Certifikatbestämmelser för Södra

Datum
2010-01-14

Tjänsteställe, handläggare
Dag Ygdevik

Version	Datum	Kommentar
	2008-05-13	Första utkastet
	2008-09-09	Uppdaterat utkastet efter kommentarer
1.0	2010-01-14	Fastställd version
2.0	2017-01-22	Uppdaterad fastställd version

Tjänsteställe, handläggare
Dag Ygdevik

1 Introduktion

1.1 Översikt

Dessa certifikatbestämmelser beskriver grundläggande vilka rutiner och säkerhetskrav som ska finnas för utfärdande och användande av mjuka certifikat för identifiering och autentisering inom Södra och med samarbetspartners till Södra. De krav som anges i denna certifikatspolicy skall anses som minimikrav. En person eller funktion i reviderande roll kan kräva högre säkerhetsnivåer än vad som anges i denna policy för uttalade applikationer.

Dokumentet följer RFC 2527. För tydlighets skull har samtliga sektioner i standarden tagits med. I de fall sektionen inte har definierats används ”Ej tillämpligt”.

Södras public key infrastructure (Södra PKI) är ett två-stegs PKI bestående av tre huvudsakliga komponenter: Root CA, Utfärdande CA och Registreringsenhet. Root CA används uteslutande för att tillverka certifikat till utfärdande CA.

Certifikat i enlighet med dessa bestämmelser kan ha två olika assuransnivåer:
Låg assurans – icke-personliga certifikat. Certifikatet kan bara garantera att aktiviteter troligen utförs av innehavaren.
Medium assurans – personliga certifikat med en stark bindning till innehavaren. Certifikatet garanterar att aktiviteter utförs av den som innehar certifikatet.

Certifikat kan användas för exempelvis identifiering, autentisering och digitala signaturer.

Certifikat kan utfärdas till
Södra Person – anställda på Södra eller kontrakterad part som arbetar som anställd
Södra Organisation – organisatoriska enheter, generiska användare
Södra Klient – datorer (klienter/servrar), mobila enheter, nätverksutrustning
Södra Funktion – tjänster och applikationer

1.2 Identifiering

Detta dokument har benämningen ”Certifikatbestämmelser för Södra”.

1.3 Målgrupp och tillämplighet

Dessa certifikatbestämmelser är tillämpliga för Södra, användare inom Södra och de parter som enligt avtal samarbetar med Södra.

Certificate Authority – Utfärdare (CA) utses av Södra och ska arbeta i enlighet med dessa bestämmelser.

Dessa certifikatbestämmelser ger möjlighet att utfärda certifikat lämpliga för:

- Identifiering och autentisering av klientdatorer och serverdatorer
- Identifiering och autentisering av mobila enheter och nätinfrastruktur
- Identifiering och autentisering av användare
- Kodsignering
- Smarta kort
- TLS-kommunikation, exvis för webb eller rdp

1.4 Kontaktuppgifter

Dessa certifikatbestämmelser ägs och förvaltas av Södra Skogsägarna Ekonomisk Förening. Frågor angående registrering, underhåll och tillämplighet av policyn ställs till:

Södra Skogsägarna Ekonomisk Förening
Koncern IT-säkerhetschef
Skogsudden
351 89 VÄXJÖ

Telefon: +46 470-89000
E-post: pki@sodra.com

2 Allmänna bestämmelser

Detta kapitel redogör allmänt för de bestämmelser som gäller för Certificate Authority - CA (Utfärdare), RA (Registreringsenhet) samt innehavare av certifikat.

2.1 Åtaganden

2.1.1 CA:s (Utfärdarens) åtaganden

Utfärdaren åtar sig att:

- Utfärda certifikat i enlighet med dessa bestämmelser
- Tillhandahålla kontrollåtgärder i enlighet med dessa bestämmelser
- Upprätta, förvalta och publicera utfärdardeklaration (CertificatePracticeStatement - CPS) som beskriver hur dessa bestämmelser uppfylls
- Spärra certifikat och tillhandahålla spärrtjänst i enlighet med dessa bestämmelser
- Skydda CA:s privata nycklar i enlighet med dessa bestämmelser
- Endast använda CA:s privata nycklar för signering av utfärdade certifikat och spärrlistor
- Förvara och leverera certifikat i enlighet med dessa bestämmelser
- Förse innehavare av certifikat med information för att säkerställa hur certifikat erhålls
- Utföra revision i enlighet med 2.7

