Certifikatpolicy

Serverlegitimation/ Organisationslegitimation och Stämpellegitimation

Versionshistorik			
Ver.nr	Datum	Vem	Beskrivning
0.1	2025-02-26	Teknisk dokumentatör, Erik Nilsson	Dokument skapat
1.0	2025-03-14	VD, Lasse Larsson	Dokument godkänt
1.1	2025-04-15	CAA, Linda Fagerholm	Uppdatering av definitioner och mindre textjusteringar
2.0	2025-08-21	VD, Christina Pettersson	Ny version godkänd

Dokumentets roller och ansvar			
Skrivet av:	Teknisk dokumentatör, Erik Nilsson	Datum:	2024-11-13
Granskat av:	CAA, Linda Fagerholm	Datum:	2025-04-15
Godkänt av:	VD, Christina Pettersson	Datum:	2025-08-21

Expisoft AB, Box 2934, S-187 29 Täby, Sweden
+46 8 41 00 79 00, info@expisoft.se www.expisoft.se

Innehållsförteckning

1 Inledning

Detta dokument är en Certifikatpolicy (CP) som ägs och förvaltas av Expisoft AB, nedan kallad "Utfärdaren". Denna CP beskriver tekniska och säkerhetsmässiga krav vid utfärdande, hantering, återkallande och förnyelse av de certifikat som omfattas av policyn (se avsnitt 1.1).

Certifikatpolicyn beskriver själva certifikaten och de krav som certifikaten motsvarar.
Ett separat dokument, Utfärdardeklaration (CPS, Certification Practice Statement), beskriver rutiner och processer för hur Expisoft AB uppfyller de krav som ställs i denna certifikatpolicy.

Genom att studera både denna certifikatpolicy och Expisofts Utfärdardeklaration är det möjligt för utomstående att bilda sig en uppfattning om de utfärdade certifikatens säkerhetsnivå.

Denna policy är relevant för Utfärdaren, RA-funktionen och dess personal, återförsäljare av Expisofts certifikatprodukter, beställare i en kundorganisation, förlitande parter samt e-legitimationsinnehavare.

Både CP och CPS följer och är strukturerade efter rekommendation i IETF RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" samt RFC 7382 "Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)".

1.1 Översikt

Denna policy beskriver kraven för att utfärda följande typer av certifikat:

- Serverlegitimation (organisationscertifikat).
- Stämpellegitimation (certifikat för elektronisk stämpel).

I denna policy beskrivs dessa certifikat under samlingsnamnet "e-legitimationer".

1.2 Dokumentnamn och identifierare

De certifikat som utfärdas ska innehålla objektidentifierare (OID)
motsvarande denna policy, som intygar att Utfärdaren har utfärdat och kontrollerat certifikaten i enlighet med de rutiner som fastslagits i denna policy.

Namn på policyn: Expisoft Certifikatpolicy Server- och Stämpellegitimation
Objektidentifierare (OID): 1.2.752.54.9.2.XX.X
Detta OID återfinns i attributet Certifikatprincip (Principidentifierare) i utgivna kundcertifikat.

Följande certifikat och CA-instans omfattas av denna certifikatpolicy:
OID: 1.2.752.54.9.2.13.2
Produktnamn: EID Funktion/Organisation
CA-instans: ExpiTrust EID CA v4

1.3 PKI-aktörer och deras ansvar

Detta kapitel beskriver vilka aktörer som berörs av denna certifikatpolicy samt deras åtagande och ansvarsförpliktelser.

1.3.1 Utfärdaren – Certification Authority (CA)

Med CA menas här en av ingående parter betrodd instans som utfärdar, signerar och levererar e-legitimationer och tillhörande spärrlistor (CRL) till kunder och förlitande parter i enlighet med denna policy. Utfärdaren (CA) kan använda tjänster från tredje part för att utföra sin uppgift enligt denna CP. Det åligger Utfärdaren att tillse att eventuella underleverantörer följer denna policy i tillämpliga delar.

1.3.1.1 Utfärdarens åtaganden och ansvarsförpliktelser

Utfärdaren åtar sig enligt denna policy att:

- Utfärda e-legitimationer i enlighet med kapitel 7.1.
- Tillhandahålla erforderliga kontrollåtgärder enligt kapitel 3 och 8.
- Kontroller av beställda och levererade e-legitimationer före nyckelinitiering och personalisering sker enligt kapitel 6.1.
- E-legitimationer förvaras och levereras till Beställaren enligt kapitel 6.1.2.
- Tillse att e-legitimationsinnehavaren förses med uppgifter för att säkerställa nedladdning av certifikatfiler.
- Tillhandahålla spärrtjänst enligt kapitel 4.9.
- Tillhandahålla säkerhetsåtgärder enligt kapitel 6 i denna policy.
- CA-tjänstens privata nyckel skyddas enligt kapitel 6.2.
- Säkerställa att CA-tjänstens privata nyckel *endast kan används* för att signera e-legitimationer/certifikat, spärrlistor och loggar eller andra funktioner beskrivna i denna policy.
- Ansvara för de tjänster som RA utför på uppdrag av Utfärdaren.
- Upprätta, publicera och underhålla en aktuell utfärdardeklaration (CPS).
- Granska att policyn överensstämmer utfärdardeklarationen samt korrigera eventuella avvikelser och publicera uppdaterade versioner av dokumenten.

Utfärdaren skall vidare tillhandahålla en supportfunktion som ger kunder och e-legitimationsinnehavare assistans rörande certifikatutgivning, underhåll eller återkallande av e-legitimationer.

Genom att utfärda och signera certifikat som innehåller objektidentifierare för denna policy, intygar Utfärdaren att denne har kontrollerat informationen i e-legitimationen i enlighet med de rutiner som fastslagits i denna policy.
Utfärdaren ansvarar dock inte för skada som uppkommit på grund av att uppgifterna i en e-legitimation eller spärrlista är felaktiga såvida Utfärdaren inte gjort sig skyldig till grov vårdslöshet.

1.3.2 Registration Authority (RA)

Registration Authority utses av Utfärdaren och skall arbeta i enlighet med denna policy samt följa den praxis som beskrivs i utfärdardeklarationen (CPS).
RA-funktionen och dess personal ansvarar för identifiering och verifiering av e-legitimationsinnehavare och fullmaktsinnehavare.
Utfärdaren ansvarar för de tjänster som RA utför på uppdrag av Utfärdaren såsom exempelvis utfärdande och spärr av e-legitimationer/certifikat.

1.3.2.1 RA-funktionens åtaganden och ansvarsförpliktelser

RA åtar sig enligt denna policy att:

- Vidta de åtgärder som beskrivs i kapitel 3 med syftet att säkerställa att de uppgifter som ligger till grund för den e-legitimation som skall utfärdas är korrekta.
- Aktiveringsdata för utlämnade e-legitimationer arkiveras hos RA enligt kapitel 2 i denna policy.
- Skydda sin privata nyckel i enlighet med denna policy, tillhörande utfärdar-deklaration (CPS) och avtal med Utfärdaren.
- Vid slumpmässiga stickprover bli testad i intern certifieringsprocess för att bibehålla god standard.

1.3.3 Återförsäljare av Utfärdarens e-legitimationsprodukter

1.3.3.1 Återförsäljarens åtaganden och ansvarsförpliktelser

Återförsäljare åtar sig enligt denna policy att:

- Vidta de åtgärder som beskrivs i kapitel 3 med syftet att säkerställa att de uppgifter som ligger till grund för den e-legitimation som skall utfärdas är korrekta.
- Följa det avtal som upprättats mellan Utfärdaren och Återförsäljaren som reglerar ansvar och förpliktelser gentemot Utfärdaren samt de kunder som Återförsäljaren ansvarar för.
- Logga in på Utfärdarens webbtjänst och i portalen beställa eller spärra e-legitimationer för sina kunders räkning.

1.3.4 Beställare inom en kundorganisation

1.3.4.1 Beställarens åtaganden och ansvarsförpliktelser

Beställare åtar sig enligt denna policy att:

- Vidta de åtgärder som beskrivs i kapitel 3 med syftet att säkerställa att de uppgifter som ligger till grund för den e-legitimation som skall utfärdas är korrekta.
- Följa det avtal som upprättats mellan Utfärdaren och Beställaren som reglerar ansvar och förpliktelser gentemot Utfärdaren samt den organisation som Beställaren ansvarar för.

- Logga in på Utfärdarens webbtjänst och i portalen beställa eller spärra e-legitimationer för sin organisations räkning.
- I ansökan om e-legitimation lämna sanningsenliga uppgifter.
- Om ansökan skickas direkt till Utfärdarens RA-funktion och inte till något Ombud, tillse att den av behörig person signerade fullmakten för beställning skickas som original i pappersformat till Utfärdarens RA-funktion per brev. Alternativt kan signering ske digitalt av behörig person med Mobilt BankID.

1.3.5 E-legitimationsinnehavare

Serverlegitimationer och Stämpellegitimationer innehas av juridiska personer (organisationer).

1.3.5.1 E-legitimationsinnehavarens åtaganden och ansvarsförpliktelser

E-legitimationsinnehavaren åtar sig enligt denna policy att:

- Vid ansökan om e-legitimation åta sig att följa tillämpliga rutiner beskrivna i kapitel 3 och 0 i denna policy.
- E-legitimationsinnehavaren skall tillse att denne har kontroll över sin e-legitimation samt förhindra obehörigt utnyttjande av legitimationen genom att:
  - PIN-kod, eller lösenord, inte förvaras tillsammans med e-legitimationen samt att den inte avslöjas för obehöriga.
  - e-legitimationen skyddas på motsvarande sätt som värdeföremål.
  - en aktiverad e-legitimation aldrig lämnas oskyddad.
- E-legitimationsinnehavaren skall omedelbart anmäla till sin organisation att spärrning av e-legitimationen skall ske om det föreligger anledning enligt de allmänna villkor som gäller för beställning av Expisoft E-legitimationer (finns på www.expisoft.se) eller om något av följande inträffat:
  - Om en uppgift i e-legitimationen bedöms vara inkorrekt, alternativt om någon av e-legitimationens uppgifter eller förhållanden förändrats sedan utgivandet, t.ex. för- eller efternamn.
  - Om den privata nyckel som är kopplad till e-legitimationen är röjd eller att det finns anledning att misstänka att den är röjd.
    Exempel: Misstanke finns att en obehörig kommit över organisationens server- eller stämpelcertifikat.

Notera: Utfärdaren kan även på eget initiativ spärra en e-legitimation om e-legitimationsinnehavaren inte anses fullgöra sina åtaganden, om misstanke finns att e-legitimationen blivit komprometterad eller röjd.

1.3.6 Förlitande parts åtaganden och ansvarsförpliktelser

Förlitande part är en organisation som erbjuder en e-tjänst där e-legitimationer används för identifiering och autentisering och/eller elektronisk underskrift. Beteckningen "Förlitande part" innebär att organisationen förlitar sig på att kedjan mellan utfärdare av elektroniska identiteter, användare och eventuell intygsutställare är korrekt. Det är den förlitande

partens ansvar att verifiera e-legitimationens äkthet och tillämplighet, samt dess giltighet i enlighet med kapitel 4.9, spärr och avstängning av e-legitimationer. En förlitande part – till exempel en myndighet som infört legitimering och underskrift i en av myndigheten tillhandahållen e-tjänst – kan välja att antingen utföra denna verifiering själv eller använda en underleverantör för att utföra denna funktion.

1.4 Användning av e-legitimationer (certifikatanvändning)

Det är Förlitande Part eller dennes organisation som avgör för vilka ändamål de utställda e-legitimationerna kan användas.
Lämpliga användningsområden är exempelvis:

- Identifiering av webbplatser, e-tjänster samt skyddad SSL-kommunikation mellan individer, myndigheter och företag.
- Elektronisk stämpel för digitalt godkännande av handlingar, dokument m.m.
- Legitimering (autentisering) vid tillträde och uppgiftslämnande.
- Insynsskydd (kryptering) av kommunikation eller data lagrat på olika media.
- Elektronisk underskrift för digital signering av handlingar, dokument, mejl etc.

