PBS CA

Certifikat Politik (CP)

Virksomhed og medarbejdercertifikat –

Chipkort

OID: 1.2.208.163.1.1.2

Version 1.1

24. maj 2005

1. Formål

Et certifikat udstedt i henhold til denne CP er klassificeret som et virksomhedscertifikat, hvor virksomheden er blevet identificeret og registreret med udgangspunkt i et personligt fremmøde og certifikatindehavers private nøgle er fremstillet og opbevares på et chipkort. Et virksomhedscertifikat kan også udstedes som et medarbejdercertifikat, hvor en medarbejder som er bemyndiget af certifikatindehaver kan benytte certifikatet til at logge ind og fremsende indberetninger på vegne af virksomheden.

Denne CP tjener følgende formål;

a. at tjene til information for offentligheden om sikkerhed ved administration og udstedelse af certifikater i PBS,

b. at være en del af aftalegrundlaget mellem PBS og certifikatindehaver af et af PBS udstedt certifikat,

c. at være en del af aftalegrundlaget mellem PBS og tjenesteudbyder, der modtager en digital signatur der er fremstillet på baggrund af et af PBS udstedt certifikat,

d. at være en del af aftalegrundlaget mellem PBS og virksomheder/organisationer, der efter aftale med PBS har ret til at foretage RA funktioner for PBS i tilknytning til udstedelse af certifikater.

Der indgås separat aftale mellem PBS og den virksomhed eller organisation, som varetager RA funktionen, hvori rettigheder og forpligtelser, herunder ansvar for handlinger foretaget af indehavere af certifikater og ansvar over for tredjemand reguleres.

1.1. Version

Denne CP er version nummer 1.1, som er gældende fra 1. januar 2005. Den til enhver tid gældende version af CP findes på Internet adressen http://www.pbs.dk/pbs/site/pbs_dk/dk/menu_top/it-services/certifikat.html.

Policy number: 1.2.208.163.1.1.2

1.2. Ændringshåndtering

PBS er ansvarlig for Certifikatpolitikkens vedligeholdelse.

PBS forventer, at indholdet løbende opdateres i takt med udviklingen inden for krypteringsteknologi. Opdatering kan endvidere ske som følge af ændringer i dansk og inter-

national lovgivning om kryptering og elektroniske signaturer.

1.3. Kontakt

Kommunikation til PBS CA i alle forhold vedrørende denne CP kan foregå på følgende måde:

Pr. e-mail: certifikatinfo@pbs.dk

1.4. Rettigheder

Alle certifikater, der udstedes under denne CP, er PBS' ejendom.

1.5. Referencer

1) PBS CA Certification Practice Statement (CPS)

2. Terminologi

Hvor andet ikke fremgår af den konkrete sammenhæng, skal nedenstående forkortelser og betegnelser i denne CP forstås som her beskrevet:

2.1. Generelle begreber

Meddelelse: En digital repræsentation af en mængde information, som kan omsættes til læsbar tekst.

Privat nøgle: Nøgle i en asymmetrisk kryptografisk algoritme, som skal holdes hemmelig og som er matematisk relateret til en offentlig nøgle.

Offentlig nøgle: Nøglen i et asymmetrisk kryptografisk algoritme, som er offentlig tilgængelig og som er matematisk relateret til en privat nøgle.

Digital signatur: Et matematisk resultat udregnet fra en meddelelse og en privat nøgle. På baggrund af den tilhørende offentlige nøgle kan det bestemmes om resultatet er udregnet med brug af den private nøgle og om hvorvidt meddelelsen er blevet ændret efter at resultatet er beregnet.

2.2. CA begreber

Bemyndiget: Medarbejder, der af certifikatindehaver er valgt og godkendt til at anvende certifikatet på vegne af certifikatindehaver.

Certifikat: En formateret meddelelse der som minimum indeholder: (1) certifikatudstederens navn, (2) certifikatindehaverens navn, (3) certifikatindehaverens offentlige krypteringsnøgle, (4) periode der specificerer den operationelle tid for nøglens anvendelse, (5) Certifikatudstederens Digitale Signatur på certifikatet.

