SEID-samarbeidet

Leveranse 1

Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater

Versjon 2.1

Dato: 30.05.2023

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 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.
01.06.12	1.03	PK	Oppdatert kontaktpunkt for Dokumentforvalter i kap. 4.1.
15.02.21	2.0	Buypass	Dokumentet oppdatert iht. nytt regelverk og tilpasset ETSI-standarder, som følge av møte om revisjonsbehov den 28.10.19.
30.05.23	2.1	Buypass	Dokument oppdatert med informasjon om dispensasjonsordning, bruk av URL for "skjemaet UN:NO" samt forbedret støtte for Virksomhetssertifikater til underenheter.

Innholdsfortegnelse

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.
Autentiserings-sertifikat	Et sertifikat som inneholder offentlig nøkkel som er tilegnet bruk for autentisering (for bekreftelse av identitet).
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 er merket ikke-kritiske.
Krypteringssertifikat	Et sertifikat som inneholder offentlig nøkkel som er tilegnet bruk for kryptering (sikre konfidensialitet) av data.
Kvalifisert sertifikat for elektronisk segl	Et sertifikat for et elektronisk segl som er utstedt av en kvalifisert tilbyder av tillitstjenester, og som oppfyller kravene fastsatt i eIDAS-forordningens vedlegg III.
Kvalifisert sertifikat for elektronisk signatur	Et sertifikat for elektroniske signaturer som er utstedt av en kvalifisert tilbyder av tillitstjenester, og som oppfyller kravene fastsatt i eIDAS-forordningens vedlegg I.
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.
SEID-prosjektet	Dette var et samarbeidsprosjekt for eID og eSignatur mellom en rekke aktører fra offentlig og privat sektor. Prosjektet stod i 2004 og 2005 for tre leveranser hvorav SEID-leveranse 1: Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater er bakgrunnen for dette dokumentet.
Sertifikat / Digitalt sertifikat / Elektronisk sertifikat	Et sertifikat er en form for elektronisk identitetsbevis som knytter en offentlig nøkkel til en identitet. 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.
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 person/virksomhet sertifikatet er utstedt til i henhold til sertifikatpolicy og som er innehaver av, eller kontrollerer den private nøkkelen.

Begrep	Beskrivelse
Sertifikatmottaker	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.
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 som utsteder personsertifikater eller virksomhetssertifikater i det norske markedet.
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 er identifisert i sertifikatet.
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.
Virksomhetssertifikat	Et virksomhetssertifikat har som oppgave å identifisere en juridisk person, dvs. en virksomhet som er registrert i Enhetsregisteret. Bruker av den private nøkkel assosiert med sertifikatet kan være en fysisk person autorisert av virksomheten eller en automatisert prosess under virksomhetens kontroll, for eksempel en server.

Forkortelse	Beskrivelse
CA	Certification Authority
CRL	Certificate Revocation List
eID	Elektronisk Identifikasjon
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force

Forkortelse	Beskrivelse
ISO	International Organization for Standardisation
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RFC	Request For Comments
S/MIME	Secure Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
URL	Uniform Resource Locator

2 Referanser

[1] SEID-Prosjektet: "Leveranse oppgave 1; Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater", v1.03, 1. juni 2012

[2] SEID-Prosjektet: "Leveranse oppgave 2; Grensesnitt for tilgang til Oppslagstjenester", v1.03, 1. juni 2012

[3] SEID-samarbeidet: Forvaltningsinstruks for SEID-samarbeidets leveranser, v2.0, 15. februar 2021

[4] SEID-samarbeidet: "Nasjonalt unike utstederidentifikatorer; Vedlegg til Leveranse 1; Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater"

[5] Mekanisme for forkorting av navn: Utkast benyttet for pass og ID-kort, september 2017

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

[7] IETF RFC 5280: "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile", mai 2008

[8] IETF RFC 6960: "X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP", juni 2013

[9] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites", v1.3.1 (2019-02)

[10] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures", v1.4.1 (2020-06)

[11] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons", v2.2.1 (2020-07)

[12] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons", v1.2.1 (2020-07)

[13] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements", v2.3.1 (2020-04)

[14] Regulation (EU) No 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[15] Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), LOV-2018-06-15-44

[16] Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften), FOR-2019-11-21-1578

[17] Referat fra SEID-møte 28.10.2019: Møte om revisjonsbehov for SEID-prosjektets leveranser

[18] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"

3 Innledning

SEID-prosjektet definerte i 2004 sertifikatprofiler for personsertifikater og virksomhetssertifikater for bruk i det norske markedet gjennom Leveranse oppgave 1, Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater [1].

SEID-prosjektet ble avsluttet i 2005 og ansvaret for vedlikehold av SEID-leveransene er overført til aktører som deltar i SEID-samarbeidet.

De norske SEID-sertifikatprofilene er fortsatt i bruk i Norge, men med nylige endringer i nasjonalt regelverk ([14], [15] og [16]) er det identifisert et behov for å erstatte disse norske SEID-sertifikatprofilene med sertifikatprofiler som er bedre harmonisert med gjeldende europeiske ETSI-standarder (ETSI EN 319 412-x) under eIDAS-forordningen.

Det ble avholdt et møte i regi av Nasjonal kommunikasjonsmyndighet den 28.10.2019 og der ble man enige om at SEID-leveranse 1 bør oppdateres og ikke avvikles [17].