Det är den förlitande partens beslut som avgör vilka applikationer/e-tjänster som utfärdade e-legitimationer enligt denna policy skall användas till. Till vägledning för detta beslut har den förlitande parten förutom eventuella interna regelverk denna policy samt tillhörande utfärdardeklaration (CPS).

1.5 Förvaltning av Certifikatpolicyn

1.5.1 Organisation som administrerar denna policy

Utfärdaren Expisoft AB är ansvarig för förvaltning, administration och underhåll av denna CP. Frågor rörande denna CP adresseras till:

Expisoft AB
CA-Tjänsten
Box 2934
187 29 Täby
Sweden

E-post: eid@expisoft.se
Telefonnummer: 020-120 00 44
Telefonnummer från utland: +46 8 123 502 80

1.5.2 Kontaktperson

Ansvarig person för CA-tjänsten kontaktas skriftligt enligt ovanstående adressinformation.

1.5.3 Person som avgör CPS lämplighet utifrån CP

Rollen Certificate Authority Administrator (CAA) (se 5.2.1) är ansvarig för lämplighet och tillämplighet för denna CP i tillhörande utfärdardeklaration (CPS).

1.5.4 Godkännandeprocedur för denna Certifikatpolicy (CP)

Rollen Certificate Authority Administrator (CAA) (se 5.2.1) ansvarar för godkännandeprocessen för detta dokument. Gjorda ändringar ska dokumenteras i form av en uppdaterad CP som publiceras på Utfärdarens hemsida.

1.6 Definitioner och förkortningar

Se kapitel 10 för använda definitioner och förkortningar i detta dokument.

2 Ansvar för publicering och lagring

2.1 Lagringsplatser

Information relaterad till Utfärdarens CA-tjänst, denna CP samt tillhörande CPS ska publiceras på Utfärdarens webbplats.

2.2 Publicering av certifikatrelaterad information

Utfärdaren ska tillhandahålla följande information:

- Denna policy, och tillhörande utfärdardeklaration (CPS).
- Spärrlistor (CRL).
- Samtliga rotcertifikat som utfärdats.
- Avtalsmallar och villkor för Ombud (Återförsäljare, Handläggare).
- Allmänna villkor för beställning av e-legitimationer.

Spärrlistor och rotcertifikat skall alltid finnas tillgängliga via Utfärdarens beställningstjänst.

2.3 Tidpunkter och frekvenser för publicering

För tidpunkt och frekvens avseende publicering av spärrlistor, se 4.9.7.

2.4 Behörighetskontroll för lagringsplatser

Endast av CA-tjänsten betrodd personal skall ha möjlighet att publicera och uppdatera informationen på berörda hemsidor. Ingen behörighetskontroll krävs för att hämta och läsa information enligt 2.2 ovan.

3 Identifiering och autentisering

I detta kapitel beskrivs de regler som gäller vid identifiering och autentisering av fysiska personer och organisationer involverade i processen för verifierande och utställande av certifikat. Personuppgifter ska hanteras i enlighet med personuppgiftslagen, eller annan gällande rätt/avtal som ger stöd till behandling av personuppgifterna.

Varje certifikat som utfärdas har ett antal fält som kan kopplas till den organisation och e-legitimationsinnehavare som certifikatet gäller för, se avsnitt 3.1.

3.1 Namngivning certifikat

3.1.1 Typer av namn

Följande uppgifter är obligatoriska:

Uppgift	Krav på innehåll
Namn	Organisationens namn
Organisationsnummer och löpnummer	Organisationsnummer hos Bolagsverket eller Skatteverket, samt ett löpnummer.

Unik identifierare för e-legitimation	Unik identifierare (64-bitar), används för att särskilja e-legitimationer och dess certifikat.
Common Name (CN)	Detta fält skall innehålla namnet på innehavaren, ett valfritt titelfält, samt organisationens namn.

Certifikat kan även innehålla andra typer av uppgifter (se kapitel 7.1).

3.1.2 Behov av meningsfulla namn

Namnen i certifikaten (se 3.1.1) skall vara meningsfulla i den bemärkelsen att Utfärdaren kan härleda sambandet mellan dessa namn och e-legitimationsinnehavaren.

3.1.3 Anonyma eller pseudonyma e-legitimationsinnehavare

E-legitimationer måste genom korrekta namn identifiera e-legitimationsinnehavaren, dvs anonymitet eller pseudonymer tillåts inte.

3.1.4 Regler för att tolka olika namnformer

De flesta specialtecken hanteras/tillåts inte. Sådana tecken korrigeras.

3.1.5 Unika namn

De obligatoriska uppgifterna enligt 3.1.1 skall på ett unikt sätt identifiera e-legitimationsinnehavaren. Endast officiellt registrerade identitetsuppgifter accepteras. Om organisationen är officiellt registrerad bör det registrerade namnet anges. I Sverige skall det namn användas som är registrerat hos PRV eller motsvarande.
Även om det inte rekommenderas, så finns möjligheten att samma e-legitimationsinnehavare (organisation) kan ha flera certifikat med samma identitet i ämnesfältet (subjekt-fältet). Certifikaten kan då skiljas via certifikatserienumret (ej att förväxla med serienumret i ämnesfältet).

3.1.6 Igenkänning, autentisering och roll för varumärke

Det är e-legitimationshavarens ansvar att se till att valet av namn i certifikatets ämnesfält (subject-fält) inte strider mot varumärke eller varumärkesrätt.

3.2 Verifiering av identitet vid beställning

3.2.1 Metod att bevisa innehavet av den privata nyckeln

Enbart för server- och stämpellegitimationer som beställs med CSR kan en Beställare inneha den privata nyckeln innan beställning av certifikatet, eftersom Beställaren eller dennes organisation i det fallet själv genererat nyckelparet. I de fall då Utfärdaren genererar nyckelparet innehar Beställaren inte någon privat nyckel innan certifikatet levererats till Beställaren.

3.2.1.1 Serverlegitimation och Stämpellegitimation

Som standard tillverkar CA-tjänsten hos Utfärdaren de privata och publika nycklarna i samband med att certifikatet/e-legitimationen utfärdas. En kopia av p12-filen (som innehåller både privat och publik nyckel) sparas hos CA-tjänsten. I detta fall har Beställaren inte tillgång till någon privat nyckel innan mottagande av e-legitimationen. Alternativt genererar e-legitimationsinnehavaren själv ett nyckelpar och sänder över den publika

nyckeln tillsammans med identitetsuppgifter i en CSR till CA-tjänsten. Genom att CSR är signerad med e-legitimationsinnehavarens privata nyckel kan certifikatutfärdaren vara säker på att certifikatbegäran kommer från innehavaren av den privata nyckeln.

3.2.2 Autentisering av organisationens identitet

Organisationens identitet i form av namnuppgifter i certifikatets subjektfält skall verifieras och kontrolleras tillsammans med organisationsnumret. Förkortningar och/eller olika suffix till uppgivet företags-/organisationsnamn är tillåtna under förutsättning att namnet kan associeras med organisationen. Informationen i beställningen skall verifieras och undertecknas av behörig person innan beställning skickas till Utfärdaren. För privata svenska företag krävs signering av en firmatecknare. För utländska organisationer, föreningar, kommuner, myndigheter och statliga bolag där firmatecknare inte finns eller inte är publikt tillgänglig information krävs signering av en person i en ledande chefsposition.

3.2.3 Autentisering av individens identitet

Det är den beställande personen hos beställande organisation (eller Ombud) som ansvarar för att vidta de åtgärder som är nödvändiga för att fastställa att uppgifterna för den resurs, funktion eller person inom organisationen/företaget som ligger till grund för den beställda e-legitimationen är korrekta. Alla beställningar måste signeras av en behörig person (se 3.2.2 för definition av behörig person). Om beställaren själv är behörig så kan denna själv signera beställningen.

3.2.4 Icke kontrollerade uppgifter om e-legitimationsinnehavaren

Alla parametrar i CSR ignoreras förutom CSR:s publika nyckel, som används för att kontrollera att CSR signerats med motsvarande privat nyckel.

3.2.5 Validering av behörighet hos Ombud

I de fall Kunden använder sig av ett Ombud för beställning av e-legitimationer, dvs Återförsäljare, skall parternas förhållande regleras via ett separat avtal där hänvisning till denna CP görs. Validering av behörigheten hos Ombudet skall göras genom utfärdande av en personlig e-legitimation till Ombudets handläggare. Ombudets e-legitimation skall beställas och tillverkas enligt den procedur som beskrivs i kapitel 3.2.3. Denna e-legitimation används därefter för att identifiera Ombudet när denne beställer nya e-legitimationer till sin egen organisation eller sina kunder.

3.2.6 Kriterier för samverkan

Ej tillämpligt, för de certifikat som omfattas av denna policy sker ingen samverkan med andra CA eller andra PKI:er.

3.3 Verifiering av identitet vid förnyelse av nyckelpar

Ej tillämpligt, begäran av förnyelse av nyckelpar är att betrakta som en nybeställning och sker enligt rutiner beskrivna i kapitel 4.1.

3.3.1 Identifiering och autentisering vid förnyelse av nyckelpar för giltigt certifikat

Ej tillämpligt, förnyelse av nyckelpar är att betrakta som en nybeställning och sker enligt rutiner beskrivna i kapitel 4.1.

3.3.2 Identifiering och autentisering vid förnyelse av nyckelpar efter att certifikatet blivit spärrat

Ej tillämpligt, förnyelse av nyckelpar är att betrakta som en nybeställning och sker enligt rutiner beskrivna i kapitel 4.1.

3.4 Verifiering av identitet vid begäran om spärrning

Spärrning av en e-legitimation kan antingen ske av e-legitimationsinnehavaren, ett av kundens Ombud eller Utfärdaren själv. Identifiering av e-legitimationsinnehavaren skall göras genom den unika identifierare som distribuerades till innehavaren samtidigt med e-legitimationen i ett PIN-kodsbrev. Ombud skall identifiera sig genom sin e-legitimation via inloggning till ett av CA-tjänsten tillhandahållet webbgränssnitt. Spärr kan också ske genom att kontakta Utfärdarens supportfunktion. Identifiering av e-legitimationsinnehavaren skall i detta fall genomföras. Spärrningsbegäran hanteras i enlighet med kapitel 4.9.

4 Operativa krav utifrån e-legitimationens livscykel

Detta kapitel beskriver de operationella krav som gäller för Utfärdaren, RA-funktionen, Beställare och e-legitimationsinnehavare. Kraven omfattar ansökan, utfärdande, spärrning, arkivering och loggning.

4.1 Beställning av e-legitimationer

4.1.1 Vem kan beställa en e-legitimation?

En Beställare kan ansöka om/beställa en e-legitimation genom Expisofts webbportal. Ombud (Återförsäljare för Utfärdaren) kan beställa e-legitimationer för sin respektive kund/kundgrupp.

4.1.2 Beställningsprocess och ansvar

Beställare skall identifiera sig i enlighet med kapitel 3.1, samt:

1. Fylla i ansökningshandlingar där alla villkor skall accepteras.
2. Behörig person i Beställarens organisation måste underteckna ansökningshandlingen. (För privata svenska företag krävs signering av en firmatecknare. För utländska organisationer, föreningar, kommuner, myndigheter och statliga bolag där firmatecknare inte finns eller inte är publikt tillgänglig information krävs signering av en person i en ledande chefsposition.) Detta kan antingen göras digitalt med Mobilt BankID, eller genom att skriva ut ansökan i pappersformat.
   Signaturen intygar därmed att:
   - Beställaren har rätt att göra beställningen av e-legitimationen.
   - Lämnade uppgifter i ansökningshandlingen är korrekta.
3. Om signering av beställningsformuläret på papper görs behöver Beställaren posta underskriven ansökan i original som brev till Utfärdarens RA-funktion. RA-funktionen mottar och arkiverar alla ansökningshandlingar enligt kapitel 4.3 och utfärdar därefter e-legitimationen.

Om inte felaktigheter i en beställning kan lösas i samråd med Beställaren, förbehåller sig Utfärdaren rätten att neka en beställning.