Gyldigt certifikat: Et certifikat betragtes som gyldigt såfremt:

a. Det er udstedt af PBS CA.

b. Det er distribueret til PBS CA X.500 database.

c. Det er ikke opført på PBS CA spærreliste.

d. Det ikke er udløbet.

e. Det kan verificeres med et gyldigt PBS CA certifikat.

Certifikatindehaver: En juridisk person som på baggrund af denne certifikatpolitik

har indgået en aftale med certifikatudsteder om erhvervelse og anvendelse af et PBS CA udstedt certifikat.

Certifikatholder: Person der er betroet som bruger af certifikatindehaver's certifikat.

Certifikatudsteder (CA): PBS i sin egenskab af certifikatudsteder og leverandør af tjenesteydelser i forbindelse med elektroniske signaturer.

Chipkort: Et plastkort påsat en computerchip, der indeholder indehavers private nøgle og certifikat(er). Adgang og brug af en privat nøgle kræver indtastning af en PIN kode.

CP: Certifikat Politik: Et sæt af regler, der angiver krav til udstedelse og brug af certifikat i et eller flere specifikke sammenhænge, hvor der findes fælles sikkerhedskrav.

CPS: Den detailspecifikation, der dokumenterer de procedurer, som PBS benytter ved udstedelse og administration af certifikater.

Identitet: Information, som entydigt identificerer en juridisk person inden for CA's domæne.

Klasse 1 sikkerhedsniveau: Angivelse af et specifikt sikkerhedsniveau for udstedelse af et certifikat. Certifikater med dette sikkerhedsniveau fordrer, at certifikatindehaver er identificeret og registreret med udgangspunkt i et personligt fremmøde, og at certifikatindehavers private nøgle er fremstillet og opbevares på et chipkort.

Korrekt signatur: En digital signatur som med succes kan testes ved at benytte en offentlig nøgle i et gyldigt certifikat.

Medarbejdercertifikat: Et virksomhedscertifikat hvor certifikatindehaver har bemyndiget en person til at benytte certifikatet til at logge ind og fremsende indberetninger på vegne af certifikatindehaver. Certifikatindehaver indestår for den pågældende persons identitet.

PIN kode: En personlig kode, som giver certifikatindehaveren adgang til at anvende sin private nøgle.

Registreringsenhed (RA): Virksomhed eller organisation, der er bemyndiget af PBS, til at udføre funktioner for PBS i tilknytning til udstedelse af certifikater. Denne funktion vil som minimum indebære modtagelse og kontrol af legitimationsoplysninger.

Tjenesteudbyder: Fysisk eller juridisk person, der stiller tjenester til rådighed på Internettet og som sikrer denne kommunikation med digital signatur indeholdende et af PBS udstedt certifikat.

Signeret meddelelse: En meddelelse som bærer en korrekt signatur og identiteten af certifikatindehaver.

Spærreliste: En af PBS udstedt elektronisk liste over spærrede certifikater. Spærrelisten gøres tilgængelig for tjenesteudbydere.

Tegningsberettiget: Person der har prokura i en virksomhed, organisation eller en forening til at handle/tegne på virksomhedens, organisationen eller foreningens vegne.

Virksomhedscertifikat: Certifikat udstedt af PBS CA til en juridisk person, der dermed bliver certifikatindehaver.

3. De involverede parters forpligtelser

3.1. CA forpligtelser

PBS CA vil som minimum:

Udstede, offentliggøre og spærre certifikater

a. Fremstille og signere certifikater. Sikre at certifikater kun bliver udstedt til juridiske personer hvis identitet er blevet eftervist i henhold til denne CP, og sikre at certifikatindehavers identitet og offentlige nøgle er entydige inden for PBS' CA domæne.

b. Distribuerer certifikater på udstedelsestidspunktet angivet i certifikatet.

c. Modtage og behandle anmodninger om spærring af certifikater fra certifikatindehavere eller -holdere og hurtigst muligt gøre spærrelister tilgængelige i overensstemmelse med denne CP. Kvittering herfor fremsendes til certifikatindehaver.

d. Give certifikatindehavere mulighed for at forny certifikater.

