

Tilslutningsguide mot ID-porten 2.0

Integrasjonsbeskrivelse for ID-porten – Versjon 1.4

Version 1.5

Date: 13.10.2010

Forfatter: Difi

Even Mikalsen,
Arne Berner,
Erik Stedje,
Daniel Lerum

Historie

Forandringslogg

Versjon	Dato	Beskrivelse	Ansvarlig
1.2	02.06.10	Første versjon	Even Mikalsen
1.3	18.06.10	Etter språkvask og teknisk gjennomgang	Even Mikalsen
1.4	20.09.10	Gjennomgang etter tilpassninger av tekniske løsning, lagt på krav om signert metadata og fjerning av krav om 2veis SSL på bakkanal.	Arne Berner
1.5	13.10.10	Oppdatert formatering på dokumentet	Arne Berner

Distribusjon

Versjon	Dato	Distribuert til	Sent av

Innhold

Forandringslogg	2
Distribusjon	2
1. Innledning.....	6
1.1. Formål.....	6
1.2. Bakgrunn.....	6
1.3. Ordbok.....	6
1.4. Referanser	7
2. Modell	8
2.1. Protokoll	8
2.2. Innhold.....	8
2.2.1. SAML Profiler	8
2.2.2. SAML bindings	9
2.2.3. Konfigurering av signering og kryptering.....	9
3. Detaljert beskrivelse av støttede SAML profiler.	10
3.1. ”IdP Discovery”	10
3.2. WEB SSO	10
3.2.1. “SP Authentication Request”	10
3.2.2. “IdP Authentication Response”	10
3.2.3. Assertion	10
3.3. Artifact resolution protocol	10
3.4. Single Logout	11
3.5. Metadata.....	11
3.5.1. <SPSSODescriptor>	11
3.5.2. <IDPSSODescriptor>	11
3.6. WEB Browser SSO Profil.....	12
3.6.1. User Agent prøver å nå tjeneste.....	12
3.6.2. SP sender <AuthnRequest>.....	12
3.6.3. Bruk av RequestedAuthnContext for å definere opp minimum sikkerhetsnivå.	13
3.6.4. ID-porten autentiserer brukeren.....	13
3.6.5. ID-porten sender Response	14
3.6.6. Oppsett av bak-kanal.....	14
3.6.7. SP sender ArtifactResolve via bak-kanal.	14
3.6.8. ID-porten svarer med ArtifactResponse via bak-kanal.	14
3.6.9. Overføring av autentisert bruker.....	15
3.6.10. Status i ArtifactResponse.	15

3.6.11.	SP godkjenner eller avviser forespørsel.....	16
3.7.	Single Logout Profil	17
3.8.	Identity Provider Discovery Profile.....	18
3.9.	Attribute Query/Request Profile.....	18

1. Innledning

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

1.1. Formål

Målgruppen for dokumentet er offentlige tjenesteeiere som SSL/TLS skal benytte seg av ID-porten som fellesoffentlig fødererings og SSO-løsning.

De beskrevne aktiviteter skal lede frem til at det kan gjennomføres en integrasjonstest mot den fellesoffentlige brukerstyringsløsning. Dokumentet beskriver det sett av profiler for OASIS SAML 2.0 som støttes i ID-porten versjon 2.0.

ID-porten versjon 2.0 støtter flere eId'er, og vil avløse MinID 3.0 som kjører på ID-porten 1.0.

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

1.2. Bakgrunn

Føderering og SSO-løsninger i forløperne til ID-porten har vært noe vagt beskrevet, og dermed har en kunne benytte et veldig vidt spekter av SAML-profiler mot løsningene, dette inkluderer SAML-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 SAML 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 en SAML-profil for ID-porten er det blitt 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 det videre arbeidet for ID-porten er derfor gjort med utgangspunkt i disse profilene. Det er allikevel gjort en del valg som går på tvers av de valg som er gjort for OIOSAML.

1.3. 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 (browser). 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 SAML profil
PKI	Public Key Infrastructure.
SLO	Single Logout
SP	Service Provider – 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.