Utfärdarens och e-legitimationsinnehavarens ansvarsförpliktelser beskrivs i kapitel 1.3.1.1 respektive 1.3.5.1. Beställningsprocessen kan se olika ut för olika kundgrupper men skall säkerhetsmässigt uppfylla de krav som ställs i denna policy enligt kapitel 3 när det gäller identifiering och autentisering av Beställaren. Ombudets ansvarsförpliktelser beskrivs i kapitel 1.3.3.1.

4.2 Hantering av en e-legitimationsbeställning

Registrering och hantering av de uppgifter som krävs för att utfärda en e-legitimation skall ske på ett sådant sätt så att en sammanblandning av identitetsuppgifter, certifikatfiler och nycklar förhindras.

4.2.1 Identifiering och autentisering

Identifiering och autentisering av Beställaren skall ske enligt kapitel 3.1 i denna policy. Varje beställning av en e-legitimation i Utfärdarens RA-funktion eller via ett Ombud skall vara signerad för att kunna spåras individuellt till den person som beordrade utställandet av e-legitimationen.

4.2.2 Godkännande eller avslag på beställning av en e-legitimation

Utfärdarens RA-funktion kan endast godkänna beställningen och gå vidare med att ställa ut en e-legitimation till Beställaren om både:

- Beställaren uppfyllt sina åtaganden enligt kapitel 1.3.5.1.
- Utfärdarens RA-funktion verifierat Beställarens uppgifter enligt kapitel 3.1 i denna policy.

Alla andra beställningar av e-legitimationer avslås.
En Beställare vars beställning blir avslagen skall bli informerad om vad som krävs för att beställningen skall godkännas.

4.2.3 Behandlingstid för certifikat och e-legitimationsbeställning

Utfärdarens RA-funktion skall utfärda och leverera e-legitimationer inom den leveranstid som anges vid beställningen, räknat från inkommen, undertecknad och korrekt beställning. Utfärdarens RA-funktion skall även ha möjlighet att hantera expressbeställningar.

4.3 Certifikatutfärdande

4.3.1 Aktiviteter under certifikatutfärdandet

Beskrivs i Utfärdardeklarationen.

4.3.2 Utfärdarens meddelande till beställaren om utfärdande av e-legitimation

Beställaren skall informeras skriftligt (exempelvis via e-post) av Utfärdarens RA-funktion om att den beställda e-legitimationen är utfärdad.

4.4 Acceptans av e-legitimation/certifikat

4.4.1 Handlingssätt som fastställer acceptans av utfärdad e-legitimation

Genom att lägga en beställning accepterar Beställaren de vid tidpunkten gällande villkor för utfärdande av e-legitimation enligt kapitel 4.1. Själva ansökan skall anses som en acceptans av det tänkta certifikatet från Beställaren och den behöriga person som undertecknat beställningen.

Utfärdandet av en e-legitimation bekräftar Utfärdarens acceptans av ansökan samt av de uppgifter som Beställaren lämnat i ansökan.

E-legitimationsinnehavaren accepterar utfärdad e-legitimation (certifikat) när denne identifierar sig och kvitterar mottaget PIN-kodsbrev, antingen som rekommenderat brev eller digitalt via inloggat läge i webbportalen.

4.4.2 Certifikatutfärdarens publicering av utfärdad e-legitimation

När en e-legitimation utfärdats skall denna publiceras på CA-tjänstens webbportal där Beställaren efter inloggning kan hämta sina certifikat (publik del).

4.4.3 Utfärdarens information till andra parter om utställda e-legitimationer

Ej tillämpligt, inga parter förutom Utfärdaren, Beställaren och eventuellt Ombud behöver noteras vid utfärdande av e-legitimationer.

4.5 Användning av nyckelpar kopplad till e-legitimationen

4.5.1 Användning av privat nyckel kopplad till e-legitimationen

E-legitimationsinnehavaren får bara använda e-legitimationens certifikat med tillhörande privata nycklar för de ändamål som anges i denna policy, se kapitel 1.4. Certifikatanvändningen måste överensstämma med de KeyUsage fält som ingår i certifikatet, se kapitel 6.1.7. E-legitimationsinnehavare skall även skydda sina privata nycklar från obehörig användning och avbryta användningen av e-legitimationen och dess certifikat när e-legitimationens giltighetstid gått ut eller när den spärrats.

4.5.2 Användning av publik nyckel kopplat till e-legitimationen

Innan en förlitande part (tjänsteägare) använder och accepterar en utfärdad e-legitimation och tillhörande certifikat skall den förlitande parten:

- Kontrollera att e-legitimationen är lämplig för den avsedda användningen
- Verifiera e-legitimationens giltighet, dvs att certifikatets signatur är korrekt
- Verifiera att certifikatets giltighetstid (från och till datum) stämmer
- Kontrollera att certifikatet inte är spärrat, dvs inte finns med på den senast tillgängliga spärrlistan (CRL) från CA-tjänsten och/eller kontrollera med en OCSP förfrågan att certifikatet inte är spärrat.

Om e-legitimationens status ej kan verifieras vid tidpunkten för användning, t.ex. beroende på något system- eller kommunikationsproblem så avgör den förlitande parten om denne skall acceptera och använda certifikatet eller ej.

4.6 Förnyelse av e-legitimation

Ej tillämpligt, förnyelse av en e-legitimation eller dess certifikat hanteras i denna CP som en nybeställning (se kapitel 4.1 och 4.3).

För Serverlegitimationer och Stämpellegitimationer kan Beställaren dock välja att återanvända samma nyckelpar till ett nytt certifikat, i de fall när kunden själv genererat nyckelparet och översänder det till CA-tjänsten i en CSR. Detta är inte rekommenderat förfarande men det är den beställande organisationens beslut huruvida man vill återanvända tidigare e-legitimationers nyckelpar eller inte.

4.6.1 Orsaker till förnyelse av e-legitimationen

Ej tillämpligt.

4.6.2 Vem får begära förnyelse

Ej tillämpligt.

4.6.3 Hantering av begäran om förnyelse av e-legitimationen

Ej tillämpligt.

4.6.4 Anmälan till den ansökande om nytt utfärdande av e-legitimationen

Ej tillämpligt.

4.6.5 Handlingssätt som fastställer acceptans av förnyad e-legitimation

Ej tillämpligt.

4.6.6 Utfärdarens publicering av det förnyade e-legitimationen

Ej tillämpligt.

4.6.7 Utfärdarens anmälan till andra parter om e-legitimationens utfärdande

Ej tillämpligt.

4.7 Förnyelse av certifikatets nyckelpar

Förnyelse av nyckelpar i ett certifikat är bara möjligt för Serverlegitimationer och Stämpellegitimationer när kunden själv genererat ett nyckelpar och översänder det till Utfärdaren i en CSR. I övriga fall, när Utfärdaren tillverkar nyckelparen, så genereras alltid nya krypteringsnycklar vid utfärdandet av ett certifikat. En förnyelse av ett certifikats nyckelpar hanteras i övrigt som en nybeställning (se kapitel 4.1 och 4.3).

4.7.1 Orsaker till förnyelse av certifikatets nycklar

Tekniska problem i samband med installationen av ett certifikat kan leda till en begäran om att förnya ett visst nyckelpar.

4.7.2 Vem kan begära förnyelse av certifikatets nycklar

Endast e-legitimationsinnehavaren kan begära förnyelse av ett nyckelpar, se kapitel 4.1.1.

4.7.3 Hantering av begäran om förnyelse av certifikatets nycklar

Enligt kapitel 0.

4.7.4 Anmälan till ansökanden om nytt utfärdande av certifikat

Enligt kapitel 4.3.2.

4.7.5 Handlingssätt som fastställer acceptans av certifikat

Enligt kapitel 4.4.1.

4.7.6 Utfärdarens publicering av certifikat med nya nycklar

Enligt kapitel 4.4.2.

4.7.7 Utfärdarens anmälan till andra parter vid förnyelse av nycklar

Enligt kapitel 4.4.3.

4.8 Certifikatsmodifiering

Den enda modifiering av ett certifikat som tillåts i denna certifikatpolicy är den modifiering som sker när en e-legitimationsinnehavare förnyar sitt nyckelpar genom en CSR, se kapitel 4.7.

4.8.1 Orsaker till modifiering av certifikat

Enligt 4.7.1.

4.8.2 Vem får begära modifiering av certifikat?

Enligt 4.7.2.

4.8.3 Hantering av begäran om modifiering av certifikat

Enligt 4.7.3.

4.8.4 Anmälan till ansökanden om modifiering av certifikat

Enligt 4.7.4.

4.8.5 Handlingssätt som fastställer acceptans av modifierat certifikat

Enligt 4.7.5.

4.8.6 Utfärdarens publicering av det modifierade certifikatet

Enligt 4.7.6.

4.8.7 Utfärdarens anmälan till andra parter vid certifikatsmodifiering

Enligt 4.7.7.

4.9 Spärrning av e-legitimationer

Spärrning av en e-legitimation innebär att samtliga certifikat knutna till e-legitimationen spärras. Utfärdaren skall tillhandahålla en webbtjänst för att spärra e-legitimationer, som även säkerställer information om spärrade e-legitimationer under hela

e-legitimationens livslängd. Spärrlistor (CRL) skall regelbundet publiceras mot en publik tjänst så att spärrkontroll kan göras mot dessa vid användning av e-legitimationen.

4.9.1 Anledning till spärr

En e-legitimation skall spärras om:

a) En spärrbegäran mottas från e-legitimationsinnehavaren, dennes organisation eller ett Ombud.

b) Någon uppgift i e-legitimationen är eller misstänks vara inkorrekt.

c) Den privata nyckeln eller de tillhörande koderna som är kopplade till e-legitimationen är röjda eller att det finns misstanke om att den/de är komprometterade.

d) E-legitimationsinnehavaren har förlorat sin e-legitimation, dvs certifikatfilen.

e) Någon av de uppgifter eller förhållanden som e-legitimationen innehåller t.ex. namn förändrats.

f) När certifikatet är överflödigt (till exempel ett duplikatcertifikat har utfärdats).

g) Annan anledning som gör att e-legitimationen är föråldrad eller hotar dess krypteringsnycklar.

h) E-legitimationsinnehavarens avtal med Expisoft upphör.

i) Utfärdaren har väsentliga behov av att byta ut nuvarande policy till en ny version där säkerhetsrelevanta ändringar görs.

j) Om CA-tjänstens privata nyckel misstänks vara komprometterad.

k) Om levererat certifikat ej betalats efter att 2 påminnelser skickats ut.

Utfärdaren kan på eget initiativ spärra en e-legitimation om e-legitimationsinnehavaren inte fullgör sina åtaganden som anges i denna policy eller bryter mot tillämplig lag.

4.9.2 Vem kan begära spärr

Spärrning av e-legitimationer kan begäras av e-legitimationsinnehavaren eller dennes Ombud. För de e-legitimationer som omfattas av denna policy gäller att PIN-kodsbrevet innehåller en unik identifierare, som kan användas av innehavaren om denne vill spärra e-legitimationen.

Även Utfärdaren kan på eget initiativ välja att spärra en e-legitimation/certifikat vid misstanke om obehörigt nyttjande av e-legitimationen. Övriga möjligheter till spärrning regleras i separata avtal med respektive avtalspart.

4.9.3 Rutin för spärrbegäran

Beskrivs i Utfärdardeklarationen.

4.9.4 Behandlingstid vid spärrbegäran

Spärrbegäran som sker via Utfärdarens webbtjänst eller manuellt via Utfärdarens supportfunktion, under supportens öppettider, skall utföras direkt och en ny spärrlista skall

publiceras omgående efter utförd spärrbegäran. Beslut om spärrning skall ske i direkt anslutning till spärrbegäran, efter kontroll av identitet hos den som begär spärrningen. En inkommande spärrbegäran via Utfärdarens webbtjänst under ett aviserat planerat avbrott/servicefönster hanteras i dessa fall efter det planerade avbrottet. Driftmeddelanden publiceras på beställningsportalen inför planerade avbrott.

4.9.5 Tid inom vilken CA måste behandla spärrbegäran

En spärrbegäran ska hanteras inom en arbetstimme från det att spärrbegäran inkommit.

Exempel: När e-legitimationsinnehavaren själv spärrar ett certifikat via Utfärdarens webbportal så sker spärrningen direkt, men om en skriftlig spärrbegäran inkommer till Utfärdaren under helgdag så skall denna hanteras under nästkommande arbetsdags första timme.