Man ble i møtet også enige om å definere en overgangsperiode for å sikre at applikasjoner og tjenester som forholder seg til norske SEID-sertifikatprofiler blir tilpasset nye sertifikatprofiler. I en slik overgangsperiode må aktører kunne støtte to generasjoner med sertifikatprofiler i sine applikasjoner og tjenester.

De opprinnelige sertifikatprofilene omtales heretter som SEID-sertifikatprofiler v1.0 (eller SEID v1.0 som en kortere variant), mens de nye sertifikatprofilene omtales for SEID-sertifikatprofiler v2.0 (eller SEID v2.0).

3.1 Formål

Det eksisterer standarder fra ETSI ([10], [11], [12], [13]) og IETF [[6]og[7]] som profilerer X.509v3 [18] sertifikater og disse standardene legges til grunn for de anbefalte norske sertifikatprofilene.

De anbefalte norske sertifikatprofilene inneholder imidlertid enkelte elementer som ønskes videreført fra de opprinnelige SEID-sertifikatprofilene (SEID v1.0) og som ikke er dekket av ETSI-standardene. Dette er noe av grunnlaget for å videreføre anbefalte norske sertifikatprofiler.

ETSI-standardene som legges til grunn gir en del rom for tolkning som gjør at det kan være hensiktsmessig å presisere bruken av enkelte felter/attributter i sertifikatene. Dette er også tatt med i de anbefalte sertifikatprofilene.

Det er også viktig å være tydelig på endringer fra SEID-sertifikatprofiler v1.0 til SEID-sertifikatprofiler v2.0. Dette er viktig for alle som må tilpasse applikasjoner og tjenester for å sikre at disse støtter begge generasjoner med sertifikatprofiler.

Formålet med dette dokumentet er å definere anbefalte norske sertifikatprofiler, basert på gjeldende ETSI-standarder som skal bidra til harmonisering av eksisterende og kommende løsninger både i det norske og i et europeisk marked.

En slik harmonisering skal bidra til enhetlige sertifikatprofiler fra ulike sertifikatutstedere. Dette vil 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.

Det er viktig å presisere at dette er en anbefaling og at det er dette dokumentet sammen med de underliggende standardene som utgjør de nasjonale sertifikatprofilene.

3.2 Målgruppe

Dette dokumentet er primært tilegnet tjeneste-/programvare-leverandører samt sertifikatutstedere og sertifikatmottakere som ønsker å levere eller å ta i bruk PKI-tjenester som benytter sertifikater som følger anbefalingene i dette dokumentet.

Sertifikatmottakere kan både være private aktører som leverer kommersielle elektroniske tjenester og offentlige myndigheter med elektroniske tjenester internt i forvaltningen og eksternt rettet mot innbyggerne og næringsliv.

3.3 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 for elektronisk signatur. Profilen er anvendelig for sertifikater som entydig identifiserer personer registrert i det norske folkeregisteret.

Profilen kan også benyttes for personer som ikke er registrerte i det norske Folkeregisteret, men i tilsvarende registre i andre land. I så fall vil informasjon om sertifikatinnehaver (Subject) kunne ha noe annet innhold tilpasset det enkelte land.

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

Profilen kan benyttes også for virksomheter som ikke er registrert i Enhetsregisteret, men i tilsvarende registre i andre land. Også her vil informasjon om sertifikatinnehaver kunne ha noe annet innhold tilpasset det enkelte land.

Profilene skal kunne dekke aktuelle behov innenfor et bredest mulig funksjonelt bruksområde. Dette inkluderer sertifikater til bruk for Autentisering (autentiseringssertifikat), Kryptering (krypteringssertifikat) og Signering (signeringssertifikat). Profilene åpner for at ett enkelt sertifikat skal kunne dekke flere av disse bruksområdene samtidig.

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.

Kapittel 7 inneholder en utvidelse av profilen for virksomhetssertifikater som dekker sertifikater til underenheter.

4 Dokumentets status og forvaltning

4.1 Dokumentforvalter

SEID-prosjektets styringsgruppe utpekte opprinnelig Post- og teletilsynet, nå Nasjonal kommunikasjonsmyndighet (Nkom) som Dokumentforvalter.

Kontaktpunkt hos Nkom er: seid@nkom.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 Overgangsordning

Sertifikater som følger de opprinnelige SEID-sertifikatprofilene er fortsatt i utstrakt bruk i det norske markedet.

For å sikre en smidig overgang fra bruk av SEID-sertifikatprofiler v1.0 til SEID-sertifikatprofiler v2.0 som er bedre harmonisert med felles europeiske ETSI-sertifikatprofiler, ble det innført en overgangsordning for å sikre at sertifikatutstedere kan utstede sertifikater under SEID-sertifikatprofiler v1.0 i en overgangsperiode samtidig som markedets aktører tilpasser sine løsninger til SEID-sertifikatprofiler v2.0.

Forskjellene mellom SEID-sertifikatprofiler v1.0 og SEID-sertifikatprofiler v2.0 blir tydelig beskrevet som en del av det aktuelle sertifikatfelt og profil i kapittel 5 og 6.

Overgangsperioden varte frem til 1. juni 2022. Dette betyr at sertifikatutstedere kunne utstede sertifikater iht. SEID-sertifikatprofiler v1.0 gjennom overgangsperioden. Etter at overgangsperioden er over, skal sertifikatutstedere utstede sertifikater iht. SEID-sertifikatprofiler v2.0.