2.1.2 RA:s (Registreringsenhetens) åtaganden

Registreringsenheten åtar sig att:

- Fastställa att de uppgifter som används vid certifikatutfärdande är korrekta
- Fastställa certifikatstyp och assuransnivå
- Registrering, verifiering och administration av certifikatsansökan
- Identifikation av innehavare innan utfärdande av certifikat
- Generera certifikat
- Ta emot beställningar för spärr av certifikat och utföra spärr av certifikat

2.1.3 Certifikatinnehavarens åtaganden

Innehavaren av certifikat utfärdat av Södra PKI åtar sig att:

- Följa rutiner för beställning, hantering och återkallande av certifikat i enlighet med dessa bestämmelser
- Lämna sanningsenliga uppgifter som kan styrkas
- Inte avslöja PIN-koder eller lösenord för någon
- Inte hantera certifikatet på ett försumligt sätt
- Omedelbart begära spärrning av certifikatet om det föreligger anledning att tro att certifikatet är röjt

2.1.4 Förlitande parts åtaganden

Förlitande part skall innan användning åta sig att:

- Certifikatet är lämpat för det avsedda ändamålet och av rätt certifikattyp
- Verifiera certifikatets giltighet
- Kontrollera certifikatet mot spärrlista

2.2 Ansvar

2.2.1 CA:s ansvar

Genom signering av certifikat som innehåller hänvisning till dessa certifikatbestämmelser, intygar CA (Utfärdaren) att denne, i samarbete med RA, har kontrollerat informationen i certifikatet i enlighet med de rutiner som fastställts i dessa certifikatbestämmelser.

CA (Utfärdaren) kan inte hållas ansvarig för skada som uppkommit på grund av felaktig information i certifikat eller spärrlista.

2.2.2 RA:s ansvar

RA (Registreringsenheten) ansvarar för att de uppgifter som används vid certifikatutfärdande är korrekta.

2.3 Ekonomiskt ansvar

Ej tillämpligt.

2.4 Tolkning och tvist

Enligt svensk lag.

2.5 Avgifter

Inga avgifter förekommer om inte särskilt avtal med part är upprättat.

2.6 Publicering och information

CA (Utfärdaren) ska publicera följande inom Södra:

- Dessa certifikatbestämmelser och tillhörande utfärdardeklaration (CPS)
- Spärrlistor (CertificateRevocationList, CRL)
- CA:s utfärdarcertifikat
- Utfärdade certifikat publiceras om behov uppstår
- Villkor för innehavare av certifikat

Certifikatbestämmelser, Certificate Practice Statement (utfärdardeklaration), spärrlistor och utfärdarcertifikat ska vara tillgängliga via:

http://pki.sodra.com

Lagringsplats för CA-certifikat och CRL för tillgängliggörande till förlitande part skall vara tillgängliga 24 timmar om dagen, 7 dagar i veckan med ett minimum om 100% per år inklusive planerad nedtid.

2.7 Revision

2.7.1 Frekvens för revision

CA (Utfärdaren) ska med ett intervall om 24 månader göra egna interna revisioner för att säkerställa att dessa certifikatbestämmelser efterlevs.

2.7.2 Förhållanden som ska granskas

Vid revisionen ska följande bedömas:

- Utfärdardeklarationens tillämplighet och överensstämmelse med dessa certifikatbestämmelser
- Att den praktiska tillämpningen av rutiner och säkerhetskrav enligt utfärdardeklarationen fungerar tillfredsställande

2.7.3 Information om resultatet av revision samt åtgärd vid upptäckt av brist

Resultatet av revisionen ska göras tillgängligt i en rapport där resultatet ska innehålla information om upptäckta brister som bedöms påverka förtroendet för ett utfärdat certifikat tillsammans med en riskbedömning av bristerna. Brister som väsentligen avviker från tänkt lösning ska åtgärdas av CA (Utfärdaren).