4.9.6 Krav på förlitande part vid spärrbegäran

Det är förlitande parts ansvar att antingen själv eller via en outsourcad funktion kontrollera om en e-legitimation är spärrad eller inte.
Kontrollen skall utföras på följande sätt:

- Förlitande part som hämtar spärrlista från lagringsplats skall försäkra sig om dess äkthet genom att verifiera dess digitala signatur och certifieringskedja.
- Förlitande part skall även kontrollera spärrlistans giltighetstid för att försäkra sig om att den är aktuell.
- I de fallen förlitande parts kontrollfunktion stödjer OCSP kan en giltighetskontroll av en e-legitimation och dess certifikat även göras via detta protokoll.
- Om ett certifikat är spärrat, skall e-legitimationen inte accepteras.
- Om spärrkontroll enligt ovan inte kan genomföras (till exempel på grund av driftstörningar) så bör e-legitimationen inte accepteras, men Förlitande part kan välja att på egen risk acceptera e-legitimationen i dessa fall.

4.9.7 Utgivningsfrekvens av spärrlistor

Nya spärrlistor (CRL) ska publiceras varje timme, dygnet runt och ha en giltighetstid på 24 timmar, dvs attributet nextUpdate ska vara satt till 24 timmar.

4.9.8 Maximal fördröjning vid utgivning av spärrlistor (CRL)

Fördröjningen från generering av en ny spärrlista tills den finns tillgänglig för spärrkontroll av utgivna certifikat (tillgänglig på CDP/OCSP) skall vara max 10 minuter.

4.9.9 Online spärrbegäran och status/spärrkontroll

För de certifikat som denna policy omfattar ska det även erbjudas online-spärrbegäran och status/spärrkontroll av en e-legitimation via OCSP-protokollet till förlitande parter som ett komplement till spärrlistor (CRL:er).

4.10 Tjänster avseende certifikatsstatus

4.10.1 Egenskaper

Spärrlistor ska publiceras i Utfärdarens publika register/katalog enligt de kriterier och intervall som beskrivs i kapitel 4.9. En OCSP-tjänst skall finnas tillgänglig för användare av e-legitimationerna.

4.10.2 Tillgänglighet

Både CRL- och OCSP-tjänsterna ska finnas tillgängliga 24 timmar om dygnet året runt (24/7/365) med undantag endast för kortare oförberedda avbrott eller planerat underhåll.

4.11 E-legitimationsinnehavarens abonnemang avslutas

Om behov inte längre finns av utfärdad e-legitimation ska e-legitimationsinnehavaren spärra denna.

4.12 Nyckeldeponering och nyckelåterställning

Ej tillämpligt. Nyckeldeponering och nyckelåtervinning stöds ej.

5 Faciliteter, förvaltning och verksamhetsstyrning

Detta kapitel beskriver de fysiska, procedurorienterade och personella kontroller som utförs av Utfärdaren och dess RA-funktion.

5.1 Fysisk säkerhet

Fysisk säkerhet syftar till att skydda Utfärdarens lokaler, utrustning och informationskapital. CA-systemet skall skyddas mot olyckor och fel i tekniska system samt mänskliga misstag och slarv eller kriminella handlingar. Målet med fysisk säkerhet är att förhindra obehörigt fysiskt tillträde, skador och störningar i CA-systemets funktion.

5.1.1 Fysisk placering och uppbyggnad

CA-systemet skall vara fysiskt placerad i en skyddad datorhall. Rummet där CA-systemet står skall vara ett "inre" rum, dvs inte ha vägg angränsade mot en fasad eller ha fönster. Väggar, tak och golv ska vara solida. Rummet ska vara låst och tillträde ska bara ges till auktoriserad personal. Rummet skall ha ett inpasseringssystem bestående av en kortläsare med tillhörande knappsats. All behörig personal skall ha ett personligt inpasseringskort med sin egen PIN-kod.
CA-systemet skall vidare i detta utrymme förvaras i en låst bur med två fysiska hänglås. Detta utrymme kallas i denna policy för CA-systemets driftutrymme.

5.1.2 Fysiskt tillträde

CA-systemet skall skyddas mot obehörigt tillträde. Tillträdeskontroll skall användas för att kontrollera åtkomst till CA-systemets driftutrymme. Loggbok skall föras över alla som bereds tillträde till detta område. För tillträde till CA-systemet krävs även att flera personer närvarar (se avsnitt 5.2.2). Vid kritisk händelse, om det inte går att sammankalla två behöriga personer samtidigt så kan avsteg från kravet på två personer göras, men dessa avsteg måste dokumenteras noga. Utrymmet skall vidare vara försett med nödvändiga larm för att säkerställa upptäckt av varje typ av obehörigt intrång. De privata nycklarna som används för

att signera certifikat och spärrförfrågningar skall vara fysiskt skyddade i en HSM-modul så att de inte kan exponeras även om det sker ett intrång i själva lokalen.

5.1.3 Strömförsörjning och kylning

För att säkerställa CA-funktionens strömförsörjning och kylning vid drift dygnet runt varje dag året runt (24/7/365) skall systemet klara ett strömavbrott på 24 timmar. Detta skall testas minst en gång per år.

5.1.4 Vattenexponering

CA-systemet skall vara skyddad mot vattenexponering. Det ska finnas vattenlarm

5.1.5 Brandskydd

CA-systemet skall skyddas mot brand. Det ska finnas brandlarm

5.1.6 Lagring av media

Utfärdaren skall säkerställa att arkiv- och säkerhetskopior samt distributionsmedia förvaras på ett sådant sätt att förlust, manipulation eller obehörig användning av lagrad information förhindras. När det gäller hantering av personuppgifter skall den följa rådande lagstiftning på området, dvs personuppgiftslagen, dataskyddsdirektivet och GDPR.

5.1.7 Avfallshantering

Känsligt material skall förstöras på ett säkert sätt, så att det inte riskerar att hamna i orätta händer.

5.1.8 Säkerhetskopia på annan plats

Arkiv- och säkerhetskopior skall lagras skilda från det centrala CA-systemet. Kopiorna ska lagras på ett sådant sätt att den lagrade informationen är skyddad mot stöld, förvanskning, förstörelse eller obehörig användning.

5.2 Styrning av CA-funktionen, procedurer och kontroller

Utfärdaren ansvarar för administration och rutiner för utfärdande av e-legitimationer och spärrlistor. Rutiner för spårbarhet skall finnas, så att missbruk och fel i olika led av denna procedur kan upptäckas och korrigeras.

5.2.1 Betrodda roller

Följande olika roller skall finnas i CA-funktionen för utfärdande av E-legitimationer:

1. Information Systems Security Officer (ISSO). Dessa personer har högsta ansvaret för säkerheten i CA-systemet och skall närvara vid särskilt säkerhetskritiska operationer.

2. Certification Authority Administrator (CAA) - ansvarar för centrala operationer på CA-systemet. CAA ansvarar för etablering av ny CA och tilldelning av RA- och SA-behörighet. CAA utför även kontroll av loggar och ansvarar för att CP och CPS efterlevs.

3. System Administrator (SA) – ansvarar för driften. SA utför installationer, system-underhåll, byte av media för säkerhetskopiering. Personen behöver vara godkänd av CAA för arbete med CA-tjänsten men särskilt säkerhetskänsligt arbete behöver utföras under överseende av CAA eller ISSO.

4. RA-administratör hanterar beställningar samt utfärdar och spärrar certifikat.

5. Betrodd person - en av CA-tjänsten betrodd person som kan hjälpa till vid aktiviteter som kräver minst två personer men som inte kräver en specifik roll. Någon av rollerna VD, COO, CAA utser vilka personer som är betrodda.

Det finns även en kundroll Handläggare - rollen innebär att Handläggaren agerar som ett Ombud för sin egen organisation och har befogenhet att beställa, distribuera och spärra e-legitimationer för sin organisations räkning.

Förutom ovan roller som är knutna till CA-funktionen finns även en oberoende roll i form av Granskare (revisor) som har till uppgift att vid speciellt överenskomna tillfällen granska CA-personalens arbete, se avsnitt 8.

5.2.2 Krav på antal personer per uppgift

Vissa känsliga moment och arbetsuppgifter kräver närvaro av fler än en person. Denna policy föreskriver ett antal sådana moment, nämligen:

- Vid utställande av certifikat krävs medverkande av minst två betrodda personer, varav minst en person behöver ha RA-rollen.
- Vid generering av nya utfärdarnycklar och nytt rotcertifikat krävs närvaro av minst två olika personer. Båda rollerna ISSO och CAA ska vara närvarande. (se 6.2.2).
- För hantering av loggar av det centrala CA-systemet, krävs två personer närvarande. En av personerna ska ha ISSO-rollen och den andra personen ska ha någon av rollerna ISSO, CAA, SA eller Betrodd person.
- För fysisk åtkomst till den inlåsta säkerhetskopian av CA:s privata nyckel krävs närvaro av minst två olika personer. Båda rollerna ISSO och CAA ska vara närvarande.
- För fysisk åtkomst till det centrala CA-systemet krävs minst två olika personer, varav en person ska ha någon av rollerna ISSO eller CAA och den andra personen ska ha någon av rollerna ISSO, CAA, SA eller Betrodd person.

Vid kritiska händelser, när drift och tillgänglighet påverkas och det inte går att sammankalla två behöriga personer samtidigt, så går det att göra avsteg på kravet om två personer, men dessa avsteg måste dokumenteras noga för uppföljning och säkerhetsgranskning.

5.2.3 Identifiering och autentisering för respektive roll

Identifiering och autentisering för respektive roll beskriven i 5.2.1 skall göras på ett säkert sätt innebärande att stark autentisering skall användas när dessa användare utför arbets-uppgifter som involverar CA-funktionen.

5.2.4 Roller som kräver separation av uppgifter

En person med rollen Granskare kan inte samtidigt ha någon av de roller som är knutna till CA-funktionen enligt 5.2.1. Både interna och externa Granskare kan användas, det viktiga är att det är en oberoende person. Personen behöver dock vara insatt i CA-tjänstens funktion, procedurer, olika administratörsroller samt denna CP med tillhörande CPS för att kunna utföra sitt uppdrag.

5.3 Personal

5.3.1 Krav på kompetens, erfarenhet och formella kvalifikationer

Personal som innehar roller som ur säkerhetssynpunkt betraktas som kritiska skall vara särskilt utvalda och pålitliga personer som uppvisat lämplighet för sådana befattningar. Personal får inte ha några andra uppgifter som kan vara i konflikt med de åligganden och ansvar som följer av de roller som de har i CA-systemet.

5.3.2 Kontroll av bakgrund

Kontroll av anställda skall göras av Utfärdaren, och denna skall omfatta kontroll av den anställdes tidigare jobb samt personkontroll.

5.3.3 Krav på utbildning

All personal hos Utfärdaren som berörs av CA-systemet skall ges erforderlig utbildning och kunskap för att utföra sina arbetsuppgifter på ett korrekt sätt.

5.3.4 Krav på kompetensutveckling

All personal skall ges nödvändig kompetensutveckling vid förändring av system eller rutiner.

5.3.5 Arbetsrotation

Ej tillämpligt, arbetsrotation är inget krav för de certifikat som omfattas av denna policy.

5.3.6 Sanktioner vid obehöriga aktiviteter

Åtgärder skall vidtas vid obehöriga aktiviteter.

5.3.7 Krav på oberoende för leverantörer

Leverantörer och underleverantörer till CA-tjänsten får inte ha andra uppgifter som är i konflikt med de skyldigheter och ansvar som följer med deras uppgifter mot CA-tjänsten.

5.3.8 Dokumentation för personalen

Personal skall erhålla tillräckliga anvisningar för att korrekt kunna genomföra sina uppgifter i CA-systemet.

