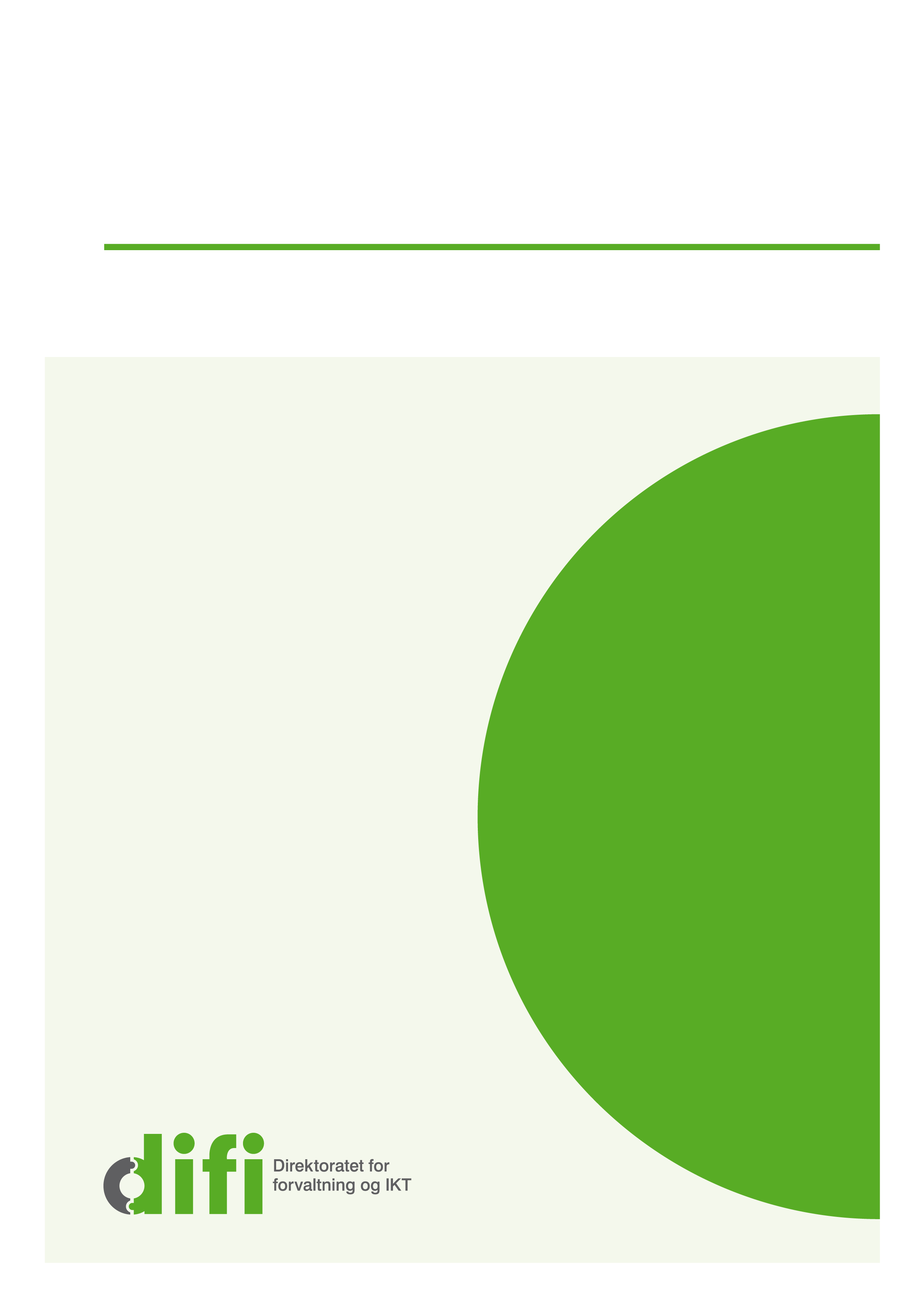
|  |
| --- |
| Integrasjonsguide ID-porten  **Integrasjonsbeskrivelse for ID-porten** |
| Date: 17.03.2014 |
|  |

****

**Endringslogg**

| Versjon | Dato | Beskrivelse | Ansvarlig |
| --- | --- | --- | --- |
|  |  |  |  |
| 1.2 | 02.06.2010 | Første versjon | Even Mikalsen |
| …. |  |  |  |
| 2.00 | 28.09.2012 | Oppdatert med informasjon om integrasjonen mot felleskomponenten Digital kontaktinformasjon  Struktur endring og forenkling av dokument. | Arne Berner |
| 2.01 | 03.10.2012 | QA | Kjetil Melheim |
| 2.02 | 04.10.2012 | Rettet skrivefeil og formuleringer. | Marianne Strypet |
| 2.3 | 22.10.2012 | Rettet skrivefeil og rettet opp i Gyldige verdier i DigitalContactInfoStatus | Arne Berner |
| 2.4 | 22.11.2012 | Lagt til info om BankID | Arne Berner |
| 2.5 | 17.03.2015 | Endret tittel og lagt til info om ny assertion | Arne Berner |

**Innhold**

[**Endringslogg** 2](#_Toc336608006)

[**Innhold** 2](#_Toc336608007)

[**Lese guide** 2](#_Toc336608008)

[1. Innledning 3](#_Toc336608009)

[2. Funksjonelt 5](#_Toc336608010)

[3. Teknisk: Innlogging 10](#_Toc336608011)

[4. Administrative rutiner 15](#_Toc336608012)

[5. Detaljertbeskrivelse av teknisk løsning 19](#_Toc336608013)

[6. Sikkerhet 21](#_Toc336608014)

[Vedlegg 1: Detaljert beskrivelse av støttede SAML2 profiler 25](#_Toc336608015)

[Vedlegg 2: SAML ekstension 31](#_Toc336608016)

[Vedlegg 3: Eksempel på metadatafil 32](#_Toc336608017)

[Vedlegg 4: krav til Sluttbruker av ID-porten 34](#_Toc336608018)

**Lese guide**

* Er du på jakt etter **en funksjonell beskrivelse** av ID-porten les kapitel: 2
* Er du **prosjektleder** og skal følge opp integrasjon mot ID-porten les kapitel: 4
* Er du **en teknikker** som skal etablere en integrasjon mot ID-porten les kapitel: 3 og 5
* Se kapitel 6 om du har spørsmål om **sikkerhet** knyttet til ID-porten.

# Innledning

Dette kapitelet beskriver formål, hensikt og terminologi for dette dokumentet.

## Formål

Målgruppen for dokumentet er offentlige virksomheter som skal benytte seg av ID-porten.

Dokumentet skal detaljere krav til virksomheter som skal ta i bruk ID-porten, slik som f.eks. krav til nøkkelhåndtering og konfigurasjon av integrasjoner.

Dokumentet beskriver også de aktiviteter som skal lede frem til bruk av ID-porten for en virksomhet.

Dokumentet beskriver det sett av profiler for OASIS SAML2 som støttes i ID-porten i tillegg til å beskrive omkringliggende krav.

Målgruppen er **IT-ansvarlige, prosjektledere, IT-arkitekter og utviklere** hos tjenesteeierne og tjenesteleverandører, som skal skape seg et overblikk over hva en tilslutning innebærer.

## Bakgrunn

Føderering og SSO-løsninger i forløperne til ID-porten har vært noe vagt beskrevet, og dermed har en kunnet benytte et veldig vidt spekter av SAML2-profiler mot løsningene, dette inkluderer SAML2-varianter som det kan være ønskelig å utfase når løsningen skal støtte tjenester på nivå 4 i henhold til [Rammeverk]. Målet med arbeidet inn mot ID-porten har vært å stramme opp dette, slik at man på en veldefinert måte kan angi nøyaktig hvilke SAML2 profiler som støttes, og dermed underforstått angi hva som ikke er støttet.

Videre er det også et mål med arbeidet og i større grad kunne binde seg opp mot profiler som virksomheter som ID-porten kan sammenlignes med, har valgt. Dette med tanke på å kunne tilby en mer standardisert løsning, som en vet blir nøye vurdert av mange uavhengige fagmiljøer med tanke på sikkerhet og også andre forhold. Under arbeidet med etableringen av SAML2-profil for ID-porten ble det mer og mer klart at den såkalte [eGov] profilen, og særlig slik den er definert i [OIOSAML] tilbyr mye av det en er ute etter, og arbeidet med ID-porten er derfor gjort med utgangspunkt i disse profilene. Det er allikevel gjort en del valg som går på tvers av de valgene som er gjort for OIOSAML.

