Vilkår for NemID til erhverv fra Nets DanID A/S

Februar 2014

1. Generelle vilkår

Følgende vilkår er gældende for anvendelse af OCES-certifikater til erhverv fra Nets DanID A/S (herefter benævnt Nets DanID).
Vilkårene finder anvendelse over for certifikatindehavere (den fysiske eller juridiske person, der har indgået aftale med Nets DanID om udstedelse af certifikater til en eller flere certifikatholdere), certifikatholdere og over for signaturmodtagere (modtagere af signerede data).

Vilkårene er udarbejdet i henhold til gældende certifikatpolitikker for henholdsvis OCES-medarbejdercertifikater (kaldet NemID medarbejdersignaturer), OCES-virksomhedscertifikater (virksomhedssignaturer) og OCES-funktionscertifikater (funktionssignaturer) fastsat af Digitaliseringsstyrelsen samt gældende certifikatpraksis (CPS) fra Nets DanID, der beskriver de procedurer, som Nets DanID følger ved håndtering af certifikater fra Nets DanID.

Disse dokumenter er tilgængelige på adressen www.trust2408.com/repository.

2. Forpligtelser og ansvar for certifikatindehaver

Med mindre andet fremgår, er såvel certifikatindehaver og den faktiske bruger af certifikatet (certifikatholder) tilknyttet certifikatindehaver forpligtet til at overholde reglerne i punkt 2.1-2.6 ved anvendelsen af OCES-certifikat fra Nets DanID.

Certifikatindehaver er ansvarlig for håndteringen af OCES-medarbejdercertifikater, -OCES-virksomhedscertifikater og OCES-funktionscertifikater internt hos certifikatindehaveren og for information til medarbejderne om anvendelse og opbevaring af de private nøgler, herunder certifikatindehaverens mulighed for at læse krypteret post.

Certifikatindehaver indestår over for tredjemand og over for Nets DanID, for at disse vilkår overholdes af certifikatholder.

2.1. Oplysninger

Certifikatindehaver/certifikatholder skal give korrekte oplysninger til brug for ansøgningen om udstedelse af et OCES-certifikat fra Nets DanID.

Certifikatindehaver/certifikatholder skal ved modtagelsen af sit OCES-certifikat sikre sig, at indholdet af OCES-certifikatet er i overensstemmelse med de faktiske forhold.

Hvis oplysninger i certifikatet ikke er i overensstemmelse med oplysninger givet i forbindelse med ansøgningen, skal der omgående gives meddelelse til Nets DanID. Tilsvarende gælder, hvis indholdet af certifikatet ikke længere er i overensstemmelse med de faktiske forhold.

I forbindelse med ansøgning om et certifikat udsteder Nets DanID en midlertidig adgangskode, der skal anvendes ved generering af certifikatet. Den midlertidige adgangskode skal opbevares fortroligt.

2.2. Nøglefils- og hardwareløsningen

Hvor nøglepar genereres og opbevares hos certifikatindehaver/certifikatholder, skal certifikatindehaver/certifikatholder generere og opbevare sin private nøgle og tilhørende midlertidige adgangskode i et sikkert it-miljø og efter de retningslinjer, som Nets DanID anviser i forbindelse med udstedelsen. Certifikatindehaver skal sikre, at it-miljøet altid er opdateret med seneste sikkerhedsopdateringer og virusbeskyttelsessoftware.

Certifikatindehaver/certifikatholder skal straks bede Nets DanID om en ny midlertidig adgangskode, hvis uvedkommende kan have fået kendskab til koden.

Certifikatindehaver/certifikatholder er forpligtet til at beskytte den private nøgle mod tab, afsløring, ændring eller uautoriseret brug.

Den private nøgle skal opbevares krypteret og beskyttet af en selvvalgt adgangskode. Adgangskoden skal bestå af mindst otte tegn og indeholde mindst et lille og et stort bogstav samt et tal (eks. *G2uw3KMs*). Anvendes anden adgangskode (eks. biometrisk kode), skal denne have en kompleksitet på minimum 2048 bit. I løsninger, der effektivt kan spærre for udtømmende søgninger, kan adgangskoden dog være minimum fire cifre.

