Utfärdardeklaration (CPS)

Versionshistorik			
Ver.nr	Datum	Vem	Beskrivning
0.1	2025-02-28	Teknisk dokumentatör, Erik Nilsson	Dokument skapat
1.0	2025-03-14	VD, Lasse Larsson	Dokument godkänt
1.1	2025-04-16	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:	2025-04-16
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 Utfärdardeklaration (CPS, Certificate Practice Statement) som ägs och förvaltas av Expisoft AB, nedan kallad "Utfärdaren". Denna CPS beskriver på vilket sätt Utfärdaren uppfyller de certifikatpolicyer som omfattas av utfärdardeklarationen (se avsnitt 1.1).

Detta dokument är relevant för Utfärdaren, RA-funktionen och dess personal, återförsäljare av utfärdarens certifikatprodukter, beställare i en kundorganisation, förlitande parter samt certifikatsinnehavare.

Utfärdardeklarationen beskriver de rutiner och processer som tillämpas av Expisoft AB vid utfärdande av certifikat. Separata dokument, certifikatpolicyer (CP) beskriver själva certifikaten och de krav som certifikaten motsvarar.

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

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 utfärdardeklaration gäller för samtliga certifikat som utfärdas av Expisoft AB.
Exempel på certifikat som omfattas:

OID: 1.2.752.54.9.2.25.3
Produktnamn: e-Tjänstelegitimation Kort
CA-instans: ExpiTrust e-Tjanstelegitimationer kort CA v4

OID: 1.2.752.54.9.2.26.3
Produktnamn: E-tjänstelegitimation fil
CA-instans: ExpiTrust e-Tjanstelegitimation CA v3

OID: 1.2.752.54.9.2.13.2
Produktnamn: EID Funktion/Organisation
CA-instans: ExpiTrust EID CA v4

1.2 Dokumentnamn och identifierare

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

1.3 PKI-aktörer och deras ansvar

Beskrivs i respektive certifikatpolicy.

1.4 Certifikatanvändning

Beskrivs i respektive certifikatpolicy.

1.5 Förvaltning av Utfärdardeklarationen

1.5.1 Organisation som administrerar denna utfärdardeklaration

Utfärdaren Expisoft AB är ansvarig för förvaltning, administration och underhåll av denna utfärdardeklaration. Frågor rörande denna CPS 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 CPS mot de certifikatpolicyer (CP) som omfattas.

1.5.4 Godkännandeprocedur för denna Utfärdardeklaration

Rollen Certificate Authority Administrator (CAA) (se kapitel 5.2.1) ansvarar för godkännandeprocessen för detta dokument.

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 CPS och berörda policys publiceras på Utfärdarens webbplats. Informationen finns tillgänglig på https://www.expisoft.se/ och https://eid.expisoft.se/.

2.2 Publicering av certifikatrelaterad information

Utfärdaren tillhandahåller information enligt respektive certifikatpolicy. Spärrlistor och rotcertifikat är tillgängliga via: https://eid.expisoft.se/.

2.3 Tidpunkter och frekvenser för publicering

Beskrivs i respektive certifikatpolicy.

2.4 Behörighetskontroll för lagringsplatser

Beskrivs i respektive certifikatpolicy.

3 Identifiering och autentisering

3.1 Namngivning certifikat

3.1.1 Typer av namn

Beskrivs i respektive certifikatpolicy.

3.1.2 Behov av meningsfulla namn

Beskrivs i respektive certifikatpolicy.

3.1.3 Anonyma eller pseudonyma certifikatsinnehavare

Beskrivs i respektive certifikatpolicy.

3.1.4 Regler för att tolka olika namnformer

Beskrivs i respektive certifikatpolicy.

3.1.5 Unika namn

Beskrivs i respektive certifikatpolicy.

3.1.6 Igenkänning, autentisering och roll för varumärke

Beskrivs i respektive certifikatpolicy.

3.2 Verifiering av identitet vid beställning

3.2.1 Metod att bevisa innehavet av den privata nyckeln

I de fall när Utfärdaren genererar nyckelparet och skapar ett filbaserat certifikat så sparas en kopia av p12-filen hos Utfärdaren. Denna fil innehåller både den privata och den publika nyckeln. I de fall när en Beställare själv genererat nyckelparet och beställer certifikat genom CSR så verifieras innehavet genom att CSR är signerad med Beställarens privata nyckel. På så vis kan Utfärdaren vara säkra på att certifikatbegäran kommer från innehavaren av den privata nyckeln.

3.2.2 Autentisering av organisationens identitet

Utfärdarens RA-funktion kontrollerar via Bolagsverket, Skatteverket och via publikt tillgänglig och tillförlitlig information på internet att organisationen/företaget existerar med rätt svenskt organisationsnummer och bokföringshistorik. Även befattningen för den person som undertecknat beställningen kontrolleras. Vid behov kompletteras informationen exempelvis genom telefonsamtal till oberoende part som kan verifiera organisationens identitet.

