Telias Utfärdardeklaration, CPS, för Telia e-legitimation

Version 1.3

Datum: 2014-03-14

Innehållsförteckning

1 Inledning

1.1 Allmänt

Detta dokument, Telias utfärdardeklaration, CPS, för Telia e-legitimation, beskriver de rutiner och processer som används vid utfärdande av Telia e-legitimation på fil, kallat mjuka certifikat. Denna CPS innehåller också Telias åtaganden och garantier vid utfärdandet samt förpliktelser för kunder och förlitande parter.
Telia e-legitimation på fil utfärdas till personer över 18 år med ett svenskt personnummer och är avsedd att användas vid kontakt med olika myndigheter eller andra offentliga förvaltningar samt privata tjänsteleverantörer.

Telia är ansvarig för denna utfärdardeklaration, CPS, och alla processer och åtaganden som finns angivna i detta dokument. Vissa delar av utfärdandetjänsten kan komma att utföras av underleverantörer eller annan part, men om så är fallet är det Telia som har det övergripande ansvaret i enlighet med denna CPS.

Telia e-legitimation ges ut under de förutsättningar som anges i ETSI:s document ”Policy requirements for certification authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1. I detta dokument finns tre olika nivåer på krav definierade. Denna CPS uppfyller de krav som ställs enligt ETSI:s ”Normalized Certificate Policy” (NCP). Telia har inte gett ut någon egen certifikatpolicy utan anser att de krav som ställs på en sådan i ovannämnda ETSI:s dokument är tillräckligt tydliga.

Denna Utfärdardeklaration, CPS, följer också RFC2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” till struktur och innehåll.

Telia Utfärdardeklaration, CPS, för e-legitimation är beslutad och godkänd av Telia CPS Management Team (CPSMT). CPSMT ansvarar för att denna CPS uppfyller alla relevanta krav som ställs i Certifikatpolicyn. CPSMT ansvarar också för att löpande kontrollera att utfärdandet av Telia e-legitimation sker i enlighet med denna CPS. I de fall denna CPS behöver uppdateras initieras detta arbete av CPSMT och innan uppdateringen träder i kraft tas ett beslut av CPSMT. Se även kapitel 8.

Denna Utfärdardeklaration, CPS, finns publicerad på https://www.trust.telia.com/e-leg

1.2 Identifiering

Telia e-legitimation innehåller följande objektidentifierare för CPS,:
ISO (1) ISO member body (2) SE (752) TeliaSonera Sverige AB (35) Certificate Policy (1) Telia e-legitimation (3)

Telia e-legitimation innehåller också följande utfärdarnamn: TeliaSonera Sverige AB
Certifikatet som används för att kontrollera signaturen på en Telia e-legitimation finns publicerat på https://repository.trust.telia.com:

CA-certifikat utfärdande CA
Issuer:
CN = Telia e-legitimation CA v3
O = TeliaSonera Sverige AB
C = SE

Subject:
CN = Telia e-legitimation CA v3
O = TeliaSonera Sverige AB
C = SE

Cerifikatets Hash-summa SHA-1: {d7 d5 34 81 7d 4a 5f 3b 86 8f 9c d3 e2 fd 26 66 f0 ad b7 dd}

Tidigare CA-certifikat för e-legitimation

CA-certifikat för Root CA
Issuer:
CN = Telia e-legitimation Root CA v1
O = TeliaSonera Sverige AB
C = SE

Subject:
CN = Telia e-legitimation Root CA v1
O = TeliaSonera Sverige AB
C = SE

Cerifikatets Hash-summa SHA-1: {c9 5a b3 af 2b 00 33 54 9b 29 48 94 7d c3 12 3c ca eb 83 32}

CA-certifikat för utfärdande CA
Issuer:
CN = Telia e-legitimation Root CA v1
O = TeliaSonera Sverige AB
C = SE

Subject:
CN = Telia e-legitimation CA v2
O = TeliaSonera Sverige AB
C = SE

Cerifikatets Hash-summa SHA-1: { c9 d2 4e a6 a8 c0 c3 56 d2 e9 37 29 52 7e 2a a4 7d fd d7 76}

De rutiner och åtaganden, som finns beskrivna i denna CPS, är enbart tillämpliga om ovanstående objektidentifierare ingår i det aktuella certifikatet.

1.3 Målgrupp och tillämplighet

1.3.1 Utfärdare av e-legitimation, Certification Authority (CA)

Telia CA för e-legitimation är en självsignerad CA.

I tidigare CA-struktur var Telia CA för e-legitimation är utfärdad av en Telia e-legitimation Root CA, dvs CA:n är inte självsignerad utan ligger under en CA-hierarki för Telias e-legitimationstjänster där Root CA:n är toppnoden.

Telia CA för e-legitimation utfärdar certifikat på fil till personer över 18 år med svenskt personnummer, samt systemcertifikat som är nödvändiga för certifikatproduktionen. Telia CA för e-legitimation kommer inte att ha några underliggande CA:n, som i sin tur ger ut certifikat.

1.3.2 Registration Authorities (RA)

Telia ansvarar för RA-funktionen för Telia CA för e-legitimation. RA-funktionen tar emot ansökningar om e-legitimation och genomför nödvändiga kontroller av varje ansökan innan en e-legitimation utfärdas. De administratörer som agerar inom ramen för RA-funktionen har genomgått relevanta utbildningar för att kunna utföra sina åtaganden. Varje administratör har ett individuellt behörighetscertifikat som används vid certifikatsadministration. Behörighetscertifikaten är utfärdade av en särskild administratörs-CA som endast används för detta ändamål.

