SEID-Prosjektet

Leveranse oppgave 2

Grensesnitt for tilgang til Oppslagstjenester

Versjon 1.03

Status: Godkjent

Dato: 01.06.2012

HISTORIKK

Dato	Versjon	Utført av	Kommentar
03.12.04	1.0	PK	Dokumentet godkjent av SEID-prosjektets styringsgruppe.
17.12.04	1.01	PK	Oppdateringer i kap. 4.1 og kap. 4.4 samt en presisering i kap. 6.1.3. Formell navneromsidentifikator tildelt for XML skjema i Bilag C.
03.02.05	1.02	PK	Oppdatert kap. 4.1
01.06.12	1.03	PK	Oppdatert kontaktpunkt for ansvarlig dokumentforvalter i kap. 4.1.

INNHOLDSFORTEGNELSE

1 Begreper og forkortelser

Begrep	Forklaring
Brukersted	Den aktør som benytter en Oppslagstjeneste fordi den har behov for å få informasjon knyttet til Sertifikatinnehaver ut over det som står i dennes sertifikat.
Frittstående Oppslagstjeneste	Oppslagstjeneste som er frikoplet fra andre tjenester, i motsetning til Integrert Oppslagstjeneste.
Fødselsnummer	Unikt nummer (11 siffer) som identifiserer norsk statsborger eller person med oppholdstillatelse i Norge. Administreres av Skattedirektoratet ved Det Sentrale Personregisteret.
Informasjonsleverandør	Leverandør av den informasjonen som det spørres etter og som utleveres gjennom Oppslagstjenesten.
Integrert Oppslagstjeneste	Oppslagstjeneste som er integrert i en Sertifikatstatustjeneste, i motsetning til Frittstående Oppslagstjeneste. Alle forespørsler og svar knyttet til Oppslagstjenesten er integrert i henholdsvis forespørsler og svar om sertifikatstatus på et sertifikat.
Meldingsforespørsel	Kommunikasjonsmelding som kan inneholde en eller flere Subjektforespørsler.
Meldingssvar	Kommunikasjonsmelding som er et svar på en Meldingsforespørsel. Ett Meldingssvar kan inneholde ett eller flere Subjektsvar.
Oppslagstjeneste	Tjeneste som et Brukersted kan benytte for å få utlevert tilleggsinformasjon knyttet til Sertifikatinnehaver, på basis av informasjon som ligger i dennes sertifikat. Eksempel på informasjon som kan utleveres er Sertifikatinnehaverens Fødselsnummer.
Personsertifikat	Et sertifikat hvor Sertifikatinnehaver er en fysisk person. I dette dokumentet er fokus rettet mot Personsertifikater som entydig identifiserer Sertifikatinnehaver gjennom knytning til vedkommendes Fødselsnummer eller D-nummer i Det Sentrale Personregisteret.
SEID-prosjektet	Prosjektet som har produsert dette dokumentet. Prosjektets fullstendige navn er "Samarbeidsprosjekt om eID og eSignatur".
Sertifikat	Et sertifikat er en form for elektronisk identitetsbevis. Sertifikater kan bl.a. anvendes som elektronisk legitimasjon eller for å validere en elektronisk signatur.
Sertifikatinnehaver	Den kunden (person/virksomhet) sertifikatet er utstedt til i henhold til sertifikatpolicy og som er innehaver av den private nøkkelen (jf. Sertifikatmottaker).
Sertifikatmottaker	Den person/aktør som har behov for å benytte den offentlige nøkkelen som ligger i et sertifikat og derfor har behov for å validere sertifikatets gyldighet og dets innhold (jf. Sertifikatinnehaver).
Sertifikatpolicy	Et dokument som inneholder regler for hvordan sertifikater utstedes og behandles, som dermed danner grunnlag for hvilken tillit man kan ha til sertifikatene, og som utsteder er ansvarlig for å følge for sine sertifikattjenester.
Sertifikatprofil	En Sertifikatprofil definerer krav til sertifikatenes innhold, syntaks og semantikk.
Sertifikatstatustjeneste	En tjeneste hvor en Sertifikatmottaker kan forespørre status (gyldig eller tilbakekalt) på et gitt sertifikat. En OCSP tjeneste er et eksempel på en slik tjeneste.

Begrep	Forklaring
Sertifikatutsteder	En Sertifikatutsteder som omtalt i dette dokumentet vil være: • en juridisk person, dvs. et rettssubjekt som ikke er en fysisk person, i dette tilfelle en organisasjon. • ansvarlig for sertifikatutstedelsen, dvs, ansvarlig for implementeringen av sertifikatpolicy (selv om den operative utførelsen kan foretas av en annen aktør). • avtalepart for Sertifikatinnehaver. • erstatningsmessig ansvarlig i henhold til gjeldende erstatningsbestemmelser i relevante nasjonale lover, forskrifter samt i sertifikatpolicy for sertifikatene som utstedes.
Subjektforespørsel	Forespørsel om informasjon knyttet til en angitt Sertifikatinnehaver (subjekt). Dette dokumentet har fokus på forespørsler om utlevering av Sertifikatinnehavers Fødselsnummer, se kap. 3.3, Avgrensninger.
Subjektsvar	Svar på Subjektforespørsel som inneholder forespurt informasjon knyttet til Sertifikatinnehaver (subjekt), jf. Subjektforespørsel.
Tjenestetilbyder	Leverandør av Oppslagstjenesten.
Unik Identifikator	En kombinasjon av siffer/tegn som legges inn i et Personsertifikat og som, gjennom knytning til et Fødselsnummer i Det Sentrale Personregisteret, entydig identifiserer personen som er Sertifikatinnehaver. Sertifikatprofilen for Personsertifikater i [4] definerer syntaks for en slik Unik Identifikator.
XML Skjema	(eng: XML schema) XML basert formalisme for å beskrive regler for syntaks, struktur og verdier for instanser av XML dokumenter.

Forkortelse	Forklaring
ASN.1	Abstract Syntax Notation no.1
AIA	Authority Information Access
cert	Sertifikat (fra eng: certificate)
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DN	Distinguished Name
HTTP	Hypertext Transport Protocol
IETF	Internet Engineering Task Force
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
SCVP	Simple Certificate Validation Protocol
SA	Sertifikat Autoritet
SIA	Subject Information Access
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security (erstatter SSL - Secure Socket Layer)
UNID	Unik Identifikator
XML	eXtensible Markup Language

2 Referanser

[1] PKI Forum, Strategi for en samfunnsinfrastruktur for elektronisk signatur og elektronisk ID i Norge, juni 2002, www.handel.no/pkiforum

[2] PKI Forum, Handlingsplan, Rapport fra "Midlertidig Prosjektgruppe" for oppfølging av PKI strategien, februar 2003, www.handel.no/pkiforum

[3] Nærings- og handelsdepartementet, "eNorge 2005", mai 2002, www.enorge.org

[4] SEID-prosjektet, Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater, versjon 1.01, september 2004, www.handel.no/pkiforum/seid

[5] Justis- og politidepartementet, Lov om behandling av personopplysninger (personopplysningsloven), 14. april 2000, www.lovdata.no

[6] Dansk standard, DS-843-2, Kommunikasjon mellom PID-leverandør og applikasjonsserviceudbyder, 2. udgave, 16. desember 2003

[7] IETF, RFC 2560, Online Certificate Status Protocol (OCSP), Juni 1999, www.ietf.org/rfc

[8] IETF, Simple Certificate Validation Protocol (SCVP), Internet Draft, juli 2004, http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-15.txt

[9] IETF, RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, juni 1999, www.ietf.org/rfc

[10] World Wide Web consortium, XML, Extensible Markup Language, april 2004, www.w3.org/TR/xml11

[11] IETF, RFC 2246, Transport Layer Security Protocol (TLS), januar 1999, www.ietf.org/rfc

[12] Arbeids- og administrasjonsdepartementet, Forskrift om behandling av personopplysninger (personopplysningsforskriften), 15. desember 2000, www.lovdata.no

[13] IETF, RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, april 2002, www.ietf.org/rfc

[14] World Wide Web consortium, XML-Signature Syntax and Processing, februar 2002, XMLDSIG, www.w3.org/TR/xmldsig-core

[15] IETF, RFC 2630, Cryptographic Message Syntax (CMS), juni 1999, www.ietf.org.rfc

[16] IETF, RFC 2315, PKCS #7: Cryptographic Message Syntax, mars 1998, www.ietf.org/rfc

[17] IETF, RFC 3850, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version

3.1 - Certificate Handling, juli 2004, www.ietf.org/rfc

[18] IETF, RFC 3851, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 - Message Specification, juli 2004, www.ietf.org/rfc

3 Innledning

3.1 Bakgrunn

Nasjonalt PKI Forum la i juni 2002 frem en strategi for en samfunnsinfrastruktur for elektronisk signatur og elektronisk ID i Norge [1]. Strategien fikk bred tilslutning i en offentlig høring høsten 2002. I oppfølgingen av strategien utarbeidet PKI Forum en Handlingsplan [2] som er grunnlaget for etableringen av et samarbeidsprosjekt for eID og eSignatur, kalt SEID–prosjektet. Prosjektet hadde oppstart i november 2003 og er basert på en avtale mellom Nærings- og handelsdepartementet (NHD), Arbeids- og administrasjonsdepartementet (AAD) og 14 private virksomheter. Prosjektet er blant annet forankret i Regjeringens IT politikk stadfestet i eNorge 2005 [3].

3.2 Arbeidsgruppens mandat og medlemmer

Dette dokument inneholder SEID-prosjektets leveranse nummer to. Da prosjektet startet omfattet mandatet for leveransen tekniske grensesnitt for katalog- og sertifikatstatustjenester generelt, herunder grensesnitt knyttet til sertifikatvalidering. Etter nærmere evaluering konkluderte prosjektet med at sistnevnte teknisk sett allerede er godt nok standardisert internasjonalt. Derimot er det et faktum at det for enkelte andre sentrale katalogtjenester, bl.a. Oppslagstjeneste for Fødselsnummer, i veldig liten grad finnes standardiserte grensesnitt. På dette området så man derfor størst potensial for SEID-prosjektet å kunne levere merverdi. Til slutt ble mandat og oppgavedefinisjon definert som:

Det skal utarbeides en spesifikasjon av et begrenset antall alternative tjenestegrensesnitt for oppslagstjenester hvor sertifikatmottager skal kunne få tilgang til identitetsinformasjon om Sertifikatinnehaver.

