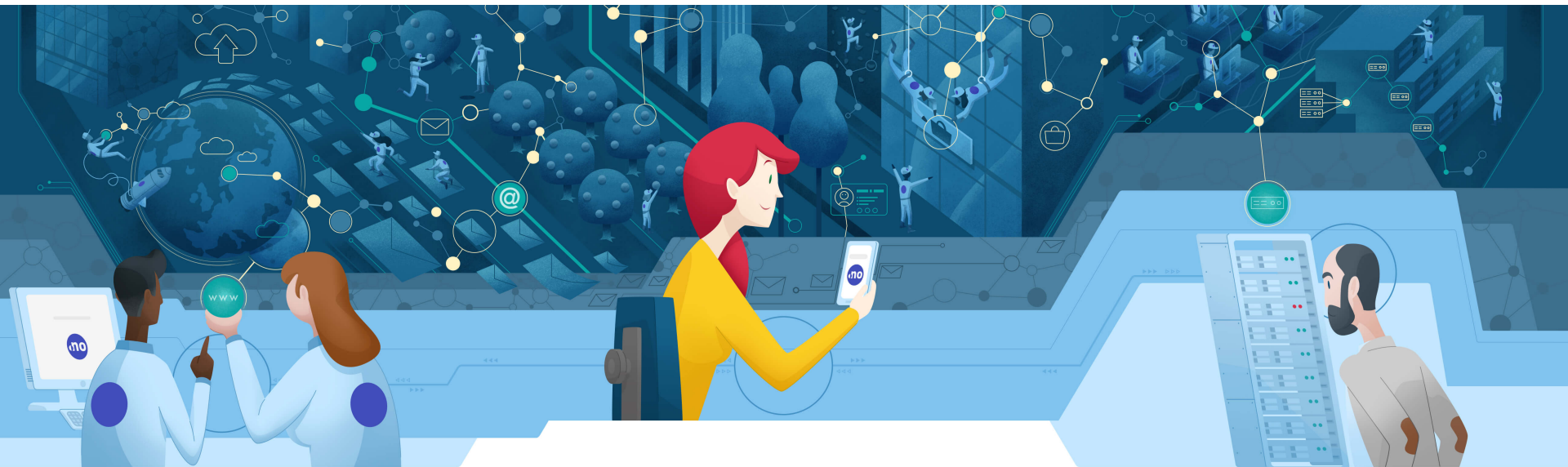




NORID DRIVER REGISTERET
FOR NORSKE DOMENENAVN
norid.no



RDAP - en ny oppslagstjeneste for domenedata

Trond Haugen, senior systemutvikler, Norid AS
Forhandlerseminar 18/11-2020

RDAP - en ny Whois!

- Vi går gjennom status for dagens løsninger for oppslag på domenedata
- Vi ser på en ny oppslagstjeneste - RDAP

Dagens situasjon

- Whois-protokollen er gammel, fra tidlig 1980-tall
- Alle registreringsenheter som har eksistert noen år har en whoistjeneste (noen har flere)
- Whoistjenesten gjør det mulig for abonnenter og verden ellers å slå opp domenedata
- Oppslag gjøres typisk fra en kommandolinjeklient, via web-proxyer eller via egenutviklet programvare

Whois-protokoll

- Minimalistisk standardisert. Fra opprinnelig protokoll-‘spesifikasjon’ <https://tools.ietf.org/html/rfc812> (1982):

```
Connect to the service host
```

```
TCP: service port 43 decimal
```

```
NCP: ICP to socket 43 decimal, establishing two 8-bit  
connections
```

```
Send a single "command line", ending with <CRLF>.
```

```
Receive information in response to the command line.
```

```
The server closes its connections as soon as the output is  
finished.
```

- Whois er dermed en ‘fritekst’-protokoll’, som gir mange begrensninger og skaper en del friheter. Begrensninger og friheter føder varianter.

