SEID-Prosjektet

Leveranse oppgave 1

Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater

Versjon 1.02

Status: Godkjent

Dato: 03.02.2005

HISTORIKK

Dato	Versjon	Utført av	Kommentar
23.06.04	1.0	PK	Dokumentet godkjent av SEID-prosjektets styringsgruppe.
07.09.04	1.01	PK	Dokumentet oppdatert med tidspunkt for første årlige revisjon (kap.4.4), samt navn og kontaktinfo for ansvarlig dokumentforvalter (kap. 4.1). Fotnote nr.6 og nr.13 er også oppdatert.
03.02.05	1.02	PK	Oppdatert kap.4.1 og kap.4.4.

INNHOLDSFORTEGNELSE

1 BEGREPER OG FORKORTELSER 4

2 REFERANSER 7

3 INNLEDNING 9

3.1 BAKGRUNN 9
3.2 ARBEIDSGRUPPENS MANDAT OG MEDLEMMER 9
3.3 FORMÅL, MÅLGRUPPE, OMFANG OG AVGRENSNINGER 10
3.4 DOKUMENTETS STRUKTUR 11

4 DOKUMENTETS STATUS OG FORVALTNING 12

4.1 ANSVARLIG DOKUMENTFORVALTER 12
4.2 STATUS OG TILGJENGELIGHET 12
4.3 OVERGANGSORDNINGER 12
4.4 VEDLIKEHOLD 12

5 ANBEFALT NORSK PROFIL FOR PERSONSERTIFIKATER 12

5.1 SAMORDNET BRUK AV SERIALNUMBER ATTRIBUTTET I SUBJECT-FELTET 21
5.1.1 Bakgrunn 21
5.1.2 Krav til bruk av serialNumber 21
5.1.3 Syntaks og semantikk 22
5.2 BRUK AV OPPSLAGSTJENESTER 22

6 ANBEFALT NORSK PROFIL FOR VIRKSOMHETSSERTIFIKATER 23

BILAG A: NASJONALT UNIKE UTSTEDERIDENTIFIKATORER 27

BILAG B (INFORMATIVT) : KEY USAGE 29

BILAG B (INFORMATIVT) : KEY USAGE 29

BILAG C (INFORMATIVT) : AVVIK FRA AKTUELLE STANDARDER OG REFERANSEPROFILER33

1 Begreper og forkortelser

Begrep	Beskrivelse
Ansattsertifikat	Et ansattsertifikat er et personsertifikat. Sertifikatet attesterer at det finnes en relasjon mellom en identifisert virksomhet og en entydig identifisert person innenfor denne virksomheten. Relasjonen vil typisk være et ansettelsesforhold, men dette er ikke et krav.
Attributt	Se Sertifikatattributt.
Autentiserings-sertifikat	Et sertifikat som inneholder offentlig nøkkel som er tilegnet bruk for autentisering (for bekreftelse av autentisitet).
Kritisk	Enhver sertifikatutvidelse som benyttes i et sertifikat kan markeres som kritisk eller ikke-kritisk. Kritisk innebærer at sertifikatmottaker er nødt til å forstå feltet for at sertifikatet skal aksepteres. Tilsvarende kan en sertifikatmottaker velge å se bort fra sertifikatutvidelser som ikke er merket kritiske.
Krypteringssertifikat	Et sertifikat som inneholder offentlig nøkkel som er tilegnet bruk for kryptering (sikre konfidensialitet) av data.
Kvalifisert sertifikat	Et personsertifikat som oppfyller de krav som som lov om elektronisk signatur [10] stiller til et slikt sertifikat. Et sertifikat som er tilegnet bruk for avansert elektronisk signatur vil kunne være kvalifisert ihht. lovens virkeområde. Et sertifikat som utelukkende er utstedt til andre bruksområder enn avansert elektronisk signatur vil ikke falle under lovens virkeområde.
Kvalifisert signatur	En avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem (se for øvrig lov om elektronisk signatur [10]).
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 norske folkeregisteret.
Profesjonsertifikat	Et profesjonssertifikat er et personsertifikat som knytter en person til et bestemt yrke/utdanning og til en eventuell autorisasjon eller godkjenning fra en myndighet eller en organisasjon.
SEID-prosjektet	Prosjektet som har produsert dette dokumentet. Prosjektets fullstendige navn er “Samarbeidsprosjekt om eID og eSignatur”.
Sertifikat / Digitalt sertifikat / Elektronisk sertifikat	Et sertifikat er en form for elektronisk identitetsbevis. Sertifikater kan anvendes bl.a. som elektronisk legitimasjon eller for å validere en elektronisk signatur.
Sertifikatattributt	Et sertifikatfelt kan inneholde forskjellige sertifikatattributter, hver med sin verdi.

Begrep	Beskrivelse
Sertifikatfelt	Et sertifikat er inndelt i ulike sertifikatfelt med ulike typer av sertifikatinformasjon. Standarden for X.509v3 sertifikater [3] deler inn feltene i basis sertifikatfelter og sertifikatutvidelser (certificate extensions).
Sertifikatinnehaver	Den kunden (person/virksomhet) sertifikatet er utstedt til i henhold til sertifikatpolicy og som er innehaver av den private nøkkelen (jfr. 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 (jfr. 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.
Sertifikatutsteder	En sertifikatutsteder som omtalt i dette dokumentet vil være: • en juridisk person, dvs. et rettssubjekt som ikke er en fysisk person, i vårt 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.
Sertifikatutvidelse (certificate extension)	Betegnelse for sertifikatfelter som ikke er basis sertifikatfelter fra den opprinnelige X.509-versjonen. Sertifikatutvidelser omfatter både standard sertifikatutvidelser (standard certificate extensions) fra nyere versjoner av samme standard, og private sertifikatutvidelser (private certificate extensions). Private utvidelser er definert i standarder fra andre organisasjoner, men kan også tilordnes og defineres av enkeltutstedere eller på nasjonalt nivå.
Signeringssertifikat	Et sertifikat som inneholder offentlig nøkkel som er tilegnet brukt for å verifisere digitale signaturer som knytter innholdet av det som er signert, til personen som står som innehaver (subject) av nøkkelen.
Unik identifikator	En kombinasjon av siffer/tegn som legges inn i et personsertifikat og som, gjennom knytning til et fødselsnummer i det norske folkeregisteret, entydig identifiserer personen som er sertifikatinnehaver. Personprofilen i kap.5 definerer syntaks for en slik unik identifikator.
Utsteder	Se sertifikatutsteder.

Begrep	Beskrivelse
Virksomhetssertifikat	Et virksomhetssertifikat har som oppgave å identifisere en juridisk person, dvs en virksomhet som er registrert i det norske enhetsregisteret. Bruker av den private nøkkel assosiert med sertifikatet kan være en fysisk person autorisert av foretaket eller en automatisert prosess under foretakets kontroll, for eksempel en server.

Forkortelse	Beskrivelse
CA	Certification Authority
CRL	Certificate Revocation List
eID	Elektronisk ID
ETSI	European Telecommunications Standards Institute
ID	Identitet
IETF	Internet Engineering Task Force
ISO	International Organization for Standardisation
NOU	Norsk Offentlig Utredning
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PID	Personspesifikke Identifikationsnumre (dansk)
PKI	Public Key Infrastructure
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SIM	Subscriber Identification Module
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TS	Technical Standard
URI	Uniform Resource Indentifier

2 Referanser

[1] PKI Forum, Strategi for en samfunnsinfrastruktur for elektronisk signatur og elektronisk ID i Norge, juni 2002.

[2] PKI Forum, Handlingsplan, Rapport fra ”Midlertidig Prosjektgruppe” for oppfølging av PKI strategien, februar 2003.

[3] ITU-T, Recommendation X.509 (2000):”Information Technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks”.

[4] ETSI TS 101 862, “Qualified Certificate Profile”, v1.3.1, mars 2004[1].

[5] IETF RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and (CRL) Profile”, april 2002.

[6] IETF RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, januar 1999.

[7] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", mars 2004[2].

[8] ETSI TS 102 280, “X.509 V3 Certificate Profile for Certificates issued to Natural Persons” ,v1.1.1, mars 2004.

[9] Arbeids- og administrasjonsdepartementet, ”Uten penn og blekk”, NOU 2001:10, mars 2001.

[10] Lov 15. juni 2001 nr. 81 om elektronisk signatur.

[11] JTC/SC6 N12599, Recommendation X.509 (2000) | ISO/IEC 9594-8:2000, Draft Technical Corrigendum 6.

[12] Nærings- og handelsdepartementet, “eNorge 2005”, mai 2002.

[13] Dansk standard DS 843-1, ”Personspesifikke identifikationsnumre (PID)”, desember 2003.

[14] ISO 15782-1, Certificate Management for Financial Services, pt. 1 Public Key Certificates.

[15] ISO 15782-2, Certificate Management for Financial Services, pt. 2 Certificate Extensions.

[16] ISO CD 21188, Public Key Infrastructure Policy and Practices Framework.