## Ordbok

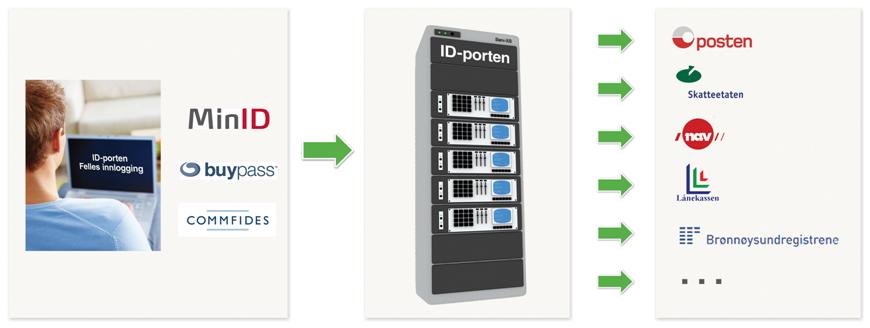
|  |  |
| --- | --- |
| Bak-kanal | Henviser til den direkte kommunikasjonskanalen mellom SP og ID-porten som ikke går gjennom UA. Dette er en SOAP over HTTPS kanal som etableres direkte mellom ID-porten og den enkelte SP. |
| COT | Circle of trust, |
| Frontkanal | Henviser til den indirekte kommunikasjonskanalen mellom SP og ID-porten som alltid går gjennom UA (nettleser). Dette er en kanal som benytter mekanismer i HTTP, som HTTP redirect og HTTP post, til å sende meldinger |
| IdP | Identity Provider – I dette dokumentet betyr dette alltid ID-porten |
| Modes | Benyttes til å beskrive de ulike variantene av en SAML2 profil |
| PKI | Public Key Infrastructure. |
| SLO | Single Logout |
| SP | Service Provider – Tjenesteleverandør - I dette dokumentet alltid den part som teknisk er tilsluttet IdP’s COT gjennom utveksling av metadata, typisk tjenesteeiers driftsleverandør. |
| SSO | Single Sign On |
| UA | User Agent – Programvaren bruker benytter til å kommunisere mot ønsket tjeneste, normalt en nettleser. |
| NTP | Network Time Protocol, se <http://en.wikipedia.org/wiki/Network_Time_Protocol> |

## Referanser

|  |  |
| --- | --- |
| [Samarbeidsavtalen] | Samarbeidsavtalen regulerer forholdet mellom Difi som eier av ID-porten og Tjenesteeier, herunder hver av partenes rettigheter og forpliktelser. Samarbeidsavtalen om bruk av ID-porten må undertegnes av begge parter før Tjenesteeier kan produksjonssette sine tjenester. <http://samarbeid.difi.no> |
| [Tilslutning DigKontakt] | Tilsluttningsguiden for Digital kontaktregister. |
| [samarbeidsportalen] | <http://samarbeid.difi.no> |
| [ID-porten designguide] | Designguide, implementasjon av ID-porten brukergrensesnitt, <http://samarbeid.difi.no/wp-content/uploads/2012/01/Designguide_IDporten_v1.pdf> |
| [eGov] | [www.projectliberty.org/liberty/content/download/4711/32210/file/Liberty\_Alliance\_eGov\_Profile\_1.5\_Final.pdf](http://www.projectliberty.org/liberty/content/download/4711/32210/file/Liberty_Alliance_eGov_Profile_1.5_Final.pdf) |
| [kravspesifikasjon PKI] | Versjon 2.0 av kravspesifikasjon for PKI. [www.difi.no/emne/ikt/eid-og-MinID/kravspesifikasjon-for-pki](http://www.difi.no/emne/ikt/eid-og-MinID/kravspesifikasjon-for-pki) |
| [OIOSAML] | Dansk versjon av eGov profilen, som vi i denne profilen har tatt sterkt utgangspunkt i. [www.oiosaml.info](http://www.oiosaml.info) |
| [Rammeverk] | Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett. April 2008. Se [www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID\_rammeverk\_trykk.pdf](http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf) |
| [SAMLCore] | S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. Se: [www.oasis-open.org/committees/security/](http://www.oasis-open.org/committees/security/). |
| [SAMLProf] | S. Cantor et al. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. Se: [www.oasis-open.org/committees/security/](http://www.oasis-open.org/committees/security/). |
| [Begrepskatalogen] | <http://begrep.difi.no> |

# Funksjonelt

Dette kapitelet gir en oversikt over de funksjoner som ID-porten tilbyr til tjenesteleverandør.



* ID-porten skal dekke funksjonalitet innenfor følgende områder:
  + Autentisering
  + Signering
  + Meldingskryptering

Pr. i dag inneholder ID-porten KUN funksjonalitet for **autentisering**.

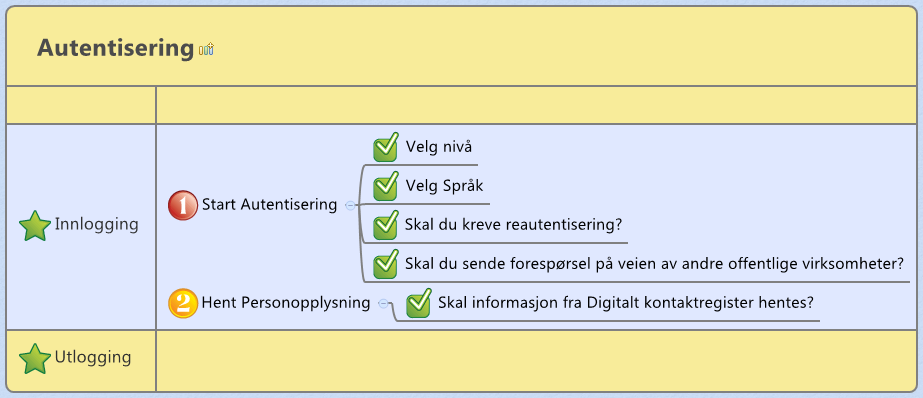
## Aktører

Dette kapitel beskriver roller og ansvar knyttet til den tekniske integrasjonen mot ID-porten. Kapitelet er et tillegg til [Samarbeidsavtalen] som i større grad omhandler det avtalemessige mellom Difi og tjenesteeierne.

|  |  |
| --- | --- |
| Aktører | Beskrivelse |
| Sluttbruker | Innbygger med eID |
| ID-porten | **ID-porten** er et ***nav/tillitsanker*** for offentlig virksomheter. ID-porten knytter de offentlige virksomhetene og e-ID leverandørene sammen. |
| Tjenesteeier | Offentlig virksomhet som har signert [Samarbeidsavtalen] |
| Tjenesteleverandør | Enten:  - Leverandør som leverer tjenester til en offentlig virksomhet.  - En tjenesteeier som forvalter egen løsning. |
| Digitalt kontaktregister | Felleskomponent for sentral ajourhold av e-post og mobilnummer i offentlig sektor. |
| e-ID leverandør | En av de 3 eID aktørene som er tilgjengelig i ID-porten:  - MinID, Commfides, Buypass, BankID |
| MinID | **MinID** er en e-ID leverandør på nivå-3, som tilbyr autentisering basert på engangskoder på sms eller pinkoder på brev. |
| Sertifikatutsteder | Sertifikatutsteder som oppfyller kravene for virksomhetssertifikater i henhold til [kravspesifikasjon PKI]. |

## Autentiseringstjenester

ID-porten tjenestetilbud for autentisering kan funksjonelt oppsummeres slik:



## Innlogging

Dette er en overordnet beskrivelse av innloggingstjenesten. For detaljer, se kapittel 5.

### Protokoll

For integrasjon mot ID-porten benytter man protokollen: SAML2.

Kanalene som benyttes til utveksling av SAML2 meldinger, er en front kanal som benytter brukerens nettleser via HTTP redirect, og en bak-kanal direkte mellom tjenesteleverandør og ID-porten over SOAP protokollen.

**Forklaring:**

1. Sluttbruker ønsker tilgang til en tjeneste hos tjenesteeier som krever at bruker er autentisert
2. Tjenesteleverandør oppretter en autentiseringsforespørsel som sendes til ID-porten
3. - 5) ID-porten gjennomfører innlogging med sluttbruker med valgt e-ID leverandør på tilfredstillende sikkerhetsnivå.
4. ID-porten klargjør sluttbruk sine personopplysninger for utlevering til tjenesteeier, og sender et svar på autentiseringsforespørselen til Tjenestelevernadør.
5. Tjenesteleverandør sender en personopplysningsforespørsel til ID-porten
6. ID-porten leverer ut personopplysninger om sluttbruker
7. Sluttbruker får tilgang til ønsket tjeneste

### Autentiseringsforespørsel

Tjenesteleverandør kan sende en forespørsel om innlogging til ID-porten. Forespørselen kan inneholde følgende informasjon som vil styre innloggingen:

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Beskrivelse** | **Referanse** |
| **Autentiseringsnivå** | Styrer hvilke eID’r brukeren kan velge | 3.2.1 |
| **Reautentisering** | Vil KREVE at brukeren gjennomfører autentisering | 3.2.2 |
| **Språk** | Styrer hvilket språk ID-porten blir vist i | 3.3 |
| **På vegne av** | Identiteten til tjenesteeieren som innloggingen gjøres på vegne av | 3.4 |

Svaret tjenesteleverandøren får etter en autentisering er en referanse id som kan brukes for å hente ut personinformasjon. Se kapitel 2.3.3 Personopplysningsforespørsel.