3.2.3 Autentisering av individens identitet

Utfärdarens RA-funktion kontrollerar att Beställaren är en person (och inte en funktion, ex. supportavdelning) samt befattningsuppgifter för den person som undertecknat beställningen. Vidare levereras PIN-kodsbrev antingen med rekommenderat brev (som kräver giltig ID-handling vid utlämning) eller digitalt då identifiering av Beställaren gjorts med hjälp av Svensk e-legitimation.

3.2.4 Icke kontrollerade uppgifter om certifikatsinnehavaren

Beskrivs i respektive certifikatpolicy.

3.2.5 Validering av behörighet hos Ombud

Alla av Utfärdaren godkända Ombud har handläggare med egna personliga e-legitimationer. Ombudets e-legitimation används för att identifiera Ombudet när denne loggar in till Utfärdarens webbgränssnitt för att beställa certifikat antingen för dennes egen organisation eller för organisationens kunder (som återförsäljare). I Utfärdarens webbgränssnitt kan Ombudets handläggare administrera, övervaka, beställa, leverera och spärra certifikat för sin respektive kundgrupp.

3.2.6 Kriterier för samverkan

Beskrivs i respektive certifikatpolicy.

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

Både certifikatsinnehavare och Beställare kan spärra certifikat direkt via Utfärdarens webbgränssnitt (detta kräver att de har tillgång till den unika identifieraren från PIN-kodsbrevet). Vid spärrning över telefon kontrolleras certifikatsinnehavarens identitet genom kontroll av PIN-kodsbrev och motringning. När det har säkerställts att spärrbegäran är legitim så spärras certifikatet direkt.

4 Operativa krav utifrån certifikatets livscykel

4.1 Beställning av certifikat

4.1.1 Vem kan beställa ett certifikat?

Beskrivs i respektive certifikatpolicy.

4.1.2 Beställningsprocess och ansvar

Beskrivs i respektive certifikatpolicy.

4.1.3 Identifiering med Mobilt BankID

Beskrivs i respektive certifikatpolicy.

4.2 Hantering av en certifikatsbeställning

Alla beställningar registreras av Beställaren i Utfärdarens webbportal, vilket säkerställer att beställningar hålls separerade från varandra. De personer hos Utfärdaren som hanterar beställningar är samtliga certifierade hos Utfärdaren vilket minskar risker för manuella fel. Dessutom tillämpas "fyra ögons princip" som innebär att två behöriga personer deltar vid utställandet av samtliga certifikat, detta för att säkerställa att inga manuella fel sker vid utställandet.

4.2.1 Identifiering och autentisering

Beskrivs i respektive certifikatpolicy.

4.2.2 Godkännande eller avslag på beställning av ett certifikat

Beskrivs i respektive certifikatpolicy. Utfärdaren meddelar Beställaren via e-post (av spårbarhetsskäl) varför en beställning avslagits och vad som krävs för att beställningen skall kunna bli godkänd.

4.2.3 Behandlingstid för certifikatsbeställning

Beskrivs i respektive certifikatpolicy.

4.3 Certifikatutfärdande

4.3.1 Aktiviteter under certifikatutfärdandet

Certifikatutfärdandet inleds med att en person med RA-rollen loggar in i CA-systemen och identifierar sig med personlig, giltig e-legitimation. Uppgifterna i ansökan/beställningen valideras enligt kapitel 3.2 i motsvarande certifikatpolicy. Nytt nyckelpar genereras, om inte kunden gjort en CSR-beställning där kunden själv genererat nyckelparet, eller om nycklar redan ligger på ett smartkort. Certifikat utfärdas enligt beställningen (till fil eller redo att läggas på smartkort). Vid utfärdande av certifikat medverkar två betrodda personer (varav minst en ha RA-rollen) för att minimera risken för manuella fel. Om beställningen gäller kortbaserade certifikat, så läggs certifikatet in på smartkort (personalisering).

4.3.2 Utfärdarens meddelande till sökande om utfärdande av certifikat

Beställaren informeras skriftligt via e-post att det beställda certifikatet är utfärdat och ett PIN-kodsbrev som även innehåller den unika identifieraren levereras till Beställaren antingen som Rekommenderat brev (REK) eller digitalt via inloggat läge i webbportalen. När Beställaren fått tillgång till den unika identifieraren så kan denne gå in i CA-tjänstens webbportal och ladda ned sitt certifikat via en självbetjäningsfunktion. Om certifikat på smartkort har beställts levereras detta via post till Beställaren separat från PIN-kodsbrevet.