1.4. Referanser

[eGov]

HTTP://www.projectliberty.org/liberty/content/download/4711/32210/file/Liberty_Alliance_eGov_Pr ofile_1.5_Final.pdf

[kravspesifikasjon PKI] Versjon 2.0 av 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. <HTTP://www.oiosaml.info/>

[Policy] Policy guide for ID-porten, som beskriver ”policy” knyttet til ulike aspekter av sikker drifting av løsningen. Legges ut på samarbeidsportalen når den er ferdigstilt.

<http://digimaker.difi.no/samarbeid.aspx?m=53690>

[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 HTTP://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf

[Samarbeidsavtalen] Legges ut på samarbeidsportalen når den er ferdigstilt.

<http://digimaker.difi.no/samarbeid.aspx?m=53690>

[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. See <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. See <HTTP://www.oasis-open.org/committees/security/>.

[XMLEnc] Donald Eastlake et al. *XML Encryption Syntax and Processing*. World Wide Web Consortium Recommendation, December 2002. See <HTTP://www.w3.org/TR/xmlenc-core/>.

[XMLSig] Donald Eastlake et al. *XML-Signature Syntax and Processing*. World Wide Web Consortium Recommendation, February 2002. See <HTTP://www.w3.org/TR/xmlsig-core/>.

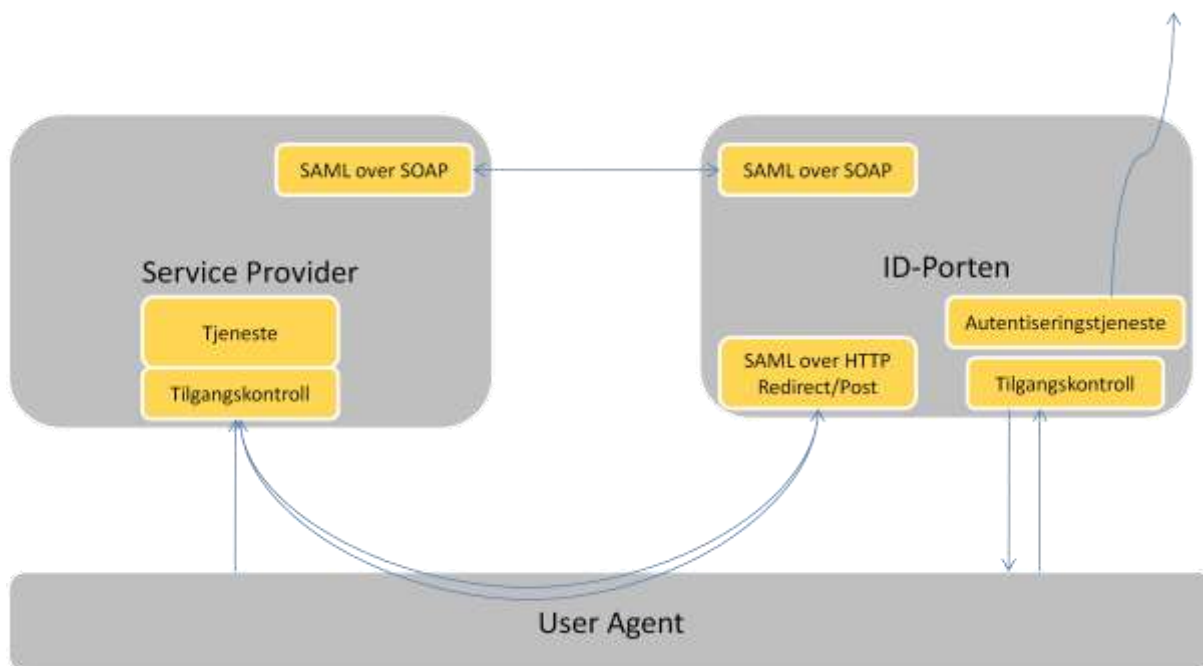
2. Modell

Her beskrives fødereringsmodellen som er valgt i ID-porten. Dette er en overordnet beskrivelse av modellen. For detaljer, se kapittel 3.

2.1. Protokoll

For føderering mot ID-porten benytter man SAML 2.0 protokollen. ID-porten støtter ikke tidligere versjoner av SAML protokollen eller andre føderingsprotokoller.

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



Figur 1: Protokoll-beskrivelse.