### Personopplysningsforespørsel

Tjenesteleverandør skal etter vellykket autentisering hente ut person informasjon om brukeren og autentiseringen. Hvilken informasjon som er tilgjengelig for tjenesteleverandør er dokumentert i kapitel 3.7.3

Merk at det er mulig for tjenesteleverandør å spesifisere hvilke attributter som de ønsker utlevert fra ID-porten om det ønskes.

## Utlogging

Når en sluttbruker er ferdig hos en tjenesteeier, skal han logge ut. Utloggingen skal skje etter følgende beskrivelse.

**Forklaring:**

1. Tjenesteleverandør sender LogoutRequest til ID-porten via frontkanal (HTTP redirect via sluttbruker).
2. ID-porten sender LogoutRequest til alle tjenesteleverandører som denne bruker er pålogget.
3. Alle tjenesteleverandører svarer på LogoutRequest med en LogoutResponse.
4. ID-porten svarer på initial LogoutRequest, med en LogoutResponse.

## Andre funksjonelle aspekt

### Brukervennlighet

DIFI har utarbeidet en egen Designguide for ID-porten. Denne inneholder tips om brukervennlighet, universell utforming og sikkerheten til brukerne av ID-porten. Se [ID-porten designguide]

### Føderering

Dersom sluttbruker er innlogget hos tjenesteeier A og velger å gå videre til en tjenesteeier B uten å logge ut, vil bruker automatisk logges inn uten at bruker må autentisere seg på nytt. Det vil gjøres forespørsler mellom tjenesteeier B og ID-porten på samme måte som ved en normal innlogging, forskjellen er kun at sluttbruker ikke opplever å få opp en autentiseringsdialog.

### Sesjonstid

Tjenesteleverandør og ID-porten holder egne sesjoner mot sluttbruker som ikke er avhengig av hverandre. Difi anbefaler at tjenesteleverandør bruker de samme sesjonstider som ID-porten, se kapitel 5.2 for mer detaljer.

### Sesjonsoppgradering

Det er mulig for en sluttbruker å gjennomføre en autentisering på nivå 3 og seinere gå til en tjeneste som krever et høyere sikkerhetsnivå. I dette tilfellet vil ID-porten be brukeren om å oppgradere sikkerhetsnivå.

### Digitalt kontaktregister

Digitalt Kontaktregister er en felles komponent i offentlig sektor for sentral ajourhold av kontaktinformasjon for sluttbruker. ID-porten er integrert mot registrert og kan videreformidle informasjon fra registeret i forbindelse med en autentiseringsforespørsel. Denne tjenesten er tilgjengelig for de tjenesteeiere som har tatt i bruk det Digitale kontaktregisteret og informasjonen blir kun videreformidlet om sluttbruker har samtykket til utlevering. Se: **[Tilsluttning DigKontakt]**

ID-porten har et del-system for å samle inn informasjon og samtykker for det Digitale kontaktregisteret i forbindelse med autentiseringen.

# Teknisk: Innlogging

I dette kapitelet beskrives tekniske detaljer omkring innloggingsfunksjonene i ID-porten

## Krav til validering

Tjenesteleverandør **må** verifisere alle returverdier fra ID-porten.

Blant annet må det sikres og valideres at ID-porten har autentisert sluttbruker på ønsket sikkerhetsnivå.

## AuthnRequest

Lokalisering av ID-porten må gjøres i forbindelse med dette steget. SAML2 profilen sier at metadata kan nyttes til denne hensikt, men ID-porten krever at tjenesteleverandør MÅ nytte data utvekslet som en del av metadata for å identifisere ID-porten.

I denne profilen MÅ forespørselen signeres. Signaturen plasseres i Signatur forespørsel strengen beskrevet for denne bindingen, og ikke i selve XML meldingen. Slik:

SAMLRequest=<req>&SigAlg=<alg>&Signature=<SIGNATUR>

### RequestedAuthnContext

Tjenesteleverandør KAN benytte *RequestedAuthnContext* til å angi ønske sikkerhetsnivå. Dette skjer på følgende måte:

* Comparison feltet settes til *minimum* da tjenesteleverandør kun skal angi laveste sikkerhetsnivå og ikke tillates å spesifisere eksakt nivå.
* Ulike AuthnContextClassRef defineres til å tilhøre ulike sikkerhetsnivå, og ved å oppgi en spesiell slik klasse sier tjenesteleverandør hvilket sikkerhetsnivå som er minimum. Tabellen under definerer opp sikkerhetsnivå for ulike klasser som er støttet i ID-porten.

|  |  |
| --- | --- |
| **nivå** | **AuthnContextClassRef** |
| **3** | urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified |
| **3** | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| **4** | urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI |

Eksempel på en forespørsel (del av) som minimum krever nivå 3 autentisering:

<samlp:RequestedAuthnContext xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Comparison="minimum">  
     <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
            urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport  
     </saml:AuthnContextClassRef>  
</samlp:RequestedAuthnContext>

ID-porten vil tolke alle forespørsler til *minimum* og at *AuthnContextClassRef* er *urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified* om *RequestedAuthnContext* ikke er inkludert i *<AuthnRequest>.*

### NameID

Det anbefales at tjenesteleverandør setter *NameID* til *transient*. ID-porten støtter både *transient* og *persistant*. Se eventuelt i Vedlegg 1: Detaljert beskrivelse av støttede SAML2 profiler for mer informasjon.

### ForceAuth

Tjenesteleverandør KAN benytte ForceAuth for å angi at sluttbruker alltid skal autentisere seg i ID-porten selv om sluttbruker har en eksisterende SSO sesjon. Dette kan brukes for å reautentisere sluttbruker.

Eksempel på en forespørsel (del av) som krever (re)autentisering:

<saml2p:AuthnRequest

AssertionConsumerServiceURL="https://idporten-sptest2.difi.no/testsp/assertionconsumer"

Destination="https://idporten-test1.difi.no/opensso/SSORedirect/metaAlias/norge.no/idp"

ForceAuthn="true" ……..

## locale

Ved å legge til parameteren ”*locale*” på requesten som inneholder SAMLRequest kan tjenesteleverandør styre språkformen ID-porten blir presentert til bruker. Locale må angis som ISO 639-1 kode.

ID-porten støtter følgende språk:

|  |  |
| --- | --- |
| **Språk** | **Språkkode** |
| Bokmål | **nb** |
| Nynorsk | **nn** |
| Samisk | **se** |
| Engelsk | **en** |

I de tilfeller der tjenesteleverandør ikke sender over språkvalg vil ID-porten benytte språket som er satt i nettleseren. Er nettleseren innstilt på et språk som ID-porten ikke støtter vil ID-porten velge standard språket bokmål.

ID-porten sender over språket som er brukt ved innlogging i assertion til tjenesteleverandør, ref. kapitel 3.7.3.

Her er et eksempel hvordan en forespørsel med språk ser ut:

https://idporten-inttest.difi.local/opensso/SSORedirect/metaAlias/norge.no/idp?SAMLRequest=<KRYPTERT SAML2 REQUEST> &SigAlg=<alg>&Signature=<SIGNATUR>&locale=nb

## Overføring av informasjon om tjenesteeier for leverandører

Kun i de tilfeller der tjenesteleverandør leverer tjenester til flere tjenesteeier under en og samme føderasjon må tjenesteleverandør sende med informasjon om den spesifikke tjenesteeier i AuthnRequest. Dette gjøres ved å bruke extensions *idpe:OnBehalfOf:*

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ...>

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">**TJENESTELEVERANDOR**</saml:Issuer>

...

<samlp:Extensions xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

<idpe:**OnBehalfOf** xmlns:idpe="https://idporten.difi.no/idporten-extensions">**TJENESTEEIER**</idpe:OnBehalfOf>

</samlp:Extensions>

...

</samlp:AuthnRequest>

## Autentisering av sluttbruker

ID-porten sjekker om brukeren har en gyldig sesjon mot ID-porten. Hvis ikke, bes brukeren om å autentisere seg. Om brukeren allerede har en gyldig sesjon mot ID-porten MÅ brukeren reautentiseres dersom:

* Tjenesteleverandør krever reautentisering gjennom å sette *ForceAuthn* attributtet i forespørselen til ”*true*”.
* Brukeren er innlogget på et lavere sikkerhetsnivå enn den inneværende tjenesteforespørsel krever. I så tilfelle vil ID-porten foreta en reautentisering av brukeren med en e-ID som minimum er på korrekt sikkerhetsnivå.

## AuthnResponse

Når ID-porten skal lokalisere tjenesteleverandør for å kunne besvare forespørselen så gjøres dette ved å benytte data utvekslet som en del av metadata.

Artifact returneres ved hjelp av http redirect. Artifact legges i en parameter med navn *SAMLart* i URL’en.

HTTP utveksling over frontkanal skjer over (en veis) SSL/TLS for å understøtte konfidensialitet i meldingene.

Respons meldingen over frontkanal behøver ikke å være signert.

Om ID-porten mottar en forespørsel fra en tjenesteleverandør som den ikke har inngått avtale med så vil forespørselen avvises uten å gi en tilbakemelding til tjenesteleverandør.