Sertifikatutstederne stod fritt til å utstede sertifikater iht. SEID-sertifikatprofiler v2.0 i hele overgangsperioden, men ble oppfordret til å gjøre en risikovurdering i forhold til applikasjoner og tjenester ikke støttet de nye sertifikatprofilene.

Tjeneste-/programvare-leverandører og sertifikatmottakere må være forberedt på å håndtere sertifikater iht. SEID-sertifikatprofiler v2.0 fra 1. september 2021. Dersom det viser seg at dette forårsaker feil eller på andre måter gjør

at sertifikatene ikke fungerer, bør sertifikatutstederne varsles om dette forholdet og problemet løses i tjenesten/applikasjonen. Dette må være fullført i løpet av overgangsperioden.

Med en slik overgangsordning vil det kunne være aktive sertifikater i bruk utstedt under SEID v1.0 i lang tid etter overgangsperiodens slutt, dvs. inntil sertifikatene utstedt i overgangsperioden utløper. Med for eksempel en levetid på tre år, vil det kunne være aktive sertifikater basert på SEID v1.0 frem til 1. juni 2025.

4.3.1 Dispensasjonsordning

Ved overgangsperiodens utløp var det fortsatt et behov for å utstede sertifikater under SEID-sertifikatprofiler v1.0. Det ble derfor etablert en *generell dispensasjonsordning* der sertifikatutstederne kunne utstede slike sertifikater frem til 1.april 2023.

Denne generelle dispensasjonsordningen ble erstattet med en *spesiell dispensasjonsordning* der sertifikatutstederne ved behov må søke om å få lov til å utstede sertifikater under SEID-sertifikatprofiler v1.0. Denne spesielle dispensasjonsordningen varer frem til 1.januar 2024.

Ingen sertifikater som utstedes under SEID-sertifikatprofil v1.0 skal være gyldige etter 1.juni 2025.

4.4 Vedlikehold

Aktørene i SEID-samarbeidet har i fellesskap besluttet at dette dokumentet skal kunne revideres ved behov.

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 [3].

5 Anbefalt norsk profil for personsertifikater

Dette kapittelet beskriver en norsk sertifikatprofil til bruk for personsertifikater utstedt til fysiske personer som har norsk fødselsnummer eller D-nummer, dvs. at de er registrerte i det norske Folkeregisteret.

Profilen kan også benyttes for personer som ikke er registrert i Folkeregisteret, se kap. 5.2 for mer informasjon.

Profilen er anvendelig for alle personsertifikater, herunder kvalifiserte sertifikater for elektronisk signatur, 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 EN 319 412-2 [11] som igjen er basert på RFC 5280 [7].

Dette kapittelet tar kun for seg sertifikatfelter hvor den anbefalte norske profilen inneholder en ytterligere profilering av, evt. avvik fra, nevnte standarder.

Kapitlet inkluderer også sertifikatfelter der det er vesentlige forskjeller mellom SEID-sertifikatprofil v1.0 og v2.0. Dette skal gjøre det enklere for aktører å sikre støtte for begge generasjoner sertifikater i overgangsperioden og inntil de siste sertifikater utstedt etter SEID v1.0 er utløpt.

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 EN 319 412-2 [11] av hensyn til interoperabilitet og samtrafikk.

Den anbefalte profilen bør benyttes for alle personsertifikater utstedt av sertifikatutstedere som utsteder sertifikater som skal kunne bekrefte et norsk fødselsnummer eller D-nummer, da spesielt etter overgangsperiodens slutt (se kap. 4.3) hvor det ikke anbefales å utstede personsertifikater etter SEID v1.0 lenger.

5.1 Issuer

Issuer skal være iht. kap. 4.2.3 i ETSI EN 319 412-2 [11], men se kap. 6.2.1 for bruk av organizationIdentifier når Issuer er en juridisk person.

5.2 Subject

Følgende attributter er obligatoriske:

- countryName (C) = 'NO'
- serialNumber: skal unikt identifisere den fysiske personen (se kap. 5.2.1)
- givenName (G): fornavn/mellomnavn slik dette er registrert i Folkeregisteret[1]
- surname (SN): etternavn slik dette er registrert i Folkeregisteret
- commonName (CN): navn på sertifikatinnehaver, dette kan være sertifikatinnehaverens foretrukne navn

Dersom en velger å utstede sertifikater med antall tegn innenfor grenseverdiene gitt i RFC 5280, vil det være behov for å forkorte enkelte navn. Det anbefales at man benytter algoritmen som er definert i [5] for dette formålet.

Dersom en sertifikatutsteder velger å gå utover disse grenseverdiene, så er det greit å være oppmerksom på at dette kan føre til kompatibilitetsproblemer med applikasjoner som forholder seg strengt til RFC-en.

I tillegg kan sertifikatfeltet inneholde andre attributter, dersom for eksempel personen assosieres med en organisasjon (som i ansattsertifikater) kan følgende attributter benyttes:

- organizationName (O) – organisasjonsnavn iht. Enhetsregisteret
- organizationIdentifier – organisasjonsnummer iht. Enhetsregisteret

Se kap. 6.2 for mer informasjon om bruk av attributter for organisasjoner.