4.4 Acceptans av certifikat

4.4.1 Handlingssätt som fastställer acceptans av utfärdat certifikat

Beskrivs i respektive certifikatpolicy.

4.4.2 Certifikatutfärdarens publicering av utfärdat certifikat

På Utfärdarens webbportal kan Beställare logga in och hämta sina beställda certifikat (publik del). Mot vissa certifikatpolicyer använder Utfärdaren en publik LDAP-katalog med certifikat och spärrlistor enligt certifikatspolicyn.

4.4.3 Utfärdarens information till andra parter om utställda certifikat

Beskrivs i respektive certifikatpolicy.

4.5 Användning av nyckelpar kopplat till certifikatet

4.5.1 Användning av privat nyckel kopplad till certifikatet

Beskrivs i respektive certifikatpolicy.

4.5.2 Användning av publik nyckel kopplad till certifikatet

Beskrivs i respektive certifikatpolicy.

4.6 Förnyelse av certifikat

Beskrivs i respektive certifikatpolicy.

4.6.1 Orsaker till förnyelse av certifikatet

Beskrivs i respektive certifikatpolicy.

4.6.2 Vem får begära förnyelse

Beskrivs i respektive certifikatpolicy.

4.6.3 Hantering av begäran om förnyelse av certifikatet

Beskrivs i respektive certifikatpolicy.

4.6.4 Anmälan till den ansökande om nytt utfärdande av certifikatet

Beskrivs i respektive certifikatpolicy.

4.6.5 Handlingssätt som fastställer acceptans av förnyat certifikat

Beskrivs i respektive certifikatpolicy.

4.6.6 Utfärdarens publicering av det förnyade certifikatet

Beskrivs i respektive certifikatpolicy.

4.6.7 Utfärdarens anmälan till andra parter om certifikatets utfärdande

Beskrivs i respektive certifikatpolicy.

4.7 Förnyelse av certifikatets nyckelpar

Beskrivs i respektive certifikatpolicy.

4.7.1 Orsaker till förnyelse av certifikatets nycklar

Beskrivs i respektive certifikatpolicy.

4.7.2 Vem kan begära förnyelse av certifikatets nycklar

Beskrivs i respektive certifikatpolicy.

4.7.3 Hantering av begäran om förnyelse av certifikatets nycklar

Beskrivs i respektive certifikatpolicy.

4.7.4 Anmälan till ansökanden om nytt utfärdande av certifikat

Beskrivs i respektive certifikatpolicy.

4.7.5 Handlingssätt som fastställer acceptans av certifikat

Beskrivs i respektive certifikatpolicy.

4.7.6 Utfärdarens publicering av certifikat med nya nycklar

Beskrivs i respektive certifikatpolicy.

4.7.7 Utfärdarens anmälan till andra parter vid förnyelse av nycklar

Beskrivs i respektive certifikatpolicy.

4.8 Certifikatsmodifiering

Beskrivs i respektive certifikatpolicy.

4.8.1 Orsaker till modifiering av certifikat

Beskrivs i respektive certifikatpolicy.

4.8.2 Vem får begära modifiering av certifikat?

Beskrivs i respektive certifikatpolicy.

4.8.3 Hantering av begäran om modifiering av certifikat

Beskrivs i respektive certifikatpolicy.

4.8.4 Anmälan till ansökanden om modifiering av certifikat

Beskrivs i respektive certifikatpolicy.

4.8.5 Handlingssätt som fastställer acceptans av modifierat certifikat

Beskrivs i respektive certifikatpolicy.

4.8.6 Utfärdarens publicering av det modifierade certifikatet

Beskrivs i respektive certifikatpolicy.

4.8.7 Utfärdarens anmälan till andra parter vid certifikatsmodifiering

Beskrivs i respektive certifikatpolicy.

4.9 Spärrning av certifikat

Utfärdaren tillhandahåller en webbtjänst där certifikatsinnehavare själv kan spärra sina certifikat. Alternativt kan certifikatsinnehavare kontakta CA-tjänstens supportfunktion och be om spärrning av certifikat. Spärrlistor publiceras mot en OCSP-tjänst.

4.9.1 Anledning till spärr

Beskrivs i respektive certifikatpolicy.

4.9.2 Vem kan begära spärr

Beskrivs i respektive certifikatpolicy.