## ArtifactResolve

### Etablering av bak-kanal

Bak-kanal benyttes til artifact resolution og til meldinger i forbindelse med single logout. Meldinger over bak-kanal sendes over etablerte HTTPS kanaler.

Artifact resolution kanal etableres alltid initiert i fra tjenesteleverandør. Tjenesteleverandør kan av ytelsesmessige hensyn velge å la en etablert HTTPS kanal bli stående oppe, slik at reetablering av kanalen ikke er nødvendig ved neste melding. Det er tjenesteleverandør sitt ansvar å sørge for at kanalen er oppe, og denne skal håndtere nødvendig reetablering i feilsituasjoner.

Når det gjelder bak-kanal for SLO så er det ID-porten som er ansvarlig for å etablere denne.

### ArtifactResolve

* ArtifactResolve melding fra tjenesteleverandør skal signeres.
* ArtifactResolve melding skal inneholde en og bare en *<artifact>* verdi.

### ArtifactResponse

Følgende attributter legges ut i assertion:

|  |  |  |
| --- | --- | --- |
| Attributt | Beskrivelse | Kommentar |
| Uid | Fødselsnummer |  |
| SecurityLevel | Sikkerhetsnivå |  |
| Culture | Språk |  |
| AuthMethod | Autentiseringsmetode |  |
| OnBehalfOf | EntityID for tjenesteeier | Om verdi er mottatt i forespørsel fra tjenesteleverandør |
| Email | e-post adresse | Kun tilgjengelig for tjenesteleverandører som har tatt i bruk Digitalt kontaktregister |
| MobilePhone | Mobiltelefonnummer | Kun tilgjengelig for tjenesteleverandører som har tatt i bruk Digitalt kontaktregister |
| DigitalContactInfoStatus | Feltet har informasjon om sluttbruker sitt samtykke til utlevering av Digitalt kontaktinformasjon | Kun tilgjengelig for tjenesteleverandører som har tatt i bruk Digitalt kontaktregister |

Gyldige verdier i **AuthMethod**:

|  |  |
| --- | --- |
| **AuthMetod** | **Beskrivelse** |
| **Minid-PIN** | Bruker har logget seg på med PIN koder fra PIN kode ark. |
| **Minid-OTC** | Bruker har logget seg på med engangskode sendt på SMS |
| **Buypass** | Bruker har logget seg på med smartkort fra Buypass |
| **Commfides** | Bruker har logget seg på med USB-pen med e-ID fra Commfides |
| **BankID** | Bruker har logget seg på med BankID med kodebrikke |

Gyldige verdier i **DigitalContactInfoStatus**:

|  |  |
| --- | --- |
| DigitalContactInfoStatus | Beskrivelse |
| SAMTYKKET\_GENERELT | Bruker har samtykket til utlevering av Digital kontaktinformasjon til alle tjenesteeiere |
| SAMTYKKET\_SPESIFIKT | Sluttbruker har samtykket til utlevering av Digital kontaktinformasjon til tjenesteeier. |
| IKKE\_SAMTYKKET | Det er ikke registrert noe samtykke for sluttbruker |
| SAMTYKKE\_AVVIST | Bruker har aktivt avvist samtykke om utlevering av Digital kontaktinformasjon |
| IKKE\_REGISTRERT | Sluttbruker er ikke registrert i Digitalt kontaktregister. |
| SYSTEMFEIL | ID-porten har ikke informasjon om Digital kontaktinformasjon, f.eks. ved feil i integrasjon mot registrert. |

### AuthnContextClassRef som informasjonsbærer om sikkerhetsnivå

Assertion vil alltid inneholde informasjon om sikkerhetsnivå benyttet under autentisering. Til dette benyttes *AuthnContextClassRef* på samme måte som i autentiseringsforespørselen. Se tabell knyttet til autentiseringsforespørsel (kap.3.2.1) for spesifisering av gyldige klasser støttet i ID-porten og deres tilhørende autentiseringsnivå.

# Administrative rutiner

Dette kapittelet har som mål å beskrive rutinene for å etablere en ny integrasjon mot ID-porten.

* **Ta kontakt med oss på:** [**idporten@difi.no**](mailto:idporten@difi.no)
* **Se Samarbeidsportalen for oppdatert informasjon om ID-porten:** [**http://samarbeid.difi.no**](http://samarbeid.difi.no)

**Følg følgende prosess:**

Det er svært individuelt hvor lang prosessen er fra første dialog med ny tjenesteeier til ny tjeneste er i produksjon.

## Den første kontakten

Ta kontakt med [idporten@difi.no](mailto:idporten@difi.no) med informasjon om prosjekt, kontaktpersoner og tidsplaner.

### Kontaktperson

Tjenesteeiere og tjenesteleverandører må oppgi navn og telefonnummer til en kontaktperson som er representant for integrering mot føderasjonen. Om denne personen byttes ut, for eksempel på grunn av bytte av jobb, er det deres ansvar å oppdatere Difi med korrekt kontaktinformasjon. Det henvises ellers til [samarbeidsportalen] for mer informasjon.

## Planlegging

Følgende punkter bør være en del av planleggingen:

* Tidsplan
* Produksjonsplan
* Forventninger omkring volum og bruk av tjeneste
* Påvirkning på brukerstøtte

Omfanget på planleggingsarbeidet er svært varierende og er påvirket av omfanget av tjenesten. Planleggingen gjøres i samarbeid med Difi.

## Inngå samarbeidsavtale

Difi vil sende over samarbeidsavtale for signering om dette ikke er gjort ved et tidligere tidspunkt. Samarbeidsavtalen må være signert før produksjonsseting.

## Etablere integrasjon i verifikasjonstest

Føderering i verifikasjonsmiljøet utføres på samme måte som i produksjon

Se hvilken informasjon som må oversendes Difi for å etablere integrasjonen med ID-porten i kapitel: 4.7. Se ellers kapitel 5 for mer informasjon om grensesnittet.

## Utføre verifikasjonstest

Difi krever at tjenester som skal beskyttes av ID-porten må gå gjennom et verifikasjonsløp før tjenesten kan produksjonssettes. Det er derfor nødvendig at tjenesteleverandør fødererer en testbasert versjon av sin tjeneste med et testmiljø hos Difi som blir referert til som verifikasjonsmiljøet. Her skal det kun benyttes fiktive data, og ikke reelle brukere.

Når både ID-porten og tjenesteleverandør er korrekt konfigurert kan fødereringen testes ved å prøve og aksessere tjenesten med en nettleser. Dette bør videresende brukeren via nettleseren til ID-porten sine websider, hvor brukeren blir spurt om å logge seg inn med et innloggingsalternativ som oppfyller minimumskravene til sikkerhet for den spesifikke eksponerte tjenesten.

DIFI har etablert en rutine for verifisering og godkjenning av integrasjon mot ID-porten. Denne finner du på Samarbeidsportalen på [https://samarbeid.difi.no](https://samarbeidsportalen.difi.no)

## Produksjonssetting

Før en produksjonssetting må samarbeidsavtalen være signert.

Før produksjonssetting må metadata filer og sertifikater være utvekslet og en detaljertplan for produksjonssettingen må være levert Difi.

Se hvilken informasjon som må oversendes Difi for å etablere integrasjonen med ID-porten i kapitel: 4.7

## Teknisk informasjon om tjenesteeier

I dette kapitelet oppsummeres det hvilken teknisk informasjon som må leveres til Difi i forbindelse med en integrasjon mot ID-porten.

All informasjon sendes på e-post til [idporten@difi.no](mailto:idporten@difi.no) .

### Informasjon om SAML2 integrasjon

Informasjon om hub-en og nodene utveksles i form av XML-filer med metadata i henhold til SAML2 standarden. Dette er en toveis kommunikasjon, så tjenesteleverandør må konfigurere sin egen programvare med xml-fil fra ID-porten, og sende sin egen konfigurasjonsfil til ID-porten.

Disse filene inneholder alle detaljene om lokasjonen for SAML2 endepunktene, og hvilke bindinger som er tilgjengelig. Et eksempel på en slik metadata-fil finner du i Vedlegg 3: Eksempel på metadatafil

Påse at følgende parametere er satt til *TRUE*:

|  |  |
| --- | --- |
| **Attributt og verdi** | **Beskrivelse** |
| AuthnRequestsSigned="true" | Dette vil si at tjenesteleverandør vil signere sine autentiseringsforspørsler. Signering av ArtifactResolve-forespørsel og SingleLogout må også håndteres av tjenesteleverandør. |
| WantAssertionsSigned="true" | Dette vil si at tjenesteleverandør krever å få Assertion signert. Kryptering vil bli håndtert av ID-porten. |

Filene anbefales navngitt som følger: *[EntityID]\_[Meta].xml*. EntityID er et attributt i rot-elementet ”EntityDescriptor”, og brukes til å identifisere tjenesten som XML filen beskriver.

