Sikkerhet

Signeringstjenesten benytter to-veis TLS for å sikre konfidensialitet og meldingsintegritet på transportlaget. Dokumentpakken med dokumentet som skal signeres er integritetssikret med ASiC-E.

To-veis TLS

For å benytte APIene trenger du et godkjent virksomhetssertifikat, som beskrevet for sikker digital post.

Du skal benytte sertifikat med `KeyUsage` som inkluderer `DigitalSignature`. Hvis sertifikatet har angitt `ExtendedKeyUsage` må den inkludere `clientAuth`. Har du fått utstedt virksomhetssertifikater fra Buypass så skal du bruke det som har satt *Bruksområde: autentisering og kryptering*.

De fleste HTTP-klienter har innebygget støtte for toveis TLS. Du kan se eksempler på implementasjonen i våre klientbiblioteker. Signeringstjenesten støtter kun TLS 1.2 for to-veis TLS.

Du benytter ditt eget sertifikat i `keystore` (det du skal identifisere deg med), og legger til tillitsankrene (CA-sertifikater) i `truststore` (det serveren skal identifisere seg med). Sertifikatet ditt vil bli brukt for å verifisere deg mot serveren, og serveren vil bruke sertifikatet til Posten Norge AS for å identifisere seg. Ved å ha tillitsankrene i `truststore` får du mesteparten av valideringen derfra (gitt at ditt språk/rammeverk håndterer dette). Det du manuelt må gjøre er å validere at sertifikatet tilhører Posten Norge AS, ved å sjekke organisasjonsnummeret som står i `Common Name`.

Et godt tips er å benytte eller hente inspirasjon fra Difi sin sertifikatvalidator, som er tilgjengelig på GitHub.

Vanlige problemer med oppsett av to-veis TLS

- Det benyttes feil `truststore` for klienten. I testmiljøet må `truststore` inneholde testsertifikatene, i produksjon må det være produksjonssertifikater.
- Sertifikatet som benyttes er ikke et virksomhetssertifikat. Virksomhetssertifikater utstedes typisk av Buypass eller Commfides.
- Klienten støtter ikke TLS v1.2. Java 6 støtter ikke TLS v1.2, i Java 7 må dette skrus på eksplisitt.
- Sertifikatet er utstedt av Commfides SHA-1 rotsertifikat. Kun sertifikater med SHA-256 fra

Commfides er støttet. Dette gjelder primært eldre sertifikater.

Personopplysninger

Personopplysninger og sensitive personopplysninger skal kun legges i følgende felter i XML-en i requestene mot API-et:

- `personal-identification-number` – undertegners fødselsnummer eller d-nummer
- `title` – tittelen/emnet til dokumentet, som oppsummerer hva signaturoppdraget handler om
- `description` – kan inneholde en personlig melding, tilleggsinformasjon til dokumentet eller beskrivelse av dokumentet

Øvrige felter skal ikke inneholde sensitive personopplysninger eller personopplysninger. Eksempelvis vil referansen (`reference`) brukes utenfor en sikker kontekst (f.eks i epost-varslinger), og kan derfor ikke inneholde personopplysninger. Se for øvrig beskrivelse av API-et lenger nede.

Se nærmere beskrivelse av begrepene personopplysninger og sensitive personopplysninger på Datatilsynet sine nettsider.