4.9.3 Rutin för spärrbegäran

Certifikatsinnehavaren eller Beställare kan själva (av valfri anledning) spärra certifikat genom Utfärdarens webbportal, så länge de har tillgång till certifikatets unika identifierare (som finns i PIN-kodsbrevet). Vid spärrbegäran över telefon sker identifiering av den som begär spärrning enligt avsnitt 3.4. Utfärdaren kan dessutom besluta om spärrning även om identifiering inte kan utföras i de fall det föreligger risk för missbruk av e-legitimation/ certifikat. Mottagen spärrningsbegäran arkiveras tillsammans med information om:

- Datum och tidpunkt
- Uppgift om vem som beordrat spärrningen
- Anledning till spärr (när Utfärdaren spärrar certifikat)
- Utförande person (vid manuell spärrning)

4.9.4 Behandlingstid vid spärrbegäran

Beskrivs i respektive certifikatpolicy.

4.9.5 Tid inom vilken CA måste behandla spärrbegäran

Beskrivs i respektive certifikatpolicy. Utfärdaren tillhandahåller en webbaserad spärrtjänst som är tillgänglig dygnet runt. Alternativt kan spärrning ske via Utfärdarens supportfunktion 09:00-16:00 helgfria vardagar.

4.9.6 Krav på förlitande part vid spärrbegäran

Beskrivs i respektive certifikatpolicy.

4.9.7 Utgivningsfrekvens av spärrlistor

Utfärdaren skapar och publicerar spärrlistor en gång per timme, dygnet runt med giltighetstid på 24 timmar. Det skapas och publiceras även en ny spärrlista direkt när CA-tjänsten mottar och utför en spärrbegäran. Detta innebär att det alltid finns en aktuell och uppdaterad spärrlista som kan hämtas och/eller användas för en OCSP-förfrågan.

4.9.8 Maximal fördröjning vid utgivning av spärrlistor (CRL)

Utfärdaren ger ut nya spärrlistor varje timme och efter några minuter finns de tillgängliga på intern och extern CDP. Om det tar mer än en timme sedan den förra spärrlistan publicerades går ett larm till Utfärdarens driftorganisation så att eventuella problem kan avhjälpas och spärrlistor åter kan publiceras som de ska. Efter en viss tidsgräns på fördröjningen aktiveras separat kontinuitetsplan för CA-tjänsten.

4.9.9 Online spärrbegäran och status/spärrkontroll

Hos Utfärdaren ingår dessa funktioner i grundtjänsten utan extra kostnad för förlitande parter. Alla svar på OCSP-förfrågningar signeras av OCSP-servern som har ett eget certifikat

utfärdat av CA-tjänsten. OCSP-tjänsten uppdateras regelbundet via CA-tjänsten spärrlista som publiceras enligt de tidsintervall som anges i 4.9.7.

Utfärdaren har två OCSP-servrar för redundans och lastbalansering, en i egen serverhall och en på annan ort.

4.10 Tjänster avseende certifikatsstatus

4.10.1 Egenskaper

Spärrlistor publiceras i Utfärdarens publika register/katalog enligt de kriterier som beskrivs i certifikatspolicyn. Såväl CRL som OCSP-tjänsten är fritt tillgänglig för alla förlitande parter.

4.10.2 Tillgänglighet

Utfärdaren nyttjar dubbla OSCP-sajter för åtkomst även om en sajt har driftstörning. CRL har giltighetstid på 24 timmar, men ny CRL ställs ut (åtminstone) varje timme. Det innebär att även vid en driftstörning rörande utgivning av ny CRL, så finns ett tidsfönster på 23 timmar innan den gamla CRL-filen slutar vara giltig.

4.11 Certifikatinnehavarens abonnemang avslutas

Beskrivs i respektive certifikatpolicy.

4.12 Nyckeldeponering och nyckelåterställning

Beskrivs i respektive certifikatpolicy.

5 Faciliteter, förvaltning och verksamhetsstyrning

5.1 Fysisk säkerhet

5.1.1 Fysisk placering och uppbyggnad

Beskrivs i respektive certifikatpolicy.
Utfärdaren uppfyller respektive certifikatspolicys samtliga krav på CA-systemets driftutrymme.

5.1.2 Fysiskt tillträde

Fysiskt tillträde till CA-systemets driftutrymme skyddas med larmad dörr med 2-faktorautentisering, digitala loggar och manuell loggbok. Tillträde kräver även närvaro av minst två personer. Kontinuitetsplan finns och avvikelserapportering skall ske vid avsteg från 2-personskravet.

5.1.3 Strömförsörjning och kylning

Utfärdaren använder en kombination av UPS och bränsledriven generator för att säkerställa kontinuerlig drift under minst 24 timmar vid ett strömavbrott. Generatorns funktion testas fyra gånger per år av underleverantör med skriftligt testprotokoll. Utfärdaren testar hela kedjan generator-UPS minst en gång per år med skriftligt testprotokoll.

5.1.4 Vattenexponering

CA-systemets driftutrymme hos Utfärdaren är försett med översvämningslarm.

5.1.5 Brandskydd

CA-systemets driftutrymme hos Utfärdaren är försett med brandlarm.