5.2.1 Samordnet bruk av serialNumber attributtet i Subject-feltet

ETSI EN 319 412-2 [11] legger ingen spesifikke føringer på innholdet i serialNumber attributtet, men gir åpninger for bruk av nasjonale tilpasninger gjennom bruk av semantiske identifikatorer (Semantics Identifiers) iht. ETSI EN 319 412-1 [10].

[1] *ETSI EN 319 412-2 [11] tillater at givenName, surname og CommonName inneholder flere tegn enn det som er spesifisert i RFC 5280 (som er henholdsvis 16, 40 og 64 tegn).*

Den foreslåtte profilen viderefører bruk av utstederspesifikke personidentifikatorer i serialNumber attributtet iht. SEID-sertifikatprofil v1.0 – se også [4].

For å sikre harmonisering etter europeiske standarder (ETSI EN 319 412-1) anbefales det å inkludere en semantisk identifikator iht. ETSI EN 319 412-1:

- UN:NO-<utstederspesifikk personidentifikator>
    - For eksempel serialNumber=UN:NO- 9578-4050-100009315

Bruken av en slik identifikator krever ifølge ETSI EN 319 412-1 følgende:

> *When a locally defined identity type reference is provided (two characters followed by ":"), the*
>
> *nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference preceding the ":" character shall be unique within the context of the specified uniformResourceIdentifier.*

Dette krever at qcStatement-2 iht. RFC 3739 er inkludert, se også ETSI EN 319 412-5.

Når denne identifikatoren brukes, skal nameRegistrationAuthorites-elementet i qcStatement-2 inneholde en URL til en nettside som sier noe om hvordan den utstederspesifikke identifikatoren under "skjemaet UN:NO" er bygget opp. Denne URL-en skal være:

> *https://www.nkom.no/english/nameRegistrationAuthority*

Bruken av qcStatement-2 og denne URL-en i sertifikatene er obligatorisk for SEID-sertifikatprofil v2.0 fra 1. april 2023.

En sertifikatutsteder kan også velge å bruke fødselsnummer eller D-nummer som identifikator i serialNumber attributtet. I tilfelle anbefales det å benytte semantisk identifikator iht. ETSI EN 319 412-1 for å angi at det brukes et nasjonalt identitetsnummer:

- PNONO-<fødselsnummer>

Bruk av semantisk identifikator skal angis ved at en inkluderer qcStatement-2 (*id-etsi-qcs-semanticsId-Natural*) (se kap. 5.4). Dette gjelder både kvalifiserte og ikke-kvalifiserte sertifikater.

Bruk av andre identifikatorer i serialNumber attributtet spesifiseres ikke her. Et tenkt eksempel er utstedelse av sertifikater med helsepersonellnummer som identifikator.

5.2.2 Profilen brukt for personer som ikke er registrert i Folkeregisteret

For personer som ikke er registrert i Folkeregisteret vil følgende attributter kunne være annerledes.

- countryName (C) kan være ulikt 'NO'
- organizationName (O) – organisasjonsnavn iht. aktuelt register
- organizationIdentifier – organisasjonsnummer iht. aktuelt register
- serialNumber: skal unikt identifisere den fysiske personen, evt. med annen offentlig identifikator (i stedet for fødselsnummer eller D-nummer)

Disse attributtene skal være iht. ETSI EN 319 412-2 [11] og evt. følge reglene for bruk av offentlige anerkjente identifikator i det enkelte land.

5.2.3 Syntaks og semantikk for utstederspesifikk personidentifikator

Dette videreføres fra SEID-sertifikatprofil v1.0 der utstederspesifikke personidentifikatorer er bygget opp av følgende elementer:

Type 3 (utstederspesifikke personidentifikatorer)

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

For å lette den visuelle lesbarheten av attributtet serialNumber skal hovedelementene skilles med bindestrek. Eks.: 9578-4000-11065534187.

En liste over tildelte nasjonale utstederidentifikatorer finnes i et eget vedlegg [4].

5.2.4 Bruk av oppslagstjenester

Dersom fødselsnummer ikke eksplisitt finnes i serialNumber feltet skal sertifikatutsteder tilby en oppslagstjeneste som gjør det mulig for autoriserte[2] sertifikatmottakere å få utlevert sertifikatinnehavers fødselsnummer[3] på bakgrunn av den unike identifikatoren som befinner seg i sertifikatets serialNumber felt.

Sertifikatfeltet *Authority Information Access* vil kunne inneholde en peker til en slik oppslagstjeneste basert på bruk av OCSP-protokollen [8]. SEID-leveranse 2 [2] inneholder spesifikasjoner av en slik oppslagstjeneste.

5.3 Sertifikatets bruksområder - Key Usage

Et sertifikat kan dekke ulike bruksområder og disse defineres gjennom bruk av sertifikatutvidelsen KeyUsage iht. RFC 5280 [7].

For personssertifikater tenker vi primært på følgende bruksområder

- Autentisering: med Key Usage = digitalSignature
- Signering: med Key Usage = nonRepudiation (også kalt contentCommitment)
- Kryptering: med Key Usage = keyEncipherment eller keyAgreement

Det er tillatt å kombinere flere bruksområder i ett og samme sertifikat, men vi anbefaler spesielt å ikke blande bruksområdet Signering med andre bruksområder.