RA-funktionen är till viss del geografiskt separerad från själva utfärdarsystemet.

1.3.3 Kunder

Telia e-legitimation på fil utfärdas enbart till fysiska personer över 18 år, som innehar ett giltigt svenskt personnummer.

1.3.4 Tillämplighet

Telia e-legitimationer utfärdas till fysiska personer för att kunna användas hos bl.a. statliga myndigheter, affärsverk eller andra organisationer inom offentlig förvaltning samt privata tjänsteleverantörer. Certifikaten ges ut i enlighet med denna CPS och under de förutsättningar och krav som stipuleras i ETSI:s dokument ”Policy requirements for certification authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1, variant NCP. Förlitande part ansvarar för att avgöra om utfärdarprocessen har tillräckligt hög nivå för den aktuella tillämpningen. Innehavare av Telia e-legitimation och Förlitande parter är bundna genom avtal med Telia. Kunden ansvarar för att lämna korrekta uppgifter vid ansökan samt att skydda sina privata nycklar på ett godtagbart sätt.

1.3.5 Användningsområde

Telia e-legitimation ska användas av fysiska personer för att kunna kommunicera elektroniskt på ett säkert sätt med svenska myndigheter och företag i egenskap av privatperson eller som företrädare för en juridisk person. För att säkerställa den elektroniska kommunikationen mellan en organisation och en fysisk person krävs en eller flera funktioner i form av legitimering/identifiering, underskrift/signering och kryptering. En ansökan om Telia e-legitimation leder till utfärdande av två olika typer av certifikat, dvs. varje godkänd ansökan innebär utfärdande av två certifikat. Det ena certifikatet med tillhörande privat nyckel ska enbart användas vid underskrift/signering. Det andra certifikatet med tillhörande privat nyckel kan användas vid legitimering/identifiering och kryptering. Kundens privata nycklar genereras i den sökandes dator då e-legitimationen skapas. Information om användningsområde finns markerat i certifikatet. Vid all användning av certifikat och tillhörande privat nyckel måste hänsyn tas till det användningsområde som finns angivet i det tillhörande certifikatet.

1.4 Kontaktuppgifter

Telia är ansvarig för all hantering och uppdatering av denna CPS. Frågor angående denna CPS adresseras till:

TeliaSonera Sverige AB
PKI
Box 5275
402 25 Göteborg
Sverige

Telefon: +46 (0)20 32 32 62
E-post: kundtjanst-eid@teliasonera.com
Web: www.telia.se

2 Allmänna bestämmelser

2.1 Åtaganden

2.1.1 CA:s åtaganden

Telia åtar sig i sin roll som CA för Telia e-legitimation att erbjuda de tjänster i form av utfärdande, spärrtjänst och spärrkontroll på det sätt som beskrivs i denna CPS. Detta åtagande innebär också att Telia uppfyller alla krav på utfärdandeprocessen som ställs i ETSI:s dokument ”Policy requirements for certification authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1, variant NCP. Telia åtar sig hela ansvaret för CA:ns verksamhet även om vissa delar av certifikatutfärdandeprocessen utförs av någon underleverantör.

Telia CA för e-legitimation garanterar att CA:ns privata nyckel enbart används för att signera Telia e-legitimation, OCSP responder samt Telias spärrlistor för Telia e-legitimation. Telia CA för e-legitimation garanterar också att CA:ns privata nyckel skyddas i enlighet med det som beskrivs i denna CPS.

2.1.2 Kundens åtaganden

Kunden, dvs. den person som innehar en Telia e-legitimation, ingår ett avtal med Telia avseende Telia e-legitimation. Kunden godkänner avtalet i samband med ansökan om en Telia e-legitimation.

Kunden förbinder sig till följande genom att godkänna avtalet:

- att den information som lämnas vid ansökan är korrekt vid tidpunkten för ansökan
- att de privata nycklarna med tillhörande certifikat enbart används till det de är avsedda för i enlighet med kapitel 7.1.
- att generera nyckelparen, i för ändamålet avsedd programvara som tillhandahålls av Telia som uppfyller kravet på att generera nycklar av god kvalité och med minsta nyckellängden satt till 2048 bitar.
- att skydda sina privata nycklar från obehörig användning.
- att inte avslöja sin säkerhetskod för aktivering av privat nyckel för någon.
- att spärra sitt certifikat utan dröjsmål om den privata nyckeln har blivit stulen eller misstänks blivit röjd eller att säkerhetskoden har förlorats eller misstänks blivit röjd, eller om informationen i certifikatet inte längre gäller.
- att inte använda den privata nyckeln efter det att den har blivit röjd eller misstänks ha kunnat blivit röjd.

2.1.3 Förlitande parts åtaganden

Den förlitande parten ansvarar för att kontrollera giltigheten av en Telia e-legitimation innan denna accepterar certifikatet. Att kontrollera giltigheten innebär att verifiera certifikatets giltighetstid och utfärdarens signatur samt att kontrollera mot aktuell spärrinformation att certifikatet inte är spärrat.

Den förlitande parten ansvarar för att bedöma om säkerhetsnivån i utfärdandeprocessen som den beskrivs i denna CPS är tillräcklig för den aktuella tillämpningen.

2.2 Ansvar

Telia CA för e-legitimation garanterar att den information som återfinns i de av Telia utfärdade certifikaten är kontrollerad och verifierad i enlighet med rutiner som framgår av denna CPS. I de fall Telia CA för e-legitimation anlitar en underleverantör för att utföra vissa delar i utfärdandeprocessen ansvarar Telia för denna del som om Telia hade utfört dem själv.