- *Det skal spesifiseres hvilke typer spørringer som skal være mulig. Som et minimum skal oversettelse mellom evt. unik identifikator i sertifikat og Sertifikatinnehavers fødselsnummer dekkes.*
- *Grensesnittbeskrivelsene må ta høyde for mulige samtrafikkmodeller for de situasjoner hvor spørretjenestene ikke leveres direkte fra sertifikatutsteder for det gitte sertifikat.*
- *Grensesnittbeskrivelsen skal omfatte nødvendige sikkerhetskrav og sikkerhetsmekanismer for aktuelle spørringer og svar.*
- *Spesifikasjonen skal i størst mulig grad baseres på aktørenes eksisterende løsninger samt relevante internasjonale standarder.*

Arbeidsgruppen har bestått av:

- Pål Kristiansen, UniBridge AS (innleid prosjektleder og leder av gruppen)
- John Bothner, Microsoft Norge AS (dokumentets redaktør)
- Rune Hagen, BankID Samarbeidet
- Atle Dingsør, Buypass AS
- Lise Blix, DnB NOR ASA
- Anund Lie, IBM Norge
- Håvard Grindheim, for Posten Norge AS / Telenor ASA
- Ole Svendsby, Posten Norge AS
- Ståle Gullbrekken, SpareBank 1 Gruppen AS
- Geir Spiten, Terra-Gruppen AS

3.3 Avgrensninger, formål, målgruppe, omfang

Avgrensninger

Arbeidsgruppens mandat, ref. kap. 3.2, åpnet for å dekke Oppslagstjenester generelt. SEID-prosjektet har ut ifra en generell behovsvurdering besluttet å utelukkende fokusere på Oppslagstjenester for utlevering av Fødselsnummer i relasjon til Personsertifikater. På den annen side, gjennom de spesifiserte grensesnittene for fødselsnummeroppslag er det bevisst laget et rammeverk som legger til rette for å legge til utvidelser som skal kunne støtte spørring på andre informasjonselementer[1].

Spesifikasjonene i dette dokumentet fokuserer utelukkende på grensesnittet mellom Brukersted og Tjenestetilbyder. Nærmere spesifikasjon av tilhørende funksjonalitet hos henholdsvis Brukersted (klientside) og Tjenestetilbyder (serverside) ligger utenfor mandatet til SEID-prosjektet. Det samme gjelder eventuelle grensesnitt mellom Tjenestetilbyder og aktører som denne må kommunisere med for å få levert Oppslagstjenesten til Brukerstedet.

Generelle sikkerhetskrav er dekket i den grad de er direkte knyttet til grensesnittet mellom Brukersted og Tjenesteleverandør. Med unntak av enkelte generelle anbefalinger er derimot valg av sikkerhetsløsning overlatt til den enkelte Tjenestetilbyder.

Dokumentet har utelukkende teknisk fokus. Policy– og forretningsmessige forhold knyttet til det å levere kommersielle Oppslagstjenester er ikke regulert.

Formål

Personsertifikater er sertifikater som blant annet entydig identifiserer den person som er Sertifikatinnehaver. I Norge identifiseres alle personer entydig gjennom sitt Fødselsnummer i Det Sentrale Personregisteret. Fødselsnummeret er således det mest sentrale person-identitetsbegrepet som anvendes for tjenester hvor sikker identifikasjon av Sertifikatinnehaver er et krav. Adgang til Fødselsnummer er nødvendig for eksempel for bank- og finansnæringen og ikke minst for ulike offentlige instanser.

[1] Et eksempel på en annen oppslagstjeneste er hvor et Brukersted kan kontrollere om det finnes en entydig relasjon mellom en gitt Unik Identifikator i et sertifikat og et oppgitt fødselsnummer. En slik tjeneste kan være aktuell for Brukersteder som ikke er autorisert til å få utlevert fødselsnummer.

Oppslag i Det Sentrale Personregisteret er regulert av konsesjonskrav. Det er lovlig, men ikke anbefalt, å publisere Fødselsnummer sammen med navnet i et sertifikat. Dette fordi det antas at en del Sertifikatinnehavere ikke ønsker dette, samt at det er en viss mulighet for at norske myndigheter i fremtiden vil kunne legge begrensninger på publisering og bruk av slike sertifikater. Flere norske sertifikatutstedere har derfor valgt å ikke inkludere Fødselsnummer i de Personsertifikatene de utsteder.

I stedet for Fødselsnummer kan Sertifikatutsteder legge inn en alternativ Unik Identifikator (UNID) i sertifikatene. Ved å benytte denne identifikatoren mot en separat Oppslagstjeneste kan autoriserte Brukersteder få utlevert det tilhørende Fødselsnummeret.

Alle Sertifikatutstedere som utsteder Personsertifikater ihht. den anbefalte norske Sertifikatprofilen fra SEID-prosjektet [4], og som ikke oppgir Fødselsnummer eksplisitt i sertifikatene, vil ha behov for å tilby en slik Oppslagstjeneste. Med det kan Sertifikatutstedere etablere tilgangskontroll slik at kun de Brukersteder med tjenestemessig behov og nødvendig autorisasjon kan få adgang til både sertifikat og Fødselsnummer. Forutsetningen for utlevering er at Sertifikatinnehaver har gitt sitt samtykke til slik utlevering, eller at Sertifikatmottakeren med hjemmel i norsk lov eller på annen måte har adgang til å få Fødselsnummeret utlevert, jf. Personopplysningslovens § 8 [5].

Det finnes ikke i dag internasjonalt standardiserte grensesnitt for denne typen Oppslagstjenester med den konsekvens at Sertifikatutstedere i Norge har måttet definere sine egne.

Formålet med dette dokumentet er å dokumentere felles, anbefalte grensesnitt som skal bidra til å legge et grunnlag for teknisk harmonisering av Oppslagstjenester for Fødselsnummer i det norske markedet på sikt. Tilsvarende er allerede gjort i Danmark [6].

Målgruppe

Dette dokumentet er primært tilegnet Sertifikatutstedere og Sertifikatmottakere (Brukersteder) som henholdsvis ønsker å levere eller å ta i bruk PKI tjenester. Sertifikatmottakere kan både være private aktører som leverer kommersielle elektroniske tjenester (nettbanker, e-handel, mm.) og offentlige myndigheter med elektroniske tjenester internt i forvaltningen og eksternt rettet mot innbyggerne og næringsliv.

Omfang

Dokumentet spesifiserer tekniske grensesnitt mot Oppslagstjenester som skal kunne utlevere Sertifikatinnehavers Fødselsnummer på bakgrunn av vedkommendes sertifikat og/eller den Unike Identifikator (UNID) som befinner seg i sertifikatet.

Dokumentet tar for seg to likestilte tjenestevarianter som benytter ulike tekniske grensesnitt:

1. Oppslagstjeneste realisert som en Integrert Oppslagstjeneste, dvs. at den er integrert i en Sertifikatstatustjeneste. Tjenestegrensesnittet vil gjøre bruk av den samme protokollen som Sertifikatstatustjenesten benytter. For denne tjenestevarianten har hovedfokus vært å beskrive en OCSP [7] basert tjeneste.
2. Oppslagstjeneste realisert som en Frittstående Oppslagstjeneste. Tjenestegrensesnittet som er spesifisert i dette dokumentet benytter XML [10] som format for informasjonsutveklsing og HTTP [9] som kommunikasjonsprotokoll.

Alternative protokoller til de som er nevnt over vil kunne anvendes, både for Integrert og Frittstående Oppslagstjeneste. Med unntak av Bilag B som skisserer bruk av SCVP som et alternativ til OCSP er bruk av andre protokoller ikke nærmere spesifisert.

3.4 Dokumentets struktur

Kapittel 4 angir ansvarlig dokumentforvalter samt status og tilgjengelighet for dokumentet.

Kapittel 5 gir en overordnet funksjonell beskrivelse av de Oppslagstjenestene som er dekket i dokumentet og beskriver overordnede sikkerhetskrav knyttet til tjenestegrensesnittet mot Brukersteder.

Kapittel 6 spesifiserer tekniske grensesnitt for de to variantene av Oppslagstjenester, Integrert og Frittstående, som nevnt i kap. 3.3.

Bilag A er et informativt Bilag som forenklet illustrerer hvordan Meldingsforespørsler og Meldingssvar er bygget opp for en Integrert Oppslagstjeneste basert på OCSP.

Bilag B er et informativt Bilag som beskriver hvordan en Integrert Oppslagstjeneste kan realiseres ved hjelp av protokollen SCVP [8], en alternativ protokoll til OCSP.

Bilag C er et normativt Bilag og beskriver et XML skjema som gjelder for grensesnittet mot en Frittstående Oppslagstjeneste, ref. kap. 3.3.

Bilag D er et informativt Bilag som begrunner noen av de designvalg som er gjort ved utarbeidelse av XML skjemaet i Bilag C.

Bilag E er et informativt Bilag som viser XML eksempler for Meldingsforespørsler og Meldingssvar basert på XML skjemaet i Bilag C.

Bilag F er et normativt Bilag som inneholder returkoder til bruk for en Frittstående Oppslagstjeneste.

Bilag G er et informativt Bilag som beskriver hvordan XML skjemaet i Bilag C kan utvides til å støtte Oppslagstjenester for utlevering av andre typer av informasjon enn Fødselsnummer.

4 Dokumentets status og forvaltning

4.1 Ansvarlig dokumentforvalter

På oppdrag fra SEID-prosjektet er Post- og teletilsynet utpekt som ansvarlig dokumentforvalter for dette dokumentet. Kontaktpunkt hos Post- og teletilsynet er:

E-post: seid@npt.no

4.2 Status og tilgjengelighet

Dette dokumentet definerer tekniske tjenestegrensesnitt mot Oppslagstjenester som anbefales benyttet av norske Sertifikatutstedere og evt. andre aktører som ønsker å levere de variantene av Oppslagstjenester som er definert i kap. 3.3.

