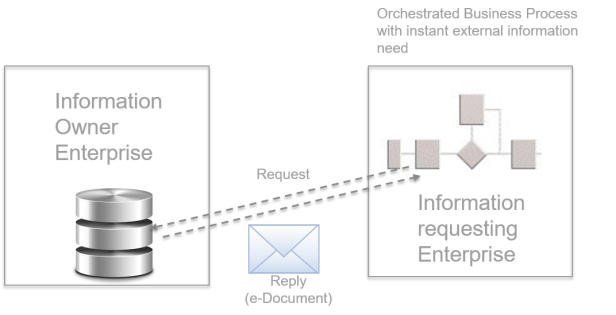
# Diskusjonsgrunnlag, sikkerhetsmekanismer

Av: Rolf Rander Næss, Acando AS, for Brønnøysundregistrene

# Utgangspunkt for diskusjonen: eOppslag

(dette er scope, slik jeg har forstått det)



* Klient gjør et kall til en tjenesten og får svar med en gang (i samme sesjon)
* I denne meldingsutvekslingen må det være mekanismer som sikrer:
  + Konfidensialitet
  + Integritet
  + Identifikasjon av klient («information requesting enterprise»)
  + Identifikasjon av tjeneste («information owner enterprise»)
* For enkelhets skyld antar vi at dette er snakk om en lese-tjeneste

## Spørsmål:

(det er mulig dette er gitt, men jeg har ikke funnet noe informasjon om det)

|  |  |
| --- | --- |
| Kan vi anta at klienten eies (utvikles og forvaltes) av en virksomhet? |  |
| Opererer klienten på vegne av seg selv/virksomheten, eller på vegne av en borger/privatperson? |  |
| Hvem er virksomheten som spør («information requesting enterprise»), og hvordan er denne sitt forhold til tjenesteeier? (i parantes er antall virksomheter det typisk dreier seg om)   * Offentlig etat med lovfestet hjemmel til å hente ut informasjon (1-10 stk) * Privat selskap med en avtale om å hente ut informasjon (10-50 stk) * Alle virksomheter med en gitt organisasjonsform (noen 1 000) * Alle virksomheter registrert i enhetsregisteret (over 1 000 000)   En virksomhet som opptrer på vegne av en annen virksomhet (for eksempel advokater, regnskapsførere, revisorer) |  |
| Når vi velger sikkerhetsmekanismer, hva skal vi optimalisere for? (kriterier)   * Ende-til-ende-sikkerhet (hva nå det betyr) * Nettverkstrafikk * Responstid * CPU-belastning på klient eller tjener * Administrativ belastning for klient eller tjener * Kode-kompleksitet for klient eller tjener |  |

## Verdivurderinger

Altså: grunnlag for å mene noe om hva som bør omfattes av mekanismer for integritet eller konfidensialitet

Med utgangspunkt i følgende enkle modell:

Klient

Tjeneste

Input

Output

### Krav til konfidensialitet

For både input til og output fra en tjeneste (klassifisering av informasjonen):

* Inneholder meldingen personopplysninger?
* Inneholder meldingen særlige kategorier av personopplysninger (tidligere kjent som: sensitive personopplysninger)?
* Inneholder meldingen informasjon dekket av forvaltningslovens § 13 (taushetsplikt)?
* Inneholder meldingen informasjon dekket av særregler for tjeneste-eier?

Dersom «ja» på noen av disse:

* Hvem har ansvar for å sikre konfidensialitet gjennom ulike ledd i en kall-kjede og ulike infrastrukturkomponenter?
* Skal referansearkitekturen legge føringer for hvordan dette skal oppnås?
  + I så fall hvilke?
  + Er disse føringene avhengig av klassifiseringen?

### Krav til integritet

* Hva er mulige konsekvenser dersom input endres? For eksempel en angriper kopierer et «token» fra en forespørsel og gjør en annen forespørsel.
* Hva er mulige konsekvenser dersom output endres?
* Hvem vil konsekvensene berøre? (klient, tjeneste, publikum, person informasjonen berører)

Og løsninger for å redusere risiko:

* Hvor viktig er ende-til-ende-integritet (for input og output)?
* Hvem må akseptere rest-risiko?
* Skal referansearkitekturen legge føringer? Eller bare åpne for muligheter?
  + I så fall hvilke?