2.3 Ekonomiskt ansvar

Utfärdande av Telia e-legitimation i enlighet med denna CPS medför inte att Telia CA för e-legitimation, ska betraktas som agent, fullmäktig eller på annat sätt som representant för kund eller förlitande part.

2.4 Tillämplig lag och tvistlösning

Svensk lag gäller vid tillämpning och tolkning av denna CPS om inget annat överenskommits.
Tvist mellan Telia och en kund ska avgöras enligt svensk lag och av svensk domstol.
Tvist mellan Telia och någon annan än kunden med anledning av denna CPS ska avgöras enligt Internationella handelskammarens (ICC) regler för förlikning och skiljedomsförfarande. Stockholms handelskammare ska administrera förlikningen enligt ICC:s regler och platsen för skiljedomsförfarandet ska vara Stockholm. Förhandlingarna ska hållas på svenska om inte parterna har kommit överens om något annat.

2.5 Publicering och åtkomst av information

Telia CA för e-legitimation tillhandahåller denna CPS, spärrinformation och samtliga utfärdade CA-certifikat. Det dokument som Telia CA för e-legitimation använder som certifikatpolicy tillhör ETSI och finns tillgänglig på ETSI:s webb, www.etsi.org .

Denna CPS, tillgång till spärrinformation och utfärdade CA-certifikat finns tillgängliga dygnet runt, året runt, förutom vid tekniska fel, vid service eller på grund av faktorer som ligger utanför Telias kontroll. Telia CA för e-legitimation åtar sig att avhjälpa tekniska fel och att utföra erforderlig service.
Spärrinformation tillhandahålls via OCSP. Vid uppdatering av denna CPS och vid utfärdande av nya CA-certifikat kommer dessa att publiceras utan dröjsmål.
Denna CPS publiceras på Telias webb enligt kapitel 1.1. Samtliga CA-certifikat som är utfärdade finns publicerade enligt kapitel 6.1.3.

2.6 Revision

Utfärdanderutinerna för Telia CA för e-legitimation granskas minst vart tredje år av en oberoende revisionsfirma. Revisionsfirman är fristående från Telia. Förutsättningen för revisionen är att kontrollera att rutiner och processer följer denna CPS och kontrollera uppfyllelse mot de krav som ställs i ETSI:s dokument ”Policy requirements for certification authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1. Revisionen inkluderar även det arbete som utförs av eventuella underleverantörer.
Om några brister upptäcks vid revisionen meddelas detta till CPS Management Team (CPSMT). CPSMT ansvarar sedan för att åtgärda de fel och brister som har upptäckts vid en revision.

2.7 Sekretess

Den information som en sökande anger vid ansökan om Telia e-legitimation kommer att betraktas som konfidentiell inklusive själva e-legitimationen. De utfärdade e-legitimationerna innehåller personuppgifter och de är bara tillgängliga för respektive person som har ansökt om ett sådant. Efter utfärdandet är det upptill kunden att sprida sitt/sina certifikat. Användande av Telia e-legitimation innebär att den publika informationen (Namn och personnummer) i certifikatet tillgängliggörs för motparten/förlitandeparten.
Telia CA för e-legitimation kommer att lämna ut konfidentiell information om domstol eller någon annan rättslig instans som lyder under svensk lag så beslutar.

2.8 Immateriella rättigheter

Telia CA för e-legitimation äger rättigheterna till denna CPS.

3 Identifiering och verifiering

3.1 Initial registrering

Följande uppgifter ingår i ansökan om e-legitimation och kommer också ingå i certifikatets ämnesfält (Subject DistinguishedName):

Uppgifter	Krav på innehåll	
Efternamn	Obligatorisk	Pseudonymer är inte tillåtna
Förnamn	Obligatorisk	Tilltalsnamn eller samtliga förnamn ska anges. Pseudonymer är inte tillåtna.
Personnummer	Obligatorisk	Ett giltigt svenskt personnummer, 12 siffror

De uppgifter som ingår i ämnesfältet i de utfärdade certifikaten är unika för varje kund.

3.1.1 Verifiering av personuppgifter

Telia CA för e-legitimation kontrollerar de uppgifter som den sökande anger i sin beställning. Uppgifterna kontrolleras mot det svenska folkbokföringsregistret SPAR eller annat av Telia godkänt register, innan certifikatbeställningen godkänns. Den sökande måste vara identifierad med hjälp av en godkänd legitimation innan den sökande kan hämta sin Telia e-legitimation.

3.2 Begäran om spärr

Telia kundtjänst för certifikattjänster ansvarar för att ta emot begäran om att spärra certifikat för e-legitimation. En kund kan spärra sin e-legitimation genom att ringa till Telias spärrtjänst. Kunden får då uppge information som gör det möjligt för kundtjänst att identifiera rätt e-legitimation. Kundtjänst är tillgänglig för att ta emot begäran om spärr dygnet runt.

4 Operationella krav

4.1 Ansökan om e-legitimation

Vid ansökan om e-legitimation ska den sökande lämna identitetsuppgifter i enlighet med kapitel 3.1 och övrig nödvändig information. Den sökande blir upplyst om de avtalsvillkor som gäller för tjänsten och måste acceptera dessa innan ansökan kan registreras.

RA-funktionen kontrollerar de i ansökan angivna uppgifterna mot SPAR eller annat av Telia godkänt register. Om uppgifterna i ansökan skiljer sig mot uppgifterna i SPAR eller annat av Telia godkänt register avslås ansökan. Den sökande får då göra en ny ansökan.

