

Certifikatpolicy

Kvalificerade elektroniska signaturer
Ver 3.00 – 2010-03-24

Table of content

Page 2 – 5 Swedish version
Page 6 – 10 English version

SignGuard Europe AB (556633-0220)
Stockholm, Sweden
Drottninggatan 61, S-111 21 Stockholm, Sweden

Swedish

Förord

En elektronisk signatur kan användas för att säkerställa att elektroniskt överförd information inte har förändrats och att informationens avsändare är den som uppges vara avsändare. För att kunna använda en elektronisk signatur i ett öppet system där parterna inte känner varandra i förväg, d v s när de mottagare som skall förlita sig på signaturen saknar varje form av avtal med undertecknaren eller certifikatutfärdaren, behöver parterna kunna inhämta information om kopplingen mellan en elektronisk signatur och en bestämd person. Därför har det utvecklats ett system för elektroniska signaturer som brukar benämnas det öppna nyckelsystemet (Public Key Infrastructure, PKI). Den som skall verifiera en signatur måste vara säker på att en bestämd nyckel verkligen hör ihop med den person som framstår som utställare av en elektronisk handling. I detta system utfärdas ett elektroniskt intyg (certifikat) av en tredje part. Ett certifikat innehåller uppgift om vem som är innehavare av en elektronisk signatur. Sådan information kan inhämtas från en certifikatutfärdare. Ett avtalsförhållande föreligger mellan utfärdare av certifikat och innehavaren av den elektroniska signaturen. Något avtalsförhållande föreligger i regel inte med tredje part som är i behov av information om innehavare av en elektronisk signatur.

Från och med den 1 januari 2001 gäller lagen om kvalificerade elektroniska signaturer i Sverige. Lagen är en implementering av Europaparlamentets och rådets direktiv 1999/93/EG om elektroniska signaturer. I lagen definieras en elektronisk signatur såsom ”Data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats”.

En kvalificerad elektronisk signatur är en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och skapad av vissa närmare angivna anordningar för signaturframställning ex.vis ett smart kort som uppfyller de krav som framgår av de standarder som rekommenderats av kommissionen avseende sådana s.k. säkra anordningar. Ett kvalificerat certifikat skall vidare innehålla vissa uppgifter och vara utfärdat av certifikatutfärdare som riktar sig till allmänheten och som anmält sig till Post- och telestyrelsen.

Lagen innehåller regler om krav på, tillsyn över och skadeståndsansvar för den som utfärdar kvalificerat certifikat till allmänheten. Vidare innehåller lagen bestämmelser om elektroniska signaturers rättsliga verkan. Lagen innehåller en regel som anger de kvalificerade elektroniska signaturernas särställning. Regeln innebär att om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kravet med elektroniska medel, skall en kvalificerad elektronisk signatur alltid anses uppfylla kravet. Användningen av elektroniska signaturer inom eller vid kommunikation med myndigheter skall dock kunna vara förenad med ytterligare krav.

SignGuard Europe AB är utfärdare av kvalificerat certifikat och i detta dokument beskrivs tillvägagångssätt och verksamhetsprinciper som följs vid beviljandet av certifikat. De mer detaljerade reglerna för framställning, utgivning och spärning m.m. av certifikat anges i SignGuard Europe ABs Certifikation Practise Statement, CPS.

Sven Peter Helldén
Styrelseledamot

1. Certifikatutfärdare

SignGuard Europe AB skall följa gällande lagstiftning på området och följa de råd, anvisningar eller beslut som meddelas av behöriga myndigheter/organ. SignGuard Europe AB skall i sin verksamhet använda den teknik och säkerhet som erfordras för att uppfylla de krav som kan ställas på verksamheten. SignGuard Europe AB skall ha tillgång till personal (egen eller genom annan leverantör) med kunskap, erfarenhet och behörighet som förutsätts för att producera certifikattjänster. SignGuard Europe AB sätter säkerhetstänkandet högst på dagordningen. SignGuard Europe AB skall bevaka teknikförändringar och verka för att alltid använda den senaste och säkraste tekniken.

2. Certifikatinnehavare

Innehavaren av certifikatet svarar för att de uppgifter är riktiga som lämnats vid ansökningen om certifikatet. Innehavaren av certifikatet svarar för användningen av certifikatet och de rättshandlingar som företagits med certifikatet samt deras ekonomiska följder. Om innehavarens smartcard förkommer eller det finns en möjlighet att certifikatet missbrukas skall innehavaren omedelbart underrätta SignGuard Europe AB. SignGuard Europe AB har sin verksamhet öppen dygnet runt genom SignGuard Europe AB:s hemsida för certifikatinnehavarna och tredje part.