[2] *En autorisert sertifikatmottaker vil si et sertifikatmottaker som har nødvendig autorisasjon for bruk av fødselsnummer.*

[3] *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.*

ETSI EN 319 412-2 [11] inneholder følgende tillatte kombinasjoner av Key Usage:

> The key usage extension shall be present and shall contain one (and only one) of the key usage settings defined in table 1 (A, B, C, D, E or F). Type A, C or E should be used to avoid mixed usage of keys.

Table 1: Key usage settings

Type	Non-Repudiation (Bit 1)	Digital Signature (Bit 0)	Key Encipherment or Key Agreement (Bit 2 or 4)
A	X		
B	X	X	
C		X	
D		X	X
E			X
F	X	X	X

> Certificates used to validate commitment to signed content (e.g. documents, agreements and/or transactions) shall be limited to type A, B or F. Of these alternatives, type A should be used (see the security note 2 below).
>
> EXAMPLE: Digital signatures which are aimed to be used as advanced electronic signatures as defined in Regulation (EU) No 910/2014 [i.5] are considered to signal commitment to signed content.

5.4 Qualified Certificate statement

Alle sertifikater som benytter utstederspesifikk identifikator eller fødselsnummer/D-nummer iht. kap. 5.2.1 må inneholde følgende QCStatement:

- qcStatement-2 iht. RFC 3739 [6] og ETSI EN 319 412-1 [10] kap. 5.1.1 med verdien *id-etsi-qcs-semanticsId-Natural*.

Sertifikater som utstedes som kvalifiserte sertifikater for elektronisk signatur skal inneholde følgende EU QCStatements iht. ETSI EN 319 412-5:

- esi4-qcStatement-1 – EU qualified certificate compliance
- esi4-qcStatement-6 – EU qualified certificate of a particular type
  - id-etsi-qct-esign – EU qualified certificate for electronic signature

Dersom, og kun dersom, sertifikatet brukes med kvalifisert elektronisk signaturframstillingssystem, det vil si at det understøtter kvalifisert elektronisk signatur, skal sertifikatet inneholde følgende EU QCStatement iht. ETSI EN 319 412-5:

- esi4-qcStatement-4 – EU qualified signature/seal compliance

Det er kun sertifikater med bruksområde Signering som kan merkes som et kvalifisert sertifikat for elektronisk signatur.

Det finnes andre EU QCStatements som også kan brukes [13], men dette er opp til den enkelte sertifikatutsteder.

5.5 Endringer fra SEID-sertifikatprofil v1.0

Sertifikatfelt eller utvidelse	**SEID v1.0**	**SEID v2.0**
Subject	countryName (C)=NO commonName (CN): Sertifikatinnehavers navn som registert i Folkeregisteret serialNumber: 9578-xxxx-123456789	countryName (C)=NO commonName (CN): Sertifikatinnehavers foretrukne navn eller iht. sertifikatutsteders policy serialNumber=UN:NO-9578-xxxx-123456789 eller serialNumber= PNONO-<fnr/D-nr> givenName (G): Sertifikatinnehavers fornavn/mellomnavn som registrert i Folkeregisteret surname (SN): Sertifikatinnehavers etternavn som registrert i Folkeregisteret
Subject med organisasjons-tilknytning	organizationName (O): <organisasjonsnavn>'-'<organisasjonsnummer> som registrert i Enhetsregisteret	organizationName (O): Organisasjonsnavn som registrert i Enhetsregisteret organizationIdentifier: Organisasjonsnummer som registrert i Enhetsregisteret, formatert iht. 6.2.1

Sertifikatfelt eller utvidelse	**SEID v1.0**	**SEID v2.0**
KeyUsage	Følgende verdier anbefalt for bruksområde Signering: • nonRepudiation, eller • digitalSignature, eller • nonRepudation + digitalSignature Følgende verder anbefalt for bruksområde kryptering: • keyEncipherment • dataEnciphement	Følgende verdier anbefalt for bruksområde Signering: • nonRepudiation Følgende verder anbefalt for bruksområde kryptering: • keyEncipherment, eller • keyAgreement Følgende verdier anbefalt for bruksområde autentisering: • digitalSignature Flere bruksområder kan kombineres i ett sertifikat
qcStatements	Gjeldende praksis hos noen utstedere har vært å inkludere QCStatements i sertifikater for alle bruksområder EU QC Statement: • esi4-qcStatement-1	qcStatement-2 benyttes når serialNumber inneholder utstederspesifikk personidentifikator iht. UN:NO-skjemaet Kun sertifikater med bruksområde Signering kan merkes som kvalifisert sertifikat: For alle sertifikater, indikasjon på bruk av semantisk identifikator: • id-etsi-qcs-semanticsId-Natural For kvalifiserte sertifikater, følgende EU QC Statements: • esi4-qcStatement-1 • esi4-qcStatement-6 ○ id-etsi-qct-esign For sertifikater som understøtter kvalifisert signatur, i tillegg: • esi4-qcStatement-4

I SEID v1.0 er lengden på O og CN begrenset iht. RFC 5280, mens for SEID v2.0 er det tillatt å gå utover disse grensene for å inkludere fullt navn i disse attributtene, det samme gjelder for givenName og surname. Sjekk med sertifikatutsteders policy for å se hva som gjelder.

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.

Profilen kan også benyttes for virksomheter som ikke er registrert i Enhetsregisteret, se kap. 6.2 for mer informasjon.

Profilen er anvendelig for alle virksomhetssertifikater, herunder kvalifiserte sertifikater for elektronisk segl, hvor sertifikatet inneholder informasjon direkte knyttet til virksomhetens identitet i Enhetsregisteret.