4.2 Utfärdande av e-legitimation

Telia e-legitimation utfärdas till en kund vars ansökan godkänts och angivna uppgifter validerats.

RA-funktionen genomför automatisk validering av varje certifikatansökan. Valideringen sker enligt en bestämd process. Valideringsprocessen är dokumenterad och loggning sker elektroniskt så att spårbarhet uppnås. Varje genomfört steg i valideringsprocessen signeras digitalt.

4.3 Acceptans av certifikat

Den sökande accepterar utfärdandet av Telia e-legitimation genom godkänna avtalsvillkoren och ladda ner e-legitimationen. Den sökande laddar ner e-legitimationen samt nödvändig klientprogramvara och anger tillhörande säkerhetskod.

4.4 Spärr av certifikat

Telia CA för e-legitimation tillhandahåller en spärrtjänst som är tillgänglig dygnet runt. Spärrinformation kan enbart erhållas via OCSP. Ingen annan form av spärrinformation tillhandahålls. Telia CA för e-legitimation tillhandahåller inte tillfällig blockering (suspension) av certifikat.

4.4.1 Anledning till spärr

Telia e-legitimation ska spärras om någon uppgift i certifikatet är felaktig eller om den tillhörande privata nyckeln har blivit röjd eller det finns misstanke om detta.
Telia CA för e-legitimation förbehåller sig rätten att spärra en kunds e-legitimation om detta anses nödvändigt.

4.4.2 Rutin för begäran om spärr

Telias spärrtjänst tar emot begäran om spärr via telefon. Det är enbart kunden eller i vissa fall Telia som kan begära att kundens e-legitimation ska spärras. När en begäran om spärr kommer in via telefon krävs att den som ringer kan ange viss nödvändig information för att kunna spärra sin e-legitimation. Den operatör som tar emot samtalet om spärr markerar aktuella certifikat som spärrade. Information om spärr uppdateras i spärrtjänsten då en e-legitimation spärrats.

4.4.3 Krav på kontroll av spärrinformation

Förlitande part ansvarar för att kontrollera giltigheten av Telia e-legitimation innan denna accepteras. En förlitande part kan inte till fullo lita på en Telia e-legitimation om inte följande kontroller har genomförts:

- Förlitande part åtar sig att genomföra kontroll genom OCSP
- Om det inte är möjligt att kontrollera spärrinformation på grund av systemfel eller liknande, så ska inte certifikatet accepteras. Om detta ändå sker är det på förlitande parts egen risk.

4.5 Loggning

4.5.1 Händelser som loggas

Följande händelser loggas antingen automatiskt av utfärdandesystemet eller genom manuella metoder:

- Uppläggning av nya konton i någon av utfärdandesystemets datorer oavsett typ av konto.

- Alla typer av transaktioner mot utfärdandesystemet
- Installation och uppdatering av programvara inklusive systemprogramvara
- Datum och tid för backuper
- Start och nedtagning av de olika systemen
- Datum och tid för uppgradering av hårdvara

Loggarna granskas och analyseras kontinuerligt för att upptäcka avvikelser. Säkerhetsloggar bevaras i minst 7 år.

Loggar skyddas mot otillbörlig förändring genom de logiska skyddsmekanismerna i operativsystemen samt genom att systemen i sig inte är fysiskt och logiskt åtkomliga annat än för behörig personal. Alla loggposter är individuellt tidsstämplade.

4.6 Arkivering

Telia CA för e-legitimation arkiverar följande data:
- Utfärdade certifikat
- Begäran om spärr
- Relevant information om spärrade certifikat

De uppgifter som arkiveras i enlighet med ovanstående behålls i minst tio år efter utgången giltighetstid. Under denna tid kommer uppgifterna också att skyddas mot förändring eller förstörelse.

4.7 Byte av nycklar

En kund byter nycklar genom att en ny Telia e-legitimation utfärdas till denne. Detta sker genom en ny ansökan.

När den maximala giltighetstiden för Telia CA för e-legitimation håller på att gå ut genereras en ny CA-nyckel och en ny självsignerad CA skapas.. Detta görs minst tre månader innan CA:n slutar producera e-legitimationer med full giltighetstid.

4.8 Katastrofplan

Telia CA för e-legitimation har en utarbetad plan i händelse av någon form av katastrof, inkluderat ifall Telia CA för e-legitimations privata nyckel misstänks vara röjd. Katastrofplanen utgår från att verksamheten ska kunna återupptas snarast möjligt beroende på omfattningen av katastrofen.

Följande åtgärder kommer att vidtas i de fall då Telia CA för E-legitimation privata nyckel misstänks vara röjd:
- Informera alla kunder, förlitande parter och andra CA:an som Telia CA för e-legitimation har avtal eller andra former av etablerade förbindelser med.
- Omedelbart avsluta möjligheten att spärra certifikat och att kontrollera spärrinformation som är knuten till den nyckel som tros vara röjd.

4.9 Upphörande av CA:s verksamhet

Upphörande av CA:s verksamhet är att betrakta som det tillstånd då all service förknippad med Telia CA för e-legitimation permanent avslutas. Det är inte detsamma som om CA:s tjänster övertas av någon annan organisation eller när CA byter signeringsnyckel.
Innan CA upphör med sin verksamhet kommer följande åtgärder att vidtas:
- Informera alla kunder som Telia CA för e-legitimation har avtal med.
- Informera övriga parter såsom andra CA eller förlitande parter som Telia CA för e-legitimation har avtal med
- Informera övriga parter som Telia CA för e-legitimation har någon form av etablerade relationer med
- Avsluta möjligheten att spärra certifikat.
- Avsluta möjligheten att kontrollera spärrinformation under Telia CA för e-legitimation

- Telia CA för e-legitimation ska se till att när verksamheten upphör ska det ändå vara möjligt att få tillgång till det data som arkiveras i enlighet med kapitel 4.6.
- Telia CA för e-legitimation ska se till att när verksamheten upphör att CA:s privata signeringsnyckel inte längre kommer att kunna användas.

