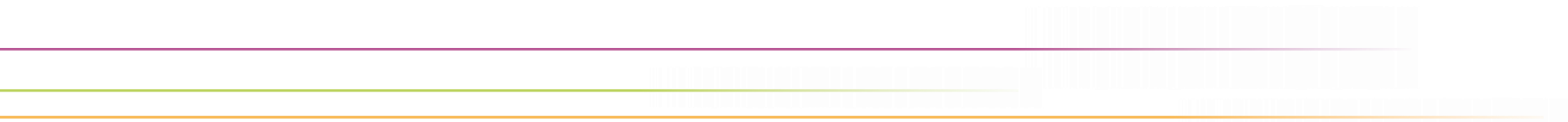


deutsches forschungsnetz

DEN



Neues aus der DFN-AAI

84. DFN-Betriebstagung | 17. März 2026

Wolfgang Pempe (pempe@dfn.de)

Zertifikate in der DFN-AAI (1)

Weitreichende Änderungen bei den Regularien für **Serverzertifikate**

- ▶ Laufzeitverkürzung
 - ▶ Aktuell: 199 Tage, seit letzter Woche von HARICA umgesetzt
 - ▶ Ab März 2027: 100 Tage
- ▶ TLS ClientAuth abgekündigt, voraussichtlich ab März 2027 nicht mehr von Google akzeptiert


Zertifikate in der DFN-AAI (2)

Fazit: Reguläre Serverzertifikate sind nicht mehr für die SAML-basierte Kommunikation in der DFN-AAI nutzbar

- ▶ Zu kurze Laufzeit -> häufige Zertifikatswechsel nicht zumutbar
- ▶ Service-Provider: Ohne ClientAuth keine Backchannel-Kommunikation für Attribut Queries oder Single Logout möglich
- ▶ Stattdessen bitte **selbst-signierte Zertifikate** oder Zertifikate aus der **DFN-Verein Community-PKI** nutzen
 - ▶ Siehe Wiki <https://doku.tid.dfn.de/de:certificates>

- ▶ Sirtfi = Security Incident Response Trust Framework for Federated Identity
 - ▶ Siehe <https://refeds.org/sirtfi>
- ▶ Security-Kontakte aus den jeweiligen IdP-/SP-Metadaten angeschrieben
 - ▶ Bitte um Rückantwort innerhalb eines Werktages
- ▶ Erfolgreiche Rückmeldungen
 - ▶ Heimateinrichtungen (IdP, SP): ~90%
 - ▶ Dienstanbieter (nur SP): ~50%
- ▶ Nächster Testlauf für den Herbst geplant

Update OpenID Federation (1)

- ▶ Spezifikation OpenID Federation mittlerweile verabschiedet 
 - ▶ https://openid.net/specs/openid-federation-1_0.html
- ▶ eduGAIN OpenID Federation Pilot (seit 30. Juni 2025, läuft 12 Monate)
 - ▶ DFN-AAI beteiligt mit Team des DFN-CERT
 - ▶ <https://wiki.geant.org/spaces/eduGAIN/pages/1072398451/eduGAIN+-+Open+ID+Federation+Pilot>
- ▶ Parallel: eduGAIN Technical Profiles Working Group
- ▶ Shibboleth OP: Unterstützung für OpenID Federation verfügbar (WIP)

Update OpenID Federation (2)

Aktuelle Themen beim eduGAIN OIDF Pilot (Auswahl)

- ▶ Skalierbarkeit und Betriebssicherheit Resolver
- ▶ (Inter-)Föderations-Topologie
 - ▶ Baumstruktur mit Signaturhierarchie (Intermediates, Trust Anchors)
vs.
 - ▶ Flache Struktur über Trust Marks
- ▶ Bestandsaufnahme verfügbarer Software
 - ▶ RP-Implementierungen sind Mangelware
- ▶ Technisches Profil, analog zu SAML

Sonstiges

- ▶ Neues Föderationsmetadaten-signaturvalidierungszertifikat
 - ▶ Download unter <https://doku.tid.dfn.de/de:metadata>
- ▶ Schulungen
 - ▶ Workshop für Fortgeschrittene, voraussichtlich im Frühsommer
 - ▶ Ankündigungen erfolgen über [dfn-aai-users](#)-Liste (bitte subscribieren)
- ▶ NFDI-Basisdienst IAM (IAM4NFDI): Folgeantrag für weitere zwei Jahre bewilligt: „Ramp-Up Phase“, Laufzeit bis Januar 2028
- ▶ edu-ID
 - ▶ Pilotphase läuft (immer noch), wichtige Komponente für NFDI und EOSC
 - ▶ Infos zum IdP-Onboarding unter <https://doku.tid.dfn.de/de:aai:eduid:idpconfig>

Vielen Dank! Fragen? Kommentare?

DFN

► Kontakt

► DFN-AAI Team

E-Mail: hotline@aai.dfn.de
Tel.: +49-30-884299-9124
Fax: +49-30-884299-370

Adresse:
DFN-Verein, Geschäftsstelle
Alexanderplatz 1
D-10178 Berlin

- Andreas Borm
- Doreen Liebenau
- Esther Ruiz Ben
- Heike Kaufmann
- Wolfgang Pempe

