



DNS-based discovery for OpenID Connect

FOSDEM'18 – DNS devroom
sanz@denic.de

Motivation



Motivation



FUSION

NEXT LEVEL



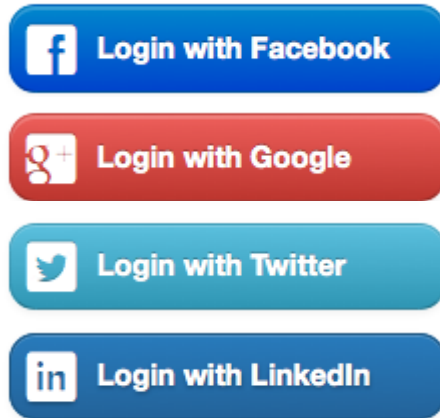
Motivation

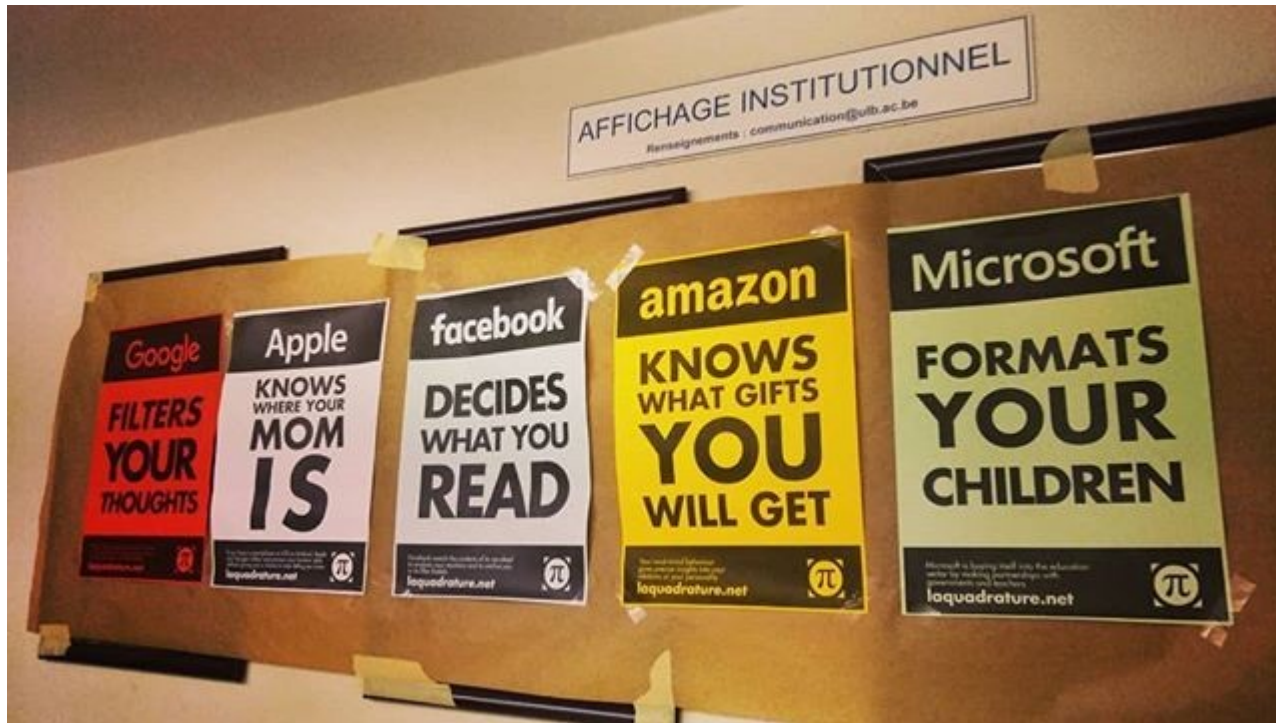


FUSION
NEXT LEVEL

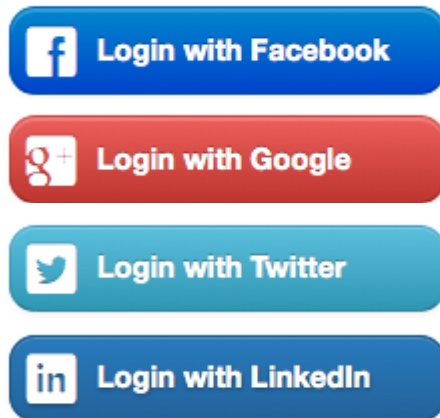


Motivation

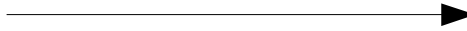




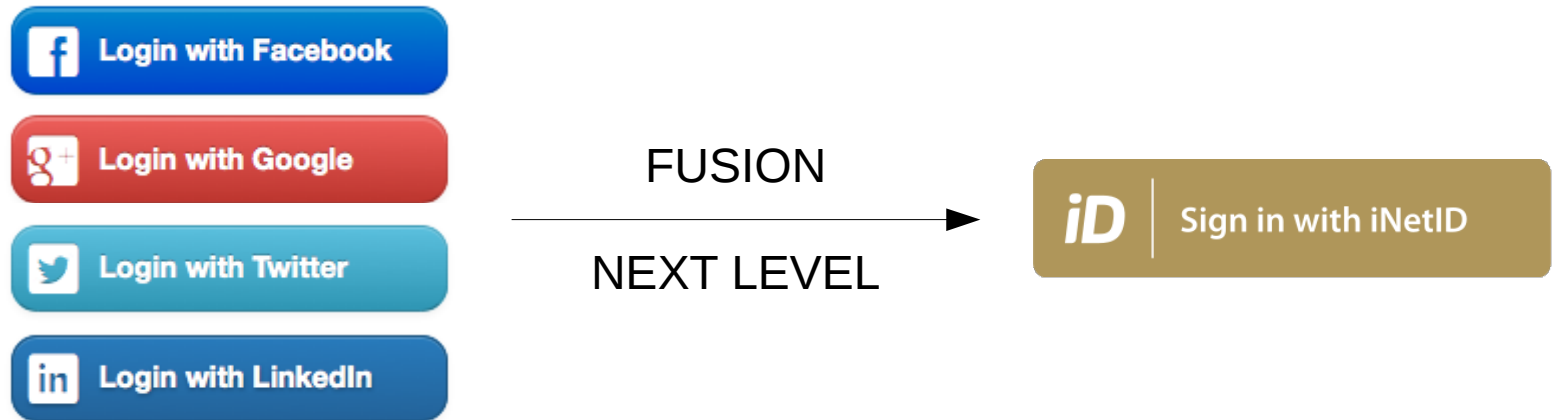
Motivation



FUSION
NEXT LEVEL



Motivation



... *iNetID*

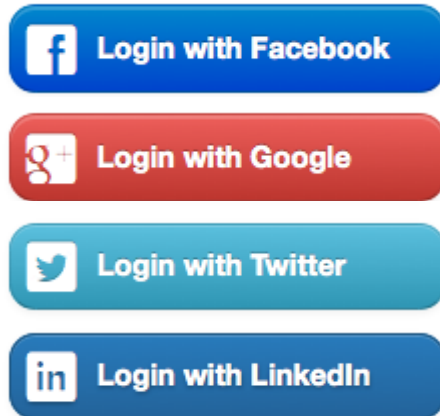
initiated by



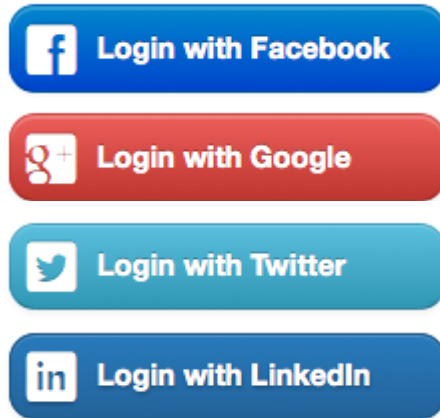
Advantages iNetID (Working Name)

- Based on **open** existing standards
- Participate in an **open** federated model
- **Free** to use your name/brand
- **Free** to pick and change your provider, or host it **yourself**
- **Owned by you**
- **Choose** whom to trust with your **privacy**, whom you share personal data with

Identity Provider Discovery



Identity Provider Discovery



- OpenID Connect Discovery
- WebFinger (RFC7033) service based

GET /.well-known/webfinger

resource=acct:joe@example.com

rel=http://openid.net/specs/connect/1.0/issuer

```
{
  "subject": "acct:joe@example.com",
  "links":
  [
    {
      "rel": "http://openid.net/specs/connect/1.0/issuer",