5 Säkerhet

5.1 Fysisk säkerhet

5.1.1 Anläggningens lokalisering och konstruktion

Utfärdarsystem som rymmer centrala utfärdarfunktioner är fysiskt placerad i en starkt skyddad datorhall.

I datorhallen är viktiga komponenter inlåsta i separata och fristående säkerhetsskåp. De privata utfärdarnycklarna är fysiskt skyddade så att de inte kan exponeras även om det sker ett intrång i själva datorhallen.

Datorhallen är låst och utrustad med inbrottslarm i form av rörelsedetektorer och står under ständig videoövervakning. Datorhallen befinner sig i en säkerhetsklassad byggnad som även den är låst och larmad.

Anläggningens externa skydd så som lås och larmanordningar kontrolleras löpande av tjänstgörande vaktpersonal hela dygnet.

5.1.2 Fysiskt tillträde

Detaljerad information av säkerhetsprocedurer för fysiskt tillträde är av säkerhetsskäl inte publikt tillgänglig.

All behörig personal har personliga inpasseringskort som skyddas med PIN-kod respektive biometri. All in- och utpassering loggas. Tillträde till vissa utrymmen kräver närvaro av minst två personer.

5.1.3 Fysisk säkerhet för RA

Några RA-funktioner kan förekomma utanför den skyddade centrala fysiska miljön. De är:

1. Identifiering av nyckelinnehavare vid ansökan med personlig närvaro.
2. Utlämning av koder.
3. Spärrtjänst för spärrning av certifikat.

Funktion enligt punkt 1 och 2 innebär ingen access till utfärdandesystemet. Denna miljö har därför inga särskilda säkerhetsföreskrifter vad avser fysisk säkerhet.

Funktioner enligt punkt 3 utförs i låsbart utrymme i kontorsmiljö. Inga nycklar eller koder lämnas utan tillsyn. Operatörskort som ger access till operativa roller i utfärdandesystemet är personliga och lämnas inte kvar då operatören lämnar lokalen. Lokalen innefattar även låsbara skåp för förvaring av arkivmaterial.

5.1.4 Lagring av media

Frånsett datorhall enligt 5.1.1 finns en annan fristående och skyddad lokal för lagring av säkerhetskopior och viktiga handlingar. I denna lokal finns särskilda individuellt låsbara säkerhetsskåp för förvaring av olika typer av loggar och arkiv. Detta för att ge skydd mot stöld, förvanskning, förstörelse eller obehörig användning av den förvarade informationen.

5.2 Säkerhetsorganisation (Procedurorienterad säkerhet)

Telia ansvarar i enlighet med 2.1.1. för alla procedurer och förhållanden som definieras i detta avsnitt. Detta innefattar allt från produktion och logistik till administration av hela processen.

5.2.1 Betrodda roller

Telia CA för e-legitimation har ett antal definierade roller som utför bestämda arbetsuppgifter. Varje roll har sin egen arbetsbeskrivning. Dessa roller får enbart innehavs av personal som uppfyller vissa kriterier, se vidare kapitel 5.3. De definierade rollerna utför bland annat en eller flera av följande arbetsuppgifter:

- Generering av CA-nycklar
- Aktivering av CA-nycklar i utfärdandesystemet
- Etablering av CA
- Validering av certifikatansökningar
- Godkännande av certifikatansökningar
- Spärr av certifikat
- Initiering av nya RA-operatörer i utfärdandesystemet
- Konfigurering och underhåll av utfärdandesystemet
- Uppläggning av nya användarkonton i utfärdandesystemet
- Konfigurering och underhåll av nätverkskommunikationen
- Hantering av backuper
- Hantering av loggar

Vissa kombinationer av roller/arbetsuppgifter är inte tillåtna att innehas av en och samma person.

5.2.2 Krav på antal personer per uppgift

För varje roll finns åtminstone en utsedd person. De olika rollerna är utsedda på ett sådant sätt att ingen person ensam kan få tillgång till hela utfärdandesystemet eller dess funktioner. För att generera nya CA:n, nya CA-nycklar och för att aktivera en CA:s signeringsnyckel krävs fler än två personer.

5.2.3 Identifiering och verifiering av personer i betrodda roller

Varje RA-operatör har egna individuella certifikat, med tillhörande privata nycklar lagrat på smart card, som används vid allt arbete med administration av e-legitimationer i utfärdarsystemet. De applikationer som används för att utföra de olika RA-funktionerna kontrollerar riktigheten av certifikaten och identiteten i certifikaten.

Operativsystemsansvariga, nätverks- och databasoperatörer har egna individuella användarkonton och lösenord på det/de system som de ansvarar för. Alternativt används individuella certifikat, på samma sätt som för RA-operatörer ovan, som ersättare för lösenord.

5.3 Personorienterad säkerhet

5.3.1 Bakgrund, kvalifikationer, erfarenhet och tillståndskrav

Roller enligt 5.2.1 tilldelas endast särskilt utvalda och pålitliga personer som uppvisat lämplighet för en sådan befattning.
Dessa personer får inte inneha annan roll som kan bedömas stå i konflikt med den tilldelade rollen.