[1] Dette dokumentet erstatter ETSI TS 101 862 v1.2.1 fra juni 2001.
[2] Dette dokumentet erstatter RFC 3039.

[17] EU direktiv 1999/93/EC, om et felles rammeverk for elektronisk signatur, desember 1999.

[18] ETSI SR 002 176: “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures”, v1.1.1, mars 2003.

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 [12].

3.2 Arbeidsgruppens mandat og medlemmer

Dette dokument inneholder SEID-prosjektets første leveranse og er basert på følgende oppgavedefinisjon og mandat:

”Med utgangspunkt i relevante internasjonale standarder, utarbeide en norsk profil for personsertifikater som skal dekke bruken av både kvalifiserte sertifikater og sertifikater med tilsvarende tillit- og kvalitetsnivå. I tillegg skal en norsk profil for virksomhetssertifikater utarbeides”.

Arbeidsgruppen har bestått av:

- Pål Kristiansen, UniBridge AS (innleid prosjektleder og leder av gruppen)
- Geir Mork Knutsen, BankID Samarbeidet (dokumentets redaktør)
- Rune Hagen, BankID Samarbeidet
- Atle Dingsør, Buypass AS
- Wenche Grelland, DnB NOR ASA
- Lise Blix, DnB NOR ASA
- John Bothner, Microsoft Norge AS
- Lise Marie Pettersen, NetCom AS
- Nils Inge Brurberg, Nordea Bank Norge ASA
- Sven Christiansen, Posten Norge AS
- Åsmund Skomedal, Posten Norge AS og Telenor ASA
- Ståle Gullbrekken, SpareBank 1 Gruppen AS
- Tor Hjalmar Johannessen, Telenor ASA
- Arve Moss, Telenor ASA

En egen høringsprosess for kvalitetssikring av resultatene er gjennomført av alle 16 aktørene i SEID-prosjektet samt av følgende eksterne referansefora:

- Post- og teletilsynet
- Koordineringsorganet for PKI i offentlig sektor (har formidlet høringssvar fra Helsedepartementet og Rikstrygdeverket).

I tillegg har Nærings- og Handelsdepertementet[3] formidlet høringssvar fra NSM (Nasjonal Sikkerhetsmyndighet), KITH (Kompetansesenter for IT i helsevesenet) og Patentstyret.

3.3 Formål, målgruppe, omfang og avgrensninger

Formål

Det finnes i dag flere standarder, både fra ETSI og IETF, som profilerer X.509v3 [3] sertifikater. Utfordringen med de internasjonalt standardiserte profilene er at de ikke alltid er detaljerte eller presise nok til å unngå ulike tolkninger av de samme standardene. Internasjonale profilstandarder alene vil derfor ikke nødvendigvis garantere enkel interoperabilitet og samtrafikk på tvers av løsninger i markedet. Videre ser man at ytterligere profilering av disse standardene ofte er nødvendig for å dekke spesielle nasjonale og lokale behov.

Formålet med dette dokumentet er å beskrive sertifikatprofiler, basert på eksisterende internasjonale profilstandarder, som skal bidra til harmonisering av både eksisterende og kommende løsninger i det norske markedet. En slik harmonisering skal videre bidra til å forenkle samvirke mellom løsninger fra ulike utstedere. I tillegg skal de gi sertifikatmottakere større forutsigbarhet når det gjelder hvilken informasjon de kan forvente å finne i sertifikater fra norske sertifikatutstedere, hvordan denne informasjonen skal tolkes og hvilken kvalitet denne informasjonen kan forventes å ha.

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 beskriver én norsk sertifikatprofil til bruk for personsertifikater og én norsk sertifikatprofil til bruk for virksomhetssertifikater.

Profilen for personsertifikat er laget for sertifikater utstedt til fysiske personer, herunder kvalifiserte sertifikater. Profilen er anvendelig for sertifikater som entydig identifiserer personer registrert i det norske folkeregisteret.

Profilen for virksomhetssertifikat er laget for sertifikater utstedt til virksomheter i Norge. Profilen er anvendelig for sertifikater som kan knyttes til en juridisk person som er registrert i Enhetsregisteret i Norge.

Profilene skal kunne dekke aktuelle behov innenfor et bredest mulig funksjonelt anvendelsesområde. Dette inkluderer sertifikater til bruk for autentisering (autentiseringssertifikater), konfidensialitet (krypteringssertifikater) og signaturverifikasjon (signeringssertifikater). Profilene åpner for at ett enkelt sertifikat skal kunne dekke flere av disse anvendelsesområdene samtidig.

[3] Nå Moderniseringsdepartementet.

Avgrensninger

Arbeidsgruppen har ikke hatt som målsetning å detaljspesifisere sertifikatprofiler til bruk for ansattsertifikater og profesjonssertifikater. Profilen for personsertifikater bør likevel kunne utgjøre en basis også for nevnte sertifikattyper i den grad informasjon, som har som formål å entydig identifisere sertifikatinnehaver, også inngår i sertifikatene.

Ved utarbeidelse av de anbefalte profilene er det i stor grad tatt utgangspunkt i internasjonale referanseprofiler fra IETF og telekommunikasjonsbransjens standardiseringsorgan ETSI. Andre bransjespesifikke standarder og referanseprofiler har ikke i samme grad vært benyttet, f.eks. standarder relevant for banknæringen referert i kap 5.

3.4 Dokumentets struktur

Kapittel 4 tar for seg regler for vedlikehold av dokumentet. I tillegg beskrives nærmere hvilke overgangsordninger som gjelder.

Kapittel 5 og 6 beskriver anbefalt norsk profil for henholdsvis personsertifikater og virksomhetssertifikater.

Bilag A er et bilag som beskriver tildelte nasjonalt unike utstederidentifikatorer til bruk i personprofilen (se kap. 5.1.3).

Bilag B er et informativt bilag som begrunner SEID-prosjektets tilnærming når det gjelder bruk av ”key usage” feltet i sertifikatprofilene.

Bilag C er et informativt bilag som beskriver hvilke avvik som er gjort i de anbefalte sertifikatprofilene i forhold til krav/anbefalinger gitt av relevante profilstandarder og referanseprofiler som disse baserer seg på.

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:

Eskil Elness, e-post: seid@npt.no

4.2 Status og tilgjengelighet

Dette dokumentet definerer sertifikatprofiler som anbefales benyttet av norske sertifikatutstedere.

Dokumentet inneholder offentlig tilgjengelig informasjon og kan distribueres fritt.

4.3 Overgangsordninger

Enkelte av SEID prosjektets aktører representerer sertifikatutstedere som allerede har operative løsninger i markedet. For å få til størst mulig grad av harmonisering av de ulike løsningene på sikt har aktørene funnet det nødvendig å gå sammen om profilanbefalinger som på enkelte områder ikke er sammenfallende med dagens løsninger. På disse områdene har det vært nødvendig å innføre fornuftige overgangsordninger som tillater avvik i en nærmere angitt overgangsperiode.

Hvilke avvik dette gjelder og hvilke overgangsperioder som gjelder for disse er dokumentert som en del av det aktuelle sertifikatfelt og profil i kapittel 5 og 6.

4.4 Vedlikehold

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 dokumentvedlikehold er regulert gjennom en egen forvaltningsinstruks utarbeidet av SEID-prosjektet.

5 Anbefalt norsk profil for personsertifikater

Dette kapittelet beskriver en norsk sertifikatprofil til bruk for personsertifikater utstedt til fysiske personer som enten er norske statsborgere eller har oppholdstillatelse i Norge. Profilen er anvendelig for alle personsertifikater, herunder kvalifiserte sertifikater, hvor sertifikatet inneholder informasjon som enten direkte eller indirekte er knyttet til personens identitet i det norske folkeregisteret. I den grad det stilles spesielle profilkrav til kvalifiserte sertifikater, og

som det ikke er naturlig å knytte til alle personsertifikater, er dette eksplisitt påpekt og håndtert i profilen.

Den anbefalte profilen er basert på ETSI TS 102 280 [8] som igjen er basert på ETSI TS 101 862 [4] for kvalifiserte sertifikater spesielt og på Internett standardene RFC 3280 [5] / RFC 2459 [6][4] og RFC 3739 [7] for generisk profilering av X.509v3 sertifikater [3] generelt. I den grad den anbefalte norske profilen avviker fra en eller flere av de ovennevnte standardene er dette eksplisitt beskrevet i Bilag C.

Foruten ovennevnte standarder finnes det bransjestandarder som enkelte utstedere vil være nødt til å forholde seg til. Som eksempel har banknæringen i Norge forpliktelser overfor internasjonale standardiseringsorgan for bank/finans gjennom blant annet ISO 15782-1 [14], ISO 15782-2 [15] og ISO CD 21188 [16]. Dersom det oppdages avvik mellom anbefalt personprofil og relevante bransjestandarder for norske utstedere bør disse rapporteres til ansvarlig dokumentforvalter (se kap.4.1) for håndtering i forbindelse med neste fastsatte profilrevisjon (se kap.4.4).