5.4 Loggning

5.4.1 Typer av händelser som registreras

Följande händelser (åtminstone) ska loggas i CA-systemet:

- Skapande av användarkonton för CA/RA-administratörer. (säkerhetslogg)

- Initiering av transaktioner såsom utfärda, spärra e-legitimationer, med information om vem som begärde transaktionen, tidpunkt, vilken typ av transaktion som initierats samt uppgift om resultatet av begärd transaktion. (säkerhetslogg)
- Beställningsunderlag inkl. signatur av behörig person samt validering av beställningar och vem som godkänt beställningen. (säkerhetslogg)
- Installation och uppdatering av mjukvara. (driftslogg)
- Relevant information om säkerhetskopiering (datum, tid m.m.). (driftslogg)
- Start och stopp av systemet. (driftslogg)
- Datum och tid för uppgradering av hårdvara. (driftslogg)
- Datum och tid för tömning av driftsloggar. (driftslogg)

5.4.2 Frekvens för analys av loggar

Loggarna ska granskas och analyseras med jämna mellanrum för att upptäcka oönskade händelser.

5.4.3 Bevaringstid för loggar

Säkerhetsloggar ska lagras i minst 10 år, som en del av den arkiverade informationen. Driftsloggar behöver inte lagras lika länge (inget tidskrav).

5.4.4 Skydd av loggar

Loggar ska skyddas mot otillbörlig förändring och vara försedda med individuella tidstämplar.

5.4.5 Säkerhetskopiering av loggar

Säkerhetskopior av loggar ska göras, så att loggarna finns bevarade även om en systemkrasch inträffar eller om en person med illvilligt uppsåt medvetet raderat loggar i CA-systemet.

5.4.6 Insamlingssystem för loggar

Det finns inget krav på insamlingssystem för loggar, så länge loggning sker av alla de händelser som listas i kapitel 5.4.1.

5.4.7 Meddelande till den som orsakat logghändelse

Av säkerhetsskäl ska inget meddelande visas om att en loggpost skapats.

5.4.8 Uppskattning av sårbarhet

En risk- och sårbarhetsanalys av CA-verksamheten ska genomföras åtminstone en gång per år.

5.5 Arkivering

5.5.1 Typ av information som arkiveras

Följande information (åtminstone) skall arkiveras:

- Transaktioner innehållande av behörig operatör signerad begäran om certifikatproduktion eller spärrning av certifikat, e-legitimationens innehåll
- Mottagna spärrningsbegäran av utgivna certifikat enligt 4.9.1
- Beställningsunderlag inkl. signatur av behörig person samt validering av beställningar och vem som godkänt beställningen.
- Historik rörande tidigare utfärdarnycklar
- Avtal rörande e-legitimationer
- Protokoll från revisioner enligt kapitel 8
- Gällande samt tidigare utgivna versioner av denna CP samt tillhörande CPS
- Utfärdade CA-certifikat (inklusive rotcertifikat)
- Säkerhetsloggar

5.5.2 Arkiveringstid

Arkiverad information enligt 5.5.1 skall lagras i informationens livstid, plus tre år. För en rotnyckel med 12 års giltighetstid innebär det en arkiveringstid på minst 15 år.

5.5.3 Skydd av arkiv

Arkivinformationen skall skyddas mot otillbörlig förändring och förlust och endast kunna läsas av behörig personal. Information om enskilda händelser kan erhållas efter begäran av involverad part, representant för involverad part eller annan behörig person. Arkiverat material som är klassat som konfidentiellt skall inte vara tillgängligt för externa parter i sin helhet annat än vad som krävs genom lag och beslut i domstol.

5.5.4 Säkerhetskopiering av arkiv

Ej tillämpligt.

5.5.5 Krav på tidsstämpling av arkivdokument

Tidpunkt för arkivering skall registreras.

5.6 Övergång till ny CA-nyckel

Minst tre månader innan ett gammalt rotcertifikats användningstid löper ut skall nya CA-nycklar (utfärdarnycklar) och ett nytt självsignerat rotcertifikat genereras. Under en övergångsperiod skall både det gamla och det nya CA-certifikatet samtidigt vara aktiva. Exempel: Om de e-legitimationer som genereras har en giltighetstid på två år, ska ett nytt rotcertifikat genereras minst två år och tre månader innan det gamla rotcertifikatet går ut.

5.7 Hantering vid katastrof avseende CA-verksamheten

5.7.1 Förfarande vid allvarliga incidenter

Om ett intrångsförsök eller annan form av möjlig kompromettering av en CA blir känt, skall detta utredas omgående för att fastställa arten och graden av skada. Omfattningen av möjliga skador bedöms utifrån detta, t.ex. huruvida CA-certifikatet behöver spärras eller ej.

5.7.2 Datorer, programvara och/eller data är skadade

Utfärdaren skall löpande skapa säkerhetskopior av system och information som möjliggör återställande av CA-systemet och verksamheten i händelse av skada på programvara, datorer eller annan utrustning. I händelse av misstanke att CA-tjänstens privata nyckel blivit röjd ska en riskanalys och utredning genomföras skyndsamt för att bedöma omfattningen av skadan och lämpliga åtgärder. Om utredningen visar att det är troligt att nyckeln blivit röjd skall en bedömning enligt 5.7.1 göras. Om beslutet blir att CA-tjänstens verksamhet skall upphöra skall aktioner enligt kapitel 5.8 utföras omgående och skyndsamt, dvs utan att beakta tidskravet på 6 månader. Om beslutet blir att CA-tjänsten kan fortsätta sin verksamhet skall Utfärdaren utföra följande åtgärder:

- Utfärda ett nytt rot-CA-certifikat och övergå till detta för certifikatutgivning, spärrlistor och OCSP-tjänst.
- Informera och distribuerade det nya rot-CA-certifikatet till alla förlitande parter, Ombud med flera.
- Spärra e-legitimationer utgivna under den gamla Utfärdarnyckeln och publicera en slutgiltig spärrlista.
- Upphöra med utgivande och publicering av spärrlistor (CRL) och OCSP-tjänst under den gamla Utfärdarnyckeln så att förlitande parter som använder spärrkontroll inte längre litar på äldre utgivna e-legitimationer.
- Kontakta e-legitimationsinnehavare som har legitimationer utgivna under den gamla nyckeln och erbjuda dem att byta ut deras e-legitimation mot en ny.

5.7.3 Förmåga till kontinuitet efter katastrof

CA-tjänsten skall ha en kontinuitetsplan (katastrofplan) som beskriver åtgärder att vidta i händelse av en katastrof. Denna plan skall exekveras i händelse av någon form av katastrof, inklusive misstanke om att CA-tjänstens privata nyckel skulle vara röjd. Planen skall ses över och uppdateras minst årligen för att vara aktuell.

5.8 Upphörande av Utfärdarens verksamhet

Med upphörande av Utfärdarens verksamhet avses en situation där samtliga tjänster kopplade till Utfärdaren upphör. Innan Utfärdaren upphör med sin verksamhet skall (minst) följande åtgärder vidtas:

- Informera alla förlitande parter, alla Ombud, samtliga e-legitimationsinnehavare och övriga parter som Utfärdaren har en relation med. Detta bör ske minst sex månader innan verksamheten upphör.
- Avsluta avtal för eventuella Ombud och underleverantörer.
- Informera publikt på marknaden om att verksamheten upphör.
- Upphöra med utfärdande av nya certifikat.
- Säkerställa att alla arkiv och loggar kan bevaras på ett betryggande sätt enligt överenskommen arkiveringstid.

6 Tekniska säkerhetsåtgärder

Detta kapitel innehåller regler för generering och installation av nyckelpar, skydd av nycklar samt andra tekniska säkerhetskontroller.

6.1 Generering och installation av nyckelpar

6.1.1 Generering av nyckelpar

Indata till samtliga nyckelgenereringsprocesser skall vara ett slumptal skapat på sådant sätt och av sådan längd att det är beräkningsmässigt ogörligt att återskapa detsamma även med kunskap om när och i vilken utrustning det genererades.

Nyckelgenereringsprocessen skall vara så beskaffad att ingen information om den privata nyckeln hanteras utanför nyckelgenereringssystemet annat än genom säker överföring till avsedd plats.
Publika nycklar skall hanteras på ett sådant sätt att deras integritet garanteras.

6.1.1.1 Utfärdarnycklar för signering av certifikat och spärrlistor

Utfärdarnycklar som används för signering av certifikat och spärrlistor skall genereras och användas i en fysiskt skyddad miljö enligt 5.1. Detta innebär bland annat att tillträde till denna enhet kräver samtidig närvaro av minst två behöriga personer, enligt kapitel 5.2.2. CA-nycklarna ska genereras i en hårdvarumodul (HSM) som är dedikerad för att lagra och använda krypteringsnycklar. Vid generering av utfärdarnycklar krävs flera personers närvaro, som var och en innehar olika roller. Hela förloppet ska dokumenteras.

6.1.1.2 Nyckelpar för e-legitimationsinnehavare

Nycklar för en e-legitimation genereras (vanligtvis) i samband med framställandet av e-legitimationen. E-legitimationsinnehavarens privata nycklar skall lagras läs- och skrivskyddade i e-legitimationen. Vid certifieringen skall nycklarnas integritet kontrolleras. Nyckelgenereringen och tillhörande kontroller (före certifiering) skall ske på sådant sätt att sannolikheten för att nyckelpar dubbleras är försumbar eller obefintlig.

6.1.2 Leverans av privat nyckel till e-legitimationsinnehavare

Det är antingen Utfärdaren, Ombud eller RA-funktionen som ansvarar för utlämning av e-legitimationer. E-legitimationen skall skyddas av en initial PIN-kod som skall distribueras till innehavaren på sådant sätt att den inte uppträder tillsammans med e-legitimationen förrän hos innehavaren. I de fall när e-legitimationsinnehavaren själv framställt ett nyckelpar (se kapitel 3.2.1.1) och skickat den publika nyckeln tillsammans med identitetsuppgifter i en CSR till CA-tjänsten, befinner sig den privata nyckeln redan hos e-legitimationsinnehavaren och behöver således inte levereras till denne.

6.1.3 Leverans av publik nyckel till certifikatutfärdare

Endast tillämpligt i de fall e-legitimationsinnehavaren använder sig av CSR, i samband med framställande av Server- eller Stämpellegitimationer. I övriga fall framställs den publika nyckeln av Utfärdaren.

6.1.4 Leverans av CA:s publika nycklar till förlitande parter

Förlitande part ansvarar för att hämta korrekta och gällande versioner av CA:s publika nycklar (se kapitel 2).

6.1.5 Nyckelstorlek

Nyckelstorlek för de RSA-nyckelpar som genereras i CA-systemet skall vara minst 2048 bitar.

6.1.6 Parametrar för generering av publik nyckel och kvalitetskontroll

E-legitimationsinnehavarens nycklar som i certifikaten markeras med användningsområdena kryptering, autentisering, och/eller verifiering av oavvislig digital information skall ges publika exponenter som förhindrar kända attacker. Även Utfärdarens nycklar skall ges publika exponenter som förhindrar kända attacker. Det förutsätts att Utfärdaren håller sig uppdaterad med teknikutvecklingen inom PKI och anpassar sina kryptoalgoritmer i enlighet med de dessa för att bibehålla en hög skyddsnivå.

6.1.7 Ändamål för nyckelanvändning (certifikatens key usage-fältet)

CA-certifikaten (inklusive rotcertifikaten) skall ha nyckelanvändning med bitarna keyCertSign och cRLSign satta i certifikatets key usage-fält (se RFC 5280). Enbart rotcertifikatet ska kunna skapa CA-certifikat (CA-certifikat skall ha pathLenConstraint satt till 0, se RFC 5280). Nyckelinnehavarnas certifikat, vilka används för signering av meddelanden, skall ha biten nonRepudiation satt i certifikatets key usage-fält. Denna bit benämns även contentCommitment (se RFC 5280).

6.2 Skydd av privata nycklar & utformning av kryptografisk modul (HSM)

Privata utfärdarnycklar avsedda att signera certifikat, spärrlistor, rotcertifikat samt andra privata nycklar i CA-systemet, skall säkras av mycket starka fysiska skydd, se kapitel 5.1 och logiska skydd (HSM). Övriga privata nycklar i Utfärdarprocessen som används utanför CA-systemets miljö och som påverkar certifikatutgivnings- och spärrkontrolltjänster skall lagras och användas i smartkort (PKCS#15) och/eller annan säkerhetsmodul (PKCS#12).