2.2. Innhold

Her gis en overordnet beskrivelse av de valg som gjøres rundt SAML-profiler og ”modes” for disse. Videre beskrives støttede bindings og hvilke krav som gjelder når det kommer til bruk av signering og kryptering. For detaljert beskrivelse av lovlige SAML-verdier, se neste kapittel.

2.2.1. SAML 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.

2.2.2. SAML bindings

Følgende valg støttes for SAML 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

2.2.3. Konfigurering av signering og kryptering

Følgende elementer skal signeres:

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

Assertion skal krypteres.

Metadata SKAL signeres for å forenkle utvekslingsprosessen. Se kap. 3 for detaljer.

3. Detaljert beskrivelse av støttede SAML profiler.

Merk følgende om dette kapitlet. SAML profilene som her presenteres er med utgangspunkt i eGov versjon 1.5.

3.1. "IdP Discovery"

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

3.2. WEB SSO

Følgende regelsett gjelder for SSO profilen i ID-porten:

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

3.2.1. "SP Authentication Request"

- MÅ kommuniseres vha "HTTP Redirect binding".
- *ForceAuthn* MÅ støttes. Det KAN bli brukt til å få ID-porten til å tvinge brukeren til å reautentisere seg.
- *<AuthnRequest>* MÅ signeres.
- *<NameIDPolicy>* MÅ støttes og MÅ STØTTE formatene "persistent" og "transient".
- *<RequestedAuthnContext>* MÅ støttes. ID-porten MÅ gjenkjenne sammenligningsfelter og evaluere de forespurte kontekst klassene.

3.2.2. "IdP Authentication Response"

- MÅ kommuniseres vha "SOAP Artifact binding".
- "Assertion" MÅ krypteres og signeres.

3.2.3. 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.

3.3. Artifact resolution protocol

- MÅ kommuniseres over SOAP beskyttet av SSL/TLS etablert vha to veis autentisering av endepunktene.

- `<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.

3.4. Single Logout

- 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.

3.5. 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.
- Signering av Metadata SKAL være støttet.
- MÅ støtte root elementene `<EntityDescriptor>` eller `<EntitiesDescriptor>`.
- `<Organization>` MÅ støttes.
- 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.

3.5.1. `<SPSSODescriptor>`

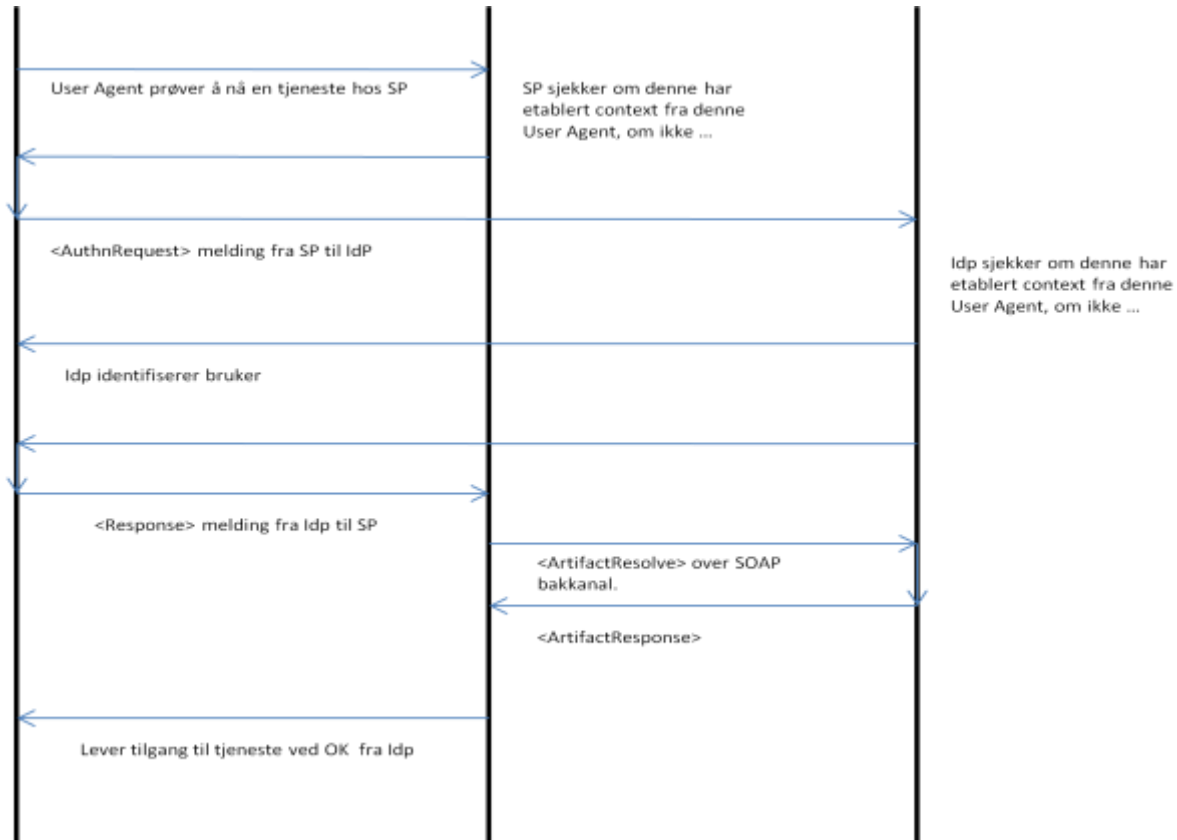
- `<KeyDescriptor>` MÅ støttes.
- `<SingleLogOutService>` MÅ støttes.
- `<AssertionConsumerService>` MÅ støttes.
- "WantAssertionSigned" MÅ støttes.
- "AuthnRequestsSigned" MÅ støttes.

