DanID
Certification Practice Statement (CPS)

V. 1.1

februar 2009

1 Introduktion

1.1 Oversigt

DanID A/S (CVR-nr. 30 80 84 60) er et 100% datterselskab ejet af PBS A/S (CVR-nr. 20 01 61 75). Årsregnskaber kan bestilles ved henvendelse.

Dette er *DanID's* Certification Practice Statement (CPS). Det beskriver, hvordan du kan få udstedt certifikater fra *DanID*.
Når du får udstedt et certifikat fra *DanID*, er der to dokumenter, du bør læse:

- Certificate Policy (CP), der hører til det givne certifikat.
- Certification Practice Statement (CPS) (dette dokument).

Disse to dokumenter indeholder oplysninger, som er relevante for alle, som kommer i kontakt med certifikater udstedt af *DanID.* De indeholder også oplysninger om, hvilken tillid man kan have til de certifikater, der udstedes af *DanID*, og en præcisering af de involverede parters ansvar.

Dette CPS skal betragtes som den offentligt tilgængelige dokumentation, der omhandler alle certifikatydelser fra *DanID*. Heri beskrives, hvordan *DanID* har valgt at indrette sit certificeringscenter med hensyn til placering, teknik, personale osv. Desuden beskrives de forskellige roller i certificeringen og de generelle procedurer for alle certifikatydelser. Ud over dette offentlige CPS kan der suppleres med yderligere dokumentation, som blandt andet er beskrevet i OCES CP. Denne dokumentation er dog fortrolig og er kun tilgængelig efter særlig aftale med *DanID*.

For hvert certifikatprodukt er der udarbejdet en CP. Denne CP beskriver det konkrete ansvar samt de forpligtelser og procedurer, der knytter sig til et bestemt/specifikt certifikat.

Som certifikatindehaver er det tilstrækkeligt at acceptere de juridiske betingelser, der er beskrevet i CP'en, og bruge CPS'et som reference.

Indholdet af denne CPS er struktureret således:

- Roller i certificeringen
- Procedurer for autentificering og certificering
- Sikkerheden hos *DanID*
- Certifikaternes indhold
- Administration af CPS.

1.2 Identifikation

CPS-navn: *DanID* CPS v. 1.1
Object Identifier: 1.3.6.1.4.1.31313.0.1.1.1

Dette CPS hører sammen med nedenstående certifikatpolitikker (CP):

- SSL Server Certifikat CP v. 1.2 fra *TDC SSL Server CA*
  Object identifier: 1.3.6.1.4.1.4386.2.1.1.2
- Certifikat Politik for klasse II-certifikat fra *TDC Internet Class II*
  Object Identifier: 1.3.6.1.4.1.4386.2.2.2.1.1

- Certifikat Politik for lukket brugergruppe-certifikat fra *Tele Danmark, Certificate Hotel II*
  Object Identifier: 1.3.6.1.4.1.4386.2.2.1.1.1
- Certifikat Politik for OCES personcertifikat
  Object Identifier: 1.2.208.169.1.1.1.1.1
- Certifikat Politik for OCES medarbejdercertifikat
  Object Identifier: 1.2.208.169.1.1.1.2.1
- Certifikat Politik for OCES virksomhedscertifikat
  Object Identifier: 1.2.208.169.1.1.1.3.1
- Certifikat Politik for OCES personcertifikat
  Object Identifier: 1.2.208.169.1.1.1.1.2
- Certifikat Politik for OCES medarbejdercertifikat
  Object Identifier: 1.2.208.169.1.1.1.2.3
- Certifikat Politik for OCES virksomhedscertifikat
  Object Identifier: 1.2.208.169.1.1.1.3.2
- Certifikat Politik for OCES personcertifikat
  Object Identifier: 1.2.208.169.1.1.1.1.3
- Certifikat Politik for OCES medarbejdercertifikat
  Object Identifier: 1.2.208.169.1.1.1.2.4
- Certifikat Politik for OCES virksomhedscertifikat
  Object Identifier: 1.2.208.169.1.1.1.3.3
- Certifikat Politik for OCES funktionsscertifikat
  Object Identifier: 1.2.208.169.1.1.1.4.1

DanID forbeholder sig ret til at oprette yderligere CP'er med reference til dette CPS.