Dokumentet inneholder offentlig informasjon og kan distribueres fritt.

4.3 Overgangsordninger

Enkelte av SEID-prosjektets aktører representerer Sertifikatutstedere som allerede har Oppslagstjenester for Fødselsnummer operative i markedet. For på sikt å få til størst mulig grad av harmonisering av tjenestegrensesnittene har aktørene funnet det nødvendig å gå sammen om å anbefale tekniske grensesnitt som på enkelte områder avviker fra dagens løsninger.

For tjenestevarianten Frittstående Oppslagstjeneste har det av den grunn vært nødvendig å innføre en overgangsordning som tillater avvik i en overgangsperiode frem til 31.desember 2005. Dette betyr at SEID-prosjektet anbefaler at markedet i denne overgangsperioden likestiller bruk av andre XML skjema for Frittstående Oppslagstjeneste med det XML skjemaet som er definert i dette dokumentet. Fra og med 1.januar 2006 SKAL alle aktører som tilbyr Frittstående Oppslagstjenester for Fødselsnummer og som ønsker å følge SEID-prosjektets anbefalinger benytte XML skjemaet som er definert i Bilag C i dette dokumentet.

4.4 Dokumentvedlikehold

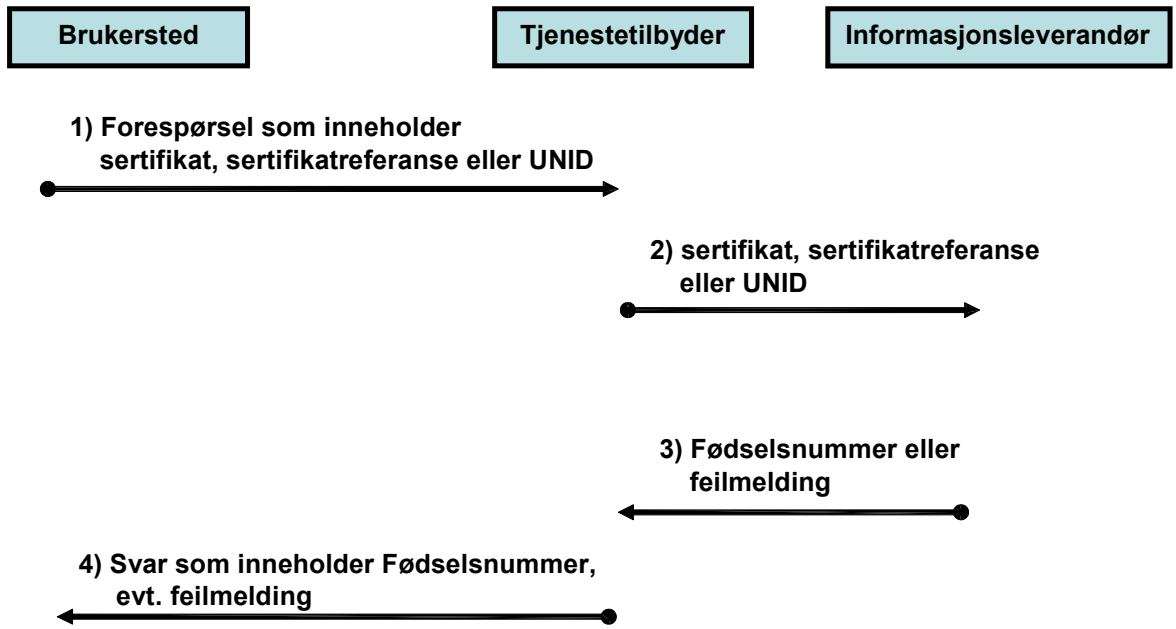
Aktørene i SEID-prosjektet har i fellesskap besluttet at dette dokumentet skal kunne revideres ved behov og at en behovsvurdering skal gjennomføres årlig.

Ansvarlig dokumentforvalter (se kap. 4.1) er kontaktpunkt for eventuelle spørsmål og konkrete endringsforslag til innholdet i dette dokumentet.

Prosedyrer for revisjon og annet dokumentvedlikehold er regulert gjennom en egen forvaltningsinstruks utarbeidet av SEID-prosjektet.

5 Tjenestebeskrivelse for Oppslagstjenester

5.1 Overordnet tjenestebeskrivelse



Figur 1 Roller og informasjonsutveksling knyttet til Oppslagstjenester for Fødselsnummer

Figuren viser roller involvert i en Oppslagstjeneste for utlevering av Fødselsnummer. Rollene som Tjenestetilbyder og Informasjonsleverandør kan deles mellom ulike aktører, eventuelt kan én og samme aktør ivareta begge roller. Punktene 2) og 3) i figuren vil for slike tilfeller representere intern prosessering hos Tjenestetilbyder.

Oppslagstjenesten gir Brukersteder tilgang til å forespørre informasjon om Sertifikatinnehaver som ikke fremgår av Sertifikatinnehavers sertifikat, i dette tilfelle Sertifikatinnehavers Fødselsnummer. Enhver forespørsel vil i så måte være knyttet til et sertifikat ved at forespørselen enten inkluderer det aktuelle sertifikat, en referanse til dette eller Sertifikatinnehavers Unike Identifikator (UNID) i sertifikatet. I enkelte tjenestetilfeller vil Tjenestetilbyder kontrollere at det aktuelle sertifikatet er gyldig før informasjonen utleveres, men dette er ikke et krav.

Koblingen mellom et sertifikat, evt. Sertifikatinnehavers Unike Identifikator i sertifikatet, og Sertifikatinnehavers Fødselsnummer forvaltes av en Informasjonsleverandør som er kilden for fremhenting av informasjonen ved en forespørsel.

Grensesnittspesifikasjonene i dette dokumentet legger opp til at en Tjenestetilbyder skal kunne tilby Brukersteder fødselsnummeroppslag for Sertifikatinnehavere enkeltvis, dvs. at en Meldingsforespørsel inneholder én enkelt Subjektforespørsel og tilhørende Meldingssvar inneholder ett enkelt Subjektsvar. Som en opsjon gir grensesnittspesifikasjonene Tjenestetilbyder mulighet til å tilby Brukersteder fødselsnummeroppslag for flere Sertifikatinnehavere samtidig. Sistnevnte løses ved å inkludere flere Subjektforespørsler i én og samme Meldingsforespørsel og tilsvarende flere Subjektsvar i ett og samme Meldingssvar.

Oppslagstjenesten kan være integrert med en Sertifikatstatustjeneste, dvs. at sertifikatstatusforespørsel/svar og Fødselsnummerforespørsel/svar er integrert i én og samme Meldingsforespørsel/svar, ref.kap 6.1. Alternativt kan Oppslagstjenesten realiseres som en frittstående tjeneste, ref. kap. 6.2.

Når det gjelder samtrafikk, vil et Brukersted kunne ha behov for å foreta fødselsnummeroppslag knyttet til sertifikater fra flere ulike sertifikatutstedere. Avhengig av hvordan de aktuelle Tjenestetilbydere og Informasjonsleverandører har samordnet sine tjenester, vil Brukerstedet måtte forholde seg til én eller flere Tjenestetilbydere og dermed ett eller flere tekniske grensesnitt. Grensesnittspesifikasjonene i dette dokumentet legger ingen spesielle føringer eller begrensninger for hvordan tjenestesamordning og dermed samtrafikk kan løses på tvers av sertifikatutstedere.

5.2 Sikkerhetskrav

Nedenfor følger et sett av minimum sikkerhetskrav som gjelder for grensesnittet mellom Brukersted og Tjenestetilbyder ved spørring på fødselsnummer. Andre sikkerhetskrav, for eksempel knyttet til håndtering av fødselsnummer, er ikke behandlet i dette dokumentet.

1) **Autentisering og "autorisasjon" av Brukersted og dennes Meldingsforespørsler:**
   - Brukerstedet SKAL autentisere seg overfor Tjenestetilbyder.
   - Tjenestetilbyder SKAL utelukkende utlevere Fødselsnummer til Brukersteder som har den nødvendige autorisasjon[2].

2) **Autentisering av Tjenestetilbyder (og evt. Informasjonsleverandør) og dennes Meldingssvar**
   - Tjenestetilbyder SKAL tilby Brukersted mulighet for autentisering.
   - Brukersted SKAL kunne velge å motta signerte Meldingssvar[3]. Signaturen på Meldingssvaret skal tilhøre Informasjonsleverandør eller representant for denne. Signaturen må kunne verifiseres opp mot et felles tillitspunkt avtalt mellom Brukerstedet og Tjenestetilbyder.

3) **Konfidensialitet av Meldingsforespørsler og Meldingssvar**
   - Meldingsforespørsel og/eller Meldingssvar som går over et åpent nett SKAL krypteres for å konfidensialitetsbeskytte koblingen mellom Fødselsnummer og en eller flere av parametrene UNID/Sertifikat/Sertifikatreferanse (se figur 1). Kravet kan kun avvikes dersom Tjenestetilbyder kan dokumentere hvordan konfidensialitetskravet er tilsvarende ivaretatt uten bruk av kryptering.

[2] Utlevering av Fødselsnummer krever at Sertifikatinnehaver har gitt sitt samtykke, eller at Brukerstedet med hjemmel i norsk lov eller på annen måte har adgang til å få Fødselsnummeret utlevert, jf. Personopplysningslovens § 8 [5]. Utover dette er autorisasjonsfunksjonen et anliggende for den enkelte Tjenestetilbyder.

