# Prosjekt: Referansearkitektur for informasjonsutveksling

**Tid:** 15.4.2017 kl 9-12

**Sted:** Difi

**Emne:** API sikkerhet

**Deltagere:**

|  |
| --- |
| Furmyr, Anne Lise |
| Nygren, Erik |
| Stav, Kristoffer |
| Heier, Ståle |
| Jendal, Håkon |
| Staff, Eivind |
| Solberg, Andreas |
| Skagemo, Steinar |
| Pedersen, Klaus Vilstrup |
| Hagen, Erik |
| Gundersen, Svanhild |
| Binningsbø, Jørgen |
| Kjørlaug, Rune |
| Alvik, Tor |

**Præsentasjon om API-sikkerhet ramme (Klaus)**

**Præsentasjon om API sikkerhetsnivåer (Håkon)**

**Slide om "autentisering og eventuell autorisering"**

Diskusjoner:

* Ta Token-debatten videre etter møtte, fordi kommer ikke i mål i dag

Navn: **Token management**  (token-utstedelse, type token, granularitet, autorisering vs. autentisering)

1. Sammenheng mellom felleskomponentene…
2. Tilgangsstyring på grovgranulært og fingranaulært nivå.

Bruk av Difi Id-Porten, Altinn autorisasjon.

Aksjonspunkt: Skatt, Anne-Lise skriver om Token Management

**Slide om Integritet og uavviselighet (ikke-benekt)**

Diskusjon rundt uavviselighet…

Tjeneste vs. løsnng, som «sporing»

Øivind: Må skille mellom

1. Uavviselighet på at tilbyder har mottat request
2. Uavviselighet på at konsumentypen har mottatt responsen

Merk: Timestamp del av signaturen og/eller juridisk logg

Aksjonspunkt: Difi/Klaus detaljererer

**Ende-til-ende konfidensialitet**

Responsbody krypteres (JWE)

Jørgen B: Ref. "spec-en";   ref. JWKS, Må ikke nødvendigvis sentralisere

Aksjonspunkt: Skatt/Erik skriver om "de to alternativene"

Merk, Erik, Skatt: JWE er uavhengig av payload JSN eller XML

**Øivind: Slide: Litt om get**

Har man behov for integritet på forespørselen, i tillegg til kryptering over TLS?

Steinar: FINT med fødselsnummer i HTTP header, behov for hashing? (personvern)

Erik: Kan putte det i URL-en

Anne-Lise: Hjemmel i get kan også være sensitivt

Andreas: Kan også legge det i token

Ikke aksjonspunkt nå, men Skatt jobber med det

**Slide: Kommentarer**

Sikkerhetsmekansiemer behøver ikke koples?

Erik: Separation of concerns, ulike nivåer

Diskusjon: Øivind tenker kopling er interessant

Andreas: Eksempel på kopling…

Kompleksitet vs. sikkerhet

Timeout! Diskuter videre neste gang

Klaus:

Confluence -> Sharepoint

Deltakere, Excel bør oppdateres med roller/kompetanser

## Opgaver

1. Token management (Skatteetaten)
2. Integritet og uavviselighet (Klaus-Erik)
3. Ende til endekonfidentialitet (Skatteetaten/Erik)
4. Integritet på forespørgsel (ikke aksjonspunktnå, Skatteetaten)
5. Administrativt: Sharepoint, deltagerliste