth und Kerberos in gemischten Umgebungen
- Authentifizierungs- und Autorisierungs-problematik der Fachinformationsdienste (FID) für die Wissenschaft

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

Kontakt

www:	https://www.aai.dfn.de
eMail:	pempe@aai.dfn.de / hotline@aai.dfn.de
Tel.:	+49-30-884299-9124 +49-711-63314-215