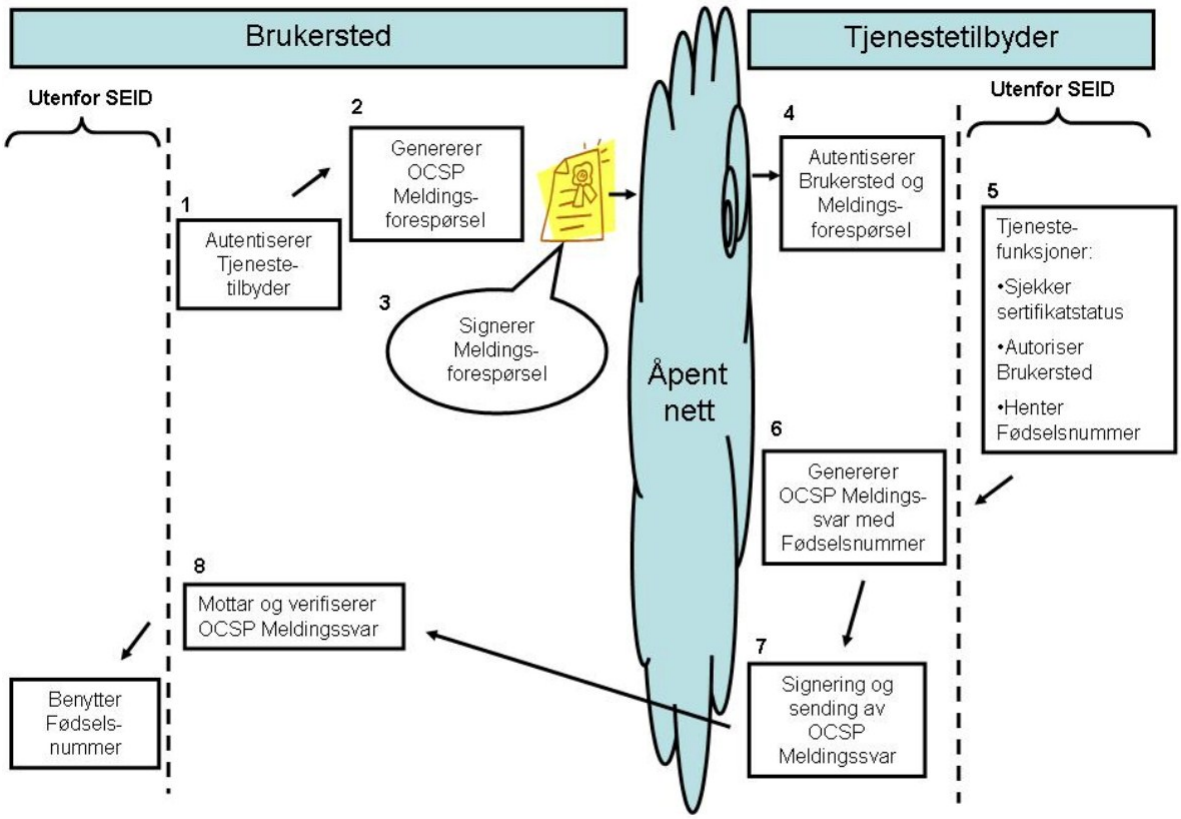
[3] Kan for eksempel være knyttet til behov for arkivering av signaturer for sporbarhet i ettertid.

6 Grensesnitt mot Oppslagstjenester

6.1 Integrert Oppslagstjeneste

Kjente protokollstandarder for Sertifikatstatustjenester som for eksempel OCSP [7] og SCVP [8] gir mulighet for å integrere Oppslagstjeneste og Sertifikatstatustjeneste, dvs. at spørring på både sertifikatstatus og Sertifikatinnehavers Fødselsnummer kan foretas i én og samme forespørsel.

6.1.1 Funksjonell beskrivelse



Figur 2 Funksjoner involvert ved bruk av en Integrert Oppslagstjeneste

Figuren viser de viktigste funksjonene ved bruk av en Integrert Oppslagstjeneste. I figuren er en OCSP tjeneste benyttet som eksempel. Rollene som Tjenestetilbyder og Informasjonsleverandør er for enkelhets skyld antatt ivaretatt av én og samme aktør sett fra Brukerstedet. Sistnevnte rolle er derfor ikke vist i figuren.

Figuren angir at enkelte funksjoner ligger ”Utenfor SEID”. Dette innebærer at utforming av krav og spesifikasjon for hvordan disse funksjonene skal realiseres ligger utenfor SEID-prosjektets mandat og således ikke er dekket i dette dokumentet. For eksempel er det utenfor prosjektets mandat å spesifisere hvordan Tjenestetilbyder autoriserer Brukerstedet før evt. Fødselsnummer utleveres.

Nedenfor følger en beskrivelse av de ulike funksjonene nummerert i figuren:

1. Brukersted autentiserer Tjenestetilbyder.
2. Brukerstedet bygger opp en OCSP Meldingsforespørsel ihht. [7] som blant annet inneholder en referanse[4] til det aktuelle sertifikat som forespørselen gjelder for.
3. Brukersted signerer Meldingsforespørselen før denne sendes til Tjenestetilbyder på autentisert og evt. kryptert forbindelse.
4. Tjenestetilbyder autentiserer Brukersted og Meldingsforespørsel.
5. Tjenestetilbyder utfører en rekke tjenestefunksjoner, herunder sjekk av sertifikatstatus, "autorisasjon" av Brukersted og uthenting av det aktuelle Fødselsnummer.
6. Tjenestetilbyder genererer et OCSP Meldingssvar ihht. [7]. Denne vil inneholde både Fødselsnummer og sertifikatstatus som forespurt for det aktuelle sertifikat.
7. Meldingssvaret signeres av Tjenestetilbyder før det sendes til Brukersted over evt. kryptert forbindelse.
8. Meldingssvaret valideres av Brukerstedet før Fødselsnummeret hentes ut og benyttes.

Brukerstedet lokaliserer Oppslagstjenesten ved å konfigurere dennes adresse i sin programvareklient. Alternativt så kan programvareklienten lokalisere tjenesten ved å anvende tilsvarende adresse som befinner seg i AIA-feltet i det aktuelle sertifikatet som spørringen relaterer seg til.

6.1.2 Meldingsforespørsler og Meldingssvar

6.1.2.1 Meldingsforespørsel

En Meldingsforespørsel vil alltid inneholde den/de aktuelle sertifikat(er) Subjektforespørslene er knyttet til, alternativt kun en referanse til disse.

Ved bruk av en Integrert Oppslagstjeneste skal Meldingsforespørselen i tillegg inneholde en OID som angir hvilken tilleggsinformasjon knyttet til Sertifikatinnehaver det spørres om. En slik angivelse gjelder da alle Subjektforespørsler i Meldingsforespørselen. Det anbefales at Brukerstedet benytter OID 2.16.578.1.16.3.2[5] for å angi at spørringen gjelder Fødselsnummer. selv om Tjenestetilbyder har mulighet til å velge en egendefinert OID i stedet. Valg av attributt for overføring av valgt OID samt tilhørende kodingsformat bestemmes av den sertifikatstatusprotokoll som anvendes, ref. kap.6.1.3. Dersom nevnte OID ikke inkluderes i Meldingsforespørselen vil Meldingssvaret heller ikke inneholde Fødselsnummer.

6.1.2.2 Meldingssvar

Som svar på Meldingsforespørsler som inneholder OID som beskrevet i kap. 6.1.2.1 skal Meldingssvaret, evt. det enkelte Subjektsvaret dersom Meldingssvaret inneholder svar på flere Subjektforespørsler, inneholde Sertifikatinnehavers 11-sifrede Fødselsnummer. Valg av attributt for overføring av Fødselsnummer samt tilhørende kodingsformat bestemmes av den aktuelle protokoll som anvendes, ref. kap. 6.1.3.

Dersom sertifikatstatus på det sertifikatet spørringen gjelder for angir at sertifikatet er ukjent eller tilbakekalt, returneres standard feilmelding og feilkode som gitt av den

[4] I OCSP benyttes alltid sertifikatreferanser i form av; en hashverdi av Sertifikatutsteders offentlige nøkkel + en hashverdi av Sertifikatutsteders navn + sertifikatets serienummer.

[5] Denne OID eies formelt av Bankenes Standardiseringskontor (BSK). BSK har gitt tillatelse til gjenbruk av denne for aktører som ønsker å etablere en Integrert Oppslagstjeneste for Fødselsnummer.

sertifikatstatusprotokollen som benyttes. I så tilfelle returneres heller ikke Fødselsnummer for det aktuelle sertifikat.

Dersom sertifikatstatus på det sertifikatet spørringen gjelder for angir at sertifikatet er gyldig, men Oppslagstjenesten samtidig ikke har mulighet til å returnere Sertifikatinnehavers Fødselsnummer (f.eks. pga. teknisk feil eller manglende autorisasjon av Brukersted) er det opp til Tjenestetilbyder å velge én av to måter å håndtere dette på:

1. Returnere standard feilmelding og feilkode som nevnt over.
2. Returnere standard Meldingssvar som angir at sertifikatet er gyldig, men hvor
    a) attributt for overføring av Fødselsnummer er utelatt, eller
    b) egnet attributt benyttes for å returnere feilkode og/eller feilmelding som er spesifikt knyttet til Oppslagstjenesten.

6.1.3 OCSP protokollmapping

Dette kapittelet beskriver hvordan en Integrert Oppslagstjeneste kan realiseres ved hjelp av OCSP, Online Certificate Status Protocol [7]. En tilsvarende beskrivelse for en alternativ tjenesteintegrasjon basert på SCVP [8] er beskrevet i Bilag B. For lesere som ikke er kjent med OCSP fra før, gir Bilag A en forenklet oversikt over hvordan Meldingsforespørsler og Meldingssvar er bygget opp.

Overføring av OID i Meldingsforespørsel og Fødselsnummer i Meldingssvar/Subjektsvar gjøres ved bruk av definerte utvidelser (extensions) i OCSP protokollen i samsvar med ASN.1-definisjonene i RFC 3280 [13].

For Meldingsforespørsler SKAL OID angis på meldingsnivå ved bruk av attributtet *requestExtensions*, ref. [7]. Dette innebærer at forespørsel om Fødselsnummer i utgangspunktet gjelder alle Subjektforespørsler (sertifikater) i Meldingsforespørselen. I praksis er det kun Subjektforespørsler knyttet til Personsertifikater det er relevant å returnere Fødselsnummer for. Tjenestetilbyder bør derfor ha tjenestelogikk som kan returnere Fødselsnummer for de sertifikatene der dette er relevant, og ignorere forespørsel om Fødselsnummer for sertifikater der dette ikke er relevant (f.eks. SA-sertifikater som del av sertifikatkjede for Personsertifikatet).