6.2.1 Standard och förfarande vid användning av kryptografisk modul

Den HSM-modul som används för att generera nycklar skall vara certifierad åtminstone enligt CC EAL4+ och FIPS 140-2 nivå 3.

6.2.2 Krav på flera personer för att hantera privat nyckel (n av m)

Fysisk access till CA-tjänstens privata utfärdarnyckel kräver samverkan av minst två personer under hela nyckelns existens, från generering tills dess att alla kopior är säkert raderade. Även för vissa känsliga arbetsuppgifter krävs närvaro av fler än en person, se 5.2.1.

6.2.3 Nyckeldeponering av privat utfärdarnyckel

Ej tillämpligt, Utfärdaren deponerar inga privata nycklar, varken privata Utfärdarnycklar, administratörernas privata nycklar eller kundernas privata nycklar i utfärdade e-legitimationer.

6.2.4 Säkerhetskopiering av privat utfärdarnyckel

Privata utfärdarnycklar avsedda att signera certifikat, spärrlistor, rotcertifikat samt andra privata nycklar i CA-systemet skall säkerhetskopieras. Hantering av backupkopian skall ha minst samma skydd som de nycklar som används i produktionsmiljön. Backupkopian skall inte vid något tillfälle finnas tillgänglig i okrypterad form utanför HSM-modulen. Kopian skall lagras säkert inlåst frånskilt från CA-systemet där två behöriga personer i förening krävs för åtkomst.

6.2.5 Arkivering av privat utfärdarnyckel

Se avsnitt 6.2.3 och 6.2.4.

6.2.6 Transport av privat utfärdarnyckel till och från kryptografisk modul

Den privata utfärdarnyckeln ska genereras i den kryptografiska modul som specificeras i avsnitt 6.2.7 och aldrig lämna modulen förutom vid arkivering av säkerhetskopia eller om nyckeln ska flyttas till en ny kryptografisk modul.

6.2.7 Lagring av privat utfärdarnyckel i kryptografisk modul

Utfärdarens privata nyckel skall lagras i en HSM-modul certifierad åtminstone enligt CC EAL4+ och FIPS 140-2 nivå 3. Tillträde till HSM-modulen kräver samtidig närvaro av minst två behöriga personer, enligt kapitel 5.2.2.

6.2.8 Metod för att aktivera den privata utfärdarnyckeln

Aktivering av CA-tjänstens privata nycklar för rotcertifikat kräver hantering av två personer och görs endast då nya rotcertifikat ska skapas. Åtkomst till HSM-modulen är begränsad (se avsnitt 5.1.2) och särskild aktiveringsinformation ska krävas för att aktivera den privata utfärdarnyckeln.

6.2.9 Metod för att deaktivera den privata utfärdarnyckeln

CA-tjänstens privata utfärdarnyckel deaktiveras genom att den förstörs, se kapitel 0.

6.2.10 Metod för att förstöra den privata utfärdarnyckeln

CA-tjänstens privata utfärdarnyckel ska förstöras då giltighetstiden gått ut eller om den blivit spärrad. Detta sker genom att den privata nyckeln raderas permanent i HSM samt att backupkopian av den privata nyckeln förstörs. Utfärdarnycklarna får dock ej förstöras om de står i strid med arkiveringskraven i certifikatpolicyn eller krav i annan lagstiftning.

6.2.11 Säkerhetsvärdering av kryptografisk modul

Ingen formell säkerhetsvärdering krävs, så länge modulen uppfyller kraven i 6.2.1.

6.3 Andra aspekter på hantering av nyckelpar

Ingen känslig information från CA-, nyckelgenererings- eller personaliseringsprocessen får lämna systemen på ett sätt som står i konflikt med denna policy. Skapande av privata nycklar sker i en skyddad miljö och kräver minst två medverkande behöriga individer. Vid service och liknande situationer då beskrivna skyddsmetoder inte kan garanteras skall lagringsmedia som innehåller känslig information i första hand ej skickas med och om det inte kan undvikas, raderas på ett säkert sätt. Utrangerade lagringsmedia skall förstöras fysiskt.

6.3.1 Arkivering av publik nyckel

Alla publika nycklar skall arkiveras av Utfärdaren, det gäller såväl Utfärdarnycklar som utgivna e-legitimationers publika nycklar, se kapitel 5.5.2.

6.3.2 Giltighetstid för e-legitimationer och nyckelpar

CA-tjänstens nyckelpar och rotcertifikat har en giltighetstid på 12 år.
Utfärdade e-legitimationer och deras nyckelpar har en giltighetstid på 2 år.

6.3.3 Ansvar för e-legitimationens PIN/PUK-koder och lösenord

E-legitimationen får inte brukas av någon annan än innehavaren. Till e-legitimationen hör en säkerhetskod (PIN) som krävs för nyttjande av e-legitimationen. E-legitimationsinnehavaren måste förvara denna kod på ett säkert sätt och inte avslöja den för någon. Vid misstanke om att någon obehörig kan ha fått tillgång till e-legitimationen måste denna omedelbart spärras.

6.4 Aktiveringsinformation

6.4.1 Generering och installation av aktiveringsinformation

Indata till samtliga genereringsprocesser av aktiveringsdata skall vara ett slumptal.

6.4.2 Skydd av aktiveringsdata

Aktiveringsinformation för CA-tjänstens privata utfärdarnyckel skall skyddas mot stöld och brand. Endast betrodda personer ska ha tillgång till aktiveringsinformationen.

6.4.3 Övriga aspekter på aktiveringsinformation

Ej tillämpligt.

6.5 IT-säkerhetskontroller

Driftsmiljön för CA-tjänsten skall vara konstruerad för att uppnå hög säkerhetsnivå, vilket innebär att den är fysiskt och logiskt separerad från Utfärdarens övriga verksamhet.
De uppgifter som utförs i driftsmiljön är uppdateringar av programvara, start och stopp av applikationer, övrigt systemunderhåll samt arbete som inbegriper hantering av CA-nycklar.
Administrationen av CA-tjänsten skall vara uppbyggt på ett sådant sätt att individuella roller enligt 5.2 kan separeras. Separering av roller på OS-nivå kan säkras genom dubbelbemanning. Inloggning i CA-tjänsten skall ske med separata användaridentiteter för att säkerställa spårbarhet vid inloggning samt administratörens fortsatta arbete i systemet.
Säkerhetsfunktionerna skall säkerställa åtkomstkontroll och spårbarhet för varje administratör på individuell nivå för de funktioner som påverkar användningen av Utfärdarens privata nyckel. RA-funktioner som rör utfärdande och spärrning av e-legitimationer eller certifikat skall utföras via webbgränssnitt mot CA-tjänsten som kräver att den begärda åtgärden signeras med administratörens e-legitimation.

6.5.1 Särskilda IT-säkerhetstekniska krav

Initiering av det system som utnyttjar privata utfärdarnycklar skall kräva samverkan av minst två betrodda operatörer. En detaljerad logg skall föras över alla manuella steg i processen.

Installation av operativsystem och CA-system skall ske i direkt anslutning till formatering av diskar och med leverantörens originalutgåva av programmen. Ett protokoll över installations- och konfigureringsprocessen skall signeras av samtliga deltagare och arkiveras. Vid registrering av initiala användare behörigheter i CA-systemet skall minst två personer i betrodda roller samverka.

6.6 Livscykeltekniska krav

6.6.1 Säkerhetskrav avseende systemutveckling

Utveckling av programvara som implementerar funktionalitet hos CA-systemet, skall utföras i en kontrollerad miljö där leverantören tillämpar ett kvalitetssäkringssystem för skydd mot införande av obehörig kod.

6.6.2 Säkerhetskrav avseende säkerhetsadministrationen

Konfigurering och modifiering av CA-systemet skall dokumenteras i form av loggar. Säkerhetsadministrationen skall endast kunna göras av person(er) som tilldelats roll för att hantera detta, se kapitel 5.2.

6.7 Nätverkssäkerhetskrav

CA-tjänsten skall vara ansluten till ett externt nätverk och skyddas av dedikerad brandvägg med tillräcklig styrka för att motstå DoS/DDoS-attacker och liknande angrepp som kan misstänkas riktas mot tjänsten. CA-tjänstens brandvägg skall vara konfigurerad för att endast tillåta passage av de protokoll som är nödvändiga för att realisera CA-funktionen.
Vidare skall CA-tjänsten och dess beställningsportal vara ansluten via (minst) två separata förbindelser för att öka tillgänglighet och driftsäkerhet. Kommunikation till och från CA-miljön skall utnyttja kryptering av en styrka som är tillförlitlig enligt vid var tid gällande praxis.

6.8 Tidsstämpling

CA-systemet skall ges tillgång till korrekt tid som uppfyller verksamhetens behov för att skapa certifikat, spärrlistor och loggar.

7 Certifikat, CRL och OCSP-profiler

Certifikat och spärrlistor ska följa standard X.509 version 3.

7.1 Certifikat som Utfärdaren kan ställa ut

Samtliga utgivna e-legitimationers publika och privata nycklar har en nyckellängd om minst 2048 bitar, se kapitel 6.1.5.

Utfärdande av e-legitimationer i enlighet med denna policy innebär att:

1. Serverlegitimation och Stämpellegitimation ställs endast ut till juridiska personer, dvs innehavaren av en sådan legitimation är en organisation.
2. Utfärdade Serverlegitimationer och Stämpellegitimationer följer PKCS#12-standarden laddas ned av Beställaren via en unik identifierare som denne erhåller

via ett rekommenderat brev eller via inloggat läge på utfärdarens beställningsportal. E-legitimationen lagras på en server och skyddas av en PIN-kod.

7.1.1 Serverlegitimation (organisation)

En Serverlegitimation är ett filcertifikat (PKCS#12), som installeras på en server och gör det möjligt att upprätta en 256-bits SSL baserad krypteringsförbindelse med anropande server/klient, signering av programvara, samt andra tjänster. En serverlegitimation är inte personlig utan knuten till en specifik server i det beställande företaget/organisationen. Serverlegitimationen skyddas av en lösenordskod om minst 8 alfanumeriska tecken. Utställda serverlegitimationer är giltiga 2 år från utgivningsdagen.

7.1.2 Stämpellegitimation (organisation)

En Stämpellegitimation är ett filcertifikat (PKCS#12) som installeras på det system organisationen önskar nyttja för utövande av organisationens elektroniska stämpel. Med en elektronisk stämpel kan olika elektroniska dokument och handlingar signeras i organisationens namn. En stämpellegitimation är inte personlig utan knuten till en specifik server/funktion i den beställande organisationen. Stämpellegitimationen skyddas av en lösenordskod om minst 8 alfanumeriska tecken. Utställda stämpellegitimationer är giltiga 2 år från utgivningsdagen.

7.2 Certifikatens profil och version

Certifikatsstandard är X.509 v3. Förekomst och användning av dataelement i certifikaten skall ske i enlighet med denna policy.

