# Diskusjonsgrunnlag, sikkerhetsmekanismer eOppslag

Av: Rolf Rander Næss, Acando AS, for Brønnøysundregistrene

Dato: 2018-05-18

# Forutsetninger og antagelser

Forutsetninger:

* Synkrone lese-tjenester over https
* Klienten eies (utvikles og forvaltes) av en virksomhet. I diskusjonen under brukes «klienten» av og til også for å referere til virksomheten som eier klienten.
* Referansearkitekturen skal være gjeldende mellom offentlige virksomheter, samt mellom offentlig og privat hvor den private aktøren er enten klient eller tjener.

Andre forutsetninger og antagelser (men som er åpne for diskusjon)

* GET-kall etter REST-mønster
* Autentisering med «bearer token» i «Authorization»-header
* Antar at det både på klientsiden og tjenersiden finnes proxy/gateway-løsninger som gjør at ende-til-ende TLS kan være vanskelig å implementere
* For «mobil-app»-scenarier antar vi at mobilen snakker med en egen tjeneste og at det er denne er klienten i kontekst av diskusjonen. Altså dette scenariet:

API («Klient»)

Tjeneste

Mobil-APP

Diskusjonen gjelder denne kommunikasjonen

# Evalueringskriterier

Hvilke problemer forsøker vi løse?

* Implementering av «PKI i offentlig sektor» og PKIX-anbefalinger i RFC-5280 er vanskelig (for eksempel RFC-5280 kapittel 6 «certification path validation»)
* Oppbevaring av privat nøkkel som hører til virksomhetssertifikat
* Konkrete trusler (for eksempel knyttet til bruk av private nøkler, levetid for tokens, DoS, innside-trusler, sårbar infrastruktur …)

Kriterier for valg av løsning(er):

* Ende-til-ende-sikkerhet (hva nå det betyr)
* Nettverkstrafikk
* Responstid
* CPU-belastning på klient eller tjener
* Administrativ belastning for klient og tjener
* Kode-kompleksitet for klient og tjener

# Scenarier

I utgangspunktet er alle disse relevante, men alle bør ha tenkt gjennom hvilke av disse som står for det største volumet (av antall tjenester, antall tjenestekall, andel av data som er berørt, antall forskjellige klient-implementasjoner)

1. Offentlig etat med lovfestet hjemmel til å hente ut informasjon (1-10 stk)
2. Privat selskap med en avtale om å hente ut informasjon (10-50 stk)
3. Alle virksomheter med en gitt organisasjonsform (noen 1 000)
4. Alle virksomheter registrert i enhetsregisteret (over 1 000 000)
5. En virksomhet som opptrer på vegne av en annen virksomhet (for eksempel advokater, regnskapsførere, revisorer)
6. utenlandske virksomheter
7. offentlig virksomhet spør en tjeneste tilbudt av et privat selskap
8. Klient gjør et kall på vegne av en borger. To varianter av dette (usikker på om de kan implementeres på samme måte, eller om det er noen nyanseforskjeller her)
   * Med «samtykke» i juridisk forstand
   * Med OAuth2