5.1.6 Lagring av media

CA-systemets lagringsmedia befinner sig inlåst tillsammans med resten av CA-systemet. Hårdvaran är redundant för att minska risken för informationsförluster vid eventuella haverier. Utfärdaren förvarar krypterade säkerhetskopior av CA-systemen både på separat backupserver och på offsite-backup. Dekrypteringsnycklar för kopiorna förvaras på separat plats från själva kopiorna. Arkivkopior med CA-information mellanlagras på separat bandrobot innan den lagras i ett dedikerat brandsäkert kassaskåp (inom Utfärdarens lokaler) till vilket bara betrodda personer har åtkomst.

5.1.7 Avfallshantering

Utfärdaren förstör känsligt material genom att anlita ett separat företag med lång erfarenhet av destruktion av datadiskar. Det känsliga materialet som ska förstöras lämnas aldrig obevakat från att det lämnar Utfärdarens lokaler tills att det är förstört.

5.1.8 Säkerhetskopia på annan plats

Säkerhetskopior av CA-systemen finns på offsite-backup. Arkivkopior för CA-information lagras i dedikerat brandsäkert kassaskåp skilt från CA-systemet.

5.2 Styrning av CA-funktionen, procedurer och kontroller

Utfärdaren har dokumenterade policys och rutiner för utfärdandet av certifikat, med versionshantering så att uppdateringar av rutinerna enklare kan spåras och spridas.

5.2.1 Betrodda roller

Beskrivs i respektive certifikatpolicy. Hos Utfärdaren finns de roller som anges i policyn. Separata rollbeskrivningar finns.

5.2.2 Krav på antal personer per uppgift

Beskrivs i respektive certifikatpolicy. Utfärdaren tillämpar tvåhandsfattning vid de tillfällen som listas i policyn.

Med "hantering av loggar" menas exempelvis att rensa/gallra gamla loggposter (äldre än krav på lagring och arkivering). Att genomföra en säkerhetskopiering av CA-systemet där loggar ingår räknas inte som hantering av loggar.

I de fall avsteg görs från kravet på flera personer, på grund av kritiska händelser och enligt kontinuitetsplan för CA-tjänsten, så dokumenteras avsteget noggrant för historik och granskning.

5.2.3 Identifiering och autentisering för respektive roll

Hos Utfärdaren har varje person knuten till CA-funktionen en CA-rollspecifik kortbaserad legitimation som används för autentisering när personen ska utföra operationer i CA-systemet.

5.2.4 Roller som kräver separation av uppgifter

Beskrivs i respektive certifikatpolicy.

5.3 Personal

5.3.1 Krav på kompetens, erfarenhet och formella kvalifikationer

Beskrivs i respektive certifikatpolicy.

5.3.2 Kontroll av bakgrund

All fast anställd personal hos Utfärdaren kontrolleras innan anställning. För tillfälliga konsulter kan kontrollen vara mindre omfattande, men det kompenseras med att konsulter inte får samma behörigheter eller åtkomst till känsliga system. RA-administratörer kvitterar att de fått information genom att bekräfta att de läst, förstått och kommer att efterleva instruktioner och rutiner (även när dessa uppdateras).

5.3.3 Krav på utbildning

Anställda hos Utfärdaren ges utbildning utifrån personliga behov och roll samt kontrolleras/granskas vid revision/granskning.

5.3.4 Krav på kompetensutveckling

All personal hos Utfärdaren ges nödvändig kompetensutveckling vid förändring av system eller rutiner. Detta kan exempelvis ske genom skriftliga eller muntliga instruktioner, eller genom fortbildning/kurser för den anställde.

5.3.5 Arbetsrotation

Beskrivs i respektive certifikatpolicy.

5.3.6 Sanktioner vid obehöriga aktiviteter

Allvarlighetsgraden i den obehöriga aktiviteten påverkar vilken sanktion/åtgärds som vidtas. Exempel på åtgärder är skriftlig varning, uppsägning eller polisanmälan.

5.3.7 Krav på oberoende för leverantörer

Beskrivs i respektive certifikatpolicy.

5.3.8 Dokumentation för personalen

Utfärdaren har dokumenterade rutiner och instruktioner för olika operationer som utförs i samband med utfärdande av certifikat. Vid återkommande intern granskning och kontroll bedöms om de befintliga instruktionerna är tillräckliga och tillfredsställande, eller om de behöver uppdateras.

5.4 Loggning

5.4.1 Typer av händelser som registreras

Beskrivs i respektive certifikatpolicy.

5.4.2 Frekvens för analys av loggar

Hos Utfärdaren utför rollen CAA granskning av säkerhetsloggarna för att upptäcka säkerhetsrelaterade incidenter. Detta sker antingen regelbundet eller vid misstanke. Driftloggar övervakas och kontrolleras vid behov av rollen SA.