I den grad det stilles spesielle profilkrav til kvalifiserte sertifikater, og som det ikke er naturlig å knytte til alle virksomhetssertifikater, er dette eksplisitt påpekt og håndtert i profilen.

Den anbefalte profilen er basert på ETSI EN 319 412-3 [12] som igjen er basert på RFC 5280 [7].

Dette kapittelet tar kun for seg sertifikatfelter hvor den anbefalte norske profilen inneholder en ytterligere profilering av, evt. avvik fra, nevnte standarder.

Kapitlet inkluderer også sertifikatfelter der det er vesentlige forskjeller mellom SEID-sertifikatprofil v1.0 og v2.0. Dette skal gjøre det enklere for aktører å sikre støtte for begge generasjoner sertifikater i overgangsperioden og inntil de siste sertifikater utstedt etter SEID v1.0 er utløpt.

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 EN 319 412-3 [12] av hensyn til interoperabilitet og samtrafikk.

Den anbefalte profilen bør benyttes for alle virksomhetssertifikater utstedt til virksomheter registrert i det norske Enhetsregisteret, da spesielt etter overgangsperiodens slutt (se kap. 4.3) hvor det ikke anbefales å utstede virksomhetssertifikater etter SEID v1.0 lenger.

6.1 Issuer

Issuer skal være iht. kap. 4.2.3 i ETSI EN 319 412-2 [11], men se kap. 6.2.1 for bruk av organizationIdentifier når Issuer er en juridisk person.

6.2 Subject

Følgende attributter er obligatoriske:

- countryName (C) = 'NO'
- organizationIdentifier – skal unikt identifisere den juridiske personen (se kap. 6.2.1)
- organizationName (O) – fullt[4] navn på den juridiske personen slik denne er registrert i Enhetsregisteret
- commonName (CN) – navn som sertifikatinnehaver foretrekker å bruke i sertifikatet

OrganizationIdentifer er et nytt attributt sammenliknet med bruken av serialNumber i SEID v1.0 som tidligere har vært brukt for å identifisere den juridiske personen unikt.

Sertifikatutsteder kan velge å inkludere serialNumber i tillegg til organizationIdentifier, men det er sistnevnte som vil identifisere den juridiske personen i sertifikatet iht. ETSI 319 412-3.

I tillegg kan sertifikatfeltet inneholde andre attributter, for underenheter kan det for eksempel være mulig å bruke:

- organizationalUnitName (OU) – navn og organisasjonsnummer på underenhet

Dersom en sertifikatutsteder velger å gå utover disse grenseverdiene, så er det greit å være oppmerksom på at dette kan føre til kompatibilitetsproblemer med applikasjoner som forholder seg strengt til RFC-en.

6.2.1 Samordnet bruk av organizationIdentifier attributtet i Subject-feltet

ETSI EN 319 412-2 legger ingen spesifikke føringer på innholdet i organizationIdentifier attributtet, men det anbefales å bruke semantiske identifikatorer (Semantics Identifiers) iht. ETSI EN 319 412-1.

For å sikre harmonisering etter europeiske standarder anbefales det å inkludere en semantisk identifikator iht. ETSI EN 319 412-1 for juridiske personer registrert i Enhetsregisteret:

- NTRNO-<organisasjonsnummer iht. Enhetsregisteret>

[4] *ETSI EN 319 412-2 tillater at O, CN og OU inneholder flere tegn enn det som er spesifisert i RFC 5280 (som alle er maksimalt 64 tegn).*

En sertifikatutsteder som velger å bruke andre identifikatorer enn de utstederspesifikke personidentifikatorene anbefales å benyttes semantiske identifikatorer iht. ETSI EN 319 412-1, for eksempel:

- LEIXG-<global Legal Entity Identifier>

I disse tilfellene bør den semantiske identifikatoren (*id-etsi-qcs-SemanticsId-Legal*) inkluderes i form av qcStatement-2 (se kap. 6.4).

6.2.2 Profilen brukt for virksomheter som ikke er registrert i Enhetsregisteret

For personer som ikke er registrert i Enhetsregisteret vil følgende attributter kunne være annerledes.

- countryName (C) kan være ulikt 'NO'
- organizationName (O) – organisasjonsnavn iht. aktuelt register
- organizationIdentifier – organisasjonsnummer iht. aktuelt register

Disse attributtene skal være iht. ETSI EN 319 412-3 [12] og evt. følge reglene for bruk av organisasjonsnummer i det enkelte land.

6.3 Sertifikatets bruksområder - Key Usage

Sertifikatprofilen for virksomhetssertifikatet følger de samme anbefalinger mht. bruksområde og KeyUsage som sertifikatprofilen for personsertifikater, se kap. 5.3.

6.4 Qualified Certificate statement

Alle sertifikater som benytter en semantisk identifikator iht. kap. 6.2.1 bør inneholde *id-etsi-qcs-semanticsId-Legal* i qcStatement-2 iht. ETSI EN 319 412-1 [10] og RFC 3739 [6].

Anbefalt sertifikatprofil for virksomhetssertifikater versjon 1.0 dekket ikke kvalifiserte sertifikater. Tradisjonelle virksomhetssertifikater kan fortsatt utstedes som ikke-kvalifiserte sertifikater, men profilen dekker nå også kvalifiserte sertifikater for elekronisk segl.