1.3 Roller og anvendelse

Følgende betegnelse anvendes i det følgende for parterne i certificeringsprocessen:

- Certification Authority (CA)
- Local Registration Authority (LRA)
- Certifikatindehaver (signaturafgiver)

Tredjemand, som ikke er direkte involveret i certificeringen, f.eks. modtager af en digital signatur hørende til et certifikat fra *DanID*, vil i det følgende blive omtalt som signaturmodtager.

1.3.1 Certification Authority (CA)

En CA er den myndighed, der står for udstedelse og administration af certifikater. Under *DanID* er følgende CA'er etableret:

- *DanID* SSL server CA
- *DanID* klasse II CA
- *DanID* lukket brugergruppe CA
- *DanID* OCES CA
- *DanID* TDC Root CA

DanID forbeholder sig ret til at etablere yderligere CA'er.

CA'er under *DanID* kan udstede følgende certifikater.

- SSL-servercertifikat (se den tilhørende CP)
- Klasse II person-, medarbejder- og virksomhedscertifikat (se den tilhørende CP)
- Lukkede brugergruppecertifikater (se den tilhørende CP)

- OCES-certifikater (se de tilhørende CP'er for henholdsvis person-, medarbejder-, funktions- og virksomhedscertifikater)
- Certifikat fra root CA (se den tilhørende CP)

DanID forbeholder sig ret til at udbyde yderligere certifikatydelser med reference til dette CPS.

1.3.2 Local Registration Authority (LRA)

En LRA er den myndighed, der står for at autentificere ansøgere til certifikater. Følgende LRA'er er etableret under *DanID*:

- *DanID* SSL server LRA
- *DanID* Klasse II LRA
- *DanID* Lukket brugergruppe LRA
- *DanID OCES-person, medarbejder, funktions og virksomheds LRA*

DanID forbeholder sig ret til at etablere yderligere LRA'er.

1.3.3 Certifikatindehavere

I overensstemmelse med de tilhørende CP'er defineres certifikatindehaveren som den, et certifikat bliver udstedt til. Certifikatindehaveren kan være:

- En person
- En virksomhed/organisation

Der udstedes kun certifikater til ansøgere, der kan identificeres entydigt, se afsnit 3.1 i dette CPS. For OCES-medarbejdercertifikater understøttes også en certifikatholderrolle. Se definition på certifikatindehaver og certifikatholder i OCES-medarbejder CP.

1.3.4 Anvendelse

Et certifikat er en digital bekræftelse på sammenhængen mellem en certifikatindehaver og dennes offentlige krypteringsnøgle.
Certifikater, der er udstedt under dette CPS, må kun bruges til de formål, der er beskrevet i den tilhørende CP.

1.4 Henvendelse til DanID

Dette CPS bliver administreret af *DanID*, jævnfør sektion 7.

Spørgsmål vedrørende dette CPS kan rettes til:

DanID A/S
Olof Palmes Allé 32
8200 Århus N
Danmark

http://danid.dk

2 Operationelle procedurer

Dette afsnit beskriver de procedurer, som certifikatansøgere skal igennem for at modtage, suspendere eller spærre et certifikat. Ligeledes beskrives, hvad man som signaturmodtager skal gøre for at verificere et certifikat. En detaljeret beskrivelse af de nedenstående procedurer for OCES-certifikater (bestilling, udstedelse og spærring af certifikater) findes på http://danid.dk

2.1 Certifikatansøgning

I forbindelse med ansøgning om et certifikat, skal ansøger generelt:

- Levere de informationer, der fremgår af den aktuelle CP.
- Generere et nøglepar, der består af en offentlig og en privat nøgle, som beskrevet i den aktuelle CP.
- Generere et certifikat-request, der svarer til ovenstående punkter (dvs. at man med den private nøgle underskriver den offentlige nøgle samt den information, der skal stå i certifikatet), eller som beskrevet i den aktuelle CP.
- Underskrive en eventuel kontrakt.