Dette kapittelet tar kun for seg sertifikatfelter hvor den anbefalte norske profilen inneholder en ytterligere profilering av, evt. avvik fra, nevnte standarder. Dette gjelder de 10 sertifikatfeltene listet i tabellen nedenfor:

Basis sertifikatfelter	Sertifikatutvidelser
• Issuer • Subject • Subject Public key Info	• Key Usage • Extended Key Usage • Subject Alternative Name • CRL Distribution Point • Authority Information Access • Subject Information Access • Qualified Certificate Statement

Sertifikatfelter som ikke er eksplisitt profilert i dette dokumentet anses å være tilstrekkelig profilert gjennom eksisterende standarder som den anbefalte profilen baserer seg på. For disse sertifikatfeltene anbefales det at utstedere i størst mulig grad følger ETSI TS 102 280 [8] av hensyn til interoperabilitet og samtrafikk.

[4] RFC 3280 er arvtageren til RFC 2459. Årsaken til at begge RFCene refereres her er at enkelte operative løsninger fremdeles antas å følge RFC 2459. I den grad disse avviker fra hverandre anbefales det å følge RFC 3280 selv om dette ikke er et krav.

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Issuer	**M**	**Ikke relevant – Gjelder kun for sertifikat-utvidelser**	**Normalt skal verdien i dette feltet entydig identifisere den juridiske person som er faktisk utsteder[5] av sertifikatet**. **For personsertifikater[6] som er utstedt innenfor en avtalebasert infrastruktur, vil det være mulig å fravike ovennevnte og benytte feltet til i stedet å entydig identifisere den juridiske person som er ansvarlig for det tekniske CA system.[7]** **Et subsett av følgende attributter skal anvendes og være nok til å sikre entydig identifikasjon av juridisk person:** • `countryName(c);` • `organizationName(o);` • `organizationalUnitName(ou);` • `serialNumber(sn);` • `commonName(cn);` **Andre felter kan anvendes i tillegg, men skal ikke være nødvendige for å sikre entydig identifikasjon av utsteder.** **Følgende attributt er obligatorisk:** • `countryName(c)` **Attributtet** `countryName` **skal angi landet hvor utsteder er etablert. For utstedere etablert i Norge skal verdien "**`NO`**" benyttes.**	**Norsk lov om elektronisk signatur sier at det skal være mulig for en fysisk person (dvs. ikke juridisk person) å stå som utsteder av kvalifiserte sertifikater. Bruk av "issuer" feltet til å identifisere en fysisk person er mao. lovlig men ikke eksplisitt dekket av denne profilen.** **Entydig identifikasjon av norske utstedere skal oppnås på en av følgende måter:** • **Ved bruk av organisasjonsnavnet som formelt registrert i Enhetsregisteret i Brønnøysund.** • **Ved bruk av organisasjonsnummer ihht. Enhetsregisteret i Brønnøysund sammen med organisasjonsnavn. I dette tilfellet kan evt. vanlig brukt navn på bedriften tillates.** • **I en overgangsperiode frem til 31.12.2008 er det tillatt å benytte vanlig navn på bedriften, selv uten bruk av organisasjonsnummer.** **Entydig identifikasjon av utstedere som ikke er etablert i Norge er ikke dekket av felles norsk profil.** **Organisasjonsnavnet skal som utgangspunkt legges i attributtet** `organizationName`**. I en overgangsperiode frem til 31.12.2008 kan organisasjonsnavnet alternativt ligge i attributtet** `domainComponent`**.** **Dersom organisasjonsnummer angis skal dette enten legges**: 1. **alene i attributtet** `serialNumber`**, eller** 2. **alene i attributtet** `organizationalUnitName`**, eller** 3. **sammen med organisasjonsnavn i attributtet** `organizationName` **(f.eks. <org.navn> - <org.nr>)** **Attributtet** `commonName` **kan benyttes for å skille mellom ulike sertifikatklasser og/eller CA systemer innenfor samme utstederorganisasjon.**

[5] Se kap.1 for definisjon av begrepet utsteder.
[6] Det forutsettes at Post- og teletilsynet uttaler seg om hvorvidt en slik bruk av issuer-feltet kan benyttes for utstedelse av kvalifiserte sertifikater.
[7] ETSI TS 101 862[4], som er en normativ anbefaling for kvalifiserte sertifikater, støtter ikke på dette tidspunkt denne bruken av issuer-feltet.

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Subject	**M**	**Ikke relevant – Gjelder kun for sertifikat-utvidelser**	**Verdien i dette feltet skal entydig innen Norge identifisere den fysiske person som er sertifikatinnehaver. Entydig identifikasjon innebærer at verdien skal ha en entydig kobling til sertifikatinnehavers 11-sifrede fødselsnummer/D-nummer[8] som registrert i det norske folkeregisteret.** **Følgende attributter er obligatoriske:** • `countryName(c)` • `serialNumber(serialNumber)`**, alternativt kan** `organizationalUnitName(ou)` **i stedet benyttes i en overgangsfase (se under).** • `commonName(cn)` **Andre attributter kan benyttes i tillegg, men skal ikke være nødvendige for å sikre entydig identifikasjon av sertifikatinnehaver.** **Informasjonsinnholdet i** `serialNumber` **attributtet alene skal entydig identifisere sertifikatinnehaver, dvs. at attributtet skal inneholde én av følgende informasjonselementer:** **a) sertifikatinnehaverens nasjonale fødselsnummer/D-nummer, eller** **b) en alternativ nasjonalt[9] unik identifikator som entydig mapper til sertifikatinnehaverens fødselsnummer/D-nummer, eller** **c) en utstederspesifikk unik identifikator som entydig mapper til personens fødselsnummer/D-nummer, også på tvers av ulike utstederdomener.** **I en overgangsperiode frem til 31.12.07 er det tillatt å ha tilsvarende informasjonsinnhold i attributtet** `organizationalUnitName`**.**	**Attributtet** `countryName` **skal inneholde verdien "NO" for sertifikater utstedt av norske utstedere.** **Dersom attributtet** `organizationName` **benyttes skal dette primært angi navnet på en organisasjon som sertifikatinnehaver er assosiert med. Hvilken type assosiasjon det er snakk om bør fremgå av utsteders sertifikatpolicy.** **For ansattsertifikater skal** `organizationName` **benyttes til å angi navn og evt. organisasjonsnummer på den organisasjon som sertifikatinnehaver er assosiert med.** **Kapittel 5.1 beskriver nærmere krav til syntaks og semantikk for informasjonen i** `serialNumber` **(evt.** `organizationUnitName`**) attributtet. I en overgangsperiode frem til 31.12.07 kan utsteder velge å benytte syntaks og semantikk som avviker fra dette. En sertifikatmottager skal forholdsvis enkelt kunne identifisere om en slik egendefinert syntaks er benyttet eller ikke (se kap.5.1.3).** **Dersom utsteder velger en sertifikatløsning hvor fødselsnummer ikke angis direkte i sertifikatet er det et krav at utstederens sertifikatpolicy kan garantere integritet og sporbarhet for knytningen mellom unik identifikator og fødselsnummer. Denne garantien vil måtte gjelde så lenge det aktuelle sertifikat skal kunne valideres.**

[8] D-nummer er et nummer, tilsvarende norsk fødselsnummer, som tildeles utenlandske statsborgere med midlertidig oppholdstillatelse i Norge.
[9] Bruk av nasjonale identifikatorer på tvers av sertifikatutstedere vil kreve etablering av en nasjonal løsning for tildeling av disse.

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Subject forts.			`commonName` **attributtet skal inneholde én av følgende tre informasjonselementer:** **a) sertifikatinnehaverens navn.** **b) "**`PSEUDONYM`**" for å angi at sertifikatet ikke inneholder sertifikatinnehaverens navn men i stedet inneholder et pseudonym i attributtet** `pseudonym`**.** **c) "**`NO NAME`**" for å angi at sertifikatet hverken inneholder sertifikatinnehaverens navn eller et pseudonym.**	**Dersom sertifikatinnehaverens navn legges inn i sertifikatet (alternativ a) skal én av følgende syntaksalternativer følges:** **a) "*Fornavn Mellomnavn Etternavn*", med mellomrom mellom navnekomponentene.** **b) "*Etternavn, Fornavn Mellomnavn*", med komma etter etternavnet og med mellomrom mellom navnekomponentene** **I en overgangsperiode frem til 31.12.2007 vil også "*Etternavn Fornavn Mellomnavn*" (uten komma etter etternavnet) være tillatt syntaks.** **For øvrig skal det framgå av utsteders sertifikatpolicy hvilke kvalitetskrav som er lagt til grunn når det gjelder grad av samsvar mellom dette navnet og personens navn i det norske folkeregister.** **Bruk av pseudonymer (alternativ b) er tillatt. I så fall skal pseudonymet legges i attributtet** `pseudonym`**. For kvalifiserte sertifikater hvor sertifikatinnehavers navn ikke legges i** `commonName` **er det et krav at et pseudonym legges i attributtet** `pseudonym`**, ref. [10].**
Subject Public Key Info	**M**	**Ikke relevant – Gjelder kun for sertifikat-utvidelser**	**Bruk av dette feltet skal som utgangspunkt følge de krav og anbefalinger som er definert i ETSI 102 280 [8].** **For kvalifiserte sertifikater stilles det som et ekstra krav, i tråd med ETSI SR 002 176 [18], at den offentlige nøkkelen skal ha en minimum nøkkellengde tilsvarende 1024 bits RSA. For øvrig anbefales det for signeringssertifikater generelt at ETSI SR 002 176 [18] følges når det gjelder krav til nøkkelkvalitet.**	