Rapporten ska inte innehålla uppgifter som kan tänkas äventyra säkerheten i lösningen om någon obehörig får reda på uppgifterna. Mottagare av rapporten är Informationsägare Södra PKI-funktion.

2.8 Konfidentiell information

2.8.1 Typ av uppgifter som är konfidentiella

Alla uppgifter och information klassificeras i enlighet med Södra Informationssäkerhetspolicy.

2.8.2 Typ av uppgifter som inte är konfidentiella

Följande uppgifter anses inte vara konfidentiella:

- Utfärdade certifikat
- Uppgift om spärrade certifikat
- Publika nycklar
- Dessa certifikatbestämmelser, och tillhörande utfärdardeklaration
- Villkoren för innehavare av certifikat

2.9 Immateriella rättigheter

Ej tillämpligt.

3 Identifiering och autentisering

Detta kapitel beskriver vilka rutiner som ska finnas för identifiering och autentisering vid certifikatsbegäran till CA (Utfärdaren) innan certifikaten tillverkas.

3.1 Initial registrering

3.1.1 Typer av namn

De uppgifter om nyckelinnehavaren som publiceras i utfärdade certifikat utgör ett urval av nedanstående attribut:

* Land
* Region
* Organisation
* Organisationsenhet
* Förnamn
* Efternamn
* Fullständigt namn i enlighet med nyckelinnehavarens normalt använda presentationsform
* Unik identifieringskod
* Tjänstetitel
* Rollbeteckning
* Namn på tjänst/funktion
* e-postadress (SMTP)

Södra Person - av ovanstående attribut kan följande förekomma i ett Södra Person:

* Land
* Region
* Organisation
* Organisationsenhet
* Förnamn
* Efternamn
* Fullständigt namn
* Unik identifieringskod
* Funktionsbeteckning
* e-postadress (SMTP)

Södra Organisation - av ovanstående attribut kan följande förekomma i ett Södra Organisation:

* Land
* Region
* Organisation
* Organisationsenhet
* Unik identifieringskod
* e-postadress (SMTP)

Södra Funktion - av ovanstående attribut kan följande förekomma i ett Södra Funktion:

* Land
* Region
* Organisation

* Organisationsenhet
* Unik identifieringskod
* Funktionsbeteckning
* e-postadress (SMTP)

Södra Klient - av ovanstående attribut kan följande förekomma i ett Södra Klient:
* Land
* Region
* Organisation
* Organisationsenhet
* Enhetsnamn
* Unik identifieringskod
* Funktionsbeteckning

Certifikat kan innehålla andra typer av uppgifter om certifikatsinnehavaren.

3.1.2 Namnsättning

De obligatoriska uppgifterna enligt 3.1.1 ska på ett unikt sätt identifiera innehavaren.

3.1.3 Fastställande av identitet

CA skall säkerställa identiteten på den blivande nyckelinnehavaren för att säkerställa att identiteten och den publika nyckeln kopplas ihop korrekt.
CA skall under autentiseringen dokumentera:

- Identiteten hos den person som utfört identifieringen.
- Metoden som använts för att identifiera individen.
- Datum när verifieringen utförts.

Identitetskontroll görs enligt någon av nedanstående procedurer.

a) Nyckelinnehavaren uppvisar godkänd och giltig legitimationshandling.

b) Nyckelinnehavaren gör en beställning i Södras beställningsportal, där autentisering sker mot Södras katalogtjänst. Beställningen kräver attest.

c) Om Nyckelinnehavaren är för organisationen känd, anställd, konsult, finns i katalogtjänst och är auktoriserad för certifikatet och spårbarhet finns i beställningar så innebär detta att ”autoenrollment certifikat” för person och dator kommer att installeras automatiskt utan krav på fysisk identitetskontroll i enlighet med a).

Övrig identitetskontroll vid beställning kräver personlig närvaro bortsett från utställande av ”autoenrollment certifikat” som inte kräver personlig närvaro.

Vid utlämnande av certifikat till personer ej anställda av Södra ska separat avtal tecknas med mottagande organisation.

4 Operationella krav

Detta kapitel beskriver de operationella krav som ställs på Utfärdare, Registreringsenhet samt certifikatinnehavare.