      "href": "https://server.example.com"
    }
  ]
}
```

DNS-based Discovery

- DNS has to be set up anyway
- No need to run a WebFinger / HTTP(S) Server
- It does not introduce a new trust dependency
- Lightweight, faster
- WebFinger not being used the way it was thought

DNS-based Discovery

- DNS has to be set up anyway
- No need to run a WebFinger / HTTP(S) Server
- It does not introduce a new trust dependency
- Lightweight, faster
- WebFinger not being used the way it was thought

Considerations

- It makes DNSSEC a MUST
- Personal identifiers in the DNS: privacy aspects
 - No lookup confidentiality

SRV RR?

NAPTR
RR?

S-NAPTR
(SRV +
NAPTR)?

A new
RR?

TXT
RR?

DNS-SD
(SRV +
TXT)?

DNS-based Discovery: Structured TXT RR

`_openid.joe.example.com`
IN TXT

`v=OID1;iss=auth.freedom-id.de/id;clp=identityagent.de`

- Scoped via underscore at the owner
- Versioned
- DKIM/DMARC-like

Feedback so far

`_openid.joe.example.com`
`IN TXT`

`v=OID1;iss=auth.freedom-id.de/id;clp=identityagent.de`

- „Oh, dear, TXT Rrs...”
- „Coordination with DNS department“
- JavaScript (client side) is sandboxed
 - draft-ietf-dnsop-dns-wireformat-http-01
 - HTTP Proxy service?

draft-sanz-openid-dns-discovery-00
<https://inetid.community>