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Key Usage	**M**	**Valgfritt - Anbefales satt til kritisk ihht. [5] og [8]**	**Aktuelle kombinasjoner av key usage verdier for det enkelte sertifikat skal følge de generelle retningslinjene for anvendelse gitt av RFC 3280 [5], med følgende presiseringer:** **For at et nøkkelpar skal kunne anvendes for avanserte elektroniske signaturer, herunder kvalifiserte elektroniske signaturer, skal én av følgende tre alternative key usage kombinasjoner inngå i sertifikatet, enten alene eller sammen med andre key usage verdier:** - `nonRepudiation`[10] - `digitalSignature`[11] - `nonRepudiation` **og** `digitalSignature` **sammen.** **For sertifikater som benyttes til å utveksle symmetriske nøkler ifm. kryptering skal** `keyEncipherment` **opsjonen benyttes, enten alene eller sammen med andre key usage verdier.** **For sertifikater som benyttes til kryptering av data skal** `dataEncipherment` **opsjonen benyttes, enten alene eller sammen med andre key usage verdier.** **Denne profilen overlater til utsteder fritt å velge aktuelt/aktuelle bruksområde(r) for det enkelte nøkkelpar og gjennom dette aktuelle key usage kombinasjoner for det tilhørende sertifikat. Eneste unntak er den lovregulerte begrensningen som gjelder for kvalifiserte sertifikater og bruk av nøkkelarkiv[12].**	**ETSI TS 102 280 [8], som vil være en normativ anbefaling for bla. kvalifiserte sertifikater, har lagt seg på en mer restriktiv linje enn det denne profilen gjør. Se Bilag B for detaljer.** **Tidligere praksis i Europa har til dels også vært enda strengere enn ETSI TS 102 280 ved å kreve key usage verdien** `nonRepudiation` **satt alene i sertifikater som benyttes til signaturformål med såkalt "ikke-benekting", herunder kvalifiserte sertifikater.** **I Bilag B argumenteres det for at en slik tilnærming i enkelte tilfeller kan virke uhensiktsmessig streng og dermed hvorfor en mer fleksibel tilnærming er valgt for denne norske profilen.** **For utstedere som har behov for å sikre seg at løsningene de velger også skal aksepteres og anvendes på europeisk basis anbefales det inntil videre å følge ETSIs krav og anbefalinger [8].** **Utstedere bør være oppmerksom på at ulike hyllevare applikasjoner vil kunne stille spesielle krav til key usage verdier i sertifikater. Utstedere er nødt til å ta hensyn til dette ved valg av hensiktsmessige key usage verdier innenfor denne sertifikatprofilen.**

[10] I et utkast til Technical Corrigendum 6 til Recommendation X.509 (2000) [11] er det foreslått å benytte navnet contentCommitment i stedet for nonRepudiation for denne key usage verdien.

[11] ETSI 102 280 [8] tillater ikke dette alternativet benyttet dersom sertifikatet er et signeringssertifikat hvor den offentlige nøkkelen skal anvendes til å validere kontrakter/transaksjoner og hvor den som foretar signeringen vil kunne bli stilt til ansvar for signaturen (dvs. formål "ikke-benekting"). Se Bilag B for detaljer.

[12] For nøkkelpar som anvendes for krypteringsformål kan enkelte utstedere tilby nøkkelarkiv som en ekstratjeneste, dvs. en tjeneste hvor utsteder oppbevarer en sikret kopi av sertifikatinnehavers private nøkkel. For kvalifiserte sertifikater sier lov om elektronisk signatur [10] at utsteder ikke har lov til å oppbevare eller kopiere sertifikatinnehaverens signaturfremstillingsdata (dvs. private nøkkel).

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Extended Key Usage	**O**	**Nei**	**Bruken av dette feltet er generelt beskrevet i RFC 3280[5].**	**En del applikasjoner benytter dette feltet til å avgjøre lovlige anvendelsesområder for det aktuelle sertifikat. Dette feltet anvendes da i tillegg til key usage feltet.**
Subject Alternative Name	**O**	**Nei**	**Bruken av dette feltet er generelt beskrevet i RFC 3280[5].**	**Enkelte applikasjoner/applikasjonsanvendelser stiller spesielle krav til anvendelse og innhold i dette feltet.** **Et eksempel er lagring av en eller flere e-post adresser som er knyttet til sertifikatinnehaver til bruk for S/MIME klienter.** **S/MIME v2 standarden, S/MIME v2 klienter samt en del e-post klienter med tidlig S/MIME v3 støtte krever at e-post adresser inkluderes i sertifikater som skal benyttes for signering av e-post. Dette gjelder bla. tidligere versjoner av Microsoft Outlook og Microsoft Outlook Express. S/MIME v3 standarden og en del nyere e-post klienter som støtter S/MIME v3 har fjernet dette som et absolutt krav og lar bruk av dette feltet i stedet være en opsjon.** **Denne profilen sier ingenting om hvilke kvalitetskrav som er lagt til grunn for å verifisere at e-postadresser som benyttes faktisk eksisterer og er tilknyttet sertifikatinnehaver. Det bør framgå av utsteders sertifikatpolicy hvilke kvalitetssjekker som er foretatt.**
CRL Distribution Point	**O/M (se komm.felt)**	**Nei**	**Dette feltet kan benyttes for å legge inn peker (URI-referanse) til en katalogtjeneste hvor tilbaketrekkingslister (CRLer) ligger lagret.**	**Dette feltet skal benyttes dersom utsteder (evt. representant for utsteder) er tilbyder av en CRL tjeneste. Minimum ett av feltene "CRL Distribution Point" eller "Authority Information Access" skal benyttes.**
Authority Information Access	**O/M (se komm.felt)**	**Nei**	**Dette feltet kan benyttes til å angi peker (URI-referanse) til en sertifikatstatus-tjeneste (eks. OCSP tjeneste) som sertifikatmottaker skal kunne benytte for å sjekke revokeringsstatus for sertifikatet.**	**Dette feltet skal benyttes dersom utsteder (evt. representant for utsteder) er tilbyder av en sertifikatstatus-tjeneste. Minimum ett av feltene "CRL Distribution Point" eller "Authority Information Access" skal benyttes.**
Subject Information Access	**O**	**Nei**	**Dette feltet kan benyttes til å angi peker (URI-referanse) til en oppslagstjeneste som på bakgrunn av informasjon i sertifikatet kan utlevere fødselsnummer eller tilsvarende identitetsinformasjon knyttet til sertifikatinnehaver.**	**Dette feltet kan benyttes dersom serialNumber feltet inneholder en unik identifikator som er forskjellig fra fødselsnummer, dvs. identifikator av type 2 eller 3 i kap. 5.1.3** **Bruk av dette feltet er ikke nødvendig dersom "Authority Information Access" feltet allerede peker til en sertifikatstatus-tjeneste som har en slik oppslagstjeneste integrert.**

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Qualified Certificate Statement	**O**	**Valgfritt**	**ETSI TS 101 862 [4] profilerer fire uavhengige anvendelser som alle kan være aktuelle for dette feltet. Tre av disse anses som spesielt viktige og er derfor gjengitt her.** **Kvalifiserte sertifikater som utstedes etter 30.juni 2005 skal inkludere i dette feltet en OID som eksplisitt forteller at sertifikatet er utstedt ihht. EU-direktivet som implementert i det landet hvor utsteder opererer. Se ETSI TS 101 862 [4] for nærmere detaljer.** **For kvalifiserte sertifikater, dersom det i utsteders sertifikatpolicy er lagt en begrensning på anvendelse av sertifikatet gjennom et verditak på enkelttransaksjoner, skal OID for denne begrensningen samt beløpets størrelse eksplisitt legges inn i dette feltet[13]. Se ETSI TS 101 862 [4] for detaljer.** **For sertifikater hvor utsteder kan gå god for at den private nøkkelen, som tilhører den offentlige nøkkelen i sertifikatet, er lagret i et såkalt sikkert signaturfremstillingssystem[14] kan dette angis i sertifikatet ved å inkludere en OID ihht. ETSI TS 101 862 [4].**	

Andre krav og anbefalinger:

- Bruk av andre sertifikatutvidelser enn de som er listet i tabellen over, reguleres av den enkelte utsteder. Det eneste kravet er at dersom slike sertifikatutvidelser benyttes så bør disse settes til å være ikke-kritiske.
- For utsteders signatur på personsertifikatene anbefales en styrke tilsvarende 2048 bit for RSA nøkler.

[13] Dette er et krav som stilles i lov om elektronisk signatur [10].
[14] §9 i lov om elektronisk signatur [10] danner grunnlag for godkjenning av sikre signaturfremstillingssystem.