For Meldingssvar kan Tjenestetilbyder velge å legge Fødselsnummer i attributtet *responseExtensions*, ref. [7]. Dette er anbefalt løsning dersom Tjenestetilbyder kun støtter Meldingssvar med ett Subjektsvar. Dersom Tjenestetilbyder støtter Meldingssvar med flere Subjektsvar skal Fødselsnumrene for det enkelte subjekt legges i attributtet *singleExtensions* for det enkelte Subjektsvar, ref. [7].

Dersom fødselsnummeroppslaget feiler er det opp til Tjenestetilbyder å velge håndtering som angitt i 6.1.2. Eventuell bruk av OCSP protokollutvidelser (extensions) for angivelse av feil vil mao. kunne være spesifikke for den enkelte Tjenestetilbyder.

Alle utvidelser (extensions) som benyttes skal markeres som ikke kritiske, både i forespørsler og svar.

6.1.4 Sikkerhetsløsning

Tjenestetilbyder har et selvstendig ansvar for å velge en sikkerhetsløsning for sitt tjenestegrensesnitt som både er hensiktsmessig og god nok til å oppfylle sikkerhetskravene i kapittel 5.2 og evt. andre krav Tjenestetilbyderen måtte stå overfor.

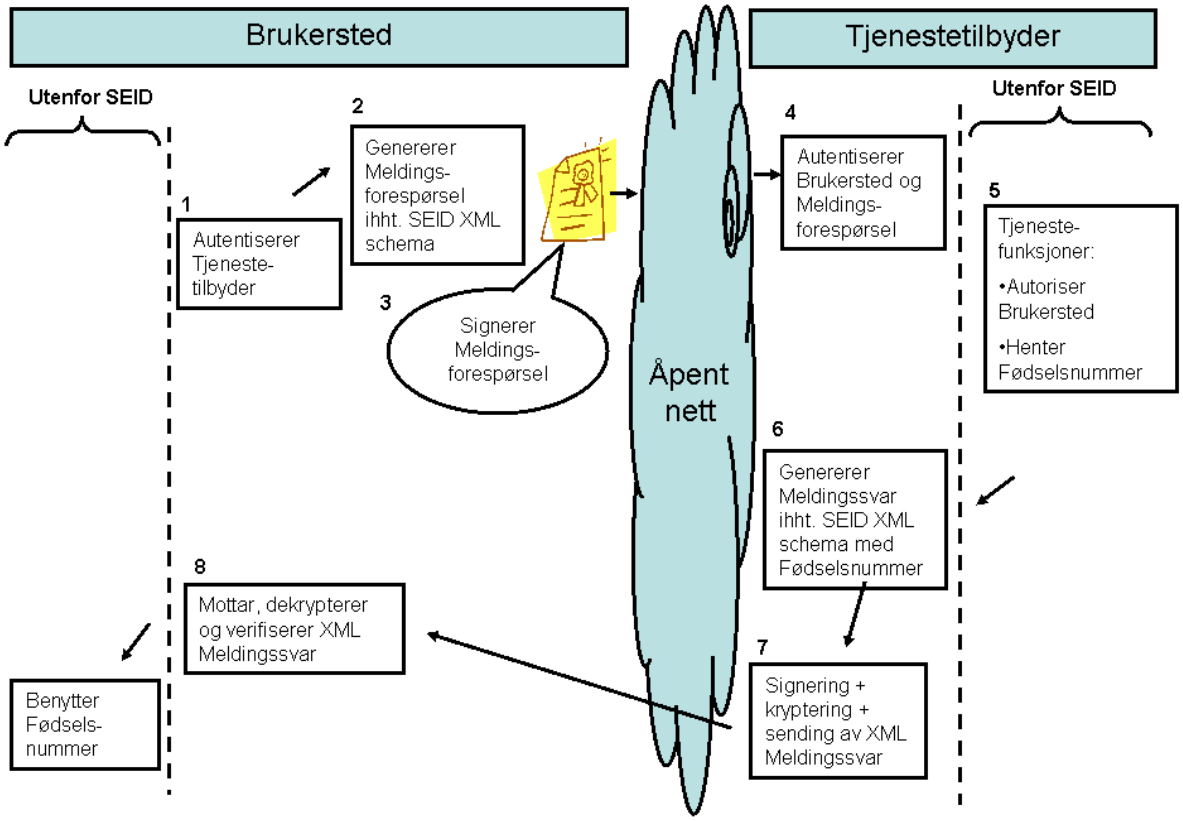
I relasjon til sikkerhetskravene i kap. 5.2 har standardprotokollene OCSP (ref. kap. 6.1.3) og SCVP (ref. Bilag B) har følgende innebygget støtte for sikkerhetsmekanismer:

- Det er en protokollopsjon i både OCSP og SCVP å signere Meldingsforespørselen. For Meldingssvar er det et krav i OCSP at den er signert, mens i SCVP må Brukerstedet i forespørselen eksplisitt angi om Meldingssvaret skal være signert eller ikke. Signaturformat på Meldingsforespørsler og Meldingssvar er gitt av den aktuelle sertifikatstatusprotokoll.

Hverken OCSP eller SCVP har innebygget støtte for kryptering av Meldingsforespørsler/Meldingssvar eller autentisering av Tjenestetilbyder ved etablering av kommunikasjonsforbindelse. TLS [11] anses godt egnet til å implementere eventuell autentisering av Brukersted og Tjenestetilbyder ved etablering av kommunikasjonsforbindelse og for eventuell kryptering av denne.

6.2 Frittstående Oppslagstjeneste

6.2.1 Funksjonell beskrivelse



Figur 3 Funksjoner involvert ved bruk av en Frittstående Oppslagstjeneste

Figuren viser de viktigste funksjonene ved bruk av en Frittstående Oppslagstjeneste. Rollene som Tjenestetilbydere og Informasjonsleverandør er for enkelhets skyld antatt ivaretatt av én og samme aktør sett fra Brukerstedet. Sistnevnte rolle er derfor ikke vist i figuren.

Figuren angir at enkelte funksjoner ligger "Utenfor SEID". Dette innebærer at utforming av krav og spesifikasjon for hvordan disse funksjonene skal realiseres ligger utenfor mandatet til SEID-prosjektet og således ikke er dekket i dette dokumentet. For eksempel er det utenfor SEID-prosjektets mandat å spesifisere hvordan Tjenestetilbyder autoriserer Brukerstedet før evt. Fødselsnummer utleveres.

Nedenfor følger en beskrivelse av de ulike funksjonene nummerert i figuren:

1. Brukersted autentiserer Tjenestetilbyder.
2. Brukerstedet bygger opp en XML Meldingsforespørsel ihht. XML skjemaet i Bilag C. Denne vil inneholde det aktuelle sertifikat som forespørselen gjelder for, alternativt Sertifikatinnehaverens UNID hentet fra det samme sertifikatet. Dersom Meldingssvaret ønskes signert skal dette eksplisitt angis.
3. Brukerstedet signerer og evt. krypterer Meldingsforespørselen før denne sendes til Tjenestetilbyder.
4. Tjenestetilbyder autentiserer Brukersted og Meldingsforespørsel.
5. Tjenestetilbyder utfører en rekke tjenestefunksjoner, herunder "autorisasjon" av Brukersted og uthenting av det aktuelle Fødselsnummer.
6. Tjenestetilbyder bygger opp et XML Meldingssvar ihht. XML skjemaet i Bilag C.
7. Meldingssvaret signeres dersom Brukerstedet i Meldingsforespørselen har bedt om dette og vil evt. krypteres av Tjenestetilbyder før det sendes til Brukersted.
8. Meldingssvaret (må evt. dekrypteres og) valideres av Brukerstedet før Fødselsnummeret hentes ut og benyttes.

Brukerstedet lokaliserer Oppslagstjenesten ved å konfigurere dennes adresse i sin programvareklient. Alternativt så kan programvareklienten lokalisere tjenesten ved å anvende tilsvarende adresse som befinner seg i SIA-feltet i det aktuelle sertifikatet som spørringen relaterer seg til.

6.2.2 XML Meldingsforespørsler og Meldingssvar

Bilag C beskriver et XML skjema for hvordan XML Meldingsforespørsler og XML Meldingssvar skal bygges opp. Dette kapittelet beskriver alle de elementer og attributter som inngår i XML skjemaet i Bilag C. Leseren henvises også til Bilag E hvor det er gitt konkrete eksempler på bruk.

- **xmlns:** Definerer meldingstypen til å følge denne spesifikasjonen fra SEID-prosjektet og dermed XML skjemaet i Bilag C. Brukerstedet skal benytte standard navneromsidentifikator ("default namespace") ved sending, dvs. uten bruk av prefiks. Tjenestetilbyder bør akseptere meldinger der navneromsidentifikator er eksplisitt angitt ved prefiks.

- **name:** Verdien "getFnrFromUnid" angir at den enkelte Subjektforespørsel i meldingen er basert på oversendelse av Unik Identifikator (UNID) fra sertifikat den aktuelle spørringen gjelder for. Verdien "getFnrFromCert" angir at den enkelte Subjektforespørsel i meldingen er basert på oversendelse av det faktiske sertifikat spørringen gjelder for. Spørring basert på sertifikatreferanse som den Integrerte Oppslagstjenesten i kap. 6.1

benytter er ikke tatt inn som en variant for Frittstående Oppslagstjeneste da de to ovennevnte variantene av spørringer anses dekkende.

- **signResponse:** Opsjonelt attributt som benyttes av Brukersted for å angi om Meldingssvaret skal være signert eller ikke. Verdien ”*true*” angir at svaret skal være signert, mens verdien ”*false*” angir at svaret skal være usignert. Dersom attributtet ikke benyttes skal Meldingssvaret som standard være usignert.

- **version:** Angir versjonsnummer for XML definisjonen. Verdien skal være 1.0.