5.3.2 Krav på utbildning

Alla innehavare av rollerna har genomgått den utbildning och träning som krävs för att på ett säkert sätt utföra sina arbetsuppgifter inom ramen för denna CPS och inom ramen för gällande säkerhetspolicy.

5.3.3 Personalorienterad säkerhet för RA

Ansvarig personal för RA-funktion hos Telia utses inom den organisation som är utsedd att utföra tilldelade arbetsuppgifter. Om sådan roll utförs av underleverantör till Telia så ansvarar denna även för att lämplig personalkontroll utförs.RA-personal som tilldelats roll i utfärdandesystemet uppfyller samma krav som för motsvarande CA-personal vad avser lämplighet och utbildning.

6 Teknisk säkerhet

6.1 Generering och installation av nyckelpar

6.1.1 Generering av nycklar

Nycklar som skapas för CA genereras utifrån ett slumptal. Processen att generera slumptal, som bas för nyckelgenerering, är slumpmässig på så sätt att det är beräkningsmässigt ogörligt att återskapa ett genererat slumptal, oavsett mängden kunskap om genereringsprocessens beskaffenhet eller vid vilken tidpunkt eller med hjälp av vilken utrustning slumptalet skapades.

Nyckelgenereringsprocessen är så beskaffad att ingen information om nycklarna hanteras utanför nyckelgenereringssystemet annat än genom säker överföring till avsedd förvaringsplats.

Nycklarnas unicitet uppnås genom att nycklarna är slumpmässigt genererade och av sådan längd att sannolikheten för att två identiska nycklar genereras är försumbar.

Utfärdarens CA-nycklar genereras i en för ändamålet anpassad lokal. Tillträde till lokalen kräver flera samtidiga personers närvaro.

CA-nycklarna genereras i en hårdvara som är dedicerad för att lagra krypteringsnycklar. CA-nycklarna exponeras inte utanför denna hårdvarumodul i okrypterad form vare sig vid generering eller vid användning. Vid själva genereringen krävs flera personers närvaro, som var och en innehar olika roller.

RA-operatörernas nyckelpar för kryptering/autentisering respektive för signering genereras i operatörskortets chip och de privata nycklarna hanteras aldrig utanför chippet.

Kundens nyckelpar för kryptering/autentisering respektive för signering genereras i den sökandes dator i samband med att kunden laddar ner sin e-legitimation. Detta sker med hjälp av den klientvara som Telia levererar till kunden. Programvaran uppfyller kraven på att generera krypteringsnycklar med god kvalitet.

6.1.2 Leverans av publika nycklar till CA

Vid en certifikatansökan för en Telia e-legitimation genereras de publika nycklarna med hjälp av den klientvara som Telia levererat till kunden och överförs till Telia CA för e-legitimation i en s.k. PKCS#10-beställning.

6.1.3 Leverans av CA:s publika nyckel till användare och förlitandeparter

I samband med att kunden hämtar sin e-legitimation laddas också certifikaten för den utfärdande CA:n ned till kundens webbläsare. Dessa CA-certifikat finns också publicerade på webben, https://repository.trust.telia.com.

6.1.4 Storlek på kryptografiska nycklar

Kryptografiska nycklar som används för Telia CA för e-legitimation består av RSA-nycklar som har minst 4096 bitars längd.

Användares och operatörers privata nycklar är minst 2048 bitar långa.

6.1.5 Generering av nycklar i maskin- eller programvara

CA-nycklar genereras i och förvaras i för ändamålet anpassad hårdvarumodul.
RA-operatörernas nycklar genereras och förvaras i operatörskortets chip.
Kundens nycklar genereras i för ändamålet avpassad klientprogramvara.

6.1.6 Användningsområde för nycklar

Fältet “keyUsage” i de utfärdade certifikaten används för att påvisa tänkt användningsområde för certifikatet med tillhörande privat nyckel. Detta gäller alla typer av certifikat som utfärdas av Telia CA för e-legitimation. Telia CA för e-legitimations privata nyckel får enbart användas för att signera e-legitimation, spärrlistor samt certifikat för OCSP-responder.

En ansökan om en Telia e-legitimation innebär att två certifikat ges ut till den sökande. Det ena certifikatet har nonRepudiation angivet i fältet keyUsage och dess motsvarande privata nyckel ska enbart användas för digitala signaturer. I det andra certifikatet är både keyEncipherment och digitalSignature angivet i fältet keyUsage, vilket innebär att certifikatet och tillhörande privata nyckel kan användas till både kryptering och autentisering.

6.2 Skydd av privata nycklar

Procedurerna enligt denna CPS vad avser generering, förvaring och distribution av privata nycklar har som syfte att till största möjliga grad borga för att privata nycklar skyddas på ett sådant sätt att de inte kan falla i orätta händer samt, vad avser nyckelinnehavares privata nycklar, att de inte i något fall exponeras eller brukas på otillbörligt sätt.

6.2.1 Standard för kryptografisk modul

Telia, såsom CA, använder kryptografiska hårdvarumoduler, som uppfyller FIPS 140-1 level 3, för generering, lagring och användning av CA-nycklarna.

6.2.2 Flerpersonskontroll av privata nycklar

CA:ns privata nyckel används och skyddas i en särskild hårdvarumodul som är inlåst i ett säkerhetsskåp vilket i sin tur förvaras inom det skalskyddade området.

Den privata signeringsnyckeln för Telia CA för e-legitimation kräver att flera personer samverkar för att generera, aktivera och radera den. Fysisk access till CA:ns privata nyckel kräver samverkan av minst två personer under hela nyckelns existens, från generering tills dess att alla säkerhetskopior är säkert raderade.