5.1 Samordnet bruk av serialNumber attributtet i subject-feltet

5.1.1 Bakgrunn

- Den foreslåtte profilen tillater mange attributter i et subject-feltet. Hvilke attributter som velges er forskjellig fra utsteder til utsteder. Flere attributter kan være teknisk motivert og ikke nødvendige for å identifisere personen. Det eksisterer mange forskjellige løsninger i dagens marked. Det er behov for at en person identifiseres på samme måte på tvers av utstedere.
- For at sertifikatmottakere lett skal kunne knytte et sertifikat til en bestemt person, ønskes et klart definert attributt som alltid kan benyttes for å identifisere personen. Dette attributtet bør kunne være stabilt over tid.
- Det er derfor foreslått å benytte serialNumber attributtet i subject-feltet til dette formål. Dette er også innenfor anbefalingene i RFC 3739 [7].

5.1.2 Krav til bruk av serialNumber

- En sertifikatmottaker skal kun behøve å forholde seg til serialNumber attributtet i subject-feltet for å identifisere personen. Dette betyr at man må sikre at to forskjellige personer aldri får samme verdi i serialNumber attributtet, selv om de benytter forskjellige utstedere.
- Profilen tillater at en person kan få utstedt ulike sertifikater med forskjellige verdier i serialNumber attributtet.
- Fødselsnummer eller annet nasjonalt tildelt nummer kan benyttes i serialNumber attributtet.
- Det er lagt opp til en semantikk i serialNumber som forsøker å tilgodese et internasjonalt aspekt.
- Det er ønskelig at dagens løsninger for bruk av serialNumber kan sameksistere i en overgangsperiode med den nye foreslåtte semantikken.
- Innenfor rammene av den overordnede strukturen er det mulig for en utsteder, eller flere samarbeidende utstedere, å definere ytterligere syntaks og semantikk. Dersom en utsteder tildeler utstederspesifikke personidentifikatorer (type 3 i kap. 5.1.3) er det utsteders ansvar å sikre entydighet for disse innenfor eget utstederdomene.
- Alle personsertifikater skal etter 31.12.07 benytte syntaks og semantikk som definert i kap.5.1.3. I en overgangsfase frem til denne dato vil det være tillatt for utsteder å benytte egendefinert syntaks/semantikk.

5.1.3 Syntaks og semantikk

Tabellen nedenfor viser tre ulike typer unike identifikatorer som er definert. Forskjellen mellom de ulike typene er bruk av personidentifikator feltet.

Type 1 og 2 (nasjonale personidentifikatorer)

Internasjonalt prefiks	Landkode	Utsteder identifikator	Personidentifikator - nasjonalt tildelt
9	578	1000	Fødselsnummer
9	578	2000	Alternativt nummer med entydig knytning til fødselsnummer

Type 3 (utstederspesifikke personidentifikatorer)

Internasjonalt prefiks	Landkode	Utsteder identifikator (nasjonalt unikt)	Personidentifikator tildelt av aktuell utsteder
9	578	4 sifret nummer (3000-9999) ihht. Bilag A	Valgfritt antall siffer/tegn

For å lette den visuelle lesbarheten av attributtet serialNumber skal hovedelementene skilles med bindestrek. Eks: 9578-1000-11065534187.

Valgt syntaks er i samsvar med Dansk standard DS 843-1 [13] for personspesifikke identifikasjonsnumre (PID).

I en overgangsperiode frem til 31.12.07 kan utsteder velge å benytte syntaks og semantikk i serialNumber attributtet som avviker fra dette. En sertifikatmottager skal forholdsvis enkelt kunne identifisere om dette er tilfelle ved å sjekke forekomst av prefiks og landkode. En sertifikatmottaker som ikke finner ”9578-” som de første siffer/tegn, kan ikke uten videre anta at verdien i serialNumber attributtet i subject-feltet er unikt, men at verdien må sees i sammenheng med øvrige attributter i subject-feltet, evt. i kombinasjon med verdien i issuer-feltet.

5.2 Bruk av oppslagstjenester

Dersom fødselsnummer ikke eksplisitt finnes i serialNumber feltet (gjelder unik identifikator av type 2 og 3 i kap. 5.1.3) skal sertifikatutsteder tilby en oppslagstjeneste som gjør det mulig for autoriserte[15] sertifikatmottakere å få utlevert sertifikatinnehavers fødselsnummer[16] på bakrunn av den unike identifikatoren som befinner seg i sertifikatets serialNumber felt.

Sertifikatfeltene Subject Information Access og/eller Authority Information Access vil kunne inneholde en peker (URI-referanse) til en slik oppslagstjeneste.

Grensesnitt og aktuelle spørringer for denne typen oppslagstjenester vil bli spesifisert nærmere i senere leveranser fra SEID-prosjektet.

[15] Et autorisert sertifikatmottaker vil si et sertifikatmottaker som har nødvendig autorisasjon for bruk av fødselsnummer.

[16] Identifikatoren i serialNumber feltet vil i praksis kunne danne grunnlag for oppslagstjenester som kan levere ut annen personrelatert informasjon enn fødselsnummer, selv om dette ikke er et krav.

6 Anbefalt norsk profil for virksomhetssertifikater

Dette kapittelet beskriver en norsk sertifikatprofil til bruk for virksomhetssertifikater utstedt til virksomheter og organisasjonsenheter etablert i Norge. Profilen er anvendelig for sertifikater som kan knyttes til en juridisk person som er registrert i Enhetsregisteret i Norge.

Sammenlignet med personsertifikater finnes det få internasjonalt standardiserte profiler for virksomhetssertifikater spesielt. I Norge har NOU 2001:10 [9] vært en anerkjent referanse på området, en profil som igjen er basert på Internett standardene RFC 3280 [5]/RFC 2459[6] for generisk profilering av X.509v3 [3].

Sertifikatprofilen i dette kapittelet vil erstatte NOU 2001:10 som anbefalt profil for virksomhetssertifikater i Norge. Profilen er basert på NOU 2001:10 [9] og RFC 3280 [5]/RFC 2459[6]. I den grad den anbefalte norske profilen avviker fra en eller flere av de ovennevnte standardene er dette eksplisitt beskrevet i Bilag C.

Dette kapittelet tar kun for seg sertifikatfelter hvor den anbefalte norske profilen inneholder en ytterligere profilering av eksisterende standarder. Dette gjelder de 8 sertifikatfeltene listet i tabellen nedenfor:

Basis sertifikatfelter	Sertifikatutvidelser
• Issuer • Subject	• Key Usage • Extended Key Usage • Subject Alternative Name • CRL Distribution Point • Authority Information Access • Qualified Certificate Statement

Sertifikatfelter som ikke er eksplisitt profilert i dette dokumentet anses å være tilstrekkelig profilert gjennom eksisterende standarder som den anbefalte profilen baserer seg på.

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Issuer	**M**	**Ikke relevant – Gjelder kun for sertifikat-utvidelser**	**Bruken av dette feltet er den samme som for Personsertifikater og beskrevet i kap 5.**	
Subject	**M**	**Ikke relevant – Gjelder kun for sertifikat-utvidelser**	**Dette feltet skal alene entydig identifisere innen Norge den juridiske person (virksomhet) som er sertifikatinnehaver. Entydig identifikasjon innebærer at verdiene i nevnte felt/felter har en entydig knytning til virksomhetens organisasjonsnummer som registrert i det norske enhetsregisteret.** **Følgende attributter er obligatoriske:** • `countryName(c)` • `organizationName(o)` • `serialNumber(serialNumber)`**, alternativt kan** `organizationalUnitName(ou)` **benyttes i stedet i en overgangsfase (se under).** **Andre attributter kan benyttes i tillegg, men skal ikke være nødvendige for å sikre entydig identifikasjon av sertifikatinnehaver.** **Attributtet** `organizationName` **skal inneholde sertifikatinnehavers navn slik det er registrert i det norske enhetsregisteret.** **Sertifikatinnehavers organisasjonsnummer slik det er registrert i det norske enhetsregisteret skal angis:** **a) alene i attributtet** `serialNumber`**, eller** **b) sammen med organisasjonsnavn i attributtet** `organizationName` **(f.eks. <org.navn> - <org.nr>)** **I en overgangperiode frem til 31.12.09 er det tillatt å legge organisasjonsnummeret i attributtet** `organizationalUnitName` **som et alternativ til bruk av** `serialNumber`**.**	**Attributtet** `countryName` **skal angi landet hvor sertifikatinnehaver er etablert. For virksomheter etablert i Norge skal verdien "NO" benyttes.** **Dersom attributtet** `commonName` **benyttes bør det inneholde sertifikatinnehaverens navn eller annet vanlig benyttet navn, f.eks. en forkortelse eller et domenenavn. Et Internett domene navn vil normalt plasseres i dette attributtet dersom sertifikatet skal anvendes for sikring av kommunikasjon med SSL/TLS.**