Se dog den relevante CP for detaljer om ansøgningen for de enkelte certifikattyper.

2.2 Certifikatudstedelse

CA kontrollerer før udstedelse, at informationerne i ansøgningen er afgivet og verificeret i overensstemmelse med dette CPS og den tilhørende CP, og at nøglerne er et samhørende nøglepar.
Er dette tilfældet, udsteder CA et certifikat. Dette sendes til certifikatansøgeren og gemmes desuden i CA'ens certifikatdatabase.

2.3 Certifikatmodtagelse

Certifikatansøgeren kan modtage certifikatet på forskellige måder alt efter certifikattype. Se den relevante CP for yderligere oplysninger om dette. Typisk vil internet og e-mail være understøttet som transportmekanisme.

2.4 Certifikatspærring

Status for et certifikat kan ændres til spærret af certifikatindehaveren samt af CA, som beskrevet i den aktuelle CP.

2.4.1 Af certifikatindehaveren

Certifikatindehaveren kan på et hvilket som helst tidspunkt anmode om at få spærret sit certifikat. Vilkår for spærring fremgår af den relevante CP. Specielt for OCES-certifikater gælder, at disse kan spærres ved indsendelse af e-mail signeret med det aktuelle certifikat til emailadressen support@certifikat.dk samt døgnet rundt ved kontakt til telefon 80801616.

2.4.2 Af CA

Hvis CA får mistanke om, at certifikatindehaveren ikke har handlet i overensstemmelse med dette CPS eller den relevante CP, kan CA vælge at spærre et certifikat.

Certifikatindehaveren bliver informeret om en eventuel spærring via e-mail eller almindelig post.

Se relevant OCES CP for en samlet liste over parter med myndighed til at begære et certifikat spærret samt de procedurer, der er forbundet hermed.

2.5 Certifikatverifikation

DanID udsteder en Certificate Revocation List (CRL) hørende til hver CP. Dette er spærringslisten over spærrede certifikater. Disse lister opdateres periodisk, som angivet i den certifikatpolitik, der hører til certifikatet. Specielt gælder for OCES-certifikater, at spærrelisten opdateres ved spærring af certifikat, dog minimum hver tolvte time.

Tekniske referencer til spærrings- og suspenderingsfunktionerne findes i den CP, der hører til certifikatet. Specielt indeholder de enkelte OCES-certifikater HTTP- og LDAP-adresse på spærreliste i certifikat-extention CRLDistributionPoint.

2.6 Procedurer for sikkerhedskontrol

DanID foretager løbende intern auditering af driftsmiljøer og procedurer omkring udstedelse af certifikater. *DanID* har én gang årligt en ekstern audit, der gennemføres af en statsautoriseret revisor.

Resultatet af denne audit indmeldes årligt til IT- og Telestyrelsen. Resultatet af audits offentliggøres ikke, men kan stilles til rådighed af *DanID,* hvis man skønner, at der er behov for det.

DanID er etableret med en daglig ledelse bestående af personer med forretnings- og informationssikkerhedsmæssige kompetencer.

DanID driftsmiljø og procedurer opfylder dansk lov samt EU-krav til nøglecentre, der ønsker at udstede kvalificerede samt OCES-certifikater. Dette indebærer blandt andet et dedikeret driftsmiljø og en rolleopdelt driftsorganisation med spidskompetence inden for tilgængelighed, sikkerhed og certifikatteknologi.

2.7 Arkivering af information

Information, der har været offentliggjort, samt information udvekslet med certifikatindehavere og de forskellige dele af certificeringssystemet, arkiveres. Det drejer sig om følgende information:

- Certifikat-request og relateret kommunikation
- Underskrevne kontrakter
- Indhold af udstedte certifikater
- Certifikatfornyelse og anden kommunikation med certifikatindehavere
- Registreringer vedrørende CA-nøglefornyelse
- Spærrings- og suspenderingsanmodninger og relateret kommunikation
- CRL'er
- Kontrolresultater
- CPS og CP'er

Disse oplysninger opbevares som hovedregel i seks år.