5.4.3 Bevaringstid för loggar

Beskrivs i respektive certifikatpolicy. Loggarna lagras på band och banden lagras i brandsäkert skåp i 5-15 år beroende på innehåll.

5.4.4 Skydd av loggar

Hos Utfärdaren skyddas loggarna mot otillbörlig förändring genom de logiska skydds-mekanismerna i operativsystemen samt genom att CA-systemen i sig bara är fysiskt och logiskt åtkomliga för behörig personal. Samtliga loggar/händelser är försedda med integritetsskydd och individuella tidstämplar.

5.4.5 Säkerhetskopiering av loggar

Säkerhetskopiering sker av hela CA-systemet, som även innehåller loggarna. Vidare lagras arkivkopior, som också innehåller loggar, se avsnitt 5.5.

5.4.6 Insamlingssystem för loggar

Utfärdaren använder inget specifikt insamlingssystem för loggar.

5.4.7 Meddelande till den som orsakat logghändelse

Av säkerhetsskäl visas inget meddelande för den som orsakat en logghändelse. I händelse av att en person med illvilligt uppsåt påverkar systemet är det bättre att denne inte vet att systemet loggar de handlingar som utförs.

5.4.8 Uppskattning av sårbarhet

Hos Utfärdaren genomförs risk- och sårbarhetsanalys av CA-verksamheten vid behov, dock minst en gång per år.

5.5 Arkivering

5.5.1 Typ av information som arkiveras

Beskrivs i respektive certifikatpolicy.

5.5.2 Arkiveringstid

Beskrivs i respektive certifikatpolicy.

5.5.3 Skydd av arkiv

Enligt certifikatpolicyn. Arkiverat material förvaras i ett brandsäkert kassaskåp. Kassaskåpet är placerat i avgränsad, kameraövervakad lokal med besöksregistrering.

5.5.4 Säkerhetskopiering av arkiv

Beskrivs i respektive certifikatpolicy.

5.5.5 Krav på tidsstämpling av arkivdokument

Hos Utfärdaren registreras tiden för arkiveringen dels i loggarna enligt 5.4.1, plus att arkiv-kopiorna namnges med datum i namnet.

5.6 Övergång till ny CA-nyckel

Förlitande parter, kända för Utfärdaren, kontaktas av Utfärdaren i god tid innan övergång till ny CA-nyckel ska ske.

5.7 Hantering vid katastrof avseende CA-verksamheten

5.7.1 Förfarande vid allvarliga incidenter

Beskrivs i respektive certifikatpolicy.

5.7.2 Datorer, programvara och/eller data är skadade

Utfärdaren skapar löpande säkerhetskopior av både information och system. Vid misstanke om röjd privat nyckel följs förfarandet som beskrivs i certifikatspolicyn.

5.7.3 Förmåga till kontinuitet efter katastrof

Hos Utfärdaren fokuserar kontinuitetsplanen på att verksamheten ska kunna återupptas snarast möjligt, även om det beror på omfattningen av katastrofen. Planen ses över och uppdateras som minst årligen för att den ska vara aktuell och spegla CA-tjänstens driftmiljö. Säkerhetsansvarig för CA-tjänsten (rollen ISSO) har det övergripande ansvaret att bedöma säkerhetsläget och fastställa de åtgärder som ska vidtas.

5.8 Upphörande av Utfärdarens verksamhet

Beskrivs i respektive certifikatpolicy.

6 Tekniska säkerhetsåtgärder

6.1 Generering och installation av nyckelpar

6.1.1 Generering av nyckelpar

Beskrivs i respektive certifikatpolicy.

6.1.1.1 Utfärdarnycklar för signering av certifikat och spärrlistor

Generering och hantering av nya utfärdarnycklar sker enligt certifikatpolicyn, liksom att åtkomst till HSM-modulen kräver två personer med rätt behörighet.

6.1.1.2 Nyckelpar för certifikatsinnehavare

Beskrivs i respektive certifikatpolicy.

6.1.2 Leverans av privat nyckel till certifikatsinnehavare

För Utfärdaren sker leverans av kortbaserade certifikat med postleverans. Aktiveringsinformationen för certifikatet och tillhörande PIN-koder levereras med rekommenderat brev till Beställaren, alternativt kan PIN-koden erhållas via inloggat läge i webbportalen. Leverans av filbaserade certifikat sker via Utfärdarens webbtjänst direkt till innehavarens klient efter att Beställaren mottagit ett rekommenderat brev innehållande PIN-koden för användarens certifikat.