Validere certifikater

d. Give tjenesteudbydere mulighed for at validere certifikater.

e. Stille relevant information om udstedte certifikater til rådighed i forbindelse med kontrol af afgivne digitale signaturer, samt ved løsning af tvister om digitale signaturer.

Udføre tekniske og forretningsmæssige relevante funktioner

h. Anvende betryggende administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder.

i. Beskæftige personale med den fornødne ekspertise, erfaring og kvalifikationer, herunder personale med sagkundskab inden for signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer i forbindelse hermed.

j. Anvende pålidelige systemer og produkter, som er beskyttet imod uautoriserede ændringer, og om sikrer den tekniske og kryptografiske sikkerhed af de processer, som disse systemer og produkter understøtter.

k. Træffe foranstaltninger mod eventuelle muligheder for forfalskning af certifikaterne.

l. Til stadighed have tilstrækkelige økonomiske ressourcer til at drive CA virksomhed.

m. Påtage sig ansvaret for ydelser udført af eventuelle underleverandører til PBS. Herunder vil PBS CA indgå relevante aftaler med eventuelle RA'er og nøje kontrollere sådanne aftalers overholdelse.

3.2. RA forpligtelser

RA'en skal som minimum;

a. verificere identiteten af den juridiske person, som anmoder om at blive certifikatindehaver.

b. informere certifikatindehaver om når dennes certifikatet er udstedt.

c. opbevare al det materiale der er benyttet til at verificere certifikatindehavers identitet, herunder

- referencenummer til benyttede legitimationspapirer og deres gyldighedsperiode,
- aftaler med certifikatindehavere, samt registrering af hvem hos RA der har kontrolleret certifikatanmodningen.

d. registrere kontrollerede certifikatindehaveres oplysninger sikkert.

e. vejlede certifikatindehavere om brug og opbevaring af det chipkort, som indeholder certifikatindehavers private nøgle.

f. informere certifikatindehaver om, at sikkerheden i certifikatløsningen er afhængig af, og vil blive anset som kompromitteret, såfremt den private nøgle eller adgangen til at anvende den kommer til andres kendskab.

g. Informere certifikatholder når vedkomnes certifikat skal fornys.

h. sikre, i form af aftaler, at certifikatindehaver kender sine forpligtelser som specificeret i 3.3.

3.3. Certifikatindehavers forpligtelser

Certifikatindehaver har pligt til at iagttage følgende forhold i forbindelse med udstedelse, anvendelse, opbevaring og ophør af certifikatet:

Certifikatindehaver skal som minimum;

a. afgive korrekte og fyldestgørende oplysninger ved anmodning om udstedelse af certifikat,

b. opbevare den private nøgle og password hertil som anvist af PBS CA,

c. tage rimelige forholdsregler for at beskytte den private nøgle mod kompromittering, ændring, tab og uautoriseret brug,

d. ved modtagelse af certifikatet sikre sig, at indholdet af certifikatet er i overensstemmelse med de faktiske forhold,

e. omgående anmode PBS CA om spærring af certifikatet, hvis certifikatindehaver får mistanke om mulighed for misbrug eller brud på sikkerhed, eller hvis indholdet af certifikatet ikke længere er i overensstemmelse med de faktiske forhold,

f. kun anvende certifikatet i henhold til 5.2 og 5.4,

g. kun anvende certifikatet når det er gyldigt.

3.4. Tjenesteudbyders forpligtelser

Tjenesteudbyder skal som minimum;

a. sikre sig, at det formål, hvortil certifikatet anvendes, svarer til det aftalte formål. Som en vejledning ved denne beslutning har tjenesteudbyder CP og sin aftale med RA.

Hvis tjenesteudbyder har indgået en skriftlig aftale med accept af digitale signaturer, skal tjenesteudbyder endvidere,

b. afstå fra at gøre indsigelse mod en meddelelses gyldighed alene af den grund, at den pågældende meddelelse er modtaget i elektronisk form i stedet for fysisk skriftlig form, medmindre det er påkrævet efter gældende lovgivning.