7.2.1 Serverlegitimation (organisation)

Fält i certifikatet:

Fältnamn	Förekomst	Kommentar/Värde
Version	M	=2 (X.509 v.3)
SerialNumber	M	Utfärdaren använder sig av ett löpnummer från 1000 och uppåt.
Signature	M	SHA256WithRSAEncryption
Issuer	M	Följande attribut används - countryName (SE) - OrganisationName (Expisoft AB) - CommonName (ExpiTrust EID CA v4)
Validity	M	En giltighetstid på (minst) två år.
Subject	M	Följande attribut används: - countryName (SE) - organisationName (Officiellt kundnamn för organisationen, företaget, myndighet etc.) - title (Angiven titel vid beställning av legitimation) - surname (Angivet efternamn vid beställning) - givenName (Angivet förnamn vid beställning)

		- SerialNumber (Organisationsnummer 10 siffror följt av ett nummer, ofta ett anställningsnummer, Format: 16 XXXXXXXXXX<nr>) - CommonName
Subject PublicKey Info	M	RsaEncryption (2048 bitars nyckel)

Följande certifikatextensions används i utfärdade e-legitimationer

Fältnamn	Förekomst	Critical	Kommentar/Värde
authorityKeyIdentifier	M	non-critical	SHA-1 (hash av CA-tjänstens publika nyckel)
subjectKeyIdentifier	M	non-critical	SHA-1 (hash av certifikatets publika nyckel)
keyUsage	M	critical	- digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment
certificatePolicies	M	non-critical	PolicyIdentifier=1.2.752.54.9.2.13.2
Subject Alt Name	O	non-critical	Om e-postadresser läggs in här, ska dessa vara enligt RFC 5322 (local-part@domain). IP-adress för VPN-utrustningar kan anges i denna utökning.
Subject Directory Attributes	-	non-critical	Används ej för närvarande
CRL Distribution Points	M	non-critical	http://cdp1.certservice.se/cdp/eid/ExpiTrust%20EID%20CA%20v4.crl http://cdp2.certservice.se/cdp/eid/ExpiTrust%20EID%20CA%20v4.crl
Ext Key Usage	-	non-critical	Används ej för närvarande
authorityInfoAccess	M	non-critical	http://ocsp.certservice.se

Följande privata utökningar (extensions) används i utfärdade e-legitimationer

Fältnamn	Förekomst	Critical	Kommentar/Värde
Card Number	O	non-critical	Används ej för närvarande

7.2.2 Stämpellegitimation (organisation)

Fält i certifikatet:

Fältnamn	Förekomst	Kommentar/Värde
Version	M	=2 (X.509 v.3)

SerialNumber	M	Utfärdaren använder sig av ett löpnummer från 1000 och uppåt.
Signature	M	SHA256WithRSAEncryption
Issuer	M	Följande attribut används - countryName (SE) - OrganisationName (Expisoft AB) - CommonName (ExpiTrust EID CA v4)
Validity	M	En giltighetstid på (minst) två år.
Subject	M	Följande attribut används: - countryName (SE) - organisationName (Officiellt kundnamn för organisationen, företaget, myndighet etc.) - SerialNumber (16+Organisationsnummer 10 siffror Format: 16XXXXXXXXXX) - CommonName
Subject PublicKey Info	M	RsaEncryption (2048 bitars nyckel)

Följande certifikatextensions används i utfärdade e-legitimationer

Fältnamn	Förekomst	Critical	Kommentar/Värde
authorityKeyIdentifier	M	non-critical	SHA-1 (hash av CA-tjänstens publika nyckel)
subjectKeyIdentifier	M	non-critical	SHA-1 (hash av certifikatets publika nyckel)
keyUsage	M	critical	- digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment
certificatePolicies	M	non-critical	PolicyIdentifier=1.2.752.54.9.2.13.2
Subject Alt Name	O	non-critical	Om e-postadresser läggs in här, ska dessa vara enligt RFC 5322 (local-part@domain). IP-adress för VPN-utrustningar kan anges i denna utökning.
Subject Directory Attributes	-	non-critical	Används ej för närvarande
CRL Distribution Points	M	non-critical	http://cdp1.certservice.se/cdp/eid/ExpiTrust%20EID%20CA%20v4.crl http://cdp2.certservice.se/cdp/eid/ExpiTrust%20EID%20CA%20v4.crl
Ext Key Usage	-	non-critical	Används ej för närvarande
authorityInfoAccess	M	non-critical	http://ocsp.certservice.se

Följande privata utökningar (extensions) används i utfärdade e-legitimationer

Fältnamn	Förekomst	Critical	Kommentar/Värde
Card Number	O	non-critical	Används ej för närvarande

7.3 Profil för spärrlista (CRL)

CA-tjänsten utfärdar spärrlistor som följer CRL version 2 enligt X.509.

7.4 OCSP-profil

OCSP tillhandahålls för validering av certifikaten. OCSP-förfrågningar signeras av ett för OCSP-servern eget certifikat och inte av respektive rotcertifikat.

DNS till OCSP är ”ocsp.certservice.se”. Eftersom OCSP-anropet är digitalt signerat så används HTTP-protokollet för att anropa tjänsten.

8 Överensstämmelse utifrån revision och andra granskningar

8.1 Frekvens och omständigheter för granskning

Säkerhetsansvarig för CA-tjänsten (se 5.2.1) avgör frekvens och omständigheter för interna och externa revisioner för att säkerställa att denna policy efterlevs. Utfärdaren förbehåller sig rätten att periodiskt kräva inspektioner och revisioner av CA-tjänstens underleverantörer, Återförsäljare, Handläggare och RA-funktion för att validera de arbetar enligt säkerhetspraxis och förfarande som anges i denna CP och CPS.

8.2 Identitet/kvalifikationer för granskare

Säkerhetsansvarig för CA-tjänsten utser granskare.

8.3 Granskares relationer till bedömd enhet

Se kapitel 5.2.4.

8.4 Områden för revision

Vid revision skall följande områden granskas:

- CA-tjänstens funktionalitet rörande identifiering och autentisering.
- CA-tjänstens operativa funktioner.
- CA-tjänstens procedur- och personalkontroller.
- CA-tjänstens fysiska och tekniska säkerhet.

Granskningen skall även omfatta:

- Utfärdardeklarationens (CPS) lämplighet och överensstämmelse med denna Certifikatpolicy (CP) .
- Den praktiska implementeringen av Utfärdardeklarationen (CPS).
- Efterlevnad av avtal och samverkansförhållanden som rör CA-tjänstens Återförsäljare och underleverantörer.

8.5 Åtgärder som vidtas till följd av upptäckt brist

Utifrån sammanställning av eventuella brister skall en planering av åtgärder ske under ledning av Säkerhetsansvarig för CA-tjänsten, se 5.2.1.

8.6 Kommunikation av resultat

Sammanställning och åtgärder enligt 8.5 publiceras inte offentligt, men revisionsresultatet skall tillhandahållas på begäran av en Förlitande Part. Redovisningen skall innehålla information om samtliga upptäckta brister som är av sådan art att de kan anses påverka en Förlitande Parts förtroende för en utfärdad e-legitimation. Informationen ska innefatta typ av brist samt bedömning av eventuella risker och konsekvenser.

Redovisningen får dock inte innehålla detaljerade uppgifter om CA-tjänsten eller eventuella brister som kan tänkas äventyra säkerheten i systemet.

9 Andra affärsmässiga och juridiska frågor

9.1 Avgifter

9.1.1 Avgifter för utfärdande av e-legitimationer

Avgiften skall visas i samband med beställning av e-legitimationen, eller vara känd genom separata avtal med kunden.

9.1.2 Avgifter för åtkomst till certifikat

Ej tillämpligt.

9.1.3 Avgifter för åtkomst till spärrinformation

Ingår i grundtjänst

9.1.4 Avgifter för andra tjänster

Enligt separata avtal, i de fall det är tillämpligt.

9.1.5 Återbetalningspolicy

Ej tillämpligt.

9.2 Finansiellt ansvar

9.2.1 Försäkringsskydd

Ej tillämpligt.

9.2.2 Övriga tillgångar

Ej tillämpligt.

9.2.3 Försäkringar och garantier för slutanvändare

Ej tillämpligt.

9.3 Sekretess för affärsinformation

Ej tillämpligt. Regleras inte i detta dokument

9.3.1 Omfattning för sekretessbelagd information

Ej tillämpligt.

9.3.2 Information som inte är sekretessbelagd

Ej tillämpligt.

9.3.3 Ansvar för att skydda sekretessbelagd information

Ej tillämpligt.

9.4 Sekretess för personlig information

Ej tillämpligt. Regleras inte i detta dokument.

9.4.1 Sekretessplan

Ej tillämpligt.

9.4.2 Informations som behandlas som privat

Ej tillämpligt.

9.4.3 Information som inte bedöms som privat

Ej tillämpligt.

9.4.4 Ansvar att skydda privat information

Ej tillämpligt.

9.4.5 Anmälan och samtycke att använda privat information

Ej tillämpligt.

9.4.6 Utlämning i enlighet med juridiska och administrativa processer

Ej tillämpligt.

9.4.7 Övriga omständigheter avseende utlämning av information

Ej tillämpligt

9.5 Immateriella rättigheter

Vid spridning av denna policy får ingen information förändras, tas bort, eller läggas till. Det ska tydligt anges att Expisoft AB är utfärdare av detta policydokument.

9.6 Förpliktelser och garantier

9.6.1 CA:s förpliktelser och garantier

CA skall tillhandahålla CA-tjänster enligt denna CP.

9.6.2 RA:s förpliktelser och garantier

RA skall utföra uppgifter för identifiering och registrering enligt denna CP.

9.6.3 E-legitimationsinnehavares förpliktelser och garantier

I de fall då e-legitimationsinnehavaren själv genererar nyckelpar så skall de nycklarna genereras med god kvalitet och skyddas mot spridning och obehörig användning.

E-legitimationsinnehavaren, Beställaren eller dennes organisation ska betala till Utfärdaren den överenskomna avgiften för e-legitimationen.

9.6.3.1 Temporär spärr av e-legitimation

Om en e-legitimationsinnehavare inte betalat faktura efter tre påminnelser så förbehåller sig Utfärdaren rätten att temporärt spärra en e-legitimation och tillhörande certifikat. När fakturan väl är betald hävs den temporära spärren och e-legitimationen går att använda igen.

9.6.4 Förlitande parts förpliktelser och garantier

Vid kontroll av signaturer skall certifikatets giltighet kontrolleras. Detta innefattar även kontroll mot spärrlista.

9.6.5 Förpliktelser och garantier avseende andra deltagare

Ej tillämpligt.

9.7 Friskrivningar avseende garantier

Utfärdande av e-legitimation i enlighet med denna policy medför inte att Utfärdaren skall betraktas som agent, fullmäktige, eller på annat sätt som representant för e-legitimationsinnehavaren eller Förlitande Part.

9.8 Ansvarsbegränsningar

Utfärdaren tar inget ansvar för otillåten användning av certifikat (se kapitel 1.3).

9.9 Skadestånd och ersättningar

Ej tillämpligt.

9.10 Giltighetsperiod för denna Certifikatpolicy (CP)

9.10.1 Period startar

Denna certifikatpolicy skall gälla utifrån att den publicerats på Expisofts hemsida

9.10.2 Period upphör

Denna certifikatpolicy skall gälla tills den ersätts av ny version eller tills CA upphör med sin verksamhet.

9.11 Kommunikation med ingående parter angående CA-tjänsten

Expisoft förbehåller sig rätten att när behov föreligger lämna viss typ av information om CA-tjänsten via e-post eller Expisofts webbplats, när detta inte strider mot denna policy eller tillhörande utfärdardeklaration (CPS).

9.12 Ändringar av denna Certifikatpolicy

Se kapitel 1.4.

9.13 Tvistlösningsbestämmelser

Eventuell tvist med anledning av denna policy skall slutligt avgöras genom skiljedom enligt Stockholms Handelskammares Skiljedomsinstituts Regler för Förenklat Skiljeförfarande. Skiljeförfarandet skall äga rum i Stockholm. Hänvisningen till skiljedom skall inte äga tillämpning i konsumentförhållanden.

9.14 Tillämplig lag

Svensk rätt skall äga tillämpning på denna policy samt därur uppkomna rättsförhållanden.

9.15 Överensstämmelse med gällande lag

Hantering av CA-systemet skall ske i överensstämmelse med svensk lag.

9.16 Övriga förpliktelser och bestämmelser

Ej tillämpligt.

10 Definitioner och förkortningar

Nedan tabell innehåller de begrepp, definitioner och förkortningar som används i denna CP.

Benämning	Förklaring
Aktivt kort	En plastbricka med ett chip på som kan innehålla en personlig e-legitimation med ett eller flera certifikat.
Allmänna villkor	Är de villkor som beskrivs i detta dokument och som gäller för beställning av Expisofts e-legitimationer.
Användningstid	Perioden då ett rotcertifikat och tillhörande utfärdarnycklar kan användas för att generera e-legitimationer. Användningstiden kan definieras som rotcertifikatets giltighetstid minus de utfärdade certifikatens giltighetstid. Exempel: Om rotcertifikatet har en giltighetstid på 12 år och e-legitimationernas giltighetstid är två år så blir användningstiden för rotcertifikatet 10 år.
Asymmetriskt kryptosystem	Kryptosystem där olika nycklar används för kryptering och dekryptering.
Autentisering	Verifiering/äkthetskontroll av uppgiven identitet. (Legitimering)
Avtal	Avtalet mellan Utfärdaren och den Beställande organisationen för utfärdande av en beställd e-legitimation.
Behörig person	Fysisk person hos den Beställande organisationen som får godkänna att beställningen görs i organisationens namn. För privata svenska företag krävs underskrift av en firmatecknare. För utländska organisationer, föreningar, kommuner, myndigheter och statliga bolag där firmatecknare inte finns eller inte är publikt tillgänglig information krävs underskrift av en person i en ledande chefsposition.
Beställande organisation	Den juridiska person som utför beställningen, detta kan vara kunden själv eller ett ombud/återförsäljare för kunden.
Beställare	Fysisk person i den beställande organisationen som utför beställning av e-legitimation för sin organisations räkning.
CA-miljö	CA-miljö omfattar CA-system med kringutrustning, inkluderande både hårdvara och mjukvara.

