

OPENID CONNECT ONTWIKKELINGEN

What's next at SURFconext 2019

```
34 self.logdupes = True
35 self.debug = debug
36 self.logger = logging.getLogger(__name__)
37 if path:
38     self.file = open(os.path.join(path, "requests.log"), "a")
39     self.file.seek(0)
40     self.fingerprints.update(e.request)
41
42 @classmethod
43 def from_settings(cls, settings):
44     debug = settings.getbool("SUPERFILTER_DEBUG")
45     return cls(job_dir(settings), debug)
46
47 def request_seen(self, request):
48     fp = self.request_fingerprint(request)
49     if fp in self.fingerprints:
50         return True
51     self.fingerprints.add(fp)
52     if self.file:
53         self.file.write(fp + os.linesep)
54
55 def fingerprint(self, request):
```

OpenID Connect – hoe was het ook al weer? -

- OpenID connect, een nieuw protocol uit 2014
- OAuth2 met een identity laag er bovenop
- Gebaseerd op “modernere” standaarden als JSON en REST
- Ook geschikt voor authenticatieflows in mobiele apps
- Aansluiten wordt gezien als eenvoudiger dan met SAML

OpenID Connect in SURFconext

- In productie sinds juli 2017
- Momenteel rond de 15.000 logins per week (3.000.000 totaal SURFconext)
- Ongeveer 35 Relying Parties in productie
- Nog geen ondersteuning voor mobiele apps

Huidige implementatie

- Gebaseerd op het open source project MitreID connect
- Ontwikkeling rond MitreID Connect ligt al een tijdje stil
- Aanpassingen blijken lastig te zijn
- Een aantal features ontbreken
- Integratie in de rest van het platform is niet optimaal



OIDC – The next generation

- Twee bijeenkomsten om de toekomst te bepalen:
 - December 2018: “Wisdom of the Crowd” expert meeting
 - Februari 2019: Workshop met 5 instellingen over API security
- Uitkomst:
 - Veel van de genomen architectuur beslissingen zijn nog valide
 - Instellingen willen aan de slag met mobiele apps en API's
 - Nieuwe implementatie gebaseerd op een library in plaats van een “af” product.



OIDC – The next generation: Doelen

- Een meer flexibele en beter onderhoudbare OIDC gateway
 - Gebaseerd op een open source library
 - Betere integratie in de rest van het platform
 - Ondersteuning voor PKCE (voor mobiele apps)
 - Ondersteuning voor SURFsecureID
 - Zelfde features als de huidige implementatie
- OIDC inzetbaar voor het beschermen van API's
- Onderzoek naar (nog) betere bescherming van de privacy van gebruikers

Planning

- Begin 2020: Eerste migraties
- Collegejaar 2020/2021: Eerste APIs in productie
- Mocht je al aan de slag willen met APIs: laat het ons weten!

Discussie

- Ervaringen met OpenID Connect?
- Wensen voor de toekomst?
- IdP's via OpenID Connect?