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
Key Usage	**M**	**Valgfritt**	**Aktuelle kombinasjoner av key usage verdier for det enkelte sertifikat skal følge de generelle retningslinjene for anvendelse gitt av RFC 3280 [5], med følgende presiseringer:** **For at et nøkkelpar skal kunne anvendes for avanserte elektroniske signaturer skal én av følgende tre alternative key usage kombinasjoner inngå i sertifikatet, enten alene eller sammen med andre key usage verdier:** - `nonRepudiation`[17] - `digitalSignature` - `nonRepudiation` **og** `digitalSignature` **sammen.** **For sertifikater som benyttes til å utveksle symmetriske nøkler ifm. kryptering skal** `keyEncipherment` **opsjonen benyttes, enten alene eller sammen med andre key usage verdier.** **For sertifikater som benyttes til kryptering av data skal** `dataEncipherment` **opsjonen benyttes, enten alene eller sammen med andre key usage verdier.** **Denne profilen overlater til utsteder fritt å velge aktuelt bruksområde(r) for det enkelte nøkkelpar som sertifiseres og gjennom dette aktuelle key usage kombinasjoner for det tilhørende sertifikat.**	
Extended Key Usage	**O**	**Nei**	**Dette feltet anvendes bla. for SSL/TLS serversertifikater.** **Forøvrig er bruken av dette feltet er den samme som for Personsertifikater og beskrevet i kap 5.**	**For serversertifikater som skal benyttes for SSL/TLS serverautentisering skal dette feltet inneholde key usage verdien** `Server Authentication` **(OID 1.3.6.1.5.5.7.3.1).** **For serversertifikater som skal benyttes for å autentisere SSL/TLS klienter skal dette feltet inneholde key usage verdien** `Client Authentication` **(OID 1.3.6.1.5.5.7.3.2).**
Subject Alternative Name	**O**	**Nei**	**Bruken av dette feltet er den samme som for Personsertifikater og beskrevet i kap 5.**	

[17] I et utkast til Technical Corrigendum 6 til Recommendation X.509 (2000) [11] er det foreslått å benytte navnet contentCommitment i stedet for non-repudiation for denne key usage verdien.

Felt	Forekomst M=Mandatory O=Optional	Kritisk (Ja/Nei/ Valgfritt)	Verdi	Kommentar
CRL Distribution Point	**O/M (se komm.felt)**	**Nei**	**Bruken av dette feltet er den samme som for Personsertifikater og beskrevet i kap 5.**	**Dette feltet skal benyttes dersom utsteder (evt. representant for utsteder) er tilbyder av en CRL tjeneste. Minimum ett av feltene "CRL Distribution Point" eller "Authority Information Access" skal benyttes.**
Authority Information Access	**O/M (se komm.felt)**	**Nei**	**Bruken av dette feltet er den samme som for Personsertifikater og beskrevet i kap 5.**	**Dette feltet skal benyttes dersom utsteder (evt. representant for utsteder) er tilbyder av en sertifikatstatus-tjeneste. Minimum ett av feltene "CRL Distribution Point" eller "Authority Information Access" skal benyttes.**
Qualified Certificate Statement	**O**	**Valgfritt**	**ETSI TS 101 862 [4] profilerer fire uavhengige anvendelser for dette feltet. Med unntak av den ene av disse anvendelsene som kun gjelder for kvalifiserte sertifikater[18] kan de tre øvrige være aktuelle. Dette gjelder spesielt de to anvendelsene som angitt nedenfor.** **Dersom det i utsteders sertifikatpolicy er lagt en begrensning på anvendelse av sertifikatet gjennom et verditak på enkelttransaksjoner, kan denne begrensningen med beløpets størrelse eksplisitt legges inn i dette feltet. Se ETSI TS 101 862 [4] for detaljer.** **Dersom utsteder kan gå god for at den private nøkkelen, som tilhører den offentlige nøkkelen i sertifikatet, er lagret i et såkalt sikkert signaturfremstillingssystem kan dette angis i sertifikatet ved å inkludere en OID ihht. ETSI TS 101 862 [4].**	**Dette feltet er tradisjonelt tilegnet bruk for kvalifiserte personsertifikater, men enkelte anvendelser identifisert i ETSI TS 101 862 [4] kan ha nyttig anvendelse også for virksomhetssertifikater.**

Andre krav og anbefalinger:

- Bruk av andre sertifikatutvidelser enn de som er listet i tabellen over, reguleres av den enkelte utsteder. Eneste kravet er at dersom slike sertifikatutvidelser benyttes så bør disse settes til å være ikke-kritiske.
- Anbefalt nøkkellengde for utsteders signatur er som for personsertifikater, dvs. en styrke tilsvarende 2048 bit for RSA nøkler

[18] Et virksomhetssertifikat vil ikke kunne være kvalifisert.

Bilag A: Nasjonalt unike utstederidentifikatorer

Introduksjon

Alle utstedere som ønsker å utstede personsertifikater i henhold til personprofilen i kap.5 og med utstederspesifikke personidentifikatorer i serialNumber feltet (type 3 ihht. syntaks definert i kap.5.1.3) har behov for å få tildelt en nasjonalt unik utstederidentifikator (4-sifret nummer) ihht. dette bilaget.

Én enkelt utstederorganisasjon med ansvar for flere tekniske CAer vil kunne velge å registrere og benytte ulike utstederidentifikatorer for disse.

Tilsvarende er det mulig for flere utstedere å gå sammen om å benytte én og samme utstederidentifikator. Dette krever imidlertid at disse koordinerer seg i forhold til å sikre at de sammen oppfyller kravet i kap.5.1.2 om at personidentifikatorer som benyttes skal være entydige på tvers av disse utstederne.

Registrerte utstederidentifikatorer

Følgende nummerserier er dedikerte:

- 1000 – angir at personidentifikatoren er et fødselsnummer. Nummerserien 1001-1999 skal ikke benyttes.
- 2000 – angir at personidentifikatoren er et alternativt nasjonalt nummer som entydig mapper til et fødselsnummer. Nummerserien 2001-2999 skal ikke benyttes.
- 5000-5999 skal utelukkende benyttes for utstedere innenfor BankID samarbeidet i Norge.

Tabellen nedenfor lister de nasjonalt unike identifikatorer som er registrert.

Utsteder	Utstederidentifikator
Fokus Bank	5994
Utstedere under Terra-gruppen	5995
Gjensidige NOR	5996
Utstedere under Sparebank1-gruppen	5997
Nordea	5998
DnB	5999
NetCom	3000-3010
ZebSign	4000-4010
Buypass	4050

Prosedyre for registrering av nye numre

Utstedere som ikke er identifisert i tabellen over og som ønsker å utstede personsertifikater med utstederspesifikke personidentifikatorer i henhold til personprofilen i kap.5 må få registrert et unikt 4-sifret nummer dersom utstederen ønsker å benytte utstederspesifikke identifikatorer (unik identifikator av type 3 ihht. kap. 5.1.3) i serialNumber feltet.

Prosedyren for registrering vil være at utsteder selv velger et 4 sifret nummer som ikke allerede er registrert i dette bilaget og gir dette til ansvarlig dokumentforvalter (se kap. 4.1) med beskjed om å oppdatere dette bilaget. Dokumentforvalteren vil kontrollere at nye identifikatorer som registreres ikke allerede er i bruk.

Etter at registrering av ny identifikator har funnet sted er utstederen selv ansvarlig for å melde fra til eventuelle parter/aktører som kan ha behov for denne informasjonen.

Bilag B (Informativt) : Key usage

Introduksjon

Det har lenge pågått en diskusjon når det gjelder bruk av key usage verdier i sertifikater.

ETSI TS 102 280 [8], som er en normativ anbefaling for bla. kvalifiserte sertifikater, har lagt seg på en linje hvor:

- det er et krav for kvalifiserte sertifikater at key usage verdier for kryptering (keyEncryption og keyEncipherment) aldri skal kombineres med key usage verdier for signering (nonRepudiation og digitalSignature).
- det er et krav at keyUsage nonRepudiation aldri skal benyttes sammen med key usage verdier for kryptering (keyEncryption og keyEncipherment).
- det er et krav at key usage nonRepudiation skal benyttes, og en tilsvarende anbefaling at key usage nonRepudiation settes alene, dersom det aktuelle nøkkelparet skal anvendes til å signere/validere kontrakter/transaksjoner og hvor den som foretar signeringen vil kunne bli stilt til ansvar for signaturen (dvs. formål ”ikke-benekting”).
- det er en anbefaling at key usage feltet markeres som en kritisk attributt.

Konsekvensen av nevnte krav/anbefalinger er at en utsteder som ønsker å utstyre brukere med en elektronisk ID som skal ha en bred anvendelse (f.eks. avanserte elektroniske signaturer, autentisering og kryptering) pålegges å utstyre brukeren med minimum to eller flere nøkkelpar. Det er rimelig å anta at det først og fremst er sikkerhetsmessige aspekter som er forsøkt ivaretatt og som ligger til grunn for disse kravene/anbefalingene.