Inden en transaktion med signatur accepteres, skal tjenesteudbyder:

a. Kontrollere om det modtagne certifikat er spærret eller suspenderet efter anvisning fra PBS.

b. Kontrollere at spærrelisten er gyldig signeret af PBS CA.

c. Kontrollere at det modtagne certifikat anvendes til et formål og inden for en eventuel begrænsning, der er angivet i certifikatet.

Transaktioner med signatur skal opbevares af tjenesteudbyder for at sikre bevis ved en eventuel senere tvist.

Hvis det ikke er muligt at få verificeret certifikatstatus på grund af systemfejl eller lignende, må certifikatet ikke accepteres. Enhver accept af et certifikat uden verifikation sker på egen risiko.

4. Ansvar, ansvarsbegrænsning og ansvarsfraskrivelser

4.1. PBS' ansvar

Når PBS CA signerer et certifikat i overensstemmelse med denne CP, godtgør PBS, at PBS CA har kontrolleret certifikatet samt de deri anførte oplysninger.

PBS er ansvarlig efter dansk rets almindelig erstatningsregler for manglende overholdelse af de procedurer og forholdsregler ved udstedelse, administration og ophør af certifikater, der er beskrevet i denne CP.

PBS er erstatningsansvarlig, hvis PBS på grund af fejl eller forsømmelser opfylder aftalte forpligtelser for sent eller mangelfuldt.

Selv på de områder, hvor der gælder et strengere ansvar, er PBS ikke ansvarlig for tab, som skyldes;

a. nedbrud i/manglende adgang til IT-systemer eller beskadigelser af data i disse systemer, der kan henføres til nedennævnte begivenheder, uanset om det er PBS selv eller en ekstern leverandør, der står for driften af systemerne,

b. svigt i PBS' strømforsyning eller telekommunikation, lovindgreb eller forvaltningsakter, naturkatastrofer, krig, oprør, borgerlige uroligheder, sabotage, terror eller hærværk (herunder computervirus og -hacking),

c. strejke, lockout, boykot eller blokade, uanset om konflikten er rettet mod eller iværksat af PBS selv eller dens organisation, og uanset konfliktens årsag. Det gælder også, når konflikten kun rammer dele af PBS, eller

d. andre omstændigheder, som er uden for PBS' kontrol.

PBS' ansvarsfrihed gælder ikke hvis:

e. PBS burde have forudset det forhold, som er årsag til tabet, da aftalen blev indgået eller burde have undgået eller overvundet årsagen til tabet, eller

f. lovgivningen under alle omstændigheder gør PBS ansvarlig for det forhold, som er årsag til tabet.

4.2. Begrænsning af PBS' ansvar

PBS er ikke ansvarlig for indirekte tab og følgeskader. PBS fraskriver sig ethvert ansvar for den anden parts tab af goodwill og kontrakter, tabt fortjeneste og rentetab.

PBS er heller ikke ansvarlig for manglende adgang til de edb-systemer, som PBS anvender, der skyldes nogle af de i denne CPs førnævnte punkt om ansvar nævnte omstændigheder.

I det omfang, dette ikke strider mod gældende dansk ret, er PBS' ansvar over for certifikatindehaver og tjenesteudbyder underlagt visse begrænsninger. Forudsat at PBS CA har overholdt procedurer og forholdsregler angivet i denne CP, er PBS under ingen omstændigheder ansvarlig for;

a. certifikatindehavers overtrædelse af indgåede aftaler eller egen bemyndigelse,

b. certifikatindehavers afgivelse af falske oplysninger og legitimationspapirer i forbindelse med udstedelse af certifikater,

c. om en tjenesteudbyder kan modtage eller accepterer at modtage den digitale signatur som bevis for certifikatindehaverens identitet,

d. om lovgivning eller retspraksis i det konkrete tilfælde anerkender anvendelse af en digital signatur,

e. tab ved at den kryptografiske kode brydes før certifikatets udløb, dog forudsat at der anvendes algoritmer og tilhørende nøglelængder, der på udstedelsestidspunktet betragtes som tilstrækkeligt sikre,