### Annen informasjon

Under er et eksempel på hvilken informasjon som trengs i tillegg til informasjonen i SAML2 integrasjonen:

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Eksempel verdi** | **Beskrivelse** |
| ENTITY\_ID | eksempel\_101 | Dette feltet må være lik entityID i metadata-filen. |
| NAME | Norsk data og eksempelforening | Dette blir brukt av ID-porten under innlogging og beskriver tjenesteeier til innbyggeren i ulike sammenhenger. |
| URL | http://www.eksempel.no/ | Dette er URL til tjenesteleverandør som benyttes for å rute innbyggeren tilbake til tjenesteleverandør ved avbryting av innlogging eller feilsituasjoner. |
| REFERRING\_SP | Eksempel\_202 | Dette parameter blir kun brukt ved bruk av: onBehalfOf, se kapitel: 3.4 |
| DIGITALCONTACTINFO\_NAME | NorskDataForeningProd | Dette parametere blir kun brukt for tjenesteeiere som har tatt i bruk Digitalt kontaktregister.  Navnet er det unike navnet som tjenesteeier bruker for oppslag mot Digitalt kontaktregister sitt webservice |

Dette gjelder per integrasjon man har med ID-porten, så om man har flere integrasjoner kan disse ha ulike verdier.

### logo format

Logoen må oppfylle følgende krav:

|  |  |
| --- | --- |
| **Egenskap** | **Verdi** |
| **Filformat** | .png, .jpg eller gif. |
| **Størrelse** | maksimal høgde 90 pixel og en bredde som ikke bør overskride 135 pixel |
| **Farge** | Bakgrunnsfargen på ID-porten er ***#f3f4f4***, så logoen bør enten ha denne bakgrunnsfargen eller eventuelt ha transparent bakgrunn. |

### IP-adresser

For de tjenesteleverandører som velger å bruker SLO over SOAP må det oppgis IP-adressen(e) til servere som ID-porten skal kontakte direkte, via SAML2 SOAP-bindingen. Dette gjelder både for verifikasjonsmiljøet (test) og produksjonsmiljøet.

# Detaljertbeskrivelse av teknisk løsning

## Logging

ID-porten oppbevarer som standard alle logger i 12+1 måned. Logginformasjon om når sluttbruker inngikk samtykke er eneste informasjon i ID-porten som lagres lengre, i 10 år.

Det anbefales at tjenesteleverandør logger følgende informasjon om forsøk på autentisering:

* Dato og tidspunkt
* Hvilken handling som ble forsøkt
* Resultatet av handlingen
* Brukerens IP adresse
* SessionIndex
* Personnummer.

SessionIndex er en identifikator som identifiserer bruker-sesjonen på tvers av føderasjonen. ID-porten logger mer detaljert informasjon om hver brukersesjon enn det som er vår anbefaling til tjenesteleverandør, og tjenesteeier kan be om tilgang til denne med referanse til SessionIndex. Et eksempel på en SessionIndex er “*s295ce0f891244bf4a68e468368aaa923ead5f4301*”.

Tjenesteeier sitt konkrete behov for logging må vurderes av den enkelte tjenesteeier.

## Sesjonshåndtering

ID-porten sender ikke en forespørsel om utlogging til tjenesteleverandør når en sesjon timer ut pga total lengde eller inaktivitet. Forespørsel om utlogging sendes bare når en bruker foretar en eksplisitt utlogging (ved å klikke på logout-knappen hos en tjeneste innenfor Circle of Trust). En slik forespørsel om utlogging fra ID-porten **må** resultere i en utlogging fra tjenesteeier, ellers vil Single Logout-mekanismen bli kompromittert.

### Levetid for sesjoner.

I føderasjon skal medlemmene konfigurere systemene, slik at sesjoner utløper ved inaktivitet etter høyst **30 minutter**

I ID-porten måles maksimum sesjonstid for en brukers sesjon og denne settes til **120 minutter**.

Det er valgfritt om timeout perioden nullstilles hver gang brukerens nettleser forespør en av tjenesteleverandør sin tjeneste, eller om den er uavhengig av brukeraktivitet (fast timeout periode).

Etter timeout hos en tjenesteleverandør skal brukerens nettleser ved neste http-forespørsel sendes over til ID-porten med en autentiseringsforespørsel (SAML2 <AuthnRequest>).

Det må bemerkes at timeout hos en tjenesteleverandør ikke nødvendigvis medfører at brukeren blir tvunget til at logge på ID-porten. Hvis brukeren har en aktiv sesjon hos ID-porten, kan denne svare på forespørselen fra tjenesteleverandør uten brukerdialog (dvs. foreta single sign-on). Brukeren vil dermed ikke oppdage at sesjonen blir fornyet (bortsett fra at hans nettleser muligens ”blinker” et kort øyeblikk).

Hvis en tjenesteleverandør av sikkerhetsmessige grunner vil sikre seg at brukeren blir tvunget til aktiv pålogging i ID-porten løsningen, kan man sette parameteren *ForceAuthn=true* i kallet til ID-porten, ref kapitel 3.2.2.

## Caching

Iht. Oasis sine anbefalinger er det ønskelig å holde levetiden for en SAML2 response (TTL) så lav som mulig. Dette for å hindre angrep av typen ”Man in the middle” (MITM), der en angriper kan stjele sesjonsdata og dermed sesjonen til en legitim bruker. Det anbefales derfor at tjenesteleverandør sjekker at et svar på en autentiseringsforespørsel mot ID-porten ikke er eldre enn 60 sekunder (målt i tid fra tidspunkt forespørselen ble sendt). Tilsvarende vil ID-porten selv sjekke at dette er oppfylt ved uthenting av assertion via artifact resolution profil over bak-kanal (da i forhold til tid opprinnelig AuthnRequest ble mottatt). Det er viktig at det implementeres støtte for en konfigurerbar verdi som kan angi levetiden for en artifact. Konfigurerbar slik at man kan justere tiden ettersom nye krav til løsningen medfører endrede behov knyttet til denne verdien (Det er naturlig å tenke at sikkerhetskrav kan tvinge frem lavere verdier, mens hensyn til brukervennlighet vil tvinge frem økte verdier). Disse hensyn må balanseres i dette valget.

HTTP Proxy servere og agenter må unnlate å cache SAML2 meldinger. OASIS foreslår følgende retningslinjer:

Ved bruk av HTTP 1.1 (RFC2616) bør forespørrende part

* Inkludere et Cache-Control header felt satt til ”no-cache, no-store”.
* Inkludere et Pragma header felt satt til ”no-cache”

Ved bruk av HTTP 1.1 bør respondenter:

* Inkludere et Cache-Control header felt satt til ”no-cache, no-store, must-revalidate, private”.
* Inkludere et Pragma header felt satt til ”no-cache”
* IKKE inkludere Validator-felter som Last-Modified eller ETag header.

I SAML2 sammenheng er forespørrende part og respondenter de entiteter som sender og mottar SAML2 meldinger.

Leverandører av programvare som overholder SAML2 standarden skal også overholde disse kravene.

## Tidssynkronisering

Bekreftelse på at en bruker er autentisert sendes fra ID-porten til tjenesteleverandør i form av en SAML2-assertion. En assertion inneholder tidsstempel som angir hvor lenge den er gyldig. Det er derfor viktig at alle servere som kommuniserer via SAML2 har synkroniserte klokker. ID-porten bruker NTP (”network time protocol”) for synkronisering, tidskilden er GPS-basert. Det er videre viktig at alle servere i CoT er justert korrekt for tidssone og sommertid. (CET / CEST i Norge).

For mer informasjon <http://no.wikipedia.org/wiki/Network_Time_Protocol>

Tjenesteleverandør velger selv tidskilde.

## Tegnsett

Alle SAML2 kommunikasjon er basert på utveksling av xml baserte meldinger. All SAML2 kommunikasjon krever derfor UTF-8 tegnsett.

## Meldingsformat

For HTTP Redirect bindingen må alle meldinger basert på SAML2 protokollen kodes med base64.

# Sikkerhet

Dette kapitelet beskriver krav til sertifikater, nøkler og algoritmer i forbindelse med ID-porten.

## Verifisering av informasjon fra ID-porten

Tjenesteeier er selv ansvarlig for å verifisere all informasjon mottatt fra ID-porten. Dette innebærer f.eks. at tjenesteeier skal verifisere at ID-porten har autentisert sluttbruker på ønsket nivå etter at autentiseringen er gjennomført.

## Nøkkelbehov

I dette kapitel identifiseres de nøkler som det er behov for i løsningen.

### WEB Browser SSO profil med artifact resolution protokoll.

Forklaring:

1. Tjenesteleverandør bruker privat nøkkel til signering av AuthnRequest. ID-porten verifiserer signeringen ved hjelp av tjenesteleverandørs tilhørende sertifikat.
2. ID-porten bruker privat nøkkel til signering av assertion i Response. Tjenesteleverandør verifiserer signaturen ved hjelp av ID-portens tilhørende sertifikat.
3. Ved artifact protokoll hentes assertion over SSL/TLS beskyttet bak-kanal som snakker SOAP direkte mellom den enkelte tjenesteleverandør og ID-porten. Tjenesteleverandør skal signere ArtifactResolve med sin private nøkkel. ID-porten skal med sin private nøkkel signere assertion i svaret som sendes over bak-kanalen. Det er også et krav om at ID-porten krypterer assertion, noe som gjøres med tjenesteleverandør sin offentlige nøkkel, hentet fra tjenesteleverandør’s sertifikat som enten kan utveksles på forhånd som metadata eller følge med tjenesteleverandør’s signerte forespørsel.