3.5.2. `<IDPSSODescriptor>`

- `<KeyDescriptor>` MÅ støttes.
- "WantAuthnRequestsSigned" MÅ støttes.
- `<SingleLogOutService>` MÅ støttes.
- `<SingleSignOnService>` MÅ støttes.
- `<ArtifactResolutionService>` MÅ støttes.

3.6. WEB Browser SSO Profil

Her beskrives en ytterligere spesialisering av WEB Browser SSO profilen i [SAMLProf]. Følgende figur hentet fra [SAMLProf] illustrerer dette:



Figur 2 Steg ved standard SSO

I det følgende beskrives hvert steg i detalj.

3.6.1. User Agent prøver å nå tjeneste.

Denne profilen inneholder ingen restriksjoner på dette steget ettersom dette er styrt av HTTP protokollen.

Som beskrevet i SAML profilen KAN RelayState mekanismen benyttes av SP til å assosiere senere profil-utvekslinger med den originale forespørselen. Men av hensyn til brukerens anonymitet må denne parameteren ikke røpe noen detaljer rundt forespørselen.

3.6.2. SP sender <AuthnRequest>

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

Ingen kommunikasjon i produksjonsmiljøet skal finne sted mellom ID-porten og en SP før nødvendige avtaler er på plass og metadata utvekslet.

Denne profilen bruker HTTP redirect binding med DEFLATE koding i dette steget.

HTTP utvekslingen må skje over (en veis) SSL/TLS for å sikre konfidensialitet knyttet til meldingen.

I denne profilen MÅ forespørselen signeres, og signering (se [policy] for detaljer) må utføres vha SP's private nøkkel, hvis tilhørende sertifikat er utvekslet under utveksling av metadata. Signaturen plasseres i Signatur forespørsel strengen beskrevet for denne bindingen, og ikke i selve XML meldingen.

SP kan spesifisere hvilket autentiseringsnivå brukeren skal autentiseres på ved bruk av AuthnContext i forespørselen. Om autentiseringsnivå ikke er satt kan IdP la brukeren velge en eID på et hvilket som helst autentiseringsnivå.

Autentiseringsnivå for en tjeneste utveksles ikke som en del av metadata-utveksling, og vil derfor bare kommuniseres i autentiseringsforespørselen fra SP.