SignGuard Europe AB lämnar inte ut certifikat utan att innehavarens identitet är tillförlitligt fastställd.

2.1 Vem kan ansöka om kvalificerade certifikat

Enbart fysiska personer kan ansöka om kvalificerade certifikat hos SignGuard Europe AB. Certifikatsökandens rättigheter och skyldigheter anges i ansökningsdokumentet som utgör ett avtal med sökanden av certifikat. I ansökningsdokumentet framgår de avtalsvillkor som SignGuard Europe AB tillämpar vid varje tillfälle. Information om den fysiska personens ställning och befogenhet i en juridisk person eller annan information som gäller den juridiska personen och certifikatinnehavaren kan läggas in i certifikatet under förutsättning att den juridiska personen biträder ansökan med sådana uppgifter. SignGuard Europe AB förbehåller sig rätten att neka en ansökan.

2.2 Krav på ansökan

Ansökan om kvalificerade certifikat sker på sätt som anges på SignGuard Europe AB's hemsida. Biträder en juridisk person skall denna dock skriftligen bekräfta uppgifterna till SignGuard Europe AB. Ansökningshandlingar sparas digitalt hos SignGuard Europe AB. SignGuard Europe AB kräver att sökanden skall kunna ange fullständigt namn, medborgarskap, personnummer, folkbokföringsadress.

2.3 Identifikation av sökanden

Certifikat lämnas ut till sökanden förts efter att identifieringsprocessen genomförts i enlighet med SignGuard Europe ABs villkor som framgår på SignGuard Europe ABs hemsida.

Sökanden skall innan certifikatet lämnas ut kunna styrka sin identitet med godkända svenska identitetshandlingar. För att registrera ett nytt användarkonto hos SignGuard Europe AB krävs ett identitetskort utgivet av skatteverket. Med stöd av "Skatteverkets" identitetskort kan den

sökande skapa ett nytt användarkonto hos SignGuard. Användaruppgifter såsom namn, personnummer, certifikatsnummer och giltighetstid för den utfärdade legitimationen utgör basen i detta förfarande. Avtalet med SignGuard Europe AB signeras med det befintliga signaturcertifikatet på Skatteverkets id-kort. Innan användaren kan ges tillåtelse att beställa kvalificerade signaturcertifikat genomförs en spärrförfrågan hos utfärdaren av legitimationen. Förutsatt att den använda legitimationen är giltig kan användaren beställa ett kvalificerat signaturcertifikat. Alternativt kan även användarkonton skapas där SignGuard Europe AB eller något av SignGuard Europe AB befullmäktigat ombud genomför en identifiering av den sökande. Underlagen för identitetskontrollansökan lagras sedan digitalt hos SignGuard Europe AB.

2.4 Certifikatets giltighetstid m.m.

Certifikatets giltighetstid är tidsbegränsat i enlighet med de villkor som meddelades vid ansökningstillfället. Andra villkor framgår av certifikatet. Certifikatet kan förnyas online innan giltighetstidens utgång enligt de villkor som framgår av SignGuard Europe AB's hemsida.

När sökanden identifierats och mottagit certifikatet enligt ovan och då underlaget kommit SignGuard Europe AB tillhanda skall utfärdandet slutligen godkännas och registreras av SignGuard Europe AB. Certifikatet anses utfärdat vid denna tidpunkt då SignGuard Europe AB registrerar godkännandet. Certifikatet är giltigt under giltighetstiden och upphör vid utebliven förnyelse i tid eller då återkallelse registrerats hos SignGuard Europe AB.

2.5 Certifikatinnehavarens aktsamhetskrav

Certifikatinnehavaren ansvarar för att smartcard och koder (nycklar) inte kommer i annans besittning. Koder (nycklar) och smartcard får aldrig förvaras tillsammans. Certifikatinnehavaren får aldrig avslöja sin privata kod (nyckel) eller låta annan använda certifikatet. Certifikatinnehavaren ansvarar för att certifikatet endast används av innehavaren.

2.6 Förnyelse av nycklar

Förnyelse av nycklar kan inte ske. Betraktas som nybeställning av certifikat.

3. Tredje part

SignGuard Europe AB skall via sin hemsida tillhandahålla information om verksamheten, certifikatinnehavare och spärrlistor dygnet runt. SignGuard Europe AB har enligt lag ett tvingande skadeståndsansvar mot tredje part och har ekonomiska förutsättningar att säkerställa eventuell skadeståndsskyldighet. SignGuard Europe ABs ansvar för skada är begränsat till 100,00 € per certifikat.