Problemer med whois

- Tekstlig og fritt format. Forskjellige måter å vise oppslagsresultat på.
- På grunn av mangel på standardisering har hver registreringsenhet utviklet sin egen whois-variant
- Det gjør det vanskeligere å slå opp og tolke resultat:
 - Maskinelt oppslag og uthenting av data er vanskeligere. Man er tvunget til å lage spesialprogrammer for å parse og tolke hver whoisvariant.
 - Mennesker sliter med å tolke resultatene, som er teknisk orientert. Mange registreringsenheter tilbyr derfor en web-proxy med mer brukervennlig oppførsel som kan brukes i stedet. Norid har:
 - <https://www.norid.no/no/domeneoppslag/hvem-har-domenenavnet>
- Andre problemer finnes også, som representasjon av forskjellige tegnsett og manglende aksess-styring

Whois hos Norid

- Norid driver to forskjellige whois-tjenester, en åpen for verden (whois), og en lukket med utvidet funksjonalitet for forhandlere (registrarwhois/forhandlerwhois)
 - Den åpne tjenesten viser ganske lite informasjon og har begrenset antall nøkkelord man kan slå opp (grunnet GDPR)
 - Den lukkede tjenesten viser mer data, og man kan også gjøre oppslag på flere nøkkelord
- Utviklings- og driftsmessig må Norid holde liv i to forskjellige whois-tjenester, det er ineffektivt

Norids variant - åpen whois hos .no

Legg merke til formatet på visningen, dvs. Norid sin måte å vise resultatet på. Abonnent-info mangler, man må bruke web-proxy for å se slike detaljer (GDPR-konsekvens).

```
% whois -h whois.norid.no norid.no
```

Domain Information

```
NORID Handle.....: NOR18456D-NORID
Domain Name.....: norid.no
Registrar Handle.....: REG2-NORID
Tech-c Handle.....: UH9R-NORID
Name Server Handle.....: NAC2H-NORID
Name Server Handle.....: NN14H-NORID
Name Server Handle.....: NSUN1239H-NORID
Name Server Handle.....: SERV41H-NORID
DNSSEC.....: Signed
DS Key Tag      1.....: 21199
:
Digest          3.....: 555cd4da5203e4d74a1c94e3433502ec9d8d4a09a28e6a85f47ade020137f423
```

Additional information:

```
Created:      1999-11-15
```

IIS sin variant - åpen whois hos .se

Legg merke til formatet på visningen, dvs. Internetstiftelsen (IIS) sin måte å vise resultatet på. De henviser ellers brukeren til sin web-proxy for å se detaljer f.eks. for holder/abonnet (GDPR-konsekvens).

```
% whois -h whois.iis.se iis.se
:
state:                active
domain:               iis.se
holder:               stifte6931-00001
admin-c:              -
tech-c:               -
billing-c:            -
created:              2000-05-04
modified:             2020-07-09
expires:              2023-03-09
transferred:          2019-01-25
nserver:              i.ns.se
nserver:              ns.nic.se
nserver:              ns3.nic.se
dnssec:               signed delegation
registry-lock:        unlocked
status:               ok
registrar:            Internetstift
```


RDAP

- RDAP (Registration Data Access Protocol) er en ny oppslagstjeneste for domenedata
- RDAP er etterkommer av Crisp/IRIS, som kom i 2005-2006, og som var et forsøk på å erstatte whois. Forsøket strandet i 2013, bla. fordi protokollen ble for kompleks (XML++)
- RDAP er mye enklere. RDAP tilbys over http med et REST-API som returnerer et JSON-formattert resultat, og er derfor velegnet for automatiserte oppslag
- Standardisert RDAP-protokoll (RFCer)
- Ferdige klienter og biblioteker finnes og kan brukes
- RDAP løses dermed mange av problemene med whois (standardisering, maskinoppslag, tegnsett, autentisering, aksesslag)