Sertifikater som utstedes som kvalifiserte sertifikater for elektronisk segl skal inneholde følgende EU QCStatements iht. ETSI EN 319 412-5:

- esi4-qcStatement-1 – EU qualifed certificate compliance
- esi4-qcStatement-6 – EU qualifed certificate of a particular type
    - id-etsi-qct-eseal – EU qualified certificate for electronic seal

Dersom, og kun dersom, sertifikatet brukes med kvalifisert elektronisk seglframstillingssystem, det vil si at det understøtter kvalifisert elektronisk segl, skal sertifikatet inneholde følgende EU QCStatement iht. ETSI EN 319 412-5:

- esi4-qcStatement-4 – EU qualified signature/seal compliance

Det er kun sertifikater med bruksområde Signering (og/eller Autentisering) som kan merkes som et kvalifisert sertifikat for elektronisk segl.

Det finnes andre EU QCStatements som også kan brukes, men dette er opp til den enkelte sertifikatutsteder.

6.5 Endringer fra SEID-sertifikatprofil v1.0

Sertifikatfelt eller utvidelse	**SEID v1.0**	**SEID v2.0**
Subject	countryName (C)=NO organizationName (O): Organisasjonens fulle navn iht. Enhetsregisteret serialNumber: Organisasjonsnummer fra Enhetsregisteret commonName (CN): Navn som sertifikatinnehaver foretrekker å bruke i sertifikatet	countryName (C)=NO organizationName (O): Organisasjonens fulle navn iht. Enhetsregisteret organizationIdentifier=Organisasjonsnummer fra Enhetsregisteret formatert iht. 6.2.1 commonName (CN): Navn som sertifikatinnehaver foretrekker å bruke i sertifikatet
Underenhet	organizationalUnitName (OU): <organisasjonsnavn>'-'<organisasjonsnummer> for underenhet som registrert i Enhetsregisteret	organizationalUnitName (OU): <organisasjonsnavn>'-'<organisasjonsnummer> for underenhet som registrert i Enhetsregisteret Se også kap 7
KeyUsage	Følgende verdier anbefalt for bruksområde Signering: • nonRepudiation, eller • digitalSignature, eller • nonRepudation + digitalSignature Følgende verder anbefalt for bruksområde kryptering: • keyEncipherment • dataEnciphement	Følgende verdier anbefalt for bruksområde Signering: • nonRepudiation Følgende verder anbefalt for bruksområde kryptering: • keyEncipherment, eller • keyAgreement Følgende verdier anbefalt for bruksområde autentisering: • digitalSignature Flere bruksområder kan kombineres i ett sertifikat

Sertifikatfelt eller utvidelse	SEID v1.0	SEID v2.0
qcStatements		Virksomhetssertifikater kan utstedes som ikke-kvalifiserte sertifikater[5] Kun sertifikater med bruksområde Signering (og/eller Autentisering) bør merkes som kvalifisert sertifikat: For alle sertifikater, indikasjon på bruk av semantisk identifikator: • id-etsi-qcs-semanticsId-Legal For kvalifiserte sertifikater i tillegg følgende EU QC Statements: • esi4-qcStatement-1 • esi4-qcStatement-6 ○ id-etsi-qct-eseal For sertifikater som understøtter kvalifisert segl, i tillegg: ○ esi4-qcStatement-4

I SEID v1.0 er lengden på O, CN og OU begrenset iht. RFC 5280, mens for SEID v2.0 er det tillatt å gå utover disse grensene for å inkludere fullt navn i disse attributtene. Sjekk med sertifikatutsteders policy for å se hva som gjelder.

7 Virksomhetssertifikater til underenheter

I forbindelse med innføring av SEID-sertifikatprofil v2.0 er det identifisert et behov for å definere en mer tydelig standard for Virksomhetssertifikater utstedt til underenheter.

[5] *Virksomhetssertifikater har tradisjonelt vært ikke-kvalifisert (dvs. på NCP/NCP+-nivå). Det er dette som er situasjonen vi kommer fra med SEID v1.0. For SEID v2.0 er tanken å videreføre profiler for disse nivåene, samtidig som vi introduserer «kvalifiserte virksomhetssertifikater» som et nytt begrep (dvs. på QCP-nivå).*

Gjeldende praksis under SEID v1.0 har vært basert på bruk av attributtet organizationalUnitName (OU) i Virksomhetssertifikatene. Dersom OU har inneholdt et 9-sifret (organisasjons)nummer, har dette vært brukt som en identifikator for en underenhet, mens hovedenheten er identifisert av de andre attributtene i sertifikatet.

Med SEID v2.0 ønsker vi å endre denne praksisen og innfører en mer detaljert formatering av innholdet i OU-attributtet når dette brukes for å identifisere en underenhet.

Denne endringen har virkning fra 1.januar 2024 for alle virksomhetssertifikater utstedt til underenheter.

7.1 Hovedenheter og underenheter

Det er Brønnøysundregistrene som definerer hovedenheter og underenheter.

Se https://www.brreg.no/bedrift/underenhet/ for mer informasjon.

En hovedenhet er beskrevet som:

- «*Samlebegrep for selskap, foreninger, personer og annet som er registrert i Enhetsregisteret».*

Mens en underenhet er beskrevet ved:

- *«Den aktiviteten hovedenheten driver. En hovedenhet kan ha en eller flere underenheter. Underenhetene er ikke selvstendige. De vil alltid være knyttet opp mot en hovedenhet*.»