### Single Logout

Forklaring:

1. Tjenesteleverandør sender LogoutRequest til ID-porten via frontkanal (HTTP redirect via User agent). Denne skal være signert med SP-s private signeringsnøkkel.
2. ID-porten sender LogoutRequest til alle tjenesteleverandører som denne bruker er pålogget. Disse meldingene signeres alle med ID-porten-s private signerings nøkkel.
3. Alle tjenesteleverandører svarer på LogoutRequest med en LogoutResponse som signeres av den enkelte tjenesteleverandør’s private signeringsnøkkel.
4. ID-porten svarer på initial LogoutRequest, med en LogoutResponse signert med ID-porten-s private signeringsnøkkel.

.

Ut fra dette kan følgende nøkkelbehov oppsummeres:

### ID-porten

Av egne nøkler trenger denne.

* Et nøkkelpar for signering av meldinger.
* Et nøkkelpar for autentisering og etablering av SSL/TLS.

Videre må tjenesteleverandør holde følgende nøkler for den enkelte tjenesteeier.

* En offentlig nøkkel for validering av signatur gjort av SP.
* En offentlig nøkkel for kryptering av meldinger til den enkelte SP.

Dette kan være en og samme nøkkel til alt bruk, men ID-porten støtter at dette kan være forskjellige nøkler.

### Tjenesteeier

Alle sertifikat brukt i føderingen kan være utstedt til tjenesteeier. I dette dokumentet står det beskrevet at sertifikat og nøkler tilhører tjenesteleverandør, men dette er ikke et krav. Sertifikat/nøklene kan og i flere tilfeller bør være utstedt til tjenesteeier og administrert av tjenesteleverandør.

Det er tjenesteeier sitt valg om sertifikatene skal være utstedt til tjenesteleverandør.

## Meldingsbeskyttelse

Meldingsinnhold krypteres og signeres ihht [XMLSig] og [XMLEnc]. Kun følgende algoritmer og nøkkellengder er tillatt

* Kryptering skal skje med AES med minimum 128 bits nøkler.
* Signeringsalgoritmer skal være SHA1with RSA med minimum 1024 bit modulo.
* Lengre nøkler er tillatt.

## Transportbeskyttelse

*<AuthnRequest>, <SingleLogoutRequest>* og *<SingleLogoutResponse>* meldinger SKAL bruke HTTPS over SSL (v3.0 eller høyere) eller TLS (v1.0 eller høyere) for å etablere en sikker kontekst mellom SP og brukerens nettleser, men tidligere versjoner av SSL kan tillates grunnet sterk bruk av meldingssikring.

Bak-kanal mellom SP og ID-porten SKAL etableres vha HTTPS over SSL (v3.0 eller høyere) eller TLS (v1.0 eller høyere).

## Sertifikatkrav

Det kreves at tjenesteleverandør benytter nøkler utstedt som virksomhetssertifikater iht. [kravspesifikasjon PKI], og at sertifikatutstederen er selvdeklarert for dette hos Post- og teletilsynet.

Det er viktig at tjenesteleverandør konfigurerer systemet slik at bare sertifikater tillatt av ID-porten føderasjonen benyttes.

Videre må det eksplisitt sjekkes at bare de virksomhetssertifikater som er utvekslet som en del av metadatautveksling er i bruk i føderasjonen.

Programvaren for SAML2 føderering må konfigureres slik at den godtar ID-porten sertifikatene. ID-portens serversertifikat for SSL-kommunikasjon mellom tjenesteleverandør server og ID-portens server ved SAML2 SOAP-kommunikasjon er utstedt av DigiCert.

SAML2 HTTP Artifact og SAML2 SOAP bindingene må sikres med SSL både for SSO og SLO profilene. Det samme gjelder alle andre sider innenfor den sikre løsningen. Alle endepunkter hos tjenesteleverandør må derfor ha installert sertifikater på tjenersiden.

### Bestilling av virksomhetssertifikat

Merk at sertifikatutstedere av virksomhetssertifikat har noe bestillingstid, tjenesteleverandører oppfordres til å bestille sertifikat i god tid.

### Bruksområdet

Sertifikatene brukt av tjenesteleverandør kan ikke ha bare bruksområdet: non repudiation (40) (ikke avinsing (40)).

Sertifikat med følgende bruksområdet er testet og fungerer i ID-porten.

|  |  |
| --- | --- |
| **Sertifikat leverandør** | **Bruksområdet** |
| **Commfides** | Digital signatur, Ikke-avvisning, Nøkkelchiffrering, Datachiffrering, Nøkkeloverensstemmelse (f8) |
| **Buypass** | Digital signatur, Nøkkelchiffrering, Datachiffrering (b0) |

## Håndtering av nøkler

Det er sentralt for sikkerheten i løsningen at tjenesteleverandør planlegger og designer prosedyrer for god nøkkelhåndtering (Key management) for private nøkler. Hvis en privat nøkkel kompromitteres, kan en angriper utgi seg for å være tjenesteleverandør i dialogen med ID-porten og dekryptere person data sendt fra ID-porten. Slike sikkerhetsbrudd vil formodentlig i særlig grad ramme tilliten til tjenesteleverandør, men kan også tenkes å svekke tilliten til hele føderasjonen.

Følgende punkter er det viktig at man tenker igjennom i forbindelse med nøkkelhåndtering:

* Hvor oppbevares private nøkler, og hvordan sikres adgang til dem? For optimal beskyttelse kan en nøkkel oppbevares i kryptografisk hardware (HSM – hardware security module), men ofte benyttes krypterte filer som et billig, men mindre sikkert alternativ.
* Hvordan håndteres backup av nøkler og hvordan gjenetableres disse ved behov?
* Hvilket personell har tilgang til servere med private nøkler, og hvem har eventuelt tilgang til passord som kan benyttes til å dekryptere nøklene slik at de opptrer i klartekst ? Kan enkeltpersoner skaffe seg adgang til private nøkler? Ligger passord for tilgang til nøkkellager ubeskyttet i konfigurasjonsfiler?
* Hvordan håndteres fornyelse av nøkler når tilhørende sertifikater utløper? Hvis en tjenesteleverandør ikke fornyer nøkler/sertifikater innen de utløper, kan tjenester for tjenesteeier plutselig slutte å virke.
* Hva er prosedyren om en privat nøkkel kompromitteres, eller om det er mistanke om at så har skjedd?
* Hvordan loggføres nøkkelhåndteringsprosessen hos tjenesteleverandør?

En tjenesteleverandør bør analysere disse problemstillingene nøye, og utarbeide passende driftsprosedyrer som implementerer organisasjonens IT sikkerhetspolitikk.

Både [kravspesifikasjon PKI] og sertifikatutsteders policy kan gi krav som må etterleves. Krav til slike prosedyrer for håndtering av nøkler stilles også til IdP delen av løsningen, som i dette tilfellet er ID-porten.

# Vedlegg 1: Detaljert beskrivelse av støttede SAML2 profiler

SAML2 profilene som her presenteres er med utgangspunkt i eGov versjon 1.5.

## SAML2 Profiler

Følgende profiler støttes:

* WEB SSO Profile med HTTP Redirect (request) og artifact resolution over SOAP binding (reply).
* Single Logout Profile med HTTP Redirect eller SOAP binding.

Følgende “modes” vil være støttet:

* ID-porten initiert SSO.
* SP initiert SSO.
* ID-porten initiert SLO
* SP initiert SLO.

## SAML2 bindings

Følgende valg støttes for SAML2 bindings:

* SSO request binding: HTTP Redirect.
* SSO response binding: Artifact over HTTP Redirect
* SSO response binding: Artifact resolution over SOAP.
* SLO over SOAP
* SLO over HTTP Redirect

## Konfigurering av signering og kryptering

Følgende elementer skal signeres:

* SAML2 assertions.
* *<AuthRequest>*, men ikke *<Response>*
* *<ArtifactResolve>* forespørselen.
* Single Logout request og response.

Og ID-porten vil selv signere:

* Artifact response
  + som inneholder ett kryptert Assertion-elementet.
* SingleLogout request
* SingleLogout response

## IdP Discovery

Ikke støttet i føderasjonen. ID-porten er eneste IDP.

## WEB Browser SSO

Følgende regelsett gjelder for SSO profilen i ID-porten:

* SSO profil i [SAMLProf] MÅ være støttet av både tjenesteleverandør og ID-porten. Både IdP og SP initiert metode er støttet i denne versjon av ID-porten.