- **transid:** En transaksjonsID som fungerer som korrelasjonsparameter mellom en Subjektforespørsel og tilhørende Subjektsvar. Alle Subjektforespørsler og Subjektsvar skal som utgangspunkt inneholde en transaksjonsID. Attributtet kan kun utelates i Meldingssvaret dersom dette inneholder kun ett response-element. Attributtverdien må starte med en bokstav.

- **unid:** Unik Identifikator hentet fra sertifikatet som Subjektforespørselen er knyttet til. Dersom Brukerstedet sender en Subjektforespørsel som inneholder dette elementet, skal det tilhørende Subjektsvaret inneholde Fødselsnummer og samme unid verdi. Det er ikke lagt inn spesielle restriksjoner på syntaks eller format når det gjelder bruk av dette elementet. Anbefalt UNID syntaks fra SEID [4] er en av de syntaksdefinisjoner som støttes.

- **cert:** Base64 kodet sertifikat som Subjektforespørselen er knyttet til. Dersom Brukerstedet sender en Subjektforespørsel som inneholder dette elementet, skal det tilhørende Subjektsvaret inneholde Fødselsnummer og den samme cert verdien. Subjektsvaret kan som en opsjon inneholde unid-verdien fra sertifikatet i tillegg.

- **fnr:** Angir Sertifikatinnehavers 11-sifrede Fødselsnummer på formatet ”ddmmååннnnn”.

- **responseStatus:** Angir tekstlig returkodebeskrivelse for Brukerstedet. Elementet inneholder attributtet code som angir aktuell returkode ihht. tabellen i Bilag F. Som en opsjon kan Tjenestetilbyder ved feil benytte attributtet redirectURL til å angi en URL hvor Brukerstedet kan henvise Sertifikatinnehaveren.

- **signedResponse:** Angir at Meldingssvaret er signert. Meldingssvaret skal være signert dersom signResponse er satt til ”true” i den tilhørende Meldingsforespørselen. I motsatt fall skal Meldingssvaret være usignert.

Subjektsvar skal alltid inneholde samme *cert* eller *unid* element som ble benyttet i den tilhørende Subjektforespørselen.

6.2.3 HTTP protokollmapping

I utgangspunktet er det mulig å benytte ulike kommunikasjonsprotokoller for overføring av Meldingsforespørsler/svar mellom Brukersted og Tjenestetilbyder. Dette dokumentet har foreløpig kun valgt å spesifisere bruk av enkel HTTP hvor både Meldingsforespørsler og Meldingssvar sendes vha. HTTP POST.

Avhengig av hvordan meldingene er kodet (XML eller binært) skal kodingen HTTP content type settes til henholdsvis ”application/XML” eller ”application/octet-stream”. Følgende regler gjelder:

- Meldingsforespørsler og/eller Meldingssvar som enten er usignerte eller signerte vha. XMLDSIG [14] SKAL benytte content type ”application/XML”.

- Meldingsforespørsler og/eller Meldingssvar som er signerte vha. CMS [15], PKCS#7 [16] eller S/MIME [17,18], og således binærkodet, SKAL benytte content type ”application/octet-stream”.

6.2.4 Sikkerhetsløsning

Tjenestetilbyder har et selvstendig ansvar for å velge en sikkerhetsløsning for sitt tjenestegrensesnitt som både er hensiktsmessig og god nok for å oppfylle sikkerhetskravene i kapittel 5.2 og evt. andre krav Tjenestetilbyderen måtte stå overfor.

Generelt gjelder:
- TLS [11] anses godt egnet til å implementere autentisering av Brukersted og Tjenestetilbyder ved etablering av kommunikasjonsforbindelse og for eventuell kryptering av denne.
- for eventuelle signaturer på Meldingsforespørsler/Meldingssvar må Tjenestetilbyder velge hvilke(t) signaturformat(er) denne ønsker å støtte. XMLDSIG [14], CMS [15] PKCS#7 [16] eller S/MIME [17,18] er eksempler på standardiserte signaturformater som kan anvendes.

Bilag A (Informativt): OCSP skissert

Dette informative Bilaget gir en forenklet oversikt over de mest sentrale informasjonselementene som inngår i OCSP Meldingsforespørsler og OCSP Meldingssvar. Prinsippene fra tradisjonell ASN.1 er benyttet men er gjort ved bruk av mindre formalistisk pseudokode for lette lesbarheten. Beskrivelsene viser for enkelhets skyld en Meldingsforespørsel som inneholder én enkelt Subjektforespørsel og tilhørende Meldingssvar som inneholder ett enkelt Subjektsvar.

Innhold i Meldingsforespørsel:

```
OCSP-Forespørsel: SEKVENS av
                  { MELDINGSFORESPØRSEL
                    SIGNATUR – over Meldingsforespørselen }

MELDINGSFORESPØRSEL: SEKVENS av
                  { OCSP-VERSJON
                    NAVN PÅ FORESPØRRER
                    LISTE av SUBJEKTFORESPØRSEL – bestående av ett element i
                                                  dette eksempelet
                     UTVIDELSE – bestående av OID for Fødselsnummer-attributt}

SUBJEKTFORESPØRSEL: SEKVENS av
                  { SERTIFIKAT-ID
                    UTVIDELSE – benyttes ikke }

SERTIFIKAT-ID: SEKVENS av
                  { HASH-ALGORTIME – OID for hashalgoritme
                    HASH AV ”ISSUER NAME”
                    HASH AV ”ISSUER PUBLIC KEY”
                    SERIENR – for sertifikatet det spørres på. }
```

Innhold i Meldingssvar:

```
OCSP-RESPONS: SEKVENS av
                  { RESPONS STATUS
                    MELDINGSSVAR
                     SIGNATUR – over Meldingssvaret }

RESPONS STATUS:  STATUSKODE kodet med en av verdiene (0).. (6), der 0 betyr
                 at svaret er gyldig.

MELDINGSSVAR:  SEKVENS av
                  { OCSP-VERSJON
                    NAVN PÅ RESPONDER
                    PRODUKSJONSTID – for svaret
                    LISTE av SUBJEKTSVAR – bestående av ett element i dette
                                           eksempelet
                    UTVIDELSE – her returneres fødselsnummeret når
                                responsen kun inneholder ett Subjektsvar }

SUBJEKTSVAR:  SEKVENS av
                  { SERTIFIKAT-ID
                    STATUS – good, revoked or unknown
                    OPPDATERINGSTID
                    UTVIDELSE – benyttes til å returnere Fødselsnummer
                                dersom responsen inneholder flere
                                Subjektsvar }
```

Bilag B (Informativt): SCVP protokollmapping

Introduksjon

Som et alternativ til OCSP, kan SCVP (Simple Certificate Validation Protocol [8]) benyttes til å realisere en Integrert Oppslagstjeneste for Fødselsnummer. Forskjellen på en OCSP tjeneste og en SCVP tjeneste er at en sistnevnte vil kunne tilby klienter større funksjonell avlastning ved sertifikatvalidering enn det en OCSP tjeneste vil gjøre.

SCVP protokollen foreligger kun som et IETF draft og er foreløpig ikke ratifisert som en IETF RFC. På grunn av risiko for ytterligere endringer i spesifikasjonen er dette kun et informativt Bilag som viser hvordan en Integrert Oppslagstjeneste kan realiseres basert på det draft som foreligger.

Det er prinsipielt to måter å realisere en Integrert Oppslagstjeneste basert på SCVP.

- Ved bruk av dedikerte utvidelser (extensions) i forespørsler/svar, tilsvarende som beskrevet for OCSP i kap. 6.1.3
- Ved bruk av et dedikerte ”wantBack” attributter i forespørsler/svar.

Begge metoder er beskrevet her da faktisk støtte for de nevnte mekanismene vil kunne variere blant ulike kommersielle implementasjoner av SCVP. I begge tilfeller, tilsvarende som for OCSP tilfellet i kap. 6.1.3, benyttes en predefinert OID i forespørsler for å angi at Sertifikatinnehavers Fødselsnummer ønskes utlevert.

Bruk av utvidelser (extensions) i Meldingsforespørsler og Meldingssvar

SCVP støtter spørring på og utlevering av fødselsnummer på to nivåer:

1. **Meldingsnivå:** Attributtet *reqExtenisons* i Meldingsforespørsel populeres med OID og attributtet *respExtensions* i meldingssvar returnerer Fødselsnummer.
2. **Subjektnivå:** Attributtet *queryExtension* i Subjektforespørsel populeres med OID og attributtet *certReplyExtensions* i Meldingssvar returnerer Fødselsnummer.

Alternativ 2 anbefales dersom Tjenestetilbyder ønsker å støtte Meldingsforespørsler/Meldingssvar som potensielt skal kunne inneholde flere Subjektforespørsler/Subjektsvar.

Alle utvidelser (extensions) som benyttes bør markeres som ikke kritiske, både i forespørsler og svar.

Bruk av ”wantBack” attributter i meldingsforespørsler og meldingssvar

Bruk av denne metoden innebærer at forespørsler/svar knyttet til fødselsnummer integreres i Subjektforespørsler/Subjektsvar. Løsningen innebærer at attributtet *wantBack* i Subjektforespørsel populeres med OID og attributtet *replyWantBack* i tilhørende Subjektsvar returnerer Fødselsnummer.