6.2.3 Deponering av privata nycklar

Telia CA för e-legitimation deponerar varken privata CA-nycklar, RA-administratörernas privata nycklar eller kundernas privata nycklar.

6.2.4 Säkerhetskopiering av privata nycklar

Backup tas av Telia CA för e-legitimations privata nyckel. Hantering av backup-kopian omgärdas av motsvarande regler för åtkomstskydd som gäller för originalet.

Backup-kopian finns vid inget tillfälle tillgänglig i okrypterad form utanför den kryptografiska modul där den är ämnad att användas.

De säkerhetskopierade nycklarna förvaras i kassaskåp som är placerade i en larmad och övervakad lokal. Åtkomst till de säkerhetskopierade nycklarna kräver flera personers samtidiga närvaro.

Telia gör ingen säkerhetskopiering av RA-operatörers eller kunders privata nycklar. Telia CA för e-legitimation tillhandahåller heller ingen funktion för säkerhetskopiering av kundens privata nycklar.

6.2.5 Aktivering av privata nycklar

CA-nycklarna aktiveras genom att en symmetrisk nyckel matas in i den kryptografiska hårvarumodulen. För att aktivera CA-nyckeln krävs medverkan av flera olika personer varav några har varsin del av den symmetriska nyckeln. Varje persons del av den symmetriska nyckeln finns skyddad i ett smart card med tillhörande PIN-kod.

CA-nyckeln aktiveras i driftsmiljö för att kunna användas för signering av användarcertifikat, certifikat för OCSP–responder och spärrlistor.

RA-operatörernas privata nycklar finns lagrade i smart card och aktiveras med hjälp av tillhörande PIN-kod om minst sex siffror.

Kunderna skyddar sina privata nycklar med en säkerhetskod, som är minst sex tecken lång och som består av minst en stor bokstav, en liten bokstav och en siffra. Koden kan för övrigt innehålla alla typer av skiljetecken. Detta sker med funktioner i av Telia levererad klientprogramvara.

6.2.6 Förstörelse av privata nycklar

När Telia CA för e-legitimations CA-nyckel inte längre är giltig eller om verksamheten upphör förstörs nyckeln med hjälp av funktioner i den kryptografiska hårdvarumodulen som nyckeln lagras i. Backup-kopior förstörs genom att använt lagringsmedium förstörs permanent. Ovanstående sker under flera personers samtidiga närvaro. Processen dokumenteras med avseende på vilka procedurer som genomförs och närvarande personer.

För utrustning i utfärdarsystemet med operativa nycklar som lagrats på hårddisk i krypterad form, gäller följande:

1. Om utrustningen skall användas vidare i samma skyddade miljö sker överskrivning av hårddisken med hjälp av för ändamålet lämplig programvara.
2. Om utrustningen skall användas utanför den skyddade zonen eller säljas/avyttras förstörs hårddisken/arna eller eventuellt monteras ur efter radering enligt 1 och lagras i säkerhetsskåp.

6.3 Andra aspekter på nyckelhantering

Inga privata nycklar eller annan konfidentiell information inom CA och RA får lämna sin föreskrivna skyddsmiljö.

6.3.1 Arkivering av publika nycklar

Alla publika nycklar som Telia CA för e-legitimation certifierar arkiveras i certifikatet under minst tio år efter det att giltighetstiden för certifikatet har gått ut.

6.3.2 Privata och publika nycklars livslängd

Certifikat för e-legitimation och tillhörande nycklar ges en maximal giltighetstid på två år.
Telia CA för e-legitimation med tillhörande CA-nycklar ges en maximal giltighetstid på tio år.

6.3.3 Ansvar för koder

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

6.4 Säkerhet i datorsystem

Driftsmiljön, i vilken Telia CA för e-legitimation finns, är konstruerad för att uppnå högsta tänkbara säkerhetsnivå. Driftsmiljön är separerad från Telias övriga verksamhet både fysiskt och logiskt. Inloggning i utfärdarsystemet sker på individbasis för att säkerställa spårbarhet och all inloggning loggas. De funktioner som utförs från driftsmiljön är uppdateringar av programvara, start och stopp av applikationer, övrigt underhåll samt arbete som inbegriper hantering av CA-nycklar.

RA-funktioner som rör utfärdande och administration av certifikat utförs via olika typer av applikationer. Dessa applikationer kräver att en godkänd operatör signerar den åtgärd som ska utföras med ett individuellt certifikat. De operativsystem eller övriga programvaror som används i driftmiljön har ingen formell säkerhetsklassning.

Utfärdandesystemet är uppbyggt på ett sådant sätt att individuella roller enligt 5.2 kan separeras. De accesskontrollsystem som används är så konstruerade att varje operatör identifieras på individuell nivå. Separering av roller på OS-nivå säkras genom dubbelbemanning. Ovanstående gäller oavsett om en operatör agerar inifrån utfärdarsystemets centrala anläggning eller om operatören befinner sig i en utflyttad RA-funktion.

6.5 Kontroll av säkerhet hos systemet under livscykeln

6.5.1 Säkring av systemutveckling

Utfärdandesystemets mjukvara utvecklas av tillverkare som använder en kontrollerad utvecklingsmiljö med ett väl dokumenterat kvalitetssäkringssystem.

6.5.2 Säkring av säkerhetsadministration

Driftsdokumentation finns upprättad som i detalj dokumenterar hur roller och behörigheter tillämpas och vidmakthållas.