6.1.3 Leverans av publik nyckel till certifikatutfärdare

I de fall när Beställaren använder sig av CSR får Utfärdaren den publika nyckeln genom att Beställaren laddar upp nyckeln i webbportalen i samband med beställning.

6.1.4 Leverans av CA:s publika nycklar till förlitande parter

Publika utfärdarnycklar finns tillgängliga i Utfärdarens webbportal för nedladdning. I vissa fall levereras CA-certifikatet tillsammans med certifikatet, exempelvis på smartkort, och kan läsas in därifrån.

6.1.5 Nyckelstorlek

Beskrivs i respektive certifikatpolicy.

6.1.6 Parametrar för generering av publik nyckel och kvalitetskontroll

Beskrivs i respektive certifikatpolicy.

6.1.7 Ändamål för nyckelanvändning (certifikatens key usage-fältet)

Beskrivs i respektive certifikatpolicy.

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

Beskrivs i respektive certifikatpolicy.

6.2.1 Standard och förfarande vid användning av kryptografisk modul

Hos Utfärdaren används HSM-moduler certifierade enligt CC EAL4+ och FIPS 140-2 nivå 3. CA-tjänsten använder HSM-moduler bland annat för generering, lagring och användning av Utfärdarnycklarna. Hårdvaruredundans tillämpas genom att två speglade HSM-moduler används. De utgivna certifikatens privata nycklar kan lagras och användas på innehavarens dator, telefon eller annan utrustning (PKCS#12) eller på ett smartkort (PKCS#15).

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

Beskrivs i respektive certifikatpolicy.

6.2.3 Nyckeldeponering av privat utfärdarnyckel

Beskrivs i respektive certifikatpolicy.

6.2.4 Säkerhetskopiering av privat utfärdarnyckel

Beskrivs i respektive certifikatpolicy. CA-tjänstens privata nycklar kan ej läsas ut från HSM-modulen, så en säkerhetskopia skapas i samband med generering av den privata utfärdarnyckeln. Säkerhetskopian krypteras med AES 256 och lagras på ett USB-minne. Nyckeln för dekryptering skrivs fysiskt ut på ett papper som förvaras i ett kuvert tillsammans med USB-minnet med säkerhetskopian.

6.2.5 Arkivering av privat utfärdarnyckel

Beskrivs i respektive certifikatpolicy.

6.2.6 Transport av privat utfärdarnyckel till och från kryptografisk modul

Den privata utfärdarnyckeln genereras i den kryptografiska modul som specificeras i avsnitt 6.2.7 och lämnar aldrig modulen förutom vid arkivering av säkerhetskopia eller om nyckeln ska flyttas till en ny kryptografisk modul. Export sker till extern lagringsmedia (USB) där den privata nyckeln lagras krypterad.

6.2.7 Lagring av privat utfärdarnyckel i kryptografisk modul

Beskrivs i respektive certifikatpolicy.

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 CA-certifikat ska skapas. Åtkomst till HSM-modulen kräver särskild PIN-kod och särskild aktiveringsinformation krävs därefter 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 6.2.10.

6.2.10 Metod för att förstöra den privata utfärdarnyckeln

CA-tjänstens privata utfärdarnyckel förstörs 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. Backupkopian förstörs genom att använt lagringsmedium förstörs permanent. Detta sker under (minst) två behöriga personers närvaro och överseende. Processen dokumenteras med avseende på vilka procedurer som genomförts och vilka personer som närvarat. Utfärdarnycklarna får dock ej förstöras om de står i strid med arkiveringskraven i certifikatpolicyn eller krav i annan gällande lagstiftning.

6.2.11 Säkerhetsvärdering av kryptografisk modul

Beskrivs i respektive certifikatpolicy.

6.3 Andra aspekter på hantering av nyckelpar

Beskrivs i respektive certifikatpolicy.

6.3.1 Arkivering av publik nyckel

Beskrivs i respektive certifikatpolicy.

6.3.2 Giltighetstid för certifikat och nyckelpar

Beskrivs i respektive certifikatpolicy.

6.3.3 Ansvar för certifikatets PIN/PUK-koder och lösenord

Beskrivs i respektive certifikatpolicy.

6.4 Aktiveringsinformation

6.4.1 Generering och installation av aktiveringsinformation

Beskrivs i respektive certifikatpolicy.

6.4.2 Skydd av aktiveringsdata

Hos Utfärdaren är aktiveringsinformationen skyddad mot stöld och brand genom att vara inlåst i ett särskilt säkerhetsskåp dit bara ett fåtal betrodda personer har tillgång.

6.4.3 Övriga aspekter på aktiveringsinformation

Ej tillämpligt.

6.5 IT-säkerhetskontroller

Utfärdarens driftsmiljö för CA-systemen är uppsatt enligt certifikatpolicyn. Särskilda smartkort används för inloggning till CA-systemen och både inloggning och utförda handlingar i systemen loggas. Vissa uppgifter kräver tvåhandsfattning enligt avsnitt 5.2.2 i certifikatpolicyn.