De anbefalte profilene i dette dokumentet legger ikke like strenge føringer som ETSI TS 102 280 når det gjelder hvilke key usage kombinasjoner en utsteder skal kunne ha lov til å velge. Bakgrunnen er en argumentasjon i dette bilaget som viser at det er det i stor grad er de konkrete anvendelsene som nøklene vil kunne anvendes sammen med samt sikkerheten i den enkelte applikasjonsomgivelse som avgjør om det vil tilføre en ekstra sikkerhetsgevinst å benytte flere nøkkelpar. Mange nøkkelpar vil på den annen side kunne bidra til økt administrasjon for bruker og utsteder og kan i verste fall føre til at sikkerheten blir redusert.

Formålet med key usage verdiene i et sertifikat

Key usage verdiene i et sertifikat har følgende formål:

1. **For sertifikatinnehavers applikasjonsomgivelse:** Som teknisk informasjon til tiltrodde applikasjoner[19] hos sertifikatinnehaver for å:
    - gjøre det mulig for applikasjonen å velge riktig nøkkelpar til den aktuelle anvendelse dersom det finnes flere nøkkelpar å velge mellom.
    - bidra til å sikre at bruken av det enkelte nøkkelpar begrenses til det/de anvendelsesområde(ne) som utsteder har bestemt (se RFC 3280 for hvilke ulike anvendelsesområder som er definert).

[19] En tiltrodd applikasjon i dette tilfellet er en applikasjon som oppfører seg korrekt i forhold til de key usage verdier som er satt.

2. **For sertifikatmottakers applikasjonsomgivelse:** Som teknisk informasjon til sertifikatmottakers applikasjonsomgivelse når det gjelder å angi tillatte anvendelsesområder for det aktuelle nøkkelparet. Hensikten er å hindre at sertifikatmottakeren aksepterer feil bruk av nøkkelpar i forhold til det utsteder har bestemt i sin policy. Dette har bla. med ansvar å gjøre fordi en utsteder eksplisitt kan regulere sitt og sertifikatinnehavers ansvar under forutsetning av at nøkkelbruken er riktig.

Sertifikatinnehaveren selv, i de tilfeller dette er en fysisk person, kan ikke forventes å ha noe forhold til hvilke tekniske key usage verdier som er satt. Sertifikatinnehaveren vil forholde seg til sin applikasjonsomgivelse og vil styre sine handlinger på bakgrunn av applikasjonens visuelle brukergrensesnitt. En beslutning om å taste passord/PIN for å gi applikasjonsomgivelsen tilgang til sin private nøkkel vil være basert på den visuelle opplevelsen samt den konteksten den aktuelle handlingen skjer i.

Trusselbilde

Figur 1 illustrerer en applikasjonsomgivelse delt inn i logiske funksjonselementer på tre nivåer.

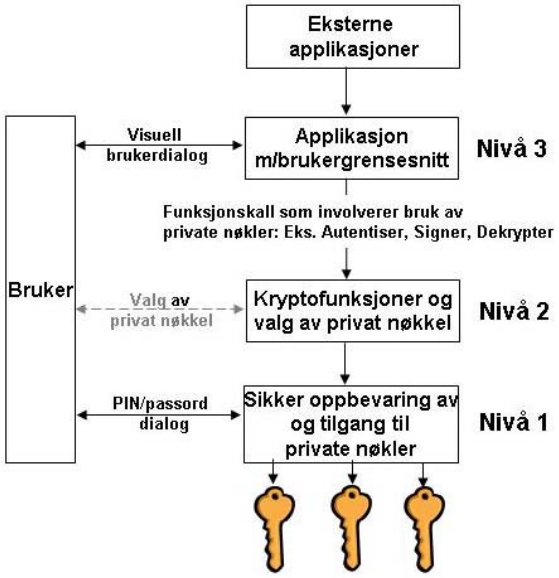

Figure 1 Applikasjonsomgivelse med logiske funksjonselementer

På nivå 1 finner vi de sikkerhetsfunksjonene som styrer tilgangen til brukerens private nøkler. Her er det behov for en autentiseringsdialog med brukeren hver gang en av de private nøklene skal anvendes (typisk PIN/passord)[20]. På nivå 2 finner vi de kryptofunksjonene som anvender de private nøklene. Dersom brukeren har flere nøkkelpar så vil funksjonene på dette nivået velge aktuell privat nøkkel for bruk, enten automatisk eller gjennom en brukerdialog. På nivå 3 finner vi den delen av applikasjonen som håndterer hoveddialogen med brukeren (eks. vise data for signering) og som kaller nødvendige kryptofunksjoner på nivå 2.

En sikkerhetsmessig diskusjon vedrørende key usage verdier og antallet nøkkelpar må ses i lys av en risikodiskusjon knyttet til muligheten for misbruk av brukerens private nøkler

[20] Det er mulig å tenke seg ubeskyttet tilgang til privat nøkler, dvs. at applikasjonsomgivelsen har tilgang uten at brukeren er involvert.

innenfor en spesifikk applikasjonsomgivelse. Hovedtrusselen er at den visuelle brukeropplevelsen på nivå 3 kan forfalskes eller på annen måte avvike fra den tekniske operasjonen som faktisk er i ferd med å utføres. Konsekvensen er at brukeren på feil grunnlag vil taste PIN/passord og på den måten gir applikasjonsomgivelsen tilgang til privat nøkkel.

Nevnte hovedtrussel kan deles i to kategorier:

- **Trussel type A:** Brukeren gir applikasjonsomgivelsen tilgang til sin private nøkkel (dvs. taster PIN/passord) i den tro at han/hun signerer en transaksjon/dokument A mens applikasjonen i virkeligheten signerer transaksjon/dokument B.
- **Trussel type B:** Brukeren gir applikasjonsomgivelsen tilgang til sin private nøkkel (dvs. taster PIN/passord) i den tro at den private nøkkelen skal benyttes for autentisering eller dekryptering mens det som i virkeligheten skjer er at applikasjonsomgivelsen benytter den private nøkkelen til å lage en elektronisk signatur (for eksempel på et for brukeren ukjent dokument). Et eksempel kan være at den private nøkkelen blir benyttet i en automatisk autentiseringsprosess (for eksempel SSL) hvor brukeren ikke er bevisst på hva som signeres. Applikasjonen kan lures til å signere det som for applikasjonen antas å være en ”challenge” (normalt en random bitstreng), men som i praksis er et dokument med meningsfullt innhold.

Ett eller flere nøkkelpar ?

Bruk av elektroniske IDer med flere nøkkelpar, hver med sine ulike dedikerte anvendelsesområder, anses som et mulig tiltak for å redusere risikoen for misbruk av private nøkler.

Dersom man ser nærmere på figuren og truslene nevnt tidligere så vil risikoen knyttet til trussel type A være helt avhengig av sikkerheten (sårbarheten) i applikasjonsomgivelsen på nivå 2 og 3. Aktuelt sikkerhetstiltak vil være å kreve sikre applikasjonsomgivelser slik som f.eks. lov om elektronisk signatur gjør for kvalifiserte signaturer. Flere nøkkelpar og dedikering av et eget nøkkelpar kun til bruk for signaturformål (avanserte elektroniske signaturer) vil ikke redusere risikoen for denne typen misbruk.

Risikoen knyttet til trussel type B er som for trussel type A avhengig av sikkerheten (sårbarheten) til den lokale applikasjonsomgivelsen. For at bruk av flere nøkkelpar skal bidra til å redusere sikkerhetsrisiko vil det være et minimumskrav at applikasjonsomgivelsen og/eller brukeren kan sikre at riktig nøkkel brukes til rett tid, dvs:

- **Alt 1:** Brukeren har forskjellig PIN/passord for tilgang til de ulike nøklene og hindrer misbruk gjennom bevisst valg av rett nøkkel basert på brukskonteksten og den visuelle opplevelsen.
- **Alt 2:** Brukeren har samme passord/PIN for tilgang til alle nøklene og overlater i praksis til applikasjonen å velge rett nøkkel. I dette tilfellet er sikkerheten helt avhengig av en tiltrodd applikasjonsomgivelse (nivå 1-3).

For trussel type B vil, i tillegg vil ovennevnte, eksterne trusler gjøre seg gjeldende ved at eksterne applikasjoner kan angripe det lokale system gjennom sårbarhet knyttet til dårlig designede sikkerhetsprotokoller, f.eks. for autentisering. Slike trusler vil som utgangspunkt gjelde uavhengig av hvor godt sikret den lokale applikasjonsomgivelsen er. Bruk av flere nøkkelpar kan i teorien bidra til å redusere risiko knyttet til dårlig designede sikkerhetsprotokoller. I praksis bør en avgjørelse kunne bygge på en nærmere risikovurdering

knyttet til aktuelle anvendelsesområder for nøklene og tilhørende aktuelle sikkerhetsprotokoller.

I tillegg til de sikkerhetsmessig aspektene vil praktiske aspekter kunne være vel så vesentlige i forhold til valg av antallet nøkkelpar:

- En bruker vil ønske seg en løsning som er så enkel som mulig i bruk. Det vil ofte være upraktisk for brukeren å individuelt måtte forholde seg til flere nøkkelpar enten det er snakk om å forholde seg ulike passord/PIN ved bruk eller ved individuell administrasjon (eks. sertifisering, revokering) av det enkelte nøkkelpar/sertifikat.
- For enkelte SIM/smartkortbaserte løsninger vil det være ønskelig av hensyn til lagringsplass, å ha så få nøkkelpar og sertifikater som mulig.