4.1 Ansökan om certifikat

Sökanden ska uppge identifikation i enlighet med dessa certifikatbestämmelser och underteckna ansökningshandlingar vilka därefter arkiveras genom RA:s försorg.

Generellt kan den som är ansvarig/behörig beställare för Södra Person, Organisation, Klient och Funktion ansöka om certifikat.

Låg assurans
Södra Organisation – beställning av certifikat görs av ansvarig linjechef för berörd organisation.
Södra Klient – beställning av certifikat görs genom automatiserad process (autoenroll) för klienter och servrar med konto i Södras katalogtjänst. Beställning av certifikat för mobila enheter och nätverksutrustning görs vid beställning av enheten av behörig beställare
Södra Funktion – beställning av certifikat görs av systemägare eller dennes företrädare

Medium assurans
Södra Person – beställning av certifikat för anställd i Södra görs automatiskt genom registreringsprocessen i Södras HR system. Beställning av certifikat för konsult som skall utföra arbete som anställd beställs av ansvarig linjechef som ansvarar för avtalet för konsulten. Detta görs normalt via automatiserad process då konto och behörigheter skapas i Södras katalogtjänst.

4.2 Utfärdande av certifikat

Utfärdandet av certifikat innebär att CA (Utfärdare) accepterar ansökan samt bekräftar de uppgifter som sökanden lämnat.

Registrering och hantering av den information som krävs för att utfärda certifikat ska ske i system och miljöer som är väl skyddade och utformade så att de förhindrar sammanblandning och obehörig spridning av identitetsuppgifter, certifikat och nycklar.

4.3 Acceptans av certifikat

Innehavaren ansvarar för att kontrollera att uppgifterna i certifikatet är korrekta. Genom att använda utfärdat certifikat godkänner innehavaren att uppgifterna är korrekta.

4.4 Återkallande av certifikat – revokering

CA (Utfärdaren) tillhandahåller tjänst för revokering av certifikat tillsammans med publicering av revokeringslista mot vilken spärrkontroll kan göras.

Certifikat revokeras när de av någon anledning inte längre bedöms vara tillförlitliga. CA (Utfärdaren) kan på eget initiativ spärra certifikat om certifikatsinnehavaren inte anses fullgöra sina åtaganden.

4.4.1 Behörighet att begära revokering

Behörig att begära revokering är:

- Certifikatinnehavaren
- Södras IT-säkerhetschef
- CA (Utfärdarenheten)
- Certifikatinnehavarens närmaste chef eller dennes överordnade

Identifiering av den som begär spärrning ska ske på lämpligt sätt. CA (Utfärdaren) kan besluta om spärrning även om identifiering inte kan utföras i de fall det föreligger risk för missbruk av certifikat.

Den som är behörig och vill spärra ett certifikat utfärdat av Södra ska kunna göra det vardagar mellan kl 08.00-16.30 svensk tid genom att ringa Södras Servicedesk på telefonnummer +46 470 89 839 alternativt dygnet runt på: http://pki.sodra.com

4.4.2 Periodicitet för utgivning av revokeringslista

Relevant information om spärrning ska publiceras i revokeringslista efter beslut om spärrning. Nya revokeringslistor ska publiceras varje vardag.

4.5 Loggning

I systemet som används av CA (Utfärdaren) ska minst följande händelser loggas, antingen manuellt, automatiskt eller både och, tillsammans med datum, tidpunkt och vilken individ som utfört händelsen:

- Start och stopp av systemet
- Lyckade och misslyckade händelser i samband med all hantering av certifikatinnehavare, deras nycklar och certifikat, inklusive hantering av CA:s nycklar och certifikat
- Lyckade och misslyckade händelser i samband med säkerhetskopiering
- Radering av loggar
- Förändringar i registernycklar
- Avvikelser och incidenter
- Icke-auktoriserade försök att få tillgång till CA-systemet
- Förändringar i utfärdardeklarationen

CA-systemadministratören ska dessutom bevara information om:

- Ändringar i och underhåll av systemets konfiguration och certifikatmallar
- Administratörers rättigheter

Loggarna ska:

- Granskas och analyseras för att upptäcka oönskade händelser
- Sparas motsvarande tid som ett utfärdat certifikat är giltigt
- Vara oåtkomliga för obehöriga och skyddas mot manipulering
- Säkerhetskopieras

4.6 Arkivering

4.6.1 Information som arkiveras

CA (Utfärdaren) ska arkivera följande information:

- Certifikatansökningar
- Begäran om spärrning, tillsammans med beslutstidpunkt, vem som har begärt spärrning, anledning till spärr samt vem som genomfört spärrningen
- Ingångna avtal
- Utfärdade certifikat

- Utfärdardeklaration (CPS)

4.6.2 Bevaringstid och skydd av arkiv

Arkiverad information ska:

- Lagras och skyddas mot förändring och förstörelse under en tid av minst ett år efter det att certifikatets giltighetstid gått ut
- Skyddas fysiskt genom att arkivet förvaras i lokaler med begränsat tillträde
- Lagras under sådana förhållanden att de är läsbara under den angivna lagringstiden

4.7 Byte av nycklar

Ej tillämpligt.

4.8 Katastrofplan vid röjda utfärdarnycklar

CA (Utfärdaren) genomför följande åtgärder för att återställa en säker miljö om det föreligger misstanke om att de privata utfärdarnycklarna skulle vara röjda:

- Lösenord till CA (Utfärdaren) system ska bytas
- Nya nyckelpar skall utfärdas för CA och nytt utfärdarcertifikat skall utfärdas (d.v.s. en ny CA skapas)
- En process för att utfärda nya certifikat med den nya CA startas
- Utfärdarcertifikat som är kopplade till de röjda nycklarna skall revokeras
- Certifikat utfärdade med de röjda nycklarna ska revokeras
- Certifikatsinnehavarna och andra parter med vilka CA (Utfärdaren) har överenskommelser eller andra etablerade relationer ska informeras
- Spärrlistor ska uppdateras
- Säkerställ att information om revokering finns tillgänglig för utfärdarcertifikat fram till dess att de spärrade certifikatens giltighetstid löpt ut

4.9 Upphörande av CA (Utfärdaren) verksamhet

I den händelse att Södra upphör med sin CA-verksamhet ska CA (Utfärdaren):

- Informera samtliga certifikatinnehavare
- Upphöra med tjänst för spärrkontroll av certifikat
- Säkerställa att arkiv och loggar kan bevaras på ett betryggande sätt under föreskriven arkiveringstid

5 Säkerhetsåtgärder

Detta kapitel beskriver fysiska, processorienterade och personella säkerhetsåtgärder.

5.1 Fysisk säkerhet

CA-systemet ska endast användas i Södras ordinarie lokaler för drift av IT-system.

Utrymme som används för drift av CA-systemet ska:

- Övervakas med avseende på värme och kraftförsörjning
- Vara brandskyddat
- Vara tillträdesbegränsat för obehöriga

CA (Utfärdaren) ska säkerställa att arkiv- och säkerhetskopior samt distributionsmedia förvaras på ett sådant sätt att förlust, manipulation eller obehörig användning av lagrad information förhindras. Arkiv- och säkerhetskopior ska förvaras på annat ställe än i den anläggning där CA (Utfärdaren) centrala funktioner finns.

Papper och elektroniska lagringsmedia som använts av CA (Utfärdaren) i produktion, och som inte längre ska användas, ska förstöras så att informationen inte går att återskapa.

5.2 Processäkerhet

Följande roller ska finnas inom CA (Utfärdaren)

Rollbenämning	Uppgifter
CA-administratör	Utför operativa åtgärder inom CA-funktionen såsom utfärda och revokera certifikat, publicera spärrlistor, säkerhetskopiera och arkivera information enligt dessa bestämmelser, granska loggar samt förvara CA-nycklar. Agerar RA (Registreringsenhet).
Systemadministratör	Utför driftoperativa åtgärder såsom installationer, konfigurationer och systemunderhåll på CA-system.

Det ska finnas två fysiska personer som kan inneha rollen som CA-administratör.

Vid driftoperativa åtgärder som utförs av Systemadministratör ska minst två fysiska personer närvara varav den ene ska utgöras av en CA-administratör.