### Authentication Request

* MÅ kommuniseres vha “HTTP Redirect binding”.
* *ForceAuthn* støttes av ID-porten. Det KAN bli brukt til å få ID-porten til å tvinge brukeren til å reautentisere seg.
* *<AuthnRequest>* MÅ signeres.
* *<NameIDPolicy>* støttes av ID-porten, både formatene ”*persistent*” og ”*transient*”.
* *<RequestedAuthnContext>* MÅ støttes. ID-porten gjenkjenner sammenligningsfelter og evaluere de forespurte kontekst klassene.
* *<RequestedAuthnContext>* BØR inneholde attributtet *Comparison* og *Comparison* SKAL være satt til *minimum*. ID-porten vil tolke alle forespørsler til *minimum* og at *AuthnContextClassRef* er urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified om elementet ikke er inkludert i forespørselen.
* *<AuthnRequest>* KAN inneholde *<samlp:Extensions>*

Følgende *<samlp:Extensions>* støttes av ID-porten:

* *<idpe:OnBehalfOf>* Unik identifikator av tjenesteeier. MÅ kun inneholde følgende tegn: *A-Z a-z 0-9 - \_* (se vedlegg 1 for xsd)

### Overstyring av NameID:

Tjenesteleverandør kan styre format på NameID ved bruk av NameIDPolicy i AuthnRequest meldingen. Dette betyr at tjenesteleverandør kan overstyre en tidligere mottatt persistent identifikator ved å oppgi ønske om transient identifikator i autentiseringsforespørselen.

### IdP Authentication Response

* MÅ kommuniseres ved hjelp av ”*SOAP Artifact binding*”.
* “Assertion” MÅ krypteres og signeres.

### Assertion

* Assertion MÅ krypteres og signeres.
* MÅ ha en *<AuthnStatement>* verdi. ”SessionIndex” parameter MÅ være tilstede, og “SessionNotOnOrAfter” MÅ IKKE være tilstede.
* MÅ støtte *<AttributeStatement>* og KAN inneholde opp til en *<AttributeStatement>*.
* MÅ støtte “NameFormat” av *<Attribute>* verdier lik “basic”, “uri” og “unspecified”.
* *<AttributeStatement>* MÅ bruke *<Attribute>* og MÅ IKKE bruke *<EncryptedAttribute>*.
* *<SubjectConfirmationData>* attributten NotOnOrAfter MÅ støttes.
* *<Conditions>* attributtene NotBefore og NotOnOrAfter MÅ støttes.
* *<Conditions>* elementet *<AudienceRestriction>* MÅ støttes.

## Artifact resolution protocol

* MÅ kommuniseres over SOAP beskyttet av SSL/TLS.
* *<ArtifactResolve>* MÅ signeres.
* *<ArtifactResolve>* MÅ inneholde en *<Artifact>* verdi.
* *<ArtifactResponse>* MÅ inneholde en *<Assertion>* som oppfyller kravene til *<Assertion>* over.
* *<Assertion>* i *<ArtifactResponse>* MÅ signeres og krypteres.
* InResponseTo verdi i *<Assertion>* MÅ være lik verdi i ID felt i *<ArtifactResolve>* forespørselen.
* *<ArtifactResponse>* KAN inneholde *<Status>* og må inneholde *<Status>* med inntil to *<StatusCode>* i feilsituasjoner.

### ID-porten svarer med <ArtifactResponse>

I assertion som sendes tilbake til tjenesteleverandør legger ID-porten med informasjon om autentisert bruker. Dette gjøres i NameID feltet knyttet til Subject i Assertion. Hvilken verdi som legges her avhenger av Format på NameID feltet.

* Ved *transient* format overføres en tilfeldig identifikator som er unik for denne brukeren på denne sesjonen mot denne tjenesteleverandøren. Identifikatoren kan benyttes ved oppslag mot ID-porten for denne sesjon for gitt tjenesteleverandør, men vil ikke lenger eksistere når sesjonen opphører.
* Ved *persistent* format overføres en tilfeldig identifikator som er unik for denne brukeren mot denne tjenesteleverandøren på tvers av alle sesjoner brukeren har mot tjenesteleverandør. Identifikatoren opprettes ved første gangs pålogging for en bruker mot en gitt tjenesteleverandør, og ID-porten tar vare på denne identifikatoren for denne bruker mot gitt tjenesteleverandør for fremtidig bruk.

Om forespørselen er behandlet vellykket vil responsen oppfylle følgende:

* Issuer elementet kan utelates, men om det inkluderes vil det inneholde en unik angivelse av ID-porten som IdP. Format attributtet MÅ enten utelates eller ha verdien *urn:oasis:names:tc:SAML:2.0:nameid-format:entity*
* En vellykket *<Response>* vil inneholde nøyaktig en *<Assertion>* med nøyaktig ett *<AuthnStatement>* element. Hvert assertions *<Issuer>* element vil inneholde en unik identifikator som angir ID-porten. Format attributtet vil enten utelates eller ha verdien *urn:oasis:names:tc:SAML:2.0:nameid-format:entity.*
* ID-porten signere og kryptere Assertion.
* Ved feilmeldinger fra ID-porten vil den IKKE returnere en assertion.
* Om ID-porten mottar en forespørsel fra en tjenesteleverandør som den ikke har inngått avtale med, vil forespørselen avvises med en beskrivende responskode.

Metadata benyttes til å identifisere hvilke tjenestelevernadør avtaler er inngått med.

### Status i ArtifactResponse.

ArtifactResponse KAN inneholde en *<Status>* angivelse og vil inneholde Status i de tilfeller håndteringen av forespørselen feiler på ID-porten. *<Status>* vil inneholde inntil to *<StatusCode>* som angir en overordnet og en underordnet feilkode iht. eksempelet under:

<samlp:Status>

<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">

<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:AuthnFailed" />

</samlp:StatusCode>

<samlp:StatusMessage>Authentication failed</samlp:StatusMessage>

<samlp:Status/>

Som det vises av eksempelet KAN ID-porten angi en *<StatusMessage>* som er en tekstmessig indikasjon av feilsituasjonen. Dette er ikke er krav.

Følgende overordnede statuskoder kan benyttes i fra ID-porten.

* **urn:oasis:names:tc:SAML:2.0:status:Success** – Forespørselen var vellykket.
* **urn:oasis:names:tc:SAML:2.0:status:Requester** – Forespørselen ble ikke behandlet grunnet en feil hos forespørrende part (SP).
* **urn:oasis:names:tc:SAML:2.0:status:Responder** – Forespørselen ble ikke behandlet grunnet en feil i ID-porten.
* urn**:oasis:names:tc:SAML:2.0:status:VersionMismatch** – Forespørselen ble ikke behandlet grunnet feil SAML versjon i forespørselen.

Følgende underordnede koder kan benyttes til ytterligere spesifisering av feilsituasjonen.

* **urn:oasis:names:tc:SAML:2.0:status:AuthnFailed** – ID-porten var ikke i stand til å gjennomføre en vellykket autentisering av brukeren.
* **urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue** – Ugyldig innhold ble oppdaget i <saml:Attribute> eller <saml:AttributeValue> elementet.
* **urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy** – Ønsket policy er ikke støttet i ID-porten.
* **urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext** – Angitte autentiseringskontekst kan ikke oppfylles i ID-porten. Kan benyttes til å indikere ulovlig forespurt sikkerhetsnivå.
* **urn:oasis:names:tc:SAML:2.0:status:NoAvailableIDP** – Skal ikke være i bruk i ID-porten som er eneste idp i ID-porten COT.
* **urn:oasis:names:tc:SAML:2.0:status:NoPassive** – ID-porten tillater ikke passiv pålogging. Denne verdien returneres alltid om dette forespørres.
* **urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP** - Kan benyttes til å indikere at en ikke finner en eID leverandør som oppfyller ønsket sikkerhetsnivå, men skal i utgangspunktet ikke være aktuell for bruk i ID-porten 2.0.
* **urn:oasis:names:tc:SAML:2.0:status:PartialLogout** – Benyttes til å indikere at single logout ikke var vellykket (alle sesjoner ble ikke terminert).
* **urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded** – Ikke støttet i ID-porten 2.0.
* **urn:oasis:names:tc:SAML:2.0:status:RequestDenied** – Benyttes i de tilfeller der ID-porten av en eller annen grunn velger å la være å behandle forespørselen. Kan f.eks benyttes ved antatt DOS angrep.
* **urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported** – ID-porten støtter ikke/forstår ikke ønsket forespørsel.
* **urn:oasis:names:tc:SAML:2.0:status:RequestVersionDeprecated** – ID-porten kan ikke håndtere forespørsler med angitt protokoll versjon.
* **urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooHigh** - ID-porten kan ikke håndtere forespørsler med angitt protokoll versjon..
* **urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooLow** - ID-porten kan ikke håndtere forespørsler med angitt protokoll versjon.
* **urn:oasis:names:tc:SAML:2.0:status:ResourceNotRecognized** – Ressursen angitt I forespørselen er ukjent eller ugyldig.
* **urn:oasis:names:tc:SAML:2.0:status:TooManyResponses** – Responsen ville inneholdt for mange elementer til at ID-porten kan håndtere det.
* **urn:oasis:names:tc:SAML:2.0:status:UnknownAttrProfile** – Ikke I bruk i ID-porten 2.0.
* **urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal** – Brukeren er ikke gjenkjent av ID-porten. Kan komme av at bruker ikke har godtatt bruksvilkår for ID-porten (samtykke), eller at dette er en utenlandsk borger.
* **urn:oasis:names:tc:SAML:2.0:status:UnsupportedBinding** – ID-porten støtter ikke forespurt SAML binding.