Konklusjon

En diskusjon om i hvilken grad det er behov for klare krav/anbefalinger om bruk av flere nøkkelpar bør være førende for hvilke kombinasjoner av key usage verdier som skal være tillatte i de anbefalte sertifikatprofilene. Dette er en diskusjonen hvor både sikkerhetsmessige og praktiske elementer må sees i sammenheng.

Med en totalt sikker applikasjonsomgivelse (nivå 1-3) vil antallet nøkkelpar som utgangspunkt ikke spille noen rolle sett i forhold til truslene identifisert i dette bilaget. Eneste unntak er dårlig designede sikkerhetsprotokoller som en sikker applikasjonsomgivelse ikke vil kunne gi beskyttelse mot. Flere nøkkelpar kan gi sikkerhetsmessig gevinst mot denne typen trusler under forutsetning av at risikoen er reell. Med en totalt usikker applikasjonsomgivelse vil flere nøkkelpar i utgangspunktet kun gi en sikkerhetsmessig gevinst dersom de private nøklene har ulike PIN/passord, en løsning som i praksis er lite anvendelig fra et brukerperspektiv. For løsninger som ligger mellom disse ytterpunktene bør et sikkerhetsmessig valg av antall nøkkelpar baseres på en risikovurdering av den/de totale applikasjonsomgivelser nøklene skal anvendes sammen med.

På bakrunn av de klare key usage krav/anbefalingene i ETSI TS 102 280 kan det virke som det implisitt er forutsatt hva slags applikasjonsomgivelser som profilene er tenkt å understøtte uten at dette er eksplisitt formulert. En slik tilnærming anses ikke som hensiktsmessig for denne profilen og krav til key usage i ETSI TS 102 280 er derfor ikke direkte videreført. Med unntak av kravet om at en utsteder av kvalifiserte sertifikater må dedikere forskjellige nøkkelpar for signering/signaturvalidering og kryptering/dekryptering i de tilfeller hvor utsteder benytter nøkkelarkiv[21], har de anbefalte profilene i dette dokumentet overlatt til den enkelte utsteder å avgjøre antallet nøkkelpar og tilhørende key usage kombinasjoner for disse ut ifra en risikomessig og praktisk totalvurdering.

[21] Dette kravet er forankret i lov om elektronisk signatur [10].

Bilag C (Informativt) : Avvik fra aktuelle standarder og referanseprofiler

Introduksjon

Dette bilaget identifiserer og begrunner de konkrete avvik som er gjort i de anbefalte sertifikatprofilene i forhold til krav/anbefalinger gitt av relevante profilstandarder og referanseprofiler som disse baserer seg på. Avvikene er kategorisert per sertifikatfelt.

Anbefalt personprofil

Sertifikatfelt	Standard/ Referanseprofil	Avvik	Begrunnelse
Issuer	**ETSI TS 102 280**	**ETSI krever bruk av `organizationName` for lagring av fullt registrert organisasjonsnavn. Anbefalt profil åpner for å legge organisasjonsnavn i alternative attributter i tilfeller hvor `organizationName` attributtet ikke anvendes.**	**ZebSign benytter i dag attributtet `domainComponent` for å angi navn på utsteder.**
Issuer	**ETSI TS 102 280**	**Attributtene `stateOrProvinceName` og `localityName` er fjernet fra attributtlisten.**	**Disse attributtene anses ikke aktuelle for å sikre entydighet i Norge.**
Subject	**ETSI TS 102 280**	**Den anbefalte profilen krever at verdien i serialNumber alene skal være nok til entydig å identifisere personen som er sertifikatinnehaver. ETSI derimot definerer en liste av attributter hvor verdiene i et vilkårlig subsett av disse kan velges for å oppnå det samme.**	**Den unike identifikatoren som SEID-profilen har spesifisert er per definisjon entydig, uavhengig av andre attributter som blir benyttet i dette sertifikatfeltet.**
Key Usage	**ETSI TS 102 280**	**ETSI TS 102 280 [8], som vil være en normativ anbefaling for bla. kvalifiserte sertifikater, har lagt seg på en mer restriktiv linje enn den anbefalte profilen når det gjelder hvilke key usage kombinasjoner som er tillatt. Se Bilag B for detaljer.**	**Bakgrunnen er at det kan virke som kravene/anbefalingene fra ETSI TS 102 280 implisitt bygger på en del sikkerhetsmessige antagelser som i praksis ikke behøver å ha generell gyldighet. Se Bilag B for en mer detaljert argumentasjon.**
CRL Distribution Point	**ETSI TS 102 280**	**Av bl.a. hensyn til interoperabilitet har ETSI TS 102 280 valgt å kreve at dette attributtet anvendes, dvs. at attributtet er obligatorisk. Anbefalt profil har derimot valgt å kreve bruk av dette attributtet kun dersom det ikke finnes en alternativ sertifikatstatustjeneste (eks. OCSP).**	**BankID benytter i dag kun OCSP for tilgang til katalogtjenester. Et krav om bruk av attributtet CRL Distribution Point innebærer implisitt et krav om at en CRL tjeneste skal tilbys i tillegg. Et slikt krav er ikke innført da dette gir uakseptable forretningsmessige føringer.**

Anbefalt virksomhetsprofil

Sertifikatfelt	Standard/ Referanseprofil	Avvik	Begrunnelse
Issuer	**NOU 2001:10**	**Attributtene** `organizationUnitName` **og** `domainComponent` **er lagt til attributtlisten i forhold til NOU 2001:10**	**Feltet defineres på samme måte som for Person sertifikater.**
Issuer	**NOU 2001:10**	**Attributtet** `commonName` **er ihht. NOU 2001:10 obligatorisk. Anbefalt profil har derimot valgt å definere dette attributtet som opsjonelt.**	**Feltet defineres på samme måte som for Person sertifikater** **I anbefalt profil anses** `commonName` **attributtet som opsjonelt da det som utgangspunkt vil være andre attributter som prefereres ifht. entydig identifikasjon av utsteder.**
Subject	**NOU 2001:10**	**NOU 2001:10 stiller krav til bruk av attributtet** `organizationUnitName` **og anbefaling når det gjelder bruk av attributtet** `commonName`**.** **Anbefalt profil har valgt å ikke profilere disse attributtene.**	**BankID benytter i en overgangsfase** `organizationUnitName` **for lagring av organisasjonsnummer. Dette er ikke ihht. NOUens krav.** `commonName` **attributtet anses som opsjonelt da det som utgangspunkt vil være andre attributter som prefereres ifht. entydig identifikasjon av virksomheten.**
Key Usage	**NOU 2001:10**	**NOU 2001:10 stiller krav om at dersom** `nonRepudiation` **velges så skal denne verdien figurere alene i sertifikatet.** **Anbefalt profil har valgt å ikke videreføre dette kravet. Det er likevel fullt mulig å følge NOUens krav innenfor anbefalt profil.**	**Se Bilag B for nærmere argumentasjon.**
Key Usage	**NOU 2001:10**	**NOU 2001:10 stiller krav til at dette feltet skal flagges som et kritisk felt.** **Anbefalt profil har valgt å la det være valgfritt om feltet skal flagges kritisk eller ikke-kritisk. Det er likevel fullt mulig å følge NOUens krav innenfor anbefalt profil.**	**De-facto praksis og tilsvarende anbefalinger varierer. Prosjektet har derfor ikke sett behov for å sette det som et krav at feltet skal flagges kritisk.**

Sertifikatfelt	Standard/ Referanseprofil	Avvik	Begrunnelse
Subject Alternative Name	**NOU 2001:10**	**NOU 2001:10 anbefaler å legge inn firmapostadresse for virksomheten i dette feltet.** **Anbefalt profil har valgt å ikke videreføre dette anbefalingen. Det er likevel fullt mulig å følge NOUens anbefaling innenfor anbefalt profil.**	**Entydig identifikasjon av virksomheten oppnås ved bruk av subject-feltet alene.**
CRL Distribution Point	**NOU 2001:10**	**NOU 2001:10 har valgt å kreve dette som et obligatorisk attributt. Anbefalt profil har derimot valgt å kreve bruk av dette attributtet kun dersom det ikke finnes en alternativ sertifikatstatustjeneste (eks. OCSP).**	**BankID benytter i dag kun OCSP for tilgang til katalogtjenester. Et krav om bruk av attributtet CRL Distribution Point innebærer implisitt et krav om at en CRL tjeneste skal tilbys i tillegg. Et slikt krav er ikke innført da dette gir uakseptable forretningsmessige føringer.**
Qualified Certificate Statement	**NOU 2001:10**	**Dette feltet er ikke nevnt i NOU 2001:10 for virksomhetssertifikater**	**Feltet kan brukes på tilsvarende måte som for Person sertifikater for bl.a. å inkludere beløpsgrenser.**