CA-policy	Se Certifikatpolicy
CA-system	Det isolerade systemet där Utfärdarens privata nyckel lagras och används (i en speciell maskinvara – HSM).
CA-tjänst	Den funktion hos Utfärdaren som ansvarar för att ge ut, hantera och spärra certifikat och e-legitimationer.
Certification Authority Administrator (CAA)	Roll med övergripande ansvar för att hantering och skapande av certifikat sker enligt gällande styrdokument och att vår CA fortsätter att vara en betrodd utgivare.
Certifikat	Ett elektroniskt, av CA-tjänsten, signerat X.509 certifikat av en publik nyckels tillhörighet till en specifik person eller funktion i en organisation.
Certifikatkedja	Ordnad sekvens av (kors-) certifikat som med hjälp av en rotnyckel för det första certifikatet medger att det sista (användar-) certifikatet kan verifieras.
Certifikatpolicy (CP)	Regelverk som Utfärdaren skall tillämpa vid utfärdande av certifikat.
Certifikatutfärdare	Betrodd organisation som tillhandahåller en CA-tjänst som har till uppgift att skapa och ge ut certifikat (e-legitimationer).
Digital signatur	Är en digital (elektronisk) motsvarighet till en traditionell pappersbaserad underskrift. Den digitala signaturen skapas genom att användaren signerar angiven digital information med sin privata nyckel enligt en speciell procedur. Den digitala signaturen kan användas dels för att spåra vem som signerat informationen (oavvislighet), dels för att verifiera att informationen inte förändrats (integritet) sedan den signerades.
eid.expisoft.se	Expisofts beställningstjänst för e-legitimationer och certifikat. Kallas även för Expisofts beställningsportal.
E-legitimationer	En gemensam benämning för de olika certifikat som Utfärdaren ställer ut. En e-legitimation är ett samlat begrepp för ett eller flera certifikat som innehåller uppgifter som gör att innehavaren kan identifiera sig eller signera något elektroniskt.
E-legitimationsinnehavare	Den organisation eller person inom en organisation som står som innehavare av ett utfärdat certifikat och använder det.
Elektronisk ID (EID)	Se e-legitimation
Elektronisk identifiering	Se autentisering.
E-tjänst	Digital tjänst som tillhandahålls av en myndighet eller annan organisation. E-legitimation används för att identifiera den som ansluter mot tjänsten.
E-tjänstelegitimation Fil	Är en personlig e-legitimation bestående av två certifikat; det ena certifikatet används för att autentisera innehavaren och det andra certifikatet används för att låta innehavaren digitalt signera olika handlingar och/eller dokument. En personlig e-legitimation kallas även för e-tjänstelegitimation då den knuten till en visst företag/myndighet och används i tjänsten. E-legitimationen används för elektronisk kommunikation inom en organisation eller för kommunikation med andra organisationer. E-tjänstelegitimation Fil är som namnet anger en e-legitimation som kan lagras på innehavarens dator eller annan enhet (ex. smartphone) i form av en fil i PKCS#12-format. E-legitimationen är skyddad av ett lösenord.

E-tjänstelegitimation Kort	Är en personlig e-legitimation bestående av två certifikat; det ena certifikatet används för att autentisera innehavaren och det andra certifikatet används för att låta innehavaren digitalt signera olika handlingar och/eller dokument. En personlig e-legitimation kallas även för e-tjänstelegitimation då den knuten till en visst företag/myndighet och används i tjänsten. E-legitimationen används för elektronisk kommunikation inom en organisation eller för kommunikation med andra organisationer. E-tjänstelegitimation Kort är som namnet anger en smartkortbaserad e-legitimation som lagras på ett aktivt kort i PKCS#15-format. Plastbrickan som chipet sitter på kan förses med visuell identitet som komplement till den elektroniska identiteten. E-legitimationen skyddas av en PIN-kod.
E-tjänsteägare	Myndighet eller annan organisation som tillhandahåller en digital tjänst.
Tjänsteägare	Se e-tjänsteägare
Fakturaadress	Adress dit fakturan ska adresseras.
Fakturareferens	Referens som kunden vill ha på fakturan. Används ofta för att kunna identifiera vem/vilken funktion som ska ta kostnaden.
Filcertifikat	Se Mjuka certifikat
Fullmakt	Ett dokument som visar att någon har rättighet att göra något i annans ställe
Förlitande Part	Part som litar på uppgifter i ett certifikat för sina beslut och sina e-tillämpningar.
Försändelse	En försändelse är något som skickas från en plats till en annan.
Giltighetstid	En period mellan två datum och klockslag då certifikatet är giltigt och fungerar att använda.
Handläggare	Betrodd person hos Ombud som av den egna organisationen fått befogenhet att beställa och distribuera e-legitimationer för sin organisation och de kunder som man agerar ombud åt.
Hårdvarusäkerhetsmodul (HSM)	En hårdvarusäkerhetsmodul (HSM) är en fysisk enhet som skyddar och hanterar (asymmetriska) krypteringsnycklar. Krypteringsnycklar kan aldrig läsas ut ur HSM enheten utan de kan endast användas för kryptering och signering av data som skickas till enheten.
Hårda Certifikat	Certifikat som lagras på smarta kort och skyddas av PIN-kod, se E-tjänstelegitimation Kort.
Identifiering	Process där en användare eller resurs anger (presenterar/påstår) sin identitet. Efter uppgivande av identitet så äkthetskontrolleras identiteten (se autentisering).
Information Systems Security Officer (ISSO)	Övervakande roll med ansvar för CA funktionen.
Initial PIN	Den PIN-kod som påförs av Utfärdaren vid personalisering av det aktiva kortet.
Integritetsskydd	Skydd mot att information obehörigen eller oavsiktligt modifieras utan att det kan upptäckas.
Katalog/X.500 katalog	Ett elektroniskt register som innehåller utgivna certifikat inklusive publika nycklar och spärrlistor.
Korscertifikat	Certifikat utfärdat av en certifikatutfärdare, som associerar en annan certifikatutfärdare med dennes publika nyckel.
Kort	Se aktivt kort.

Kryptering	Omvandling av klartext till kryptotext med hjälp av ett krypteringssystem och en krypteringsnyckel i syfte att förhindra obehörig åtkomst (läsning) av konfidentiell information.
Kryptotext	Information som bildas av klartext genom kryptering i avsikt att göra innehållet oläsbart för obehöriga.
Kund	En organisation/juridisk person som köper e-legitimation av Utfärdaren.
Kunduppgifter	De uppgifter om Beställare, Beställande organisation/Kund som Utfärdaren behöver för att kunna utfärda e-legitimationen.
Leveransadress	Adress dit beställd produkt ska levereras.
Logg	(Kontinuerligt) insamlad information om de operationer som utförs i ett system.
Mjuka Certifikat	Certifikat som lagras (i PKCS#12 format) på andra medier än smarta kort, exempelvis lokalt på en PC eller på ett USB minne.
Nyckelgenerering	Den process under vilken publika och privata nyckelpar skapas.
Oavvislighet	Princip med innebörden att utförande av en specifik handling inte i efterhand skall kunna förnekas av utföraren. Oavvislighet åstadkoms genom att e-legitimationsinnehavaren digitalt signerar handlingen.
Objektidentifierare (OID)	En typ inom standarden för ASN.1 (Abstract Syntax Notation One), SS-ISO 8824 (§ 26), som tillhandahåller en mekanism lämpad för tilldelning av unika namn på objekt, t.ex. denna policy. Informationstekniska Standardiseringen, ITS, ansvarar för registrering av unika OID i Sverige.
Ombud	Ett Ombud är en återförsäljarorganisation som getts befogenhet att beställa, hantera, distribuera och spärra e-legitimationer till egna kunder.
Ordernummer	Kallas på svenska även beställningsnummer. Unikt nummer för en beställnings som görs i vår beställningsportal.
Organisationsnummer	Unikt nummer som identifierar en organisation i Sverige.
Personalisering	Processen att förse det aktiva kortet med den grafiska och logiska information som erfordras för att knyta kortanvändaren till ett specifikt kort.
PIN	Personal Identification Number, lösenord oftast bestående enbart av siffror.
PIN-kodsbrev	Ett brev kopplat till det beställda certifikatet som innehåller de koder som behövs för att ladda ner/installera, använda och spärra e-legitimationen.
Privat nyckel	Hemlighållen nyckel (dekrypteringsnyckel) i ett asymmetriskt kryptosystem. Används främst vid generering av digitala signaturer samt för dekryptering av krypterad information.
Publik nyckel	Nyckel som kan göras känd och som används vid kryptering i ett asymmetriskt kryptosystem. Kan även användas vid verifiering av den publika nyckelägarens digitala signaturer.
Registration Authority (RA)	Roll som arbetar med att hantera och ställa ut certifikat enligt företagets certifikatpolicy. Är betrodd att svara för registrering och autentisering av användare och deras personuppgifter så att de kan tilldelas korrekta certifikat.
Revokeringslista	Se Spärrlista
Rotcertifikat	Certifikat som intygar att en viss publik nyckel är publik nyckel för en specifik CA.
Serverlegitimation	Även kallad Organisationslegitimation. Är en organisatoriskt knuten e-legitimation bestående av ett autentiseringscertifikat. Certifikatet baseras på organisationsnumret och används för att autentisera innehavaren. Serverlegitimationen lagras på organisationens server i form av en fil i PKCS#12-format. Serverlegitimationen är skyddad av ett lösenord.
Signera	Förse ett meddelande eller en datamängd med en digital signatur/underskrift.

Smartkort	Se aktivt kort.
Spärrlista	Periodiskt uppdaterad, tidstämplad och signerad lista, utgiven av Utfärdaren, som anger certifikat som återkallats innan deras giltighetstid gått ut.
Stämpellegitimation	Är en organisatoriskt knuten e-legitimation bestående av ett signeringscertifikat; Certifikatet baseras på organisationsnumret och används för att signera olika elektroniska handlingar för organisationens räkning. Stämpellegitimationen lagras på organisationens server i form av en fil i PKCS#12-format. Stämpellegitimationen är skyddad av ett lösenord.
System Administrator (SA)	Roll inom IT med övergripande ansvar för CA funktionens IT-stöd.
Säkerhetskoder	Koder/lösenord som kunden erhåller i ett PIN-kodsbrev vid leverans av den beställda e-legitimationen.
Tjänstecertifikat	En e-legitimation som utfärdas till en person inom en organisation, för elektronisk kommunikation internt eller med andra organisationer.
Tjänstekatalog	Expisofts förteckning över de e-tjänster och e-tjänsteägare som litar på Expisofts certifikat.
Unik identifierare	Unik kod/ lösenord som används för att göra PIN-kodsbrev och/eller privata nycklar tillgängliga endast för innehavaren av en e-legitimation samt för att innehavaren ska kunna spärra certifikatet .
Utfärdardeklaration	Ett dokument som tas fram av Utfärdaren och som beskriver hur kraven som stipuleras i Certifikatpolicyn uppfylls.
Utfärdare	Se Certifikatutfärdare.
Verifiering	Processen att kontrollera att ett antagande är korrekt. Detta begrepp avser främst processen att kontrollera att en signatur är framställd av den som av den signerade informationen framstår som dess utställare.
Webbsida	https://eid.expisoft.se/ eller annan webbsida som Utfärdaren meddelar den Beställande Organisationen
Återförsäljare	Se Ombud