4. Verifiering av certifikat

SignGuard Europe AB tillhandahåller möjlighet att dygnet runt kontrollera giltighet och identitet för utfärdade certifikat. Kontroll kan enbart ske online på SignGuard Europe AB's hemsida. SignGuard Europe AB utfärdar även på begäran intyg om certifikat och identitet.

5. Spärrtjänst

SignGuard Europe AB har en spärrtjänst på sin hemsida som är tillgänglig dygnet runt. Innehavaren av certifikat kan återkalla sitt certifikat. Innehavaren skall återkalla sitt certifikat omgående om hans smartcard förlorats eller det kan misstänkas att så skett. SignGuard Europe AB kan även återkalla ett certifikat om det kan misstänkas att certifikatet missbrukas eller att smartcardet förlorats. SignGuard Europe AB har dygnetrunt bevakning av spärrtjänsten. Spärrlistan uppdateras kontinuerligt och senast en timma efter erhållen spärrinformation.

6. Tillgänglighet

SignGuard Europe AB har sin hemsida öppen dygnet runt för verifiering och spärrtjänst.

7. Ansvar

Enligt lag 2000:832 om kvalificerade elektroniska signaturer skall SignGuard Europe AB ersätta förlitande part i vissa fall. De närmare förutsättningarna framgår av lagens 14 §.

8. Säkerhet och teknik

SignGuard Europe AB använder den maskinvara och programvara och övriga säkerhetsrutiner som överensstämmer med sådana standarder som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapens officiella tidning. SignGuard Europe AB har som målsättning att ha den senaste och säkraste tekniken.

9. Kompetens

SignGuard Europe ABs krav är att den personal som utför tjänster åt SignGuard Europe AB skall ha kompetens för sina uppgifter och erhålla den kompetensutveckling som kan aktualiseras utifrån verksamhetskraven och arbetsuppgift.

10. Ekonomiska medel

SignGuard Europe AB har eget kapital för att klara av eventuella skadeståndsanspråk som kan riktas mot bolaget.

11. Avtalsvillkor

Allmänna avtalsvillkor mellan SignGuard Europe AB och certifikatinnehavare framgår av SignGuard Europe ABs hemsida. De särskilda villkoren som träffats framgår på certifikatinnehavarens tilldelade användarkonto.

12. Tvister

Svensk lag tillämpas vid svensk domstol.

English

Preface

An electronic signature can be used to ensure that electronically transmitted information has not been changed and that the sender of the information is designated as the sender.

To use an electronic signature in an open system where the parties do not know each other beforehand, i.e. when the recipient must rely on the signature without any agreement with the signatory or the certificate issuer, the parties need to be able to obtain information about the link between an electronic signature and one particular person. Therefore, it has been developed a system for electronic signatures, usually called the public key system, Public Key Infrastructure (PKI). Anyone who wants to verify a signature must be sure that a given key really is linked to the person presenting himself as an exhibitor of an electronic document. In this system an electronic certificate is issued by a third party. A certificate contains information about the identification of the holder of an electronic signature. Such information can be obtained from an issuer of a certificate. A contractual relationship exists between the issuer of the certificate and the holder of the electronic signature. No contractual relationship exists in general with third parties who are in need of information about the holder of an electronic signature.

The law of qualified electronic signatures in Sweden exists since the 1st of January 2001. The law is an implementation of the European Parliament and Council Directive 1999/93/EC of electronic signatures. The Act defines an electronic signature as "data in electronic form which are attached to or logically associated with other electronic data, used to verify that the content originates from the person presenting himself as a exhibitor and that it has not been manipulated".

A qualified electronic signature is an advanced electronic signature based on a qualified certificate and created by certain specified facilities for signature petition, for example a smart card which meets the requirements laid down by the standards recommended by the commission in respect of such so-called secure devices. A qualified certificate shall contain certain information and be issued by a certificate issuer with the public as target and who has applied with the National Post and Telecom Agency.

The Act provides requirements, supervision and liability for the issuing of qualified certificates to the public. Furthermore, the Act contains provisions for the legal consequences of electronic signatures. The Act contains a rule that specifies the special status of a qualified electronic signature. The rule involves that if the law or regulation requires a handwritten signature or equivalent, and if it is permissible to satisfy the requirement by electronic means, the qualified electronic signature should always be considered to meet this requirement. The use of electronic signatures within or in communication with the authorities could however be connected with additional requirements.

SignGuard Europe AB is issuer of qualified certificates and this document describes the approach and business principles that are followed in the granting of certificates. The detailed rules governing the preparation, issuance and revocation of a certificate are specified in SignGuard Europe AB's Certificate Practice Statement, CPS.

Sven Peter Helldén
Member of Board of Directors

1. Certificate Authorities

SignGuard Europe AB must