TLP:WHITE = Offentliggjøring er ubegrenset

DSOP
DIGITAL SAMHANDLING OFFENTLIG PRIVAT

SBL-endringer

- **<u>Sammenstilt dokumentasjon fra følgende kilder</u>:**
  - Digitaliseringsdirektoratet
  - Altinn
  - Skatteetaten

Kartverket Digdir Skatteetaten POLITIET POLITIDIREKTORATET nav Brønnøysundregistrene BITS Finans Norge

1. SBL-endringene – kort forklart
2. Leverandør-aspektet
3. Samtykkeløsningen
4. Maskinporten
5. Maskinporten + Samtykkeløsningen
6. SBL-API-ene

SBL-endringene – kort forklart

Forhåndsregistrerte samtykkeforespørsler

- Opprettes via REST-kall.
  - Støtter RequestMessage i flere språk
  - Konsument kan sjekke status på en gitt samtykkeforespørsel (åpnet/innfridd/nektet) uavhengig av redirectURL-flyt
  - Mer informasjon om feilmeldinger
- Mulighet for å trekke forespørsel via REST.
- Ingen forandring for sluttbruker.
- Minimal endring i flyt.
  - I stedet for at lenke konstrueres manuelt, registreres en forespørsel som returnerer en permalenke som sluttbruker sendes til
- Samtykkeforespørsler krever autentisering.
  - Maskinporten

Maskinporten-migrering

Skatteetaten beskytter sine SBL API-er med Maskinporten, som sikrer autentisering av konsument og autorisasjon til å uthente data. En stor fordel ved bruk av Maskinporten er bruk av delegeringsfunksjonalitet. Maskinporten muliggjør at konsument kan delegere rettigheter til sin leverandør for å opptre på vegne av dem.

Ved bruk av delegering, vil ikke konsument måtte dele API-nøkkel og virksomhetssertifikater med sin leverandør. Leverandørforholdet valideres i et access token fra Maskinporten via feltet «HandledBy».

- Ta i bruk Maskinporten som konsument.
- Ta i bruk Maskinporten som leverandør.

Leverandør-aspektet

- Prosessen med å utføre samtykkeforespørsler og Maskinporten-forespørsler er annerledes avhengig av om man bruker en leverandør, eller ikke.

- Om leverandør opererer på vegne av en konsument, vil forespørslene inneholde et eget claim som valideres for å bekrefte leverandør/konsument-forholdet.

Samtykkeforespørsel
Claim: *HandledBy*

HandledBy-claimet inneholder **leverandørens** org.nr.

Maskinporten-forespørsel
Claim: *consumer_org*

Consumer_org-claimet inneholder **konsumentens** org.nr

- Tidligere benyttet Skatteetaten tjenesteeierstyrt rettighetsregister (SRR) for å kontrollere leverandør/konsument-forholdet. Dette krever dog aktiv forvaltning fra Skatteetatens side, ettersom de manuelt må legge inn leverandører som godkjente «HandledBy's» for deres bank(er).

- Koblingen mellom konsument og leverandør uttrykkes i delegeringen av «Tilgang til å administrere samtykkeforespørsler og samtykketokens» i Altinn. Denne rettigheten gjør at leverandør kan hente ut et leverandørtoken fra Maskinporten som bekrefte leverandør-forholdet.

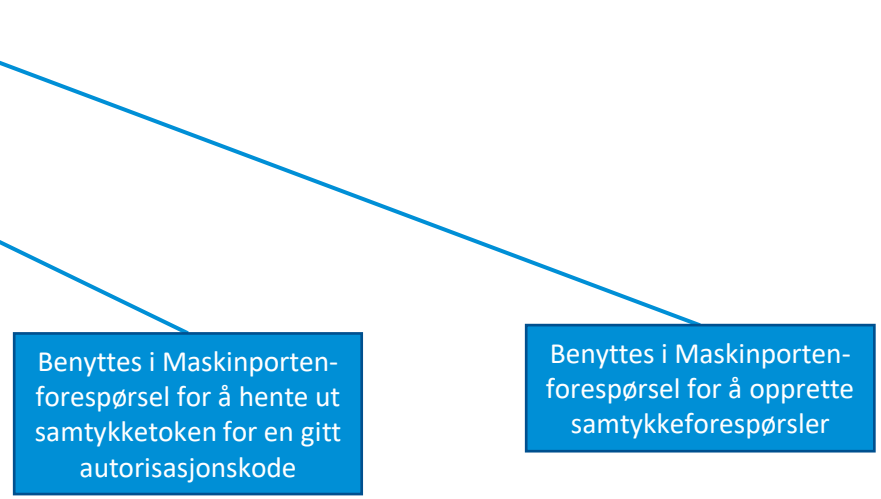
Samtykkeløsningen

Leverandører

- **Forutsetning**: *konsument har delegert tilgang til Altinn-rettigheten «Tilgang til å administrere samtykkeforespørsler og samtykketokens» til leverandøren.*