f. tab, der måtte opstå ved misbrug af et certifikat, herunder eventuelt misbrug i perioden fra PBS' CA modtagelse af anmodning om spærring, til spærrelisten er gjort offentligt tilgængelig,

g. tab, der opstår på grund af certifikaters anvendelse i strid med certifikatets eget indhold,

h. tab, der opstår på grund af certifikatindehavers, eller tjenesteudbyders manglende overholdelse af denne CP,

i. tab, som certifikatindehaver måtte lide, såfremt PBS CA på egen foranledning måtte spærre et certifikat, eller såfremt PBS CA følger en forkert anmodning om spærring af et certifikat,

j. tab, som certifikatindehaver eller tjenesteudbyder måtte lide, såfremt X.500 databasen i kortere perioder ikke måtte være tilgængelig, og

k. tab, som måtte opstå ved anvendelse eller accept af et udløbet eller spærret certifikat.

PBS' erstatningsansvar i henhold til denne CP er under alle omstændigheder begrænset til et beløb på kr. 50.000,- pr. certifikat.

4.3. Certifikatindehavers ansvar over for PBS

Certifikatindehaver er over for PBS ansvarlig efter dansk rets almindelige erstatningsregler for det tab, som PBS måtte lide ved certifikatindehavers manglende overholdelse af denne CP.

Certifikatindehavers eventuelle ansvar over for tjenesteudbyder er ikke reguleret af denne CP.

Certifikatindehaver skal i videst muligt omfang medvirke til at forebygge og begrænse en potentiel skades negative konsekvenser for opfyldelse af sine forpligtelser. Certifikatindehaver skal straks give meddelelse om en skadesbegivenhed, ligesom certifikatindehaver straks efter ophøret af skadens negative konsekvenser skal genoptage leverancen af sine aftalte ydelser.

4.4. Tjenesteudbyders ansvar overfor PBS

Tjenesteudbyders ansvar for manglende overholdelse af denne CP følger dansk rets almindelige erstatningsregler.

Certifikatindehavers eventuelle ansvar over for tjenesteudbyder er ikke reguleret af denne CP.

Tjenesteudbyder skal i videst muligt omfang medvirke til at forebygge og begrænse en potentiel skades negative konsekvenser for opfyldelse af deres forpligtelser. Tjenesteudbyder skal straks give meddelelse om en skadesbegivenhed, ligesom tjenesteudbyder straks efter ophøret af skadens negative konsekvenser skal genoptage leverancen af sine aftalte ydelser.

5. Certifikater

PBS CA optræder som en betroet tredjepart ved at udstede certifikater, som over for modtageren af et certifikat, fungerer som bevis for, at den til certifikatet hørende private nøgle er udstedt til den juridiske person, der er angivet som indehaver af certifikatet.

5.1. PBS CA eget certifikat

PBS CA attesterer certifikater ved brug af PBS CA eget certifikat (PBS' CA eget rod-certifikat.) Dette rod-certifikat er et selvcertificeret certifikat. Under rod-certifikatet har PBS udstedt CA certifikater, der benyttes til at udstede de forskellige typer certifikater, der benyttes af kunderne. Disse CA certifikater benyttes også til at signere spærrelister med.

5.2. Godkendte formål

Formålet med certifikater udstedt under denne CP er at medvirke til at skabe sikker datakommunikation mellem virksomheder. Certifikater kan dermed benyttes til f.eks. sikring af e-post (S/MIME) og Web-kommunikation (Secure Socket Layer SSL).

5.3. Interoperabilitet og varemærke

PBS CA udsteder forskellige typer certifikater, som kan benyttes til at sikre kommunikationen med forskellige applikationer. Disse applikationer kan have behov for forskellige sikkerhedsniveauer og forskellige krav til indholdet af identitetsoplysningerne i certifikatet.

PBS har udarbejdet et varemærke, som skal tilkendegive at et certifikat tilhører et givent sikkerhedsniveau (er et klasse 1 certifikat) og at indholdet af identitetsoplysningerne i certifikatet er standardiseret med hensyn til syntaks og semantik. Chipkort der er udstyret med disse certifikater, kan anvendes på tværs af forskellige applikationer og kan dermed opnå interoperabilitet.