## Single Logout

SAML2 støtter konseptet Single Logout og beskriver både en Single Logout protokoll i [SAMLCore] og en Single Logout profile i [SAMLProf]. Disse gir IDP og SP mulighet til å terminere multiple sesjoner ved å sende *<LogoutRequest>* og *<LogoutResponse>* meldinger. På denne måten kan brukeren logge ut fra alle sesjoner som springer ut fra en IDP i noe som for brukeren kan virke som en operasjon. Brukeren kan initiere prosessen både hos en ønsket SP eller direkte i IdP’en. Figuren under viser bildet i forbindelse med logout initiert hos en SP. Bildet blir noe enklere om dette initieres via IdP’en.

Merk at bildet kan se noe annerledes ut avhengig av valg av SAML2-binding for bruk ved Single Logout. Ved bruk av Redirect binding vil alle meldinger flyte via User Agent. Dette bildet viser bruken av bak-kanal mellom den enkelte SP og IdP, dvs bruk av SOAP binding. Begge deler er støttet i ID-porten.

OASIS skiller klart på denne første meldingen og de etterfølgende meldingene. Den første er ønskelig foretatt over en frontkanal, og ID-porten krever at dette er et HTTP redirect kall. Grunnen til dette er at det gir ID-porten mulighet til å samle inn data knyttet til brukerens sesjon, slik som nettleser Cookies.

Med andre ord gjelder følgende krav for Single Logout i ID-porten

* HTTP redirect binding MÅ brukes for første kall fra SP til ID-porten
* Enten SOAP binding eller HTTP redirect binding MÅ benyttes for etterfølgende forespørsler/svar
* Alle SP og ID-porten MÅ støtte HTTP redirect binding.
* Støtte for SOAP binding hos SP er valgfritt.
* Alle forespørsler og svar skal være være signert.
* Kommunikasjon over bak-kanal (SOAP) skal sikres vha klient autentisert (en veis) SSL/TLS

SP må håndtere *<LogoutRequest>* fra ID-porten for brukere som ikke lenger er innlogget, for eksempel fordi brukerens har logget ut fra denne ene tjenesten tidligere eller fordi levetiden på brukerens sesjon er utløpt.

* SP-initiert ”Single Logout” og IdP-initiert ”Single Logout” MÅ støttes.
* ”Single Logout” binding KAN være HTTP Redirect eller SOAP.
* *<LogoutRequest>* MÅ signeres.
* *<LogoutResponse>* MÅ signeres.
* SP MÅ tilby full SLO.

## Metadata

Valget av metadata informasjon er i stor grad et implementasjonsvalg. Men alle støttede

SP og IdP implementasjoner MÅ støtte korrekt bruk av metadata elementer, attributter og spesifikasjoner listet i denne seksjonen.

* SP og IdP BØR autentisere metadata.
* MÅ støtte root elementene *<EntityDescriptor>* eller *<EntitiesDescriptor>*.
* Attributt “validUntil” OG “cacheDuration” MÅ støttes.
* Sertifikater i metadata MÅ støttes.
* “Certificate revocation methods of Online Certificate Status Protocol” (OCSP), “Certificate Revocation List” (CRL), “CRL Distribution Point” (CDP) utvidelser MÅ støttes.

### <SPSSODescriptor>

* *<KeyDescriptor>* MÅ støttes.
* *<SingleLogOutService>* MÅ støttes.
* <AssertionConsumerService> MÅ støttes.
* “WantAssertionSigned” MÅ støttes.
* “AuthnRequestsSigned” MÅ støttes.

### <IDPSSODescriptor>

* *<KeyDescriptor>* MÅ støttes.
* ”WantAuthnRequestsSigned” MÅ støttes.
* *<SingleLogOutService>* MÅ støttes.
* *<SingleSignOnService>* MÅ støttes.
* *<ArtifactResolutionService>* MÅ støttes.

### SP godkjenner eller avviser forespørsel.

SP skal utføre de sjekker som er påkrevet iht. SAML2 profilen som benyttes. I tillegg må SP sjekke at autentiseringsnivå som returneres fra ID-porten er på et nivå som tjenesten krever. Ved godkjent validering av sesjonsinfo fra ID-porten opprettes en sesjon for brukeren mot tjenesten.

Forutsatt at SPs tilgangskontroll aksepterer tilgang fra denne autentiserte brukeren gis det så tilgang til ønsket tjeneste.

## Identity Provider Discovery Profile

Dette er ikke støttet i ID-porten.

## Attribute Query/Request Profile

Dette er ikke støttet i ID-porten.

# Vedlegg 2: SAML ekstension

ID-porten benytter seg av en ekstensjon (*<Extensions>*) i *<AuthnRequest>* forespørselen med et eget XML navnerom som beskrevet i SAML Core 2.0 spesifikasjon, kapittel 3.2.1 og 7.

Følgende skjema (XSD) er definert for ekstensjonen:

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" version="1.0"

targetNamespace="https://idporten.difi.no/idporten-extensions">

<xs:element name="IDPortenExtensions">

<xs:complexType>

<xs:sequence>

<xs:element name="OnBehalfOf" type="xs:string" minOccurs="0" />

</xs:sequence>

</xs:complexType>

</xs:element>

</xs:schema>

# Vedlegg 3: Eksempel på metadatafil

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"

entityID="idporten-sptest5.difi.local">

<SPSSODescriptor AuthnRequestsSigned="true"

ID="sad6ab0783dd890c52c2e11922642fc8046b67592"

WantAssertionsSigned="true"

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />

<Reference URI="#sad6ab0783dd890c52c2e11922642fc8046b67592">

<Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

<DigestValue>9MVtYkYRlpPer/Fs45xFAHpNMoY=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>

asRRK9ZXtGBPwuaivWWzTMluzpL7+2FQb57kKrk96kDtf5Ryoeib5dWCiGi8KI4r2dUvI+54R37W

79zqMwOzCXelb0fjzTJbxagCz4lGT8TjrBlWHaLdQOl8REzS+xHLIIwuI8iegvkAAZ3X+gq7m04K

yCgebOF+cVX0xnRo44g=</SignatureValue>

<KeyInfo>

<X509Data>

<X509Certificate>

</ds:X509Certificate>

</X509Data>

</KeyInfo>

</Signature>

<KeyDescriptor use="signing">

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:X509Data>

<ds:X509Certificate>

</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</KeyDescriptor>

<KeyDescriptor use="encryption">

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:X509Data>

<ds:X509Certificate> </ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">

<xenc:KeySize xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

128</xenc:KeySize>

</EncryptionMethod>

</KeyDescriptor>

<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"

Location="http://idporten-sptest5.difi.local:8080/opensso/SPSloRedirect/metaAlias/sp"

ResponseLocation="http://idporten-sptest5.difi.local:8080/opensso/SPSloRedirect/metaAlias/sp" />

<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="http://idporten-sptest5.difi.local:8080/opensso/SPSloSoap/metaAlias/sp" />

<NameIDFormat>

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>

<NameIDFormat>

urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>

<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"

Location="http://idporten-sptest5.difi.local:8080/opensso/Consumer/metaAlias/sp"

index="0" isDefault="true" />

</SPSSODescriptor>

</EntityDescriptor>

# Vedlegg 4: krav til Sluttbruker av ID-porten

Følgende krav settes til sluttbruker:

**Nettleser**

Følgende nettlesere blir testet av DIFI i forbindelse med nye versjoner av ID-porten:

|  |  |  |
| --- | --- | --- |
| **Nettleser** | **Versjon** | **Operativsystem** |
| **Internet Explorer** | Alle hoved versjoner siste 12 mnd | Windows |
| **Firefox** | Alle hoved versjoner siste 12 mnd | Windows |
| **Chrome** | Alle hoved versjoner siste 12 mnd | Windows/Mac |
| **Opera** | Alle hoved versjoner siste 12 mnd | Windows |
| **Safari** | Alle hoved versjoner siste 12 mnd | Mac |

NB! På Internet Explorer 6 under Windows kan skjønnhetsfeil tolereres, men nettstedet skal fungere.

**Javascript**

Javascript er brukt i deler av løsningen og er nødvendig for å gjennomføre innlogging på nivå 4.

**Java runtime**

Sluttbruker må ha java runtime installert for å gjennomføre innlogging på nivå 4. For detaljer omkring hvilke JRE versjoner som kreves vises det til den enkelte e-ID leverandør.