- For at forholdet leverandør/konsument skal bekreftes, skal leverandørtoken* inkluderes i samtykkeforespørselen fra leverandør.

- Når tilgang til rettigheten *«Tilgang til å administrere samtykkeforespørsler og samtykketokens»* er delegert til leverandør, tilgjengeliggjøres følgende scopes:
  - *altinn:consentrequests.write*
  - *altinn:consentrequests.read*
  - *altinn.consenttokens*



*Leverandørtoken = access token fra Maskinporten

Maskinporten

Leverandør

- Leverandøren må også opprette en klient i Maskinporten. Det er par viktige momenter ved opprettelse av leverandør-integrasjon i Maskinporten:
  - Leverandør må opprette integrasjon som tilhørende seg selv, og ikke velge «på vegne av en kunde» eller «på vegne av flere kunder».
  - Når leverandør-integrasjon skal forespørre tokens på vegne av konsument, må konsumentens org.nr. oppgis i claimet *consumer_org* i JWT-grantet. Maskinporten sjekker da Altinn om et gyldig delegeringsforhold finnes mellom konsument og leverandør for aktuelt scope.
    - Altinn vil bekrefte dette ettersom konsument allerede har delegert tilgang til rettigheten «Tilgang til å administrere samtykkeforespørsler og samtykketokens» til leverandøren.

Eksempel: før leverandør gjør en samtykkeforepørsel på vegne av en konsument, må leverandør hente ut et leverandør-token fra Maskinporten. I scopet-claimet i Maskinporten-forespørselen skrives «altinn:consentrequests.write». Maskinporten sjekker så med Altinn om leverandør har fått delegert tilgang til dette scopet – og det har leverandøren fått gjennom rettigheten «Tilgang til å administrere samtykkeforespørsler og samtykketokens».

Maskinporten

Leverandør

- For å få ut et access token må man sende en JWT-grant til token-endepunktet til Maskinporten:
  - https://ver2.maskinporten.no/token

- Første steg blir da å generere en JWT-grant. To eksempler:

Eksempel JWT-grant: leverandør-token ved samtykkeforespørsel

Header
{
«x5c» : {*virksomhetssertifikat*}
«alg» : «RS256»
}

Body
{
«aud» : «https://ver2.maskinporten.no»,
«scope» : «altinn:consentrequests.write»;
«iss» : «*client_id*»
«exp» : {*utløpstidspunkt*}
«iat» : {*issued at*}
«jti» : «*unik ID for JWT*»
«consumer_org» : «*konsuments org.nr.*»
}
.
<<signature-value>>

Eksempel JWT-grant: leverandør-token ved veksling av autorisasjonskode med samtykketoken

Header
{
«x5c» : {*virksomhetssertifikat*}
«alg» : «RS256»
}

Body
{
«aud» : «https://ver2.maskinporten.no»,
«scope» : «altinn:consenttokens.read»;
«iss» : «*client_id*»
«exp» : {*utløpstidspunkt*}
«iat» : {*issued at*}
«jti» : «*unik ID for JWT*»
«consumer_org» : «*konsuments org.nr.*»
}
.
<<signature-value>>

JWT-grant sendes til token-endepunktet: https://ver2.maskinporten.no/token.