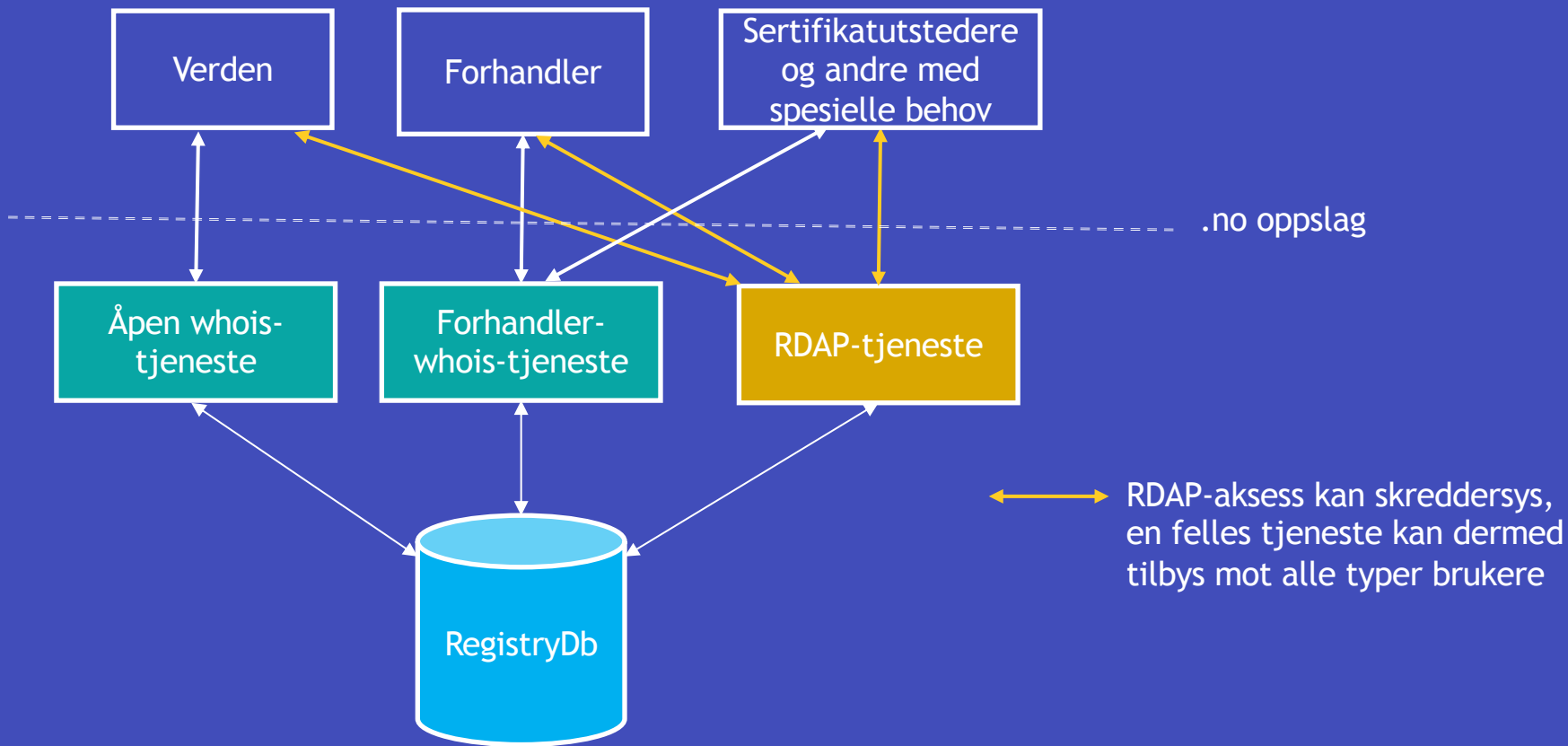
RDAP - sikkerhet/aksess

- Kjøre over https, med de sikkerhetsfordelene det gir (kryptering/TLS)
- Kan autentisere en bruker, via 'basic auth' mekanisme i http eller via fødererte mekanismer (OAuth/OpenID etc)
- Mulighet for autorisering og aksesskontroll:
 - Lagdelt aksess gir forskjellige brukere mulighet for å se forskjellige mengder data
 - Løses i praksis ved å bruke egne http- eller json-headere som utveksler aksesstokens
 - Aksesstokens kan være utdelt på forhånd, eller mottatt via en føderert mekanisme

RDAP-tjenesten hos Norid

- Norids RDAP-tjeneste følger RDAP-standarden
- Lansert som prototypetjeneste i 2018, nå status som en produksjonstjeneste
- Håndterer ratebegrensninger og er beskyttet mot misbruk på samme måte som whoistjenestene
- Http GET for å slå opp data
- Http HEAD for å sjekke om et objekt finnes eller ikke (DAS-mekanisme)
- RDAP-tjenester finnes også hos flere andre registreringstjenester

Oppslagstjenester og brukere



RDAP i praksis - hvordan?