Bilag C (Normativt): XML skjema

Introduksjon

Dette Bilaget spesifiserer XML skjema for den Frittstående Oppslagstjenesten definert i kap. 6.2. Skjemaet er tildelt følgende offisielle navneromsidentifikator (namespace) med knytning til ansvarlig dokumentforvalter; *http://www.npt.no/seid/xmlskjema/oppslagstjeneste/*

XML skjema-definisjon

```
<?xml version="1.0" encoding="UTF-8"?>
<!--  XML skjema-definisjon for SEIDs oppslagstjeneste. -->
<xsd:schema version="1.0"
        targetNamespace="http://www.npt.no/seid/xmlskjema/oppslagstjeneste/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns="http://www.npt.no/seid/xmlskjema/oppslagstjeneste/"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified">

        <xsd:annotation>
                <xsd:documentation xml:lang="no">XML-signatur-skjemaet benyttes
                        for Signature-elementer (valgfritt). Det er bare
                        nødvendig med xmlns-deklarasjoner for XML-signatur i
                        XML-instansen når den faktisk benytter XML-signaturer.
                </xsd:documentation>
        </xsd:annotation>
        <xsd:import
                namespace="http://www.w3.org/2000/09/xmldsig#"  schemaLocation="xmldsig-core-schema.xsd"/>

        <xsd:simpleType name="methodName">
                <xsd:annotation>
                        <xsd:documentation xml:lang="no">Dette skjemaet
                                definerer metodenavnene: getFnrFromCert og
                                getFnrFromUnid.
                                Utvidelser kan definere nye metodenavn, som må
                                kvalifiseres med namespace-prefiks for skjemaet
                                de er definert i.
                        </xsd:documentation>
                </xsd:annotation>
                <xsd:union memberTypes="xsd:QName"/>
        </xsd:simpleType>

        <xsd:element name="method">
                <xsd:annotation>
                        <xsd:documentation xml:lang="no">Rot-elementet i
                                XML-instansene er method, både for forespørsel
                                og svar. For forespørsler inneholder
                                method-elementet bare request-elementer, for
                                svar bare response-elementer. name identifiserer
                                hvilken type oppslag det er (metodenavn).
                                signResponse="true" benyttes i forespørsler for
                                å indikere at klient (Brukersted) ønsker signert
                                svar. signedResponse="true" benyttes i svar når
                                svaret er signert. version identifiserer versjonen
                                av protokollen, og skal være 1.0 for denne.
                        </xsd:documentation>
                </xsd:annotation>
                <xsd:complexType>
                        <xsd:sequence>
                                <xsd:choice>
                                        <xsd:element ref="request" maxOccurs="unbounded"/>
                                        <xsd:element ref="response" maxOccurs="unbounded"/>
                                </xsd:choice>
                                <xsd:element ref="ds:Signature" minOccurs="0"/>
                        </xsd:sequence>
                        <xsd:attribute name="name" type="methodName" use="required"/>
                        <xsd:attribute name="signResponse" type="xsd:boolean" use="optional" default="false"/>
                        <xsd:attribute name="signedResponse" type="xsd:boolean" use="optional" default="false"/>
                        <xsd:attribute name="version" type="xsd:string" use="required"/>
```

```
		</xsd:complexType>
	</xsd:element>

	<xsd:element name="subjectAttribute" abstract="true"/>
	<xsd:simpleType name="unidType">
		<xsd:restriction base="xsd:string">
		</xsd:restriction>
	</xsd:simpleType>
	<xsd:simpleType name="fnrType">
		<xsd:restriction base="xsd:string">
			<xsd:pattern value="\d{11}"/>
		</xsd:restriction>
	</xsd:simpleType>
	<xsd:element name="unid" type="unidType" substitutionGroup="subjectAttribute"/>
	<xsd:element name="cert" type="xsd:base64Binary" substitutionGroup="subjectAttribute"/>
	<xsd:element name="fnr" type="fnrType" substitutionGroup="subjectAttribute"/>
	<xsd:element name="request">
		<xsd:annotation>
			<xsd:documentation xml:lang="no">Forespørsel: XML-skjemaet
				tillater liste av vilkårlige subjekt-attributter.
				Metodenavnet på method-elementet bestemmer hvilke
				subjekt-attributter som kan/skal være med.
				Id-attributtet benytes for å knytte forespørselen
				til svaret.
			</xsd:documentation>
		</xsd:annotation>
		<xsd:complexType>
			<xsd:sequence>
				<xsd:element ref="subjectAttribute"/>
			</xsd:sequence>
			<xsd:attribute name="transid" type="xsd:ID" use="required"/>
		</xsd:complexType>
	</xsd:element>

	<xsd:element name="response">
		<xsd:annotation>
			<xsd:documentation xml:lang="no">Svar: XML-skjemaet tillater
				liste av vilkårlige subjekt-attributter. Metodenavnet på
				method-elementet bestemmer hvilke subjekt-attributter
				som skal være med.
				Tjenestetilbyder kan velge å levere flere
				subjekt-attributter ut over dette. id-attributtet
				kobler respons-elementet til tilsvarende
				request-element i meldingen fra klient (Brukersted).
			</xsd:documentation>
		</xsd:annotation>
		<xsd:complexType>
			<xsd:sequence>
				<xsd:element ref="subjectAttribute" minOccurs="0" maxOccurs="unbounded"/>
				<xsd:element ref="responseStatus"/>
			</xsd:sequence>
			<xsd:attribute name="transid" type="xsd:ID" use="optional"/>
		</xsd:complexType>
	</xsd:element>

	<xsd:element name="responseStatus">
		<xsd:annotation>
			<xsd:documentation xml:lang="no">Respons-status:
				code 0 betyr OK, 1 betyr at det mangler data.
				For andre koder, se standarden. text-elementet
				kan inneholde beskrivende/forklarende tekst,
				primært for logging og feilfinning. Teksten er
				ikke ment å bli presentert for sluttbruker.
			</xsd:documentation>
		</xsd:annotation>
		<xsd:complexType>
			<xsd:simpleContent>
				<xsd:extension base="xsd:string">
					<xsd:attribute name="code" type="xsd:nonNegativeInteger" use="required"/>
					<xsd:attribute name="redirectURL" type="xsd:string"/>
				</xsd:extension>
			</xsd:simpleContent>
		</xsd:complexType>
	</xsd:element>

</xsd:schema>
```

Bilag D (Informativt): Designvalg knyttet til XML skjema

Dette kapittelet beskriver noen av de designvalg som er gjort ved utarbeidelse av XML skjemaet i Bilag C.

Utvidbarhet
Skjemaet er bygget slik at det kan utvides av andre skjemaer, som da må defineres med eksplisitt navneromsidentifikator (og normalt eksplisitt prefiksing), slik at det er klart at man går ut over spesifikasjonen i dette dokumentet. Det som primært kan gjøres er å tilføye nye attributter (elementer i substitutionGroup=”subjectAttribute”). Nye metodenavn defineres også i prinsippet i nytt skjema, men det er ikke noen eksplisitt definisjon av metodenavn siden det ikke lar seg gjøre å beholde utvidbarheten samtidig med at XML-prosessoren kontrollerer at metodenavn er ett av de definerte, se nedenfor.

Type for metodenavn
Metodenavn (”name”-attributtet på method-elementet) er definert som QName (XML kvalifisert navn). Logikken er at nye metodenavn kan defineres, men bare i alternative navneromsidentifikatorer, og det kreves altså at navneromsidentifikator kan identifiseres entydig. Under parsing vil XML-prosessorer tilføye default navneromsidentifikator for det normale tilfellet at SEID-skjemaet er default navneromsidentifikator. Det ser imidlertid ikke ut til at det går an å bruke enumeration-restriksjoner på typen slik at metodenavnene begrenses av skjemaprosessoren til bare de definerte metodenavnene. Kommentaren i skjemaet viser hvordan det kunne vært gjort, men i så fall er det ikke mulig å tilføye nye navn i nye skjema. (Verdimengden for en simple type kan aldri utvides etter at den først er definert; det finnes ikke noen mekanisme tilsvarende substitution group for simple type.)
Den mest ryddige måten å håndtere dette på (mest i XML skjema-spesifikasjons ”ånd”) hadde vært å definere nye metoder som utvidelser eller restriksjoner (subtyper) av method, slik at ”<method name=”xyz”> hadde blitt ”<method xsi:type=”xyz”>. Dette hadde blitt et større avvik fra den danske standarden, og vil kanskje også stille litt større krav til XML-verktøyene som brukes for å parse og generere meldinger.

Typing av request og response-elementer
Request- og response-elementer inneholder vilkårlige lister av ”subjectAttribute” (1 til mange, hhv. 0 til mange). Det er ikke gjort noe forsøk i skjema på å begrense attributtlistene til bare de attributtene som er relevante for en gitt metode. Dette kunne gjøres ved å lage restriksjoner på request- og response-elementene. Se over for generelle kommentarer om dette.

transid-attributtet
Attributtet ”transid” benyttes for å koble response til tilhørende request, og kan også benyttes for å referere fra en XML-signatur til requesten eller responsen som er signert. Pga. det siste formålet er den definert med type XML ID. Dette sikrer også at verdiene er unike over en hel XML-melding. Det virker kanskje litt ikke-intuitivt at ikke transid er definert som IDREF (referanse til ID) i response, men request og response forekommer aldri i samme XML-melding, så det ville ikke ha noen hensikt.

Tegnkoding
Så lenge det ikke er definert noen attributter som inneholder noe annet enn ren ASCII er det ikke avgjørende hvilken tegnkoding som er spesifisert. Derfor er det ingen grunn til å la dette

dokument gi noen føringer på det, og det antas at de fleste aktuelle XML-parsere vil håndtere tegnkoding nokså transparent. Eksemplene og skjemaet i dette dokument benytter UTF-8, dette er standard i XML, og er mest generelt. UTF-8 er i tillegg det som benyttes når DN kodes tekstlig ihht. RFC 2253. UNID feltet kan inneholde samtlige tegn med unntak av tab, newline og return.

XML-signatur: profil
Det er ikke definert noen egen profil på XML-signatur-spesifikasjonen. Dette er i tråd med det som ellers er gjort mhp. sikkerhetsmekanismer i spesifikasjonen i SEID Oppslagstjeneste, hvor sikkerhet må reguleres i avtale mellom Tjenestetilbyder og Brukersted. Dette dokument tar ikke for seg detaljer i hvordan sikkerhetsmekanismene benyttes, men antar at verktøy som implementerer beste gjeldende praksis for de gjeldende standardene stort sett vil være mulig å konfigurere til å dekke behovene, slik at interoperabiliteten ikke blir skadelidende ved dette.