POST https://ver2.maskinporten.no/token
Header
{
«content-type»: application/x-www-form-urlencoded
}

Body
{
«grant_type»: urn:ietf:params:oauth:grant-type:jwt-bearer
«assertion»: «*JWT-grant*»
}

- exp – iat <= 120 sek

Maskinporten + Samtykkeløsningen

Leverandør

- Leverandør-tokens fra Maskinporten inkluderes i forespørslene som gjøres mot Samtykkeløsningen:

Eksempel-forespørsel: samtykkeforespørsel

POST https://tt02.altinn.no/api/ConsentRequest

Header:
Host: www.altinn.no
Accept: application/json
ApiKey: {*API-nøkkel}*
Content-Type: application/hal+json
Authorization: Bearer {*token}*

Body:

```
{
  "CoveredBy": "DERES_ORG_NR",
  "OfferedBy": "FØDSELSNUMMER",
  "OfferedByName": "ETTERNAVN"
  "RequiredDelegator": "FØDSELSNUMMER",
  "ReguiredDelegatorName": "ETTERNAVN"
  "HandledBy": "TREDJEPARTS_ORG_NR",
  "ValidTo": "2021-06-01T13:17:31.495Z",
  "RedirectUrl": "https://WWW.DERES_URL.NO",
  "RequestResources": [
    {
      "ServiceCode": "4628",
      "ServiceEditionCode": 1,
       "Metadata" : {
                 "Navn" : "BankensNavn"
    }
   }
    ],
"requestMessage": { }
}
```

Forespørselen oppretter autorisasjonskode (samtykke) hos Altinn. Koden sendes i eget felt i responsen.

HandledBy-feltet i forespørselen spesifiserer at det er en leverandør som opptrer på vegne av konsumenten (CoveredBy).

- *Man trenger ikke ha med «?ForceEIAuthentication» i endepunktet da dette feltet brukes for å tvinge autentisering med virksomhetssertifikat. Det er ikke nødvendig når dette skjer med Maskinporten-token.*

Eksempel-forespørsel: token-uthenting

GET https://tt02.altinn.no/api/authorization/token/{Autorisasjonskode}

Header:
Accept: application/json
ApiKey: {*API-nøkkel}*
Authorization: Bearer {*token}*

Body:

```
{
    "AuthorizationCode": "89860470-ca02-4e5f-9d65-28d808d962cc"
    "coveredBy": "DERES_ORG_NR",
    "offeredBy": "FØDSELSNUMMER",
    "offeredByName": "ETTERNAVN",
    "requiredDelegator": "FØDSELSNUMMER",
    "requiredDelegatorName": "ETTERNAVN",
    "validTo": "2020-11-04T11:29:56.577Z",
    "redirectUrl": "https://WWW.DERES_URL.NO",
    "requestResources": [
        {
            "serviceCode": "4628",
            "serviceEditionCode": 1
            "Metadata": {
                "Navn": "Bankens Navn"
  }
        }
    ],
    "requestMessage": {}
}
```

Når kunden har gitt sitt samtykke er autorisasjonskoden (samtykket) aktivt 10 dager frem i tid. Samtykketoken har 30 sek varighet. Be om nytt samtykketoken med samme autorisasjonskode når token er utgått.

Samtykketoken som returneres vil være en JSON-streng bestående av et JWT.

- *Accept: application/xml → token er omsluttet av en <string>-tag*

SBL API-ene

- Følgende API-er omfattet av SBL:
  - Inntektsmottaker API
    - **Scope**: *skatteetaten:inntekt*
  - Spesifisert Summert Skattegrunnlag API
    - **Scope**: *skatteetaten:spesifisertsummertskattegrunnlag*
  - Tilgjengeligdata API
    - **Scope**: scopet er p.t. omfattet av scopet til SSS

- SBL API-ene er sikret med Maskinporten. Dvs. man må inkludere et access token fra Maskinporten i headeren i forespørselen til API-ene.

- SBL API-ene er samtykketjenester, mao. må også et samtykketoken fra Altinn inkluderes i headeren i forespørselen til API-ene.

SBL API-ene

- En eksempel-forespørsel vil da kunne se slik ut:

Eksempel-forespørsel: inntektsmottaker API

GET https://api-at.sits.no/api/innrapportert/inntektsmottaker/sbl/12345678901/oppgave/inntekt?fraOgMed=2016-11&tilOgMed=2017-01
Header
AltinnSamtykke: «*JWT-samtykketoken*»
Authorization: Bearer «*token*»

- Det er viktig å huske på at det kun er «access_token»-claimet som skal inkluderes i Authorization: Bearer «*token*»:

```
{
  "access_token" : "IxC0B76vlWl3fiQhAwZUmD0hr_PPwC9hSIXRdoUslPU=",
  "token_type" : "Bearer",
  "expires_in" : 599,
  "scope" : "difitest:test1"
}
```