3.6.3. Bruk av RequestedAuthnContext for å definere opp minimum sikkerhetsnivå.

SP kan benytte RequestedAuthnContext til å angi ønske sikkerhetsnivå. Dette skjer på følgende måte:

- Comparison felt settes alltid lik minimum da SP kan angi laveste sikkerhetsnivå, men ikke tillates å spesifisere eksakt nivå.
- Ulike AuthnContextClassRef defineres til å tilhøre ulike sikkerhetsnivå, og ved å oppgi en spesiell slik klasse sier SP hvilket sikkerhetsnivå som er minimum. Tabellen under definerer opp sikkerhetsnivå for ulike klasser som er støttet i ID-porten.

nivå	AuthnContextClassRef
3	<u>urn:oasis:names:tc:SAML:2.0:ac:classes: Unspecified</u>
3	<u>urn:oasis:names:tc:SAML:2.0:ac:classes: PasswordProtectedTransport</u>
4	<u>urn:oasis:names:tc:SAML:2.0:ac:classes: SmartcardPKI</u>

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>
```

3.6.4. ID-porten autentiserer brukeren.

ID-porten sjekker om brukeren har en gyldig sesjon mot ID-porten. Hvis ikke, bes brukeren om å velge eID fra en meny av de eIDene som kan brukes på valgt sikkerhetsnivå, og ID-porten autentiserer brukeren autentiseres med valgt eID og den protokollen som brukes for denne eIDen.

Om brukeren allerede har en gyldig sesjon mot ID-porten MÅ brukeren reautentiseres dersom:

- SP krever reautentisering gjennom å sette ForceAuthn attributtet i forespørselen til "true". ID-porten MÅ adlyde en slik forespørsel.

- Brukeren er innlogget på et lavere sikkerhetsnivå enn den inneværende tjenesteforespørsel krever. I så tilfelle MÅ ID-porten foreta en reautentisering av brukeren med en eId som minimum er på korrekt sikkerhetsnivå.

3.6.5. ID-porten sender Response

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

Artifact returneres vha http redirect. Artifact legges i en parameter med navn SAMLart i URL'en.

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

Respons meldingen over frontkanal behøver ikke å være signert.

Ved feilmelding fra ID-porten MÅ denne IKKE returnere en assertion.

Om ID-porten mottar en forespørsel fra en SP som den ikke har inngått avtale med, skal forespørselen avvises med en beskrivende responskode. Responskoder fra ID-porten er beskrevet i detalj i kapittel 3.6.10.

3.6.6. Oppsett av bak-kanal.

Bak-kanal skal settes opp med SOAP over HTTPS. Det er SP som er ansvarlig for å sette opp bak-kanalen. *<ArtifactResolutionService>* i ID-porten's metadata skal benyttes som endepunkt for etablering av bak-kanal. Bak-kanal kan av ytelsesmessige hensyn bli gjenbrukt til senere sesjoner etter at den er etablert. Se for øvrig [policy] for ytterligere detaljer om etablering av bak-kanal og nøkkelhåndtering.

3.6.7. SP sender ArtifactResolve via bak-kanal.

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

3.6.8. ID-porten svarer med ArtifactResponse via bak-kanal.

Om forespørselen er behandlet vellykket MÅ responsen oppfylle følgende:

- Issuer elementet kan utelates, men om det inkluderes MÅ det inneholde en unik angivelse av ID-porten som IdP. Se [Policy] for ytterligere detaljer. Format attributtet MÅ enten utelates eller ha verdien urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- En vellykket *<Response>* MÅ inneholde nøyaktig en *<Assertion>* med nøyaktig ett *<AuthnStatement>* element. Hvert assertions *<Issuer>* element MÅ inneholde en unik identifikator (se [policy]) som angir ID-porten. Format attributtet MÅ enten utelates eller ha verdien urn:oasis:names:tc:SAML:2.0:nameid-format:entity. Om IsPassive attributtet var satt i *<AuthnRequest>*, så MÅ ID-porten returnere statuskode urn:oasis:names:tc:SAML:2.0:status:NoPassive