Følgende varemærke skal anvendes:

5.4. Ikke-godkendte formål

Certifikatindehavere må ikke optræde som certificeringsmyndighed på samme vis, som PBS CA til at certificere andre certifikater.

Certifikater må ikke anvendes, når de er udløbet eller spærret. Certifikater må endvidere ikke anvendes i strid med;

a. bestemmelserne i denne CP,

b. de begrænsninger certifikatet selv angiver,

c. begrænsninger angivet i certifikatindehavers aftale med RA

d. begrænsninger, der følger af gældende dansk ret.

6. Udstedelse af certifikater

Dette kapitel beskriver krav til den praksis og de procedurer, der følges ved identifikation af personer og virksomheder i forbindelse med udstedelse af certifikater.

6.1. Registrering

Alene ansøgninger hvor alle felter på rekvisitionen er behørigt udfyldt, vil blive behandlet. Ansøgeren skal læse vilkårene for det pågældende certifikat inden ansøgningsskemaet fremsendes.

Følgende elementer kontrolleres, for at sikre, at et givent certifikat udstedes til den rette person i en given virksomhed:

a. Eksistensen og identiteten af virksomheden.

b. Identiteten af den person, som tegner virksomheden.

c. Ansøgning om certifikat.

Det skal derfor sikres, at ansøgningen er fuldstændigt udfyldt, at den er udfyldt korrekt og at den er behørigt godkendt af tegningsberettigede.

6.2. Identitetsoplysninger i certifikatet

Følgende virksomhedsoplysninger registreret i certifikatet:

Virksomhedscertifikat

Oplysninger	Krav	Kommentarer
CountryName:	O	Landekode for hvor virksomheden er registreret
OrganizationName:	O	Virksomhedens fulde navn, evt. inkl. CVR-nummer
OrganizationalUnitName:	F	Afdelingsbetegnelse
SerialNumber:	O	CVR-nr. efterfulgt af løbenummer
CommonName	O	Certifikatindehaverens navn
PostalAddress	F	Virksomhedens postadresse
EmailAddress	F	Virksomhedens e-postadresse

O: Obligatorisk

F: frivillig

Medarbejdercertifikat

Oplysninger	Krav	Kommentarer
CountryName:	O	Landekode for hvor virksomheden er registreret
OrganizationName:	O	Virksomhedens fulde navn, evt. inkl. CVR-nummer
OrganizationalUnitName:	F	Afdelingsbetegnelse
SerialNumber:	O	RID referencenummer
CommonName	O	Medarbejderens navn
PostalAddress	F	Virksomhedens postadresse
EmailAddress	F	Virksomhedens e-postadresse

O: Obligatorisk

F: frivillig

7. Certifikatprofil

Certifikater udstedt af PBS CA overholder ISO/IEC 9794-8 1998 (X.509v3).

7.1. Certifikatindhold

Feltnavn	Indhold	Feltbeskrivelse
Version	2	(X.509 version 3).
SerialNumber		Entydig reference til certifikatet.
Signature	SHA-1/RSA	Identifikation af den kryptografiske algortitme som benyttes af PBS.
Issuer	PBS Klient Klasse 1 CA 2014	Identifikation af udsteder af certifikatet (CA).
Validity	3 år	Periode der angiver hvilken dato certifikatet er gyldigt fra og hvornår det udløber.
Subject		Identifikation af certifikatindehaver (se tillige kapitel 6.2).
Subject PublicKey info		Identifikation af certifikatindehavers algoritme og den offentlige nøgle.
Extensions		
Key Usage		Definerer anvendelsen af den offentlige nøgle indeholdt i certifikatet.
Subject Alternatives Names	OID	Anden information som identificerer certifikatindehaveren.
SignatureAlgorithm	SHA-1/RSA	Identifikation af den algoritme som CA benytter til at signere certifikatet.
SignatureValue	Bitstring	CA's signatur på certifikatet