Tokenbasert virksomhetsautentisering

# Bakgrunn

I dagens løsninger for maskingrensesnitt mellom offentlige etater, og mellom private og det offentlige, brukes i stor grad virksomhetssertifkater for autentisering over TLS tilkoblinger.

Bruk av virksomhetssertifikater er forankret i følgende:

* <https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/>
* <https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/>
* <https://lovdata.no/dokument/SF/forskrift/2004-06-25-988>

TODO: Det er flere eksempler på forvaltning av sertifikater i de dokumentene som brytes i dag. Oppsummer.

Trenden de siste årene, er at man går mot mindre tjenester, med separate ansvarsområder. Det er også en stadig større grad av automatisering av prosesser som krever større grad av kommunikasjon mellom systemer.

Bruken av virksomhetssertifikater for kommunikasjon mellom systemer har enkelte utfordringer.

## Vide rettigheter

Det er ikke mulig å begrense bruken av et virksomhetssertfikat i dag, utover å si noe om bruksområdet. Et virksomhetssertifikat som kan brukes mot en tjeneste, kan derfor brukes mot alle andre tjenester. Dette er uheldig når drift av tjenester settes bort til forskjellige grupper, og virksomhetssertifikatet må spres.

## Beskyttelse av nøkler og langlivede nøkler

For at et virksomhetssertifikat skal være sikkert, krever det at de private nøklene er godt beskyttet. Større organisasjoner har også krav om hardwarebeskyttelse av nøkler.

En god beskyttelse av nøkler er svært vanskelig på industristandard infrastruktur i dag. Selv om det finnes hardwareløsninger for beskyttelse av nøkler hos de store skyleverandørene, er ikke de enkle å integrere med applikasjoner som skal konsumere tjenester (TODO: Sjekk.. CloudHSM er iallefall krøkkete).

Virksomhetssertifkater har levetid på flere år (TODO: Finnes nok et krav en eller annen plass). En eventuell lekasje av nøkler gjør at de kan misbrukes lenge.

Selv om klient-side TLS validering er en teknologi som har vist seg å være sikker og stabil, er ikke problemstillingene rundt nøkkelhåndtering ukjente.

Prosjekter som letsencrypt og servic mesh implementasjoner som lener seg på TLS, har derfor fokus på hurtig nøkkelrotering og kort levetid på sertifikater.

## Komplisert validering på tjenestesiden

Virksomhetssertifikater er vanskelig å validere riktig, og konfigurasjonen er ofte vanskelig å validere godt. I tillegg må det konfigureres etter på sjekke for revokering. Flere anerkjente produkter gjør ikke det ut av boksen, og mye brukte programmeringsspråk som Java, gjør det ikke i standardkonfigurasjon.

## Vanskelige feilmeldinger

Manglende godkjenning av virksomhetssertifkat resulterer i at en TLS-forbindelse ikke blir satt opp, og det er ikke mulig å gi gode feilmeldinger til klienter.

## Umuliggjør ett API for mobilapper, webapplikasjoner og maskin-integrasjoner

TODO: Poeng å skrive noe om?

# Tokenbasert identifikasjon og grovkornet autorisasjon

Svært mange API som eksponeres over Internett, bruker tokenbasert autentisering og autorisasjon.

Noen eksempler:

* Open Bank project: <https://github.com/OpenBankProject/OBP-API/wiki/Authentication>
* OpenBanking: <https://openbanking.atlassian.net/wiki/spaces/DZ/pages/83919096/Open+Banking+Security+Profile+-+Implementer+s+Draft+v1.1.2>
* HealtIT: <https://www.healthit.gov/sites/default/files/privacy-security-api.pdf>

TODO: Fyll på med det som kreves av eksempler. Utviklervennlighet. Gjenkjennbarhet.

# Difi som autoriativ kilde for token for virksomheter

I dag fungerer IDPorten som autoriativ kilde for borgerpålogginger. Tjenester tilbudt borgere kan dermed forholde seg til en enklet aktør for å etablere identitet på brukere av løsninger. IDPorten skjuler kompleksitet knyttet til flere identitesprovidere. Når offentlige sluttbrukerløsninger må forholde seg til EU-borgere, blir disse besparelsene enda større.

For virksomheter finnes ikke tilsvarende funksjonalitet.

## Ønsker av en tjeneste for autentisering av virksomheter

TODO: Dette er mye jobb...

### Prosess godkjenning av tilgang til enkelttjenester på vegne av virksomhet?

### Autentisering for ikke-norske bedrifter? Behov?

### Oversikt over hvem som er gitt rettigheter til hva?

# OAuth2.0 for virksomhetsautentisering

OAuth2.0 er en protokoll for delegert autorisasjon. Innenfor protokollen er det mulig å implementere en løsning for å tilby token til en virksomhet som har rettigheter til å kunne brukes mot en enkelt tjeneste. Det muliggjør en vesentlig innskrenkning muligheter for misbruk sett opp mot virksomhetssertifikater.

# Alternativer

* Det er mulig for hver enkelt etat å implementere en løsning selv. Neppe ønskelig.
* Fortsette å bruke virksomhetssertifikater.

# Uavklart

* Tokenformat
* Bruk av/mot private
* Det krever endel av Difi hvis det skal bli bra. Klarer vi å få det prioritert?
* Hva trengs av endringer av offentlige rammeverk og retningslinjer?