6.5.3 Säkring av nätverk

Brandvägg finns implementerad som strikt avgränsar all typ av informationsutväxling som definierats som otillåten. Endast den typ av informationsutväxling som strikt behövs för CA-tjänsten är tillåten.
Viktig informationsutväxling mellan RA och CA är krypterad och transaktioner som påverkar användningen av CA:s privata utfärdarnycklar är individuellt signerade. Alla kommunikationsportar i utfärdandesystemet som inte behövs är deaktiverade och tillhörande mjukvarurutiner som inte används är blockerade.

7 Certifikatprofiler

7.1 Certifikatprofil

Certifikat för hårdvarubaserad Telia e-legitimation utformas i enlighet med specifikationen “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” (RFC 6818) med de förtydliganden, förändringar och tillägg som redovisas i detta avsnitt.

7.1.1 Versionsnummer

Certifikat utfärdas enligt X.509 v3, dvs. versionsfältet i certifikaten har värdet 2.

7.1.2 Certifikatextensioner

Följande certifikatextensioner används i Telia e-legitimation:

Fältnamn	**Critical**	**Kommentar/Värde**
authorityInfoAccess	non-critical	http://ocsp.trust.telia.com
authorityKeyIdentifier	non-critical	Sha-1 (hash av CA:ns publika nyckel)
certificatePolicies	non-critical	PolicyIdentifier=1.2.752.35.1.3 Policy Qualifier Id=CPS Qualifier: ”https://repository.trust.telia.com“
subjectKeyIdentifier	non-critical	Sha-1 (hash av användarens publika nyckel)
keyUsage	critical	- nonRepudiation - digitalSignature och keyEncipherment

7.1.3 Objektidentifierare för använda algoritmer

I Telia e-legitimation används RSA-algoritmen tillsammans med hash-algoritmen SHA-1. Följande objektidentifierare används i certifikatets signaturalgoritmfält:
Sha-1WithRSAEncryption OBJECT IDENTIFIER:== iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5

7.1.4 Användning av namnfält

De namnfält som används är Issuer DistinguishedName (utfärdare) och Subject DistinguishedName (ämne).

Följande attribut kan användas för Issuer DistinguishedName:

Attribut	**Kodning**	**Innehåll**
country (C)	printableString	SE
organization (O)	utf8String	TeliaSonera Sverige AB
organizational Unit (OU)	utf8String	
commonName (CN)	utf8String	CA:ns namn

Följande attribut används för Subject DistinguishedName i Telia e-legitimation:

Attribut	**Kodning**	**Innehåll**
country (C)	printableString	SE
surName (S)	utf8String	Efternamn
givenName (G)	utf8String	Förnamn (samtliga)
commonName (CN)	utf8String	Tilltalsnamn Efternamn
serialNumber (SN)		Personnummer med formatet YYYYMMDDXXXX

I CA-certifikat, relaterade till certifikat utfärdade enligt denna CPS, kan följande attribut användas för beskrivning av utfärdande CA i Subject DistinguishedName:

Attribut	**Kodning**	**Innehåll**
country (C)	PrintableString	SE
organization (O)	utf8String	TeliaSonera Sverige AB
organizational Unit (OU)	utf8String	
commonName (CN)	utf8String	CA:ns namn

7.1.5 Objektidentifierare för certifikatpolicy

Den objektidentifierare som används i Telia e-legitimation för denna CPS är i enlighet med kapitel 1.2.

8 Förvaltning och revisionshantering av detta dokument

8.1 Regler för revidering av detta dokument

8.1.1 Förändringar som kan ske utan underrättelse

Telia kan komma att uppdatera denna CPS med omedelbar verkan om uppdateringarna har någon av följande karaktär:

- Förändring i kontaktinformation
- Förändringar i URL information
- Språkliga förändringar som inte påverkar de utfärdade certifikatens säkerhetsnivå eller trovärdighet
  eller uppfyllelse av de krav som ställs i ETSI:s dokument ”Policy requirements for certification
  authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1, variant NCP.

8.1.2 Förändringar som ska ske med underrättelse

Telia är ansvarigt för denna CPS och ansvarar också för eventuella uppdateringar. Revidering av denna CPS, som inte faller under kapitel 8.1.1, ska göras tillgänglig åtminstone 15 dagar innan de föreslagna förändringarna träder i kraft. Under denna period är det möjligt att lämna synpunkter på de föreslagna förändringarna. CPS Management Team (CPSMT) beslutar om de slutgiltiga förändringarna som ska ske av CPS:en efter denna tidpunkts utgång. Förändringarna får inte innebära att krav som ställs i ETSI:s dokument ”Policy requirements for certification authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1, variant NCP, inte längre kan uppfyllas.

8.1.3 Övriga förändringar

Det är inte tillåtet att införa sådana förändringar i denna CPS så att den inte längre uppfyller de krav som ställs i ETSI:s dokument ”Policy requirements for certification authorities issuing public key certificates”, ETSI EN 319 411-3 V1.1.1, variant NCP eller att uppdateringen kräver att certifikatens policy-OID måste ändras.

8.2 Publicering och meddelanden

Aktuell version av denna CPS finns tillgänglig på Telias webb, https://repository.trust.telia.com.
Eventuell revidering eller förslag till uppdatering av denna CPS meddelas på Telias webb på adressen, https://repository.trust.telia.com.
Denna CPS innehåller alla relevanta processer och beskrivningar, som gör det möjligt för utomstående att bilda sig en uppfattning om de utfärdade certifikatens säkerhetsnivå. Därutöver finns ett antal dokument som i detalj beskriver processer och rutiner för varje del i utfärdandeprocessen, tekniska beskrivningar av utfärdandesystemet, lokalritningar och olika former av säkerhetsdokument. Dessa dokument är inte publikt tillgängliga.