JSON-formatet er ikke lett å lese for mennesker, men enkelt for maskiner.

Som forhandler kan du:

- Programmere din egen RDAP-klient
- Bruke en ferdig RDAP-klient
- Fra din nettleser, bruke en RDAP-webtjeneste direkte

RDAP-klienter og -biblioteker (1/2)

Det finnes spesialiserte klienter som presenterer JSON-dataene på en lesbar form. Følgende klienter og biblioteker er tilgjengelig som åpen kildekode:

- OpenRDAP (Go):
 - <https://github.com/openrdap/rdap>
 - Klienten kan også kjøres via <https://www.openrdap.org>
- NicInfo (Ruby):
 - <https://github.com/arineng/nicinfo>
- Net::RDAP (Perl):
 - <https://metacpan.org/pod/Net::RDAP>

RDAP-klienter og biblioteker (2/2)

- rdap-klient rdapper (Perl):
 - bruker Net::RDAP
 - <https://metacpan.org/pod/release/GBROWN/rdapper-0.08/rdapper>
- NOLookup (Perl):
 - bruker Net::RDAP
 - <https://metacpan.org/pod/NOLookup> (Utviklet av Norid)
 - Inneholder en RDAP-klient 'no_rdap.pl' som gir noen ekstra funksjoner for å utnytte Norids RDAP-tjeneste.

Prøv selv: Norids RDAP-tjeneste

- Slå opp 'norid.no' med http GET
 - <https://rdap.norid.no/domain/norid.no>
 - curl <https://rdap.norid.no/domain/norid.no>
 - JSON-struktur returneres
- Sjekk om 'norid.no' er tilgjengelig med http HEAD:
 - curl --head <https://rdap.norid.no/domain/norid.no>

Prøv selv: RDAP-klienter

- En RDAP-klient gir mer brukervennlig presentasjon:
 - <https://www.openrdap.org/demo?cmd=rdap+-v+norid.no>
 - `nicinfo --color-scheme=NONE --pager=NO -t domain norid.no`
 - `no_rdap.pl -s https://rdap.norid.no -q norid.no`
 - `no_rdap.pl -s https://rdap.norid.no -q norid.no -w`

Veien videre

- Forhandlerne oppfordres til å ta i bruk RDAP
 - Merk at den foreløpig tilbyr anonyme oppslag, dvs. viser data som verden får lov å se, tilsvarende åpen whois
- Norid vil se på utfasing av whoistjenestene, men de vil ikke forsvinne uten varsel
 - Vi må bla. avklare om vi skal tilby et eget aksesslag for forhandlere, dvs. få til en forhandler-rdap som erstatning for forhandler-whois
- Mer informasjon vil komme

Referansemateriale

Norids RDAP-tjeneste:

- <https://teknisk.norid.no/no/integrere-mot-norid/rdap-tjenesten/>

RDAP-protokollen:

- HTTP usage in RDAP: <https://tools.ietf.org/html/rfc7480>
- Security services for RDAP: <https://tools.ietf.org/html/rfc7481>
- RDAP query format: <https://tools.ietf.org/html/rfc7482>
- JSON response for RDAP: <https://tools.ietf.org/html/rfc7483>
- RDAP bootstrap service: <https://tools.ietf.org/html/rfc7484>
- JSON format for jCard: <https://tools.ietf.org/html/rfc7095>
- Object tagging: <https://tools.ietf.org/id/draft-ietf-regext-rdap-object-tag-02.xml>

Historikk:

- <https://en.wikipedia.org/wiki/WHOIS>
- <https://blog.apnic.net/2016/05/12/rdap-whois-modern-world/>