6.5.1 Särskilda IT-säkerhetstekniska krav

Beskrivs i respektive certifikatpolicy.

6.6 Livscykeltekniska krav

6.6.1 Säkerhetskrav avseende systemutveckling

Hos Utfärdaren sker all utveckling av programvara enligt Utfärdarens utvecklingsmodell. På varje utvecklingsdator finns antivirus-programvara och andra aktiverade säkerhetsfunktioner. Inloggning på utvecklingsdatorerna sker med stark autentisering. Bygge av produktionskod sker på specifik byggmaskin. Alla nya versioner av CA-tjänstens programvara testas dessutom i en separat acceptanstestmiljö innan den produktionsätts.

6.6.2 Säkerhetskrav avseende säkerhetsadministrationen

Beskrivs i respektive certifikatpolicy.

6.7 Nätverkssäkerhetskrav

Beskrivs i respektive certifikatpolicy.

6.8 Tidsstämpling

Gemensam tid i hela CA-systemet. Tid synkroniseras med hjälp av GPS och kan ej påverkas utifrån.

7 Certifikat, CRL och OCSP-profiler

Beskrivs i respektive certifikatpolicy.

8 Överensstämmelse utifrån revision och andra granskningar

8.1 Frekvens och omständigheter för granskning

Beskrivs i respektive certifikatpolicy.

8.2 Identitet/kvalifikationer för granskare

Beskrivs i respektive certifikatpolicy.

8.3 Granskares relationer till bedömd enhet

Beskrivs i respektive certifikatpolicy.

8.4 Områden för revision

Beskrivs i respektive certifikatpolicy.

8.5 Åtgärder som vidtas till följd av upptäckt brist

Beskrivs i respektive certifikatpolicy.

8.6 Kommunikation av resultat

Beskrivs i respektive certifikatpolicy.

9 Andra affärsmässiga och juridiska frågor

9.1 Avgifter

9.1.1 Avgifter för utfärdande av certifikat

Priser för e-legitimationer finns angivna i beställningsportalen https://eid.expisoft.com, eller enligt separata avtal med kundorganisationen.

9.1.2 Avgifter för åtkomst till certifikat

Ej tillämpligt.

9.1.3 Avgifter för åtkomst till spärrinformation

Beskrivs i respektive certifikatpolicy.

9.1.4 Avgifter för andra tjänster

Ej 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 Utfärdardeklaration får ingen information förändras, tas bort, eller läggas till. Det ska tydligt anges att Expisoft AB är ägare av denna Utfärdardeklaration.

9.6 Förpliktelser och garantier

9.6.1 CA:s förpliktelser och garantier

Beskrivs i respektive certifikatpolicy.

9.6.2 RA:s förpliktelser och garantier

Beskrivs i respektive certifikatpolicy.

9.6.3 Certifikatsinnehavares förpliktelser och garantier

Beskrivs i respektive certifikatpolicy.

9.6.4 Förlitande parts förpliktelser och garantier

Beskrivs i respektive certifikatpolicy.

9.6.5 Förpliktelser och garantier avseende andra deltagare

Ej tillämpligt.

9.7 Friskrivningar avseende garantier

Beskrivs i respektive certifikatpolicy.

9.8 Ansvarsbegränsningar

Beskrivs i respektive certifikatpolicy.

9.9 Skadestånd och ersättningar

Ej tillämpligt.

9.10 Giltighetsperiod för denna Utfärdardeklaration (CPS)

9.10.1 Period startar

Denna Utfärdardeklaration gäller utifrån att den publicerats på Utfärdarens hemsida

9.10.2 Period upphör

Denna Utfärdardeklaration gäller tills den ersätts av ny version eller tills CA upphör med sin verksamhet.

9.11 Kommunikation med ingående parter angående CA-tjänsten

Utfärdaren kan vid behov komma att lämna viss typ av information om CA-tjänsten via e-post, Expisofts webbplats eller Utfärdarens webbportal när detta inte strider mot denna Utfärdardeklaration eller berörda Certifikatpolicyer (CP).

9.12 Ändringar av denna Utfärdardeklaration

Se kapitel 1.4.

9.13 Tvistlösningsbestämmelser

Eventuell tvist med anledning av denna Utfärdardeklaration 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 Utfärdardeklaration samt därur uppkomna rättsförhållanden.

9.15 Överensstämmelse med gällande lag

Hantering av CA-systemet sker 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 CPS.

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	http://eid.expisoft.se/ eller annan webbsida som Utfärdaren meddelar den Beställande Organisationen
Återförsäljare	Se Ombud