XML-signatur: hva dekkes
XML-signatur på request eller response er lagt under method (signature-elementet). På denne måten er det vanskelig å signere over method-elementet selv. Det er mulig å formulere et XPath-uttrykk som refererer method-elementet, men utelukker signature-elementet under det, slik at en ungår selvreferanse, men det er antakelig klokt å unngå kompliserte Xpath-uttrykk og begrense signaturene til å bruke enkel ID/IDREF-referanse til de signerte elementene. Alternativet ville være å legge et nytt nivå utenpå method og legge signaturen i det, altså en form for ”envelope”. I så fall er det antakelig best å bruke SOAP-envelope og legge på signatur ihht. WS-Security, det er liten grunn til å finne opp noe nytt som i prinsippet har samme funksjon som dette.
Sannsynligvis er det heller ikke noe stort behov for å signere over method-elementet. Tolkningen av en response bør neppe avhenge av method-navn. Kanonaliseringen (se nedenfor) sikrer at navneromsidentifikatoren blir med i det som signeres.

XML-kanonalisering
”Kanonalisering” sikrer at oktettstrømmen som sendes til signaturgenereringen har en veldefinert form som er robust i forhold til ikke-signifikante endringer i XML-meldingen som kan skje under transport, og som ellers ville ødelegge muligheten for validering. Samme kanonalisering gjentas før validering, og skal gi samme resultat selv om det er endringer i den mottatte XML-meldingen, f.eks. tilføyd eller fjernet ”whitespace”.
Håndteringen av navneromsidentifikatorer er spesielt viktig, siden disse påvirker tolkningen av hele meldingen.

Bilag E (Informativt): XML eksempler

Dette kapittelet beskriver, vha. eksempler, hvordan XML Meldingsforespørsler og XML Meldingssvar skal se ut. Det henvises for øvrig til Bilag C for full XML skjema spesifikasjon.

Meldingsforespørsler

Eksempel A1 hvor Brukersted sender forespørsel basert på én Unik Identifikator - UNID.

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
       xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/”
       name="getFnrFromUnid"
       signResponse="true"
       version="1.0">
  <request transid="R1112">
       <unid>9578-2000-123412</unid>
  </request>
</method>
```

Eksempel B1 hvor Brukersted sender forespørsel basert på ett sertifikat:

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
       xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/”
       name="getFnrFromCert"
       signResponse="true"
       version="1.0">
    <request transid="R1113">
       <cert>base64 encoded certificate</cert>
    </request>
</method>
```

Eksempel C1 hvor Brukersted sender flere Subjektforespørsler basert på UNID innen samme Meldingsforespørsel:

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
       xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/”
       name="getFnrFromUnid"
       signResponse="true"
       version="1.0">
  <request transid="R1113">
       <unid>9578-2000-302202</unid>
  </request>
  <request transid="R1114">
       <unid>9578-2000-301105</unid>
  </request>
</method>
```

Eksempel D1 hvor Brukersted sender flere Subjektforespørsler basert på sertifikat innen samme Meldingsforespørsel:

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
              xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/”
              name="getFnrFromCert"
              signResponse="true"
              version="1.0">
       <request transid="R1113">
              <cert>base64 encoded certificate</cert>
       </request>
       <request transid="R1114">
```

```
            <cert>base64 encoded certificate</cert>
        </request>
</method>
```

Dersom Meldingsforespørselen inneholder flere Subjektforespørsler som eksemplene C1 og D1 må alle Subjektforespørslene benytte samme input element (<*unid*> eller <*cert*>) i spørringen.

Meldingssvar

Eksempel A2 hvor Tjenestetilbyder svarer på Meldingsforespørsel A1:

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
       xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/“
       name="getFnrFromUnid"
       signedResponse="true"
       version="1.0">
  <response transid="R1112">
       <fnr>ddmmååннннн</fnr>
       <unid>9578-2000-123412</unid>
       <responseStatus code="00">text</responseStatus>
  </response>
</method>
```

Dersom Meldingsforespørselen inneholder flere Subjektforespørsler (ref. eksempel C1) vil det tilhørende Meldingssvaret inneholde flere Subjektsvar, dvs. flere response elementer.

Eksempel B2 hvor Tjenestetilbyder svarer på Meldingsforespørsel B1:

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
       xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/”
       name="getFnrFromUnid"
       signedResponse="true"
       version="1.0">
  <response transid="R1112">
       <fnr>ddmmååннннн</fnr>
       <cert>base64 encoded certificate</cert>
       <responseStatus code="00">text</responseStatus>
  </response>
</method>
```

Dersom Meldingsforespørselen inneholder flere Subjektforespørsler (ref. eksempel D1) vil det tilhørende Meldingssvaret inneholde flere Subjektsvar, dvs. flere response elementer.

Eksempel C2 hvor Tjenestetilbyder svarer på en Meldingsforespørsel B1 med feilstatus:

```
<?xml version="1.0" encoding="UTF-8" ?>
<method
       name="getFnrFromCert" version="1.0"
       xmlns="http://www.npt.no/seid/xmlskjema/oppslagstjeneste/">
    <response transid="R1113">
       <cert>base64 encoded certificate</cert>
       <responseStatus code="36"
          redirectURL="http://www.serviceprovider.com/authorize/">
         Klienten har ikke autorisert tilgang til informasjon om
         dette subjektet (denne personen).
       </responseStatus>
    </response>
</method>
```

Bilag F (Normativt): Returkoder for Frittstående Oppslagstjeneste

Alle Subjektsvar skal inneholde en returkode som beskriver resultatet av prosesseringen for den tilhørende Subjektforespørselen. Tosifrede returkoder større enn eller lik 10 indikerer feil i Subjekt- og/eller Meldingsforespørselen (request eller method ihht. Bilag C). Første siffer indikerer feilkodekategori, mens siste siffer angir ytterligere detaljer. Tjenestetilbyder KAN velge å returnere bare generelle returkoder med siste siffer lik 0. Et sett av fohåndsdefinerte returkoder finnes i tabellen nedenfor. Den enkelte Tjenestetilbyder kan fritt definere egne returkoder utover de som er angitt i tabellen.

Retur kode	Returtekst (eng)	Forklaring
00	OK	
01	Data not found	
1x	Invalid input	Ugyldig method eller request.
10	Invalid input	(hvis ingen av kodene nedenfor er dekkende)
11	XML parse error	Feil XML-format i method eller request.
12	Unknown or unsupported namespace	Angitt navneromsidentifikator (skjema) er ukjent eller støttes ikke av tjenesten.
13	Unknown or unsupported method	Metoden angitt i name-attributtet er ikke kjent eller støttet (f.eks. ukjent navneromsidentifikator).
14	Unknown or unsupported attribute	Attributt (subelement av request) er ikke kjent eller støttet.
2x	Authentication failed	Autentiseringen av forespørselen feilet
20	Authentication failed	(hvis ingen av kodene nedenfor er dekkende)
21	Signer certificate revoked	Sertifikatet som forespørselen er signert med er revokert.
22	Signer certificate invalid	Sertifikatet som forespørselen er signert med er tilbakekalt.
23	Authentication not valid	Autentiseringen er ikke gyldig, f.eks. feil passord eller nøkkel.
3x	Authorization failure	Tjeneste, metoden eller attributtene som er forespurt krever autorisasjon, men kontroll av autorisasjon feilet.
30	Authorization failure	(hvis ingen av kodene nedenfor er dekkende)
31	Not authenticated	Klienten er ikke autentisert.
32	Unknown user	Klienten er autentisert, men ikke en registrert bruker av tjenesten.
33	Access to service denied	Klienten har ikke autorisert tilgang til tjenesten.
34	Access to method denied	Klienten har ikke autorisert tilgang til metoden.
35	Access to attribute denied	Klienten har ikke autorisert tilgang til attributtet.
36	Access to subject denied	Klienten har ikke autorisert tilgang til informasjon om dette subjektet (denne personen).
90	System down, general failure	

Tabell 1 Definerte returkoder for Subjektsvar

Bilag G (Informativt): Utvidede XML forespørsler

Dette Bilaget beskriver, gjennom et eksempel, hvordan XML skjemaet i Bilag C kan utvides til å støtte Oppslagstjenester for utlevering av andre typer av informasjon enn Fødselsnummer. Tjenestetilbyder vil i så fall definere egne skjema som tas inn som utvidelser til det skjema som er spesifisert i Bilag C. Evt. nye skjema, med nye metodenavn, skal i så fall identifiseres gjennom eksplisitte navneromsidentifikatorer.

Eksempel:

```
<?xml version="1.0" encoding="UTF-8"?>
<method
            xmlns=”http://www.npt.no/seid/xmlskjema/oppslagstjeneste/”
            xmlns:lx=”http://leverandor.no/namespaces/extensions/”
            name="lx:getUnidFromPhone”
            signResponse=”true”
            version="1.0">
      <request transid=”R1112”>
            <lx:phone>90203045</lx:phone>
      </request>
  </method>
```

Eksempelet viser en tenkt utvidelse av en Meldingsforespørsel hvor Brukerstedet har angitt Sertifikatinnehavers telefonnummer, og ønsker å få oppgitt av Tjenestetilbyder den tilhørende Unike Identifikatoren.

Tjenestetilbydere SKAL besvare alle request-elementer med navneromsidentifikatorer de ikke gjenkjenner eller støtter med en returkode som angir feil (kode 10, 12 eller 14). Dersom method-elementet inneholder en xmlns-deklarasjon med en navneromsidentifikator som ikke gjenkjennes eller støttes, men dette prefikset ikke benyttes i enkelte av request-elementet, KAN Tjenestetilbyderen velge å besvare disse request-elementene på normal måte eller å besvare hele metodekallet med en returkode som angir feil (kode 10 eller 12). Method-elementer med verdier i name-attributtet som ikke gjenkjennes eller støttes besvares med returkode 10 eller 13.

Ved svar på forespørsler som benytter utvidede skjema benyttes eksplisitte navneromsidentifikatorer. Tjenestetilbyder kan også velge å returnere ekstra attributter (dvs. subelementer av response-elementet) for forespørsler definert i denne spesifikasjonen. Disse attributtene skal også identifiseres gjennom eksplisitte navneromsidentifikatorer. Brukersted KAN ignorere attributter definert i ukjente navneromsidentifikatorer. Brukersteder som kun støtter denne spesifikasjonen KAN ignorere alle attributter med eksplisitt navneromsidentifikatorprefiks.