Information kan begæres udleveret efter krav fra myndighederne.

Parter kan få stillet information til rådighed om individuelle transaktioner, de selv har deltaget i.

DanID er underlagt persondataloven. Al information, der er indhentet i forbindelse med håndtering af certifikater, behandles som fortrolig, bortset fra offentlige data i selve certifikaterne og tilhørende tjenester.

2.8 Nøgleskift

2.8.1 Skift af CA-nøgler

CA'ens private og offentlige nøgle har af sikkerhedsgrunde kun en endelig gyldighedsperiode. I god tid før udløb af CA'ens nøgler, genererer CA et nyt nøglepar, som herefter benyttes ved

udstedelse af certifikater. For at få certifikater udstedt under både den gamle og nye CA-nøgle accepteret i applikationerne, *krydscertificeres* de to CA-nøglepar. De to krydscertifikater, som er resultatet heraf, offentliggøres herefter til installation i de applikationer, der anvender certifikater hørende til den gamle og den nye CA-nøgle. Der er således et overlap mellem de to nøgler.

2.8.2 Certifikatindehavers nøgler

Skift af en certifikatindehavers nøgle vil normalt ske, fordi det udstedte certifikat står for at udløbe. Når certifikatindehaveren ansøger om at få et nyt certifikat, genereres der et nyt nøglepar.
Skift af en certifikatindehavers nøgle kan også ske, hvis brugeren har tabt kontrol over eller tillid til den private nøgle, der hører til certifikatet. Der henvises til den relevante CP for yderligere oplysninger.

2.9 Kompromittering, katastrofe og andre skader på DanID

Følgende afsnit beskriver beredskabet hos *DanID* i tilfælde, som kan påvirke funktionen af certificeringstjenesten.

2.9.1 Svigt af hardware eller software

DanID opretholder et reservedelslager, der gør det muligt at udskifte alle hardwarekomponenter i certificeringsløsningen. Reetablering af hardwarekomponenter udføres af *DanID* 24-timers vagt efter gældende driftsprocedurer.

I tilfælde af tab af data, genetableres certificeringstjenesten ud fra seneste backup.

Se også afsnit 4 for yderligere oplysninger.

Yderligere tekniske beskrivelser, der er nødvendige for at kunne vurdere driftsmiljøet og sikkerhedsprocedurerne, kan efter aftale gennemgås hos *DanID* i samarbejde med dennes sikkerhedsorganisation.

2.9.2 Spærring af CA-nøgler

Skulle CA miste adgangen til eller tilliden til den private CA-nøgle, sker der generelt følgende:

- CRL-tjeneste til den givne CA-nøgle stoppes. Dette vil forhindre, at et certifikat bliver accepteret af nogen, der forsøger at kontrollere, om det er gyldigt.
- Certifikatudstedelsen stoppes.
- Certifikatindehavere underrettes.
- En undersøgelse sættes i gang for at dokumentere hændelsesforløbet.
- En ny rodnøgle genereres.
- Certificeringstjenesten genoptages under ny rodnøgle.
- Certifikatindehavere informeres om hændelsesforløbet og tilbydes nyt certifikat.

Der kan være specielle krav omkring spærring af CA-nøgler i de enkelte certifikatpolitikker.

2.10 Kontrolleret lukning af CA

Skulle det blive aktuelt at lukke en kørende CA-tjeneste, udføres følgende:

- Alle certifikatindehavere og interessenter informeres mindst tre måneder før lukning.
- CRL-tjeneste stoppes ved lukning. Dette forhindrer, at et certifikat bliver accepteret af nogen, der forsøger at kontrollere, om det er gyldigt.
- Der lukkes for udstedelse af nye certifikater.

DanID er økonomisk sikret på en måde, som tillader, at ovenstående *altid* vil blive udført ved lukning af en kørende CA.

3 Identifikation og autentifikation

Et certifikat er en digital bekræftelse på sammenhængen mellem en certifikatindehaver og dennes offentlige krypteringsnøgle. *DanID* er ansvarlig for, at procedurerne til kontrol af denne sammenhæng overholdes.

Dette afsnit beskriver generelle forhold vedrørende identifikation af certifikatansøgere. Der vil være specifikke forhold omkring den enkelte certifikatløsning, som i så tilfælde vil være beskrevet i den tilhørende CP.

3.1 Ansøgning om certifikat

3.1.1 Navnetyper

Anvendte navne baseres på standarden X.500 Distinguished Name samt Dansk Standard.

3.1.2 Entydighed af navne

DanID garanterer global entydighed af det sæt af navne, der er i certifikatet.

3.1.3 Kontrol af besiddelse af privat nøgle

DanID understøtter kun certifikatansøgninger, hvor afsender kan bevise, at han/hun ejer den private nøgle, der hører til den offentlige nøgle, der søges certificeret.

3.1.4 Kontrol af identitet

DanID kontrollerer ansøgerens identitet i overensstemmelse med specifikke procedurer, der er angivet i den aktuelle CP. Dette kan f.eks. være kontrol baseret på fysisk fremmøde med pas, kontrol af oplysninger mod eksterne registre og lignende.
Hvor det er hensigtsmæssigt, kan *DanID* vælge at samarbejde med en LRA uden for *DanID*s organisation. I så fald vil det stadig være *DanID*, der har det overordnede ansvar for opgaver udført af LRA.

3.1.5 Aftale om udstedelse af certifikat

De vilkår, der gælder for den certifikattype, certifikatindehaveren får udstedt, præsenteres og accepteres af certifikatindehaveren i forbindelse med ansøgning og ibrugtagning af certifikat.

3.2 Fornyelse af certifikat

Som udgangspunkt sker en fornyelse af et certifikat efter samme retningslinjer som første certificering. *DanID* kan dog vælge at lade brugerens gyldige digitale signatur danne grundlag for fornyelse. Dette vil i så fald fremgå af den aktuelle CP. For OCES-certifikater gælder specielle regler for fornyelse. Disse er beskrevet i OCES-CP'erne.

3.3 Udstedelse af nyt certifikat efter spærring af gammelt

Udstedelse af nyt certifikat efter spærring af et gammelt certifikat sker på samme måde som ved en almindelig ansøgning om certifikat.

3.4 Spærringsanmodning

Spærring af et certifikat vil ske efter anmodning, når den, der anmoder, er blevet autentificeret som havende myndighed til at spærre det pågældende certifikat. Se nærmere beskrivelse i de aktuelle CP'er.

Spærring kan også, som tidligere beskrevet i afsnit 2.4.2, ske på vegne af CA alene, hvis CA modtager oplysninger eller får mistanke om, at certifikatindehaveren ikke har handlet som beskrevet i dette CPS eller den relevante CP.

4 Lokal sikkerhed

Dette afsnit beskriver nogle elementer inden for sikkerheden omkring driften af certificeringscenteret. Oplysningerne i denne offentlige del af CPS'et er ikke udtømmende, men er medtaget for at give en ide om de sikkerhedsforanstaltninger, der gælder for certificeringscenteret.

4.1 Fysisk sikkerhed

Dette afsnit beskriver den fysiske sikkerhed for steder, hvor der er installeret certificeringskomponenter.

4.1.1 Beliggenhed og konstruktion

Certificeringskomponenter er installeret i to dedikerede serverrum hos DanID. Disse serverrum er etableret efter best-practice for området.

4.1.2 Fysisk adgang

Rum, der indeholder certificeringskomponenter, undersøges periodisk for at kontrollere:

- at konstruktionen ikke er ændret
- at adgangskontrolsystemet virker
- at de tamperresistente krypto-moduler er intakte.

I det nøglecenterrum, hvorfra certifikaterne udstedes, er der dobbelt/dual adgangskontrol som gennemgående sikkerhedskontrol.
Alle de rum, der benyttes af medarbejdere samt CA-driftslokaler, overholder de krav, der er stillet i DS 484.

4.1.3 Installation og sikring

Nødstrømsanlæg sikrer, at strømforsyningen er beskyttet mod udfald.

Der er installeret køling og ventilation for at sikre et stabilt og pålideligt driftsmiljø.

Der er foretaget sikring mod vandindtrængning.

Da DanID's driftlokaler er placeret på TDC lokationer, følger DanID TDC's generelle brandsikringspolitik. Denne omfatter blandt andet branddøre, jernforede ydervægge, automatisk brandkvælning, direkte alarmering af brandvæsen samt periodisk test af beredskab.

Al information, der bruges af certificeringssystemet, er gemt i sikkerhedskopi lokalt og kopieres periodisk til anden lokation, som har samme grad af fysisk sikkerhed for at sikre hurtig reetablering efter en eventuel skade på systemet.

Kontoraffald med fortroligt indhold bliver destrueret ved makulering. Kritiske certificeringskomponenter destrueres, når de tages ud af produktion.

4.2 Procedurekontrol

Opgaver inden for certificeringscenteret er defineret i interne dokumenter.

4.2.1 Betroede roller

De betroede opgaver i *DanID* løses af personale, som udelukkende arbejder med dette område. Medarbejdergruppen har bl.a. kompetencer inden for: generel it-sikkerhed, kryptologi, operativsystemer og drift, IP- og internetprotokoller, projektledelse og lovgivning.

Følgende roller er identificeret i forbindelse med driften af en CA:

- Certification Authority Administrator (CAA)
- System Administrator (SA)
- System Security Officer (SSO)
- Local Registration Authority Administrator (LRAA)

Ansvar og besættelse af ovenstående roller er defineret i interne papirer, således at ingen enkeltperson kan bringe den sikre drift af certificeringscenteret i fare.

4.3 Personalekontrol

DanID følger anvisningerne i "lov om digitale signaturer" og krav fra OCES politikkerne på området for kontrol af medarbejdere. Dette medfører blandt andet, at alle ansatte i *DanID* får kontrolleret deres straffeattest.

5 Teknisk sikkerhed

Dette afsnit indeholder udpluk af de tekniske detaljer, som er relevante for sikkerheden.

5.1 Nøglegenerering og -installation

CA-rodnøgler genereres og opbevares i et sikkert og overvåget system.

Certifikatindehaverens nøgler genereres normalt lokalt. Der, hvor certifikatpolitikkerne tillader det, kan *DanID* dog også tilbyde løsninger, hvor certifikatindehaverens nøgler genereres centralt. Sikkerhedskrav forbundet hermed fremgår af den relevante certifikatpolitik.

CA-rodnøgler er RSA-nøgler med en længde på mindst 1024 bit, mens certifikatindehaverens nøgler er RSA-nøgler med en længde på mindst 512 bit. Der skal mindst to betroede *DanID*-operatører til for at aktivere udstedelse af certifikater. Se i den relevante CP for yderligere detaljer herom

Certifikatindehavernøgler er gyldige i en begrænset periode. Se den relevante CP.

CA-rodnøgler er gyldige i mindst fem år.

Følsomme data findes kun i krypteret form uden for produktionsmiljøet.

For OCES-certifikater overholdes specielle krav, som fremgår af den relevante OCES CP.

5.2 Systemer og produkter

DanID arbejder med markedets førende teknologileverandører, herunder bl.a. Cryptomathic A/S, Entrust Technologies, SafeNet, Sun, Oracle.

6 Certifikat og CRL

6.1 Certifikatformat, -versioner og -profil

Certifikater udstedt under dette CPS konstrueres i overensstemmelse med ISO 9594-8 (X.509).
Certifikatindholdet følger Dansk Standards anbefalinger. Se i øvrigt den aktuelle CP for detaljer om certifikatindhold.

6.2 CRL-profil

DanID understøtter X.509 version 2 CRL.

7 Administration af specifikationer

Når dette CPS ændres, er enhver ændring tilgængelig fra *DanID*. Hvis ændringen er af grundlæggende karakter, vil de berørte certifikatindehavere blive informeret.

Dette CPS kan fås på forskellige måder:

- På web-adressen http://www.danid.dk/repository
- Via e-mail ved henvendelse til support@certifikat.dk
- Via almindelig post ved at kontakte *DanID* (se afsnit 1.4)