Det ska finnas tekniska möjligheter att identifiera och autentisera ovan nämnda roller i CA-systemet.

5.3 Personell säkerhet

Personal får inte ha några andra uppgifter som kan vara i konflikt med de åligganden och ansvar som följer av de roller som de har i CA-systemet.

All personal hos CA (Utfärdaren) som berörs av CA-systemet ska ha erforderlig utbildning och kunskap för att utföra sina arbetsuppgifter.

6 Teknisk säkerhet

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

6.1 Generering och installation av nycklar

Nycklar ska vara av tillräcklig längd för att förhindra att nycklarna röjs genom kryptoanalys under en tidsperiod som motsvarar den förväntade livslängden på nycklarna. Gällande nyckelstorlek för RSA-nycklar som genereras i CA-systemet är minst 2048 bitar.

CA:s (Utfärdarens) publika nyckel för verifiering ska levereras till certifikatinnehavare på ett CA-certifikat.

6.2 Skydd av privata nycklar

CA:s (Utfärdarens) privata nycklar ska säkerhetskopieras i databasen i CA-systemet.
Certifikatinnehavarens privata nycklar säkerhetskopieras ej.

Certifikatinnehavarens privata nyckel går ej att återgenerera eller återställa.

6.3 Övrigt angående nyckelhantering

Certifikat utfärdas med en längsta livslängd på två (2) år.

Utfärdarcertifikat ska vara självsignerade och ha en längsta giltighetstid fem (5) år.

6.4 Aktiveringsdata

Ej tillämpligt.

6.5 Säkerhet i datorsystem

CA-systemet ska ha säkerhetsfunktioner för att säkerställa rollfördelningen beskriven i dessa bestämmelser.

Säkerhetsfunktionerna ska säkerställa åtkomstkontroll och spårbarhet för varje operatör på individuell nivå för de funktioner som påverkar användning av privata utfärdarnycklar.

6.6 Säkerhet under systemets livscykel

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

6.7 Nätverkssäkerhet

CA (Utfärdarens) system kan vara anslutet till ett nätverk men ska då skyddas i sådan omfattning att det kan motstå de angrepp som kan misstänkas komma att ske mot systemet.

7 Profiler för certifikat och spärrlistor

CA (Utfärdare) utfärdar certifikat enligt X.509 version 3 och spärrlistor enligt X509 version 2.

7.1 Certifikatprofil

Utfärdade certifikat ska minst innehålla följande grundläggande fält:

Fältnamn	Innehåll
Version	Version 3
Serial Number	När ett nytt certifikat skapas ska CA (Utfärdaren) system generera ett unikt serienummer inom Södras domän
Signature Algorithm	Identifierar den algoritm som CA använder för att signera certifikatet. SHA-2 ska användas för signering.
Issuer DN	Certifikatutfärdarens unika namn.
Validity	Certifikatets giltighetstid
Subject DN	Unik identifierare
Subject Public Key	Algoritmidentifierare – öppen nyckel
Signature	CA (Utfärdaren) signatur

7.2 CRLprofil

Spärrlistor ska utfärdas med minst följande innehåll:

Fältnamn	Innehåll
Version	Version 2
Signature Algorithm	Identifierar den algoritm som CA använder för att signera certifikatet.
Issuer	Identifierar den som skapat och signerat CRL
Effective Date	Datum för utfärdande
Next Update	Nästa datum för utfärdande av CRL
Revoked Certificates	Uppräkning av revokerade certifikat

8 Förvaltning av bestämmelserna

8.1 Förändring av bestämmelserna

Södra förbehåller sig rätten att ändra i dessa bestämmelser utan underrättelse till berörda parter under förutsättning att ändringarna inte påverkar säkerhetsnivån i beskrivna rutiner och regler. I annat fall kommer berörda parter att underrättas senast 30 dagar innan ändringarna träder i kraft, genom skriftlig information.

8.2 Publicering och distribution av bestämmelserna

Bestämmelserna kan erhållas elektroniskt genom kontakt med ansvarig för dessa certifikatbestämmelser alternativt genom http://pki.sodra.com .

8.3 Godkännandeprocedur

Säkerhetsansvarig för CA-tjänsten ansvarar för godkännandeprocess för detta dokument.