- ID-porten må signere og kryptere Assertion.
- Ved feilmeldinger fra Id-Porten MÅ denne IKKE returnere en assertion.
- Om Id-Porten mottar en forespørsel fra en SP som den ikke har inngått avtale med, skal forespørselen avvises med en beskrivende responskode. Responskoder fra ID-porten er beskrevet i detalj i kapittel 3.6.10.

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

3.6.9. Overføring av autentisert bruker.

I assertion som sendes tilbake til SP må ID-porten legge med informasjon om autentisert bruker. Dette gjøres i NameID feltet knyttet til Subject i Assertion. Hvilken verdi som legges ned 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 SP. Identifikatoren kan benyttes ved oppslag mot ID-porten for denne sesjon for gitt SP, men vil ikke lenger eksistere når sesjonen opphører.
- Ved *persistent* format overføres en tilfeldig identifikator som er unik for denne brukeren mot denne SP på tvers av alle sesjoner brukeren har mot SP. Identifikatoren opprettes ved første gangs pålogging for en bruker mot en gitt SP, og ID-porten tar vare på denne identifikatoren for denne bruker mot gitt SP for fremtidig bruk.
- Følgende attributter legges ut i assertion (for tilbakekompatibilitet)
 - Uid (Fødselsnummer)
 - SecurityLevel

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

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.3.6.3) for spesifisering av gyldige klasser støttet i ID-porten og deres tilhørende autentiseringsnivå.

3.6.10. Status i ArtifactResponse.

ArtifactResponse KAN inneholde en `<Status>` angivelse og MÅ 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.

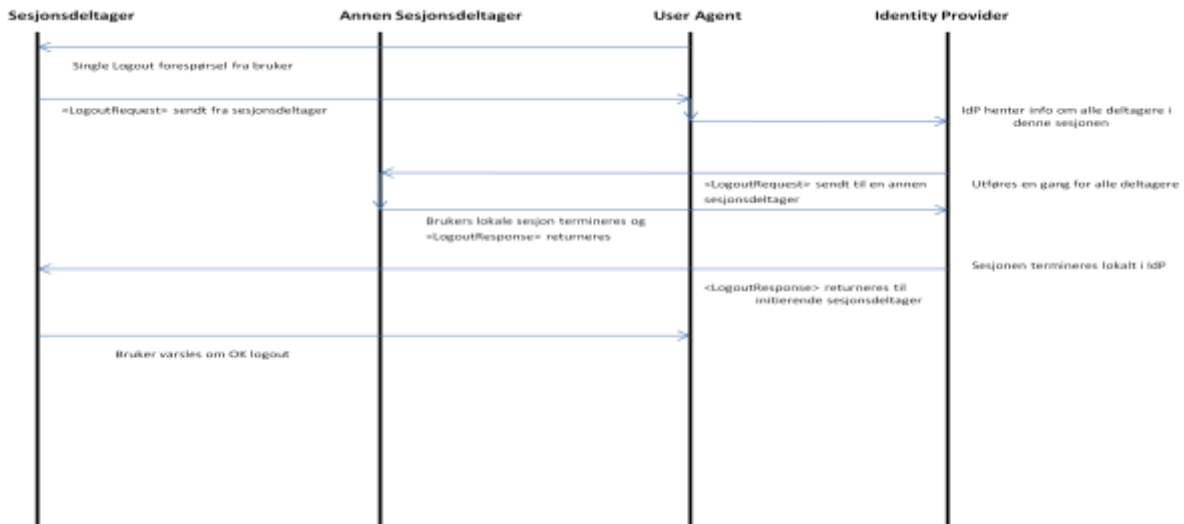
3.6.11. SP godkjenner eller avviser forespørsel.

SP skal utføre de sjekker som er påkrevet iht. SAML 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.

3.7. Single Logout Profil

Saml 2.0 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.



Figur 3 Meldingsflyt ved Single Logout

Merk at bildet kan se noe annerledes ut avhengig av valg av SAML-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, men anbefalt løsning for Single Logout er bruk av bak-kanal. Dette krever at bak-kanal blir stående oppe etter etablering. Se [policy] for detaljer.

Dette gjelder dog ikke første melding fra initierende SP. 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 Browser Cookies.

Mao 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.
- ID-porten MÅ støtte SOAP binding.
- Alle forespørsler og svar MÅ være signert.
- Kommunikasjon over bak-kanal (SOAP) må sikres vha klient autentisert (to veis) SSL/TLS

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

3.8. Identity Provider Discovery Profile

Dette er ikke støttet i denne versjonen av Id-Porten, men vurderes for senere versjoner av ID-porten. Dette spesifiseres imidlertid ikke her.

3.9. Attribute Query/Request Profile

Dette er ikke støttet i denne versjonen av Id-Porten, men vurderes for senere versjoner av ID-porten. Dette spesifiseres imidlertid ikke her.