Neues aus der DFN-AAI

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

67. DFN-Betriebstagung,
26./27. September 2017, Berlin

Neuigkeiten im Überblick

- Zwei **neue Stellen** gemeinsam für DFN-AAI und eduroam ab 1. Oktober und 1. November
- **Shibboleth Consortium:** neues Support-Modell
- **Planungen für die nähere Zukunft:**
  - Unterstützung für **OpenID Connect**
  - Unterstützung für das **Metadata Query** Protocol (MDQ) als Alternative zu statischen und v.a. großen Metadaten-Dateien
  - Neue **Metadatenverwaltung** (SAML + OpenID Connect)
  - **Verlässlichkeitsklassen** nicht mehr (nur) an Metadaten-Dateien koppeln + Interoperabilität mit internationalen Standards, Self-Assessment-Tool
  - Vorbereitung auf **EU-DSGVO** → u.a. GÉANT CoCo

OpenID Connect / OI(D)C

- „A simple identity layer on top of the OAuth 2.0 protocol”
- Standard wurde im Februar 2014 verabschiedet
- Protokoll basiert auf REST/JSON + JWT (JSON Web Token), **funktioniert auch ohne Web Browser** (→ mobile Endgeräte, Apps)
- Entwicklung wurde und wird von diversen Internet-Konzernen getrieben: Google, Facebook, Microsoft, Deutsche Telekom, PayPal, Yahoo! u.a.m.
- Kommt u.a. bei Google+ zum Einsatz
- Wird von manchen als Konkurrenz zu SAML gesehen
- Infos, Spezifikationen, Software etc. unter http://openid.net/connect/

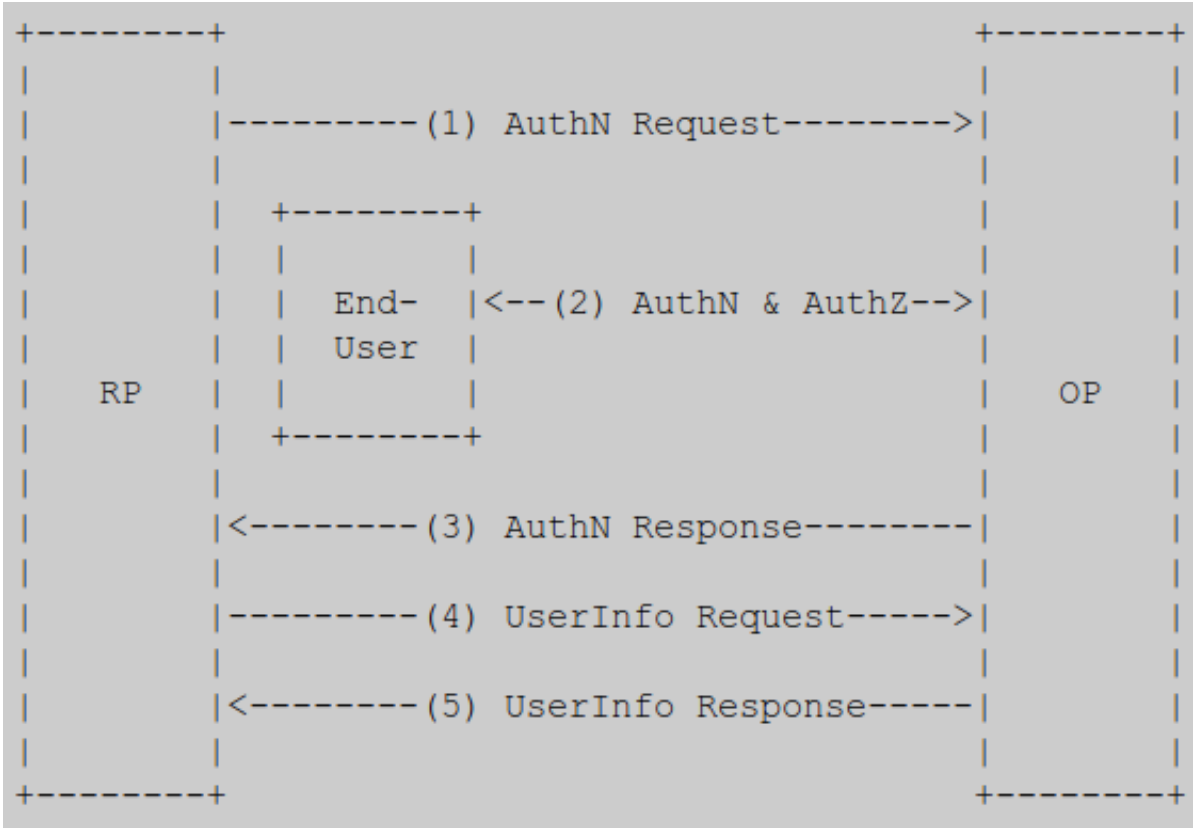
OIDC – Terminologie im Vergleich

OpenID Connect (OIDC)	SAML
OP (OpenID Provider)	IdP (Identity Provider)
RP (Relying Party), Client	SP (Service Provider)
Claim (Information über eine Entity, i.d.R. User)	Bestandteil einer Assertion (Attribute, NameID, …)

Details unter
http://openid.net/specs/openid-connect-core-1_0.html#Terminology

Flow in OpenID Connect

ähnlich wie SAML …



Quelle: http://openid.net/specs/openid-connect-core-1_0.html

OIDC – aktuelle Baustellen

- OIDC bisher auf v.a. Szenarien beschränkt, in denen Vertrauen über den jeweiligen Kontext (Organisation, Infrastruktur) hergestellt wird
- Einsatz im Föderationskontext?
  - Discovery?
  - Wie wird Vertrauen hergestellt? – Zentral verwaltete und signierte Metadaten?
  - Attributfreigabe (Konzept einer global gültigen Entity ID?)
  - Unterstützung bestimmter Attribut-Schemata (eduPerson, SCHAC, …)

→OpenID Connect Federation (Draft): http://openid.net/specs/openid-connect-federation-1_0.html

→Attribute: REFEDS OIDCre Working Group

OIDC – nächste Schritte DFN-AAI

- Betrieb OIDC-Testbed
  (NB: OIDC-Support für Shibboleth IdP wird derzeit im Rahmen von GÉANT implementiert)
- Bridging-Elemente zur Anbindung lokaler OIDC Infrastrukturen an die DFN-AAI
- Neue Version der Metadatenverwaltung: Unterstützung sowohl für OpenID Connect Federation als auch für SAML
- Embedded Discovery Service für RPs (?)

Alles weitere im AAI-Forum …

… heute Nachmittag ab 14:30, mit spannenden Themen:

- IdP Cluster-Strukturen und zentrales Logging
  S. Krinetzki, RWTH Aachen University
- Bericht über zwei 2FA-Projekte mit Shib IdP v3 von DAASI
  P. Gietz, DAASI International GmbH
- Rollout von Shibboleth Service Providern mit SaltStack
  H. Strack, ssystems
- Neues aus der DFN-AAI (Fortsetzung)
  W. Pempe, DFN-Verein

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

Kontakt
Internet: https://www.aai.dfn.de
E-Mail: aai@dfn.de
Telefon: +49 30 884299 9124