Med utgangspunkt i denne definisjonen av underenhet synes det naturlig å videreføre prinsippet med at det er hovedenheten som blir identifisert i de andre attributtene i sertifikatet, mens OU-attributtet faktisk identifiserer underenheten.

Det vil være viktig at alle applikasjoner og tjenester som forholder seg til Virksomhetssertifikater, må ta høyde for dette og sikre at sertifikatet kun kan benyttes av underenheten.

Man bør spesielt sørge for at man ikke kan bruke et slik sertifikat på vegne av hovedenheten, dvs. eventuelle autorisasjoner og tilganger skal begrenses til underenheten.

7.2 Bruk av underenheter

Ifølge Brønnøysundregistrene er det Statistisk sentralbyrå som avgjør hvilke underenheter som skal registreres. Underenheter benyttes dersom hovedenheten driver næringsvirksomhet i flere bransjer eller har næringsvirksomhet på flere geografiske steder.

Det finnes også et detaljert regelverk for offentlig forvaltning og registrering av underenheter i kommuner, fylkeskommuner og helseforetak. Se www.ssb.no for mer informasjon.

7.3 Bruk av OU-attributtet

Det er allerede tatt høyde for bruk av OU-attributtet i SEID v2.0. Vi finner følgende kommentar under kap. **6.2 Subject**:

> *I tillegg kan sertifikatfeltet inneholde andre attributter, for underenheter kan det for eksempel være mulig å bruke:*
>
> - *organizationalUnitName (OU) – navn og organisasjonsnummer på underenhet*

Vi kunne valgt å utstede et Virksomhetssertifikat direkte til en underenhet, men siden en underenhet ikke er selvstendig og alltid vil være knyttet opp til en hovedenhet, synes det naturlig å videreføre bruken av OU-attributtet for dette formålet.

7.4 Virksomhetssertifikat til underenhet

Vi trenger en klargjøring og presisering av innholdet i OU-attributtet for å gjøre det tydelig at dette er et sertifikat utstedt til en underenhet. Dagens praksis med bruk av et 9-sifret organisasjonsnummer er for svak i så måte.

OU skal formateres som angitt nedenfor for å angi at dette er en underenhet:

- OU = ER:NO-<orgnr>-<orgnavn>

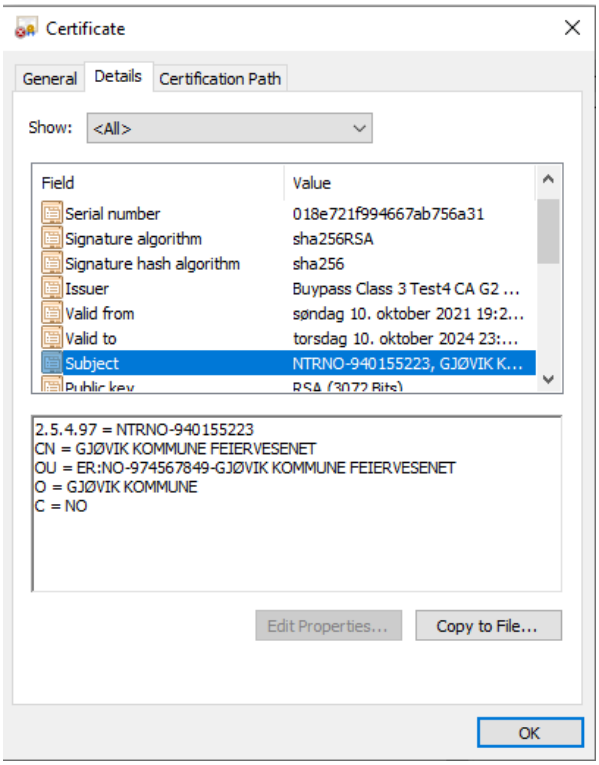
Prefiks **ER:NO** angir at attributtet inneholder organisasjonsnummer og -navn på en underenhet. Hovedenheten blir identifisert med de ordinære attributtene. ER angir at underenheten er definert i Enhetsregisteret. Vi ser for oss at dette prefikset blir harmonisert med et fremtidig nasjonalt kodeverk for å angi andre kilder enn Enhetsregisteret for underenheter.

Vi sier at et Virksomhetssertifikat som utstedes til en underenhet skal benytte følgende attributter:

- countryName (C): 'NO'
- organizationIdentifier: organisasjonsnummer som unikt identifiserer *hovedenheten* iht. Enhetsregisteret
- organizationName (O): fullt organisasjonsnavn på *hovedenheten* slik denne er registrert i Enhetsregisteret
- organizationalUnitName (OU): skal identifisere *underenheten*
- commonName (CN) – navn som sertifikatinnehaver foretrekker å bruke i sertifikatet

I henhold til RFC5280 kan ikke OU-attributtet inneholde mer enn 64-tegn mens for SEID v2.0 er det tillatt å gå utover dette. Sjekk med sertifikatutsteders policy for å se hva som gjelder.

Et virksomhetssertifikat utstedt til Feiervesenet i Gjøvik kommune vil kunne se slik ut:



Her er Feiervesenet en underenhet til Gjøvik kommune som er hovedenheten.

7.5 Krav til verifisering

Knytningen mellom hovedenhet og underenhet må verifiseres mot Enhetsregisteret i Brønnøysund.