Certifikatindehaver/certifikatholder skal sikre, at andre ikke får kendskab til adgangskoden.

Adgangskoden, som bruges til at beskytte den private nøgle, må under ingen omstændigheder opbevares på samme sted som den private nøgle og skal altid holdes hemmelig.

Certifikatindehaver/certifikatholder må ikke efterlade den private nøgle uden opsyn i en ikke-aflåst tilstand (fx en arbejdsstation, hvor adgangskoden er indtastet). Hverken den private nøgle, den midlertidige adgangskode eller den selvvalgte adgangskode må overdrages til andre.

Hvis certifikatindehaver/certifikatholder tager en sikkerhedskopi af den private nøgle, skal sikkerhedskopien ligeledes opbevares krypteret og beskyttet af adgangskode, jf. ovenfor.

Certifikatindehaver/certifikatholder skal omgående ophøre med anvendelse af certifikatet, hvis certifikatindehaver/certifikatholder får meddelelse om, at Nets DanID er blevet kompromitteret.

Data krypteret med en offentlig nøgle fra certifikatet kan kun dekrypteres med en tilhørende privat nøgle. Det betyder fx, at certifikatindehaver/certifikatholder ikke kan læse e-mail, der er krypteret med certifikatet, hvis certifikatindehaver/certifikatholder ikke længere har adgang til adgangskoden og den private nøgle.

2.3. Nøglekortsløsningen

Hvor nøglepar genereres og opbevares centralt hos Nets DanID, skal certifikatindehaver/certifikatholder straks bede Nets DanID om en ny midlertidig adgangskode, hvis uvedkommende kan have fået kendskab til koden.

Certifikatindehaver/certifikatholder skal vælge en personlig adgangskode. Koden skal være mellem 6 og 40 tegn, skal indeholde både bogstaver og tal, må ikke indeholde specialtegn eller samme tegn fire gange i træk. Koden må endvidere ikke indeholde certifikatindehavers/certifikatholders CPR- eller NemID-nummer.

Certifikatindehaver er ansvarlig for, at anvendelse af bruger-id, adgangskode og éngangskoder fra nøglekort/voice response sker i et sikkert og pålideligt it-miljø. Certifikatindehaver skal derfor altid sikre, at it-miljøet er opdateret med seneste sikkerhedsopdateringer og virusbeskyttelsessoftware. Certifikatindehaver skal også sikre, at certifikatholder ikke anvender bruger-id, adgangskode og éngangskoder fra enenhed, der ikke er opdateret med seneste sikkerhedsopdateringer. Ved enhed forstås den enhed hvorfra certifikatet benyttes fx pc, mobiltelefon eller tablet.

Certifikatindehaver skal sikre, at certifikatholder opbevarer sit bruger-id, sin adgangskode og nøglekort sikkert og forsvarligt, og sikre at andre ikke får kendskab hertil og dermed adgang til at benytte dem.

Certifikatindehaver/certifikatholder må ikke:
oplyse adgangskode, engangskoder eller overlade nøglekortet til andre, scanne, indtaste eller på anden måde kopiere éngangskoder for at opbevare dem, skrive adgangskoden ned eller opbevare adgangskoden sammen med nøglekortet.

Den private nøgle, som opbevares hos Nets DanID, vil være tilgængelig for certifikatindehaver/certifikatholder også efter spærring med henblik på, at certifikatindehaver kan dekryptere data med den private nøgle. Adgang til den private nøgle forudsætter dog anvendelse af den personlige adgangskode.

2.4. Cpr tilknytning

Ved udstedelse af OCES-medarbejdercertifikat med tilknyttet CPR-nummer giver certifikatholder samtidig samtykke til:

- at Nets DanID foretager opslag i CPR for at indhente certifikatholders navn og adresse
- at Nets DanID videregiver sammenhængen mellem certifikatet og certifikatholders CPR-nummer til den offentlige RID-tjeneste hos Digitaliseringsstyrelsen.
- at Nets DanID foretager opslag i den offentlige RID-tjeneste for at indhente eventuelt RID-nummer fra et tidligere certifikat.

2.5. Anvendelse

Certifikatet kan være begrænset med hensyn til anvendelse (formålsbegrænsning) eller med hensyn til transaktionsbeløb (beløbsbegrænsning). Certifikatindehaver/certifikatholder må alene anvende OCES-certifikatet inden for rammerne af sådanne begrænsninger, der fremgår af OCES-certifikatet.

OCES-certifikaterne er ikke kvalificerede certifikater, og de må derfor ikke bruges i situationer, hvor kvalificerede certifikater er påkrævet. Certifikaterne må ikke anvendes til signering af andre certifikater.

Den private nøgle, der udstedes i forbindelse med udstedelse af OCES-certifikat, må ikke anvendes før OCES-certifikat er modtaget, bortset fra den brug, der sker ved certifikatansøgningen.

Certifikatindehaver/certifikatholder må ikke benytte den private nøgle efter anmodning om spærring, notifikation om spærring eller efter udløb af certifikatet til andre formål end dekryptering af data, som er krypteret med den tilhørende offentlige nøgle.

2.6. Spærring

Certifikatindehaver/certifikatholder skal omgående spærre certifikatet, hvis indholdet af certifikatet ikke længere er i overensstemmelse med de faktiske forhold, eksempelvis, men ikke begrænset til, i det tilfælde, hvor en medarbejder ikke længere er tilknyttet certifikatindehaveren, eller
hvis certifikatindehaver går konkurs eller bliver opløst.

Hvor nøglepar genereres hos certifikatindehaver/certifikatholder skal certifikatindehaver/certifikatholder straks spærre sit certifikat i tilfælde af kompromittering af den private nøgle eller mistanke herom. Den private nøgle må i den forbindelse kun bruges til spærring af certifikatet eller til dekryptering af data, som er krypteret med den tilhørende offentlige nøgle.

Hvor nøglepar genereres og opbevares centralt hos Nets DanID anses den private nøgle for kompromitteret, hvis uvedkommende både får kendskab til adgangskoden og ubrugte engangskoder fra nøglekortet.

Certifikatindehaver/certifikatholder skal straks spærre nøglekortet, hvis andre har eller kan have fået kendskab til ubrugte engangskoder.

Certifikatindehaver/certifikatholder skal også straks spærre nøglekortet, hvis dette mistes.

Certifikatindehaver/certifikatholder skal straks spærre eller ændre adgangskoden, hvis certifikatindehaver/certifikatholder får mistanke om, at andre kan have fået kendskab til den.

Spærring kan ske hele døgnet på tlf. 72 2470 10.

3. Forpligtelser og ansvar for signaturmodtager

Signaturmodtageren, der modtager signerede data fra en certifikatindehaver, skal kontrollere følgende, inden vedkommende forlader sig på certifikatet:

- at certifikatet ikke er udløbet
- at certifikatet er gyldigt, ved at verificere certifikatets status. Certifikatet anses som ugyldigt, såfremt gyldighed ikke kan verificeres positivt ved opslag i aktuel spærreliste fra Nets DanID

- at certifikatet anvendes i overensstemmelse med eventuelle anvendelsesbegrænsninger som fremgår af certifikatet. Certifikatet kan være begrænset med hensyn til anvendelse (formålsbegrænsning) eller med hensyn til transaktionsbeløb (beløbsbegrænsning)
- at niveauet af sikkerhed, anses for passende i forhold til det formål, som certifikatet søges anvendt til.

4. Nets DanIDs beføjelse i tilfælde af misligholdelse

Nets DanID er berettiget til ensidigt at spærre et certifikat, såfremt Nets DanID får vished eller mistanke om, at certifikatholders private nøgle er kompromitteret eller ødelagt, medarbejderen ikke længere er tilknyttet certifikatindehaveren, de faktiske oplysninger ikke svarer overens med certifikatets indhold, certifikatindehaveren er gået konkurs eller er ophørt, eller certifikatindehaveren i øvrigt handler i strid med sine forpligtelser.

Hvor nøglepar genereres og opbevares centralt hos Nets DanID kan Nets DanID endvidere spærre:

- adgangskoden, hvis Nets DanID får mistanke om eller vished for, at andre har fået kendskab til den
- adgangskoden, hvis adgangskoden er indtastet forkert et vist antal gange
- nøglekortet, hvis Nets DanID får mistanke om eller vished for, at andre har fået kendskab til engangskoder fra nøglekortet.

5. Erstatningsansvar

Parterne er erstatningsansvarlige over for hinanden efter dansk rets almindelige regler.

Nets DanID er desuden ansvarlig for tab hos den der med rimelighed forlader sig på certifikatet (signaturmodtager), såfremt tabet skyldes:

- at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet
- at certifikatet ikke indeholder alle oplysninger som følger af OCES-CP'erne punkt 7.3.3
- at Nets DanID ikke har foretaget spærring af certifikatet efter at have modtaget anmodning fra certifikatindehaveren eller certifikatholderen herom, eller hvis forholdene i øvrigt tilsiger dette, jf. OCES-CP'erne punkt 7.3.6
- at Nets DanID har givet manglende eller fejlagtige oplysninger om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger
- at Nets DanID har tilsidesat OCES-CP'erne punkt 7.3.1
- og Nets DanID ikke kan godtgøre, at Nets DanID ikke har handlet uagtsomt eller forsætligt.

Nets DanID er ikke ansvarlig for tab hos certifikatindehaveren eller signaturmodtageren, såfremt certifikatindehaveren eller signaturmodtageren er erhvervsdrivende eller offentlige myndigheder, og

- tabet er opstået som følge af forhold, der ligger uden for Nets DanIDs kontrol, herunder forhold hos en underleverandør, strejke og lockout
- tabet er opstået som følge af, at et OCES-certifikat anvendes uden for de formålsbegrænsninger eller beløbsbegrænsninger, som gælder for certifikatet, og som fremgår af certifikatet
- tabet er et indirekte tab, herunder tabt avance, driftstab, tab som følge af tab af data, systemnedbrud eller lignende
- tabet samlet for alle skadebegivenheder hos den forulempede overstiger 50.000 kr. i løbet af et år (ved "år" forstås 1. januar - 31. december).

6. Udløb og genansøgning om certifikat

Et OCES-certifikat fra Nets DanID har en gyldighedsperiode på op til fire år. Når gyldighedsperioden udløber, skal der ansøges om nyt certifikat. Nyt certifikat kan udstedes ved brug af det gamle certifikat, såfremt fornyelse gennemføres inden udløbet af gyldighedsperioden på det gamle certifikat, og den private nøgle ikke er kompromitteret. Såfremt et OCES-certifikat er udløbet eller spærret, eller den private nøgle er blevet kompromitteret, kan det gamle certifikat ikke anvendes ved genansøgningen om OCES-certifikat.

7. Øvrige vilkår

7.1. Konfliktløsning

Enhver tvist, der måtte udspringe af brugen af OCES-certifikater udstedt af Nets DanID er underlagt dansk ret, og skal indbringes for Københavns Byret.

Tvister mellem parterne løses så vidt muligt ved forhandling mellem parterne.

7.2. Ændringer af vilkår

Nets DanID har ret til at ændre vilkårene uden varsel, og ændringerne træder i kraft ved offentliggørelse på www.trust2408.com/repository og ved afsendelse af elektronisk meddelelse til certifikatindehaveren. Ændringer af begunstigende karakter, eller som ikke medfører indskrænkninger i certifikatindehaverens rettigheder, kan dog ske uden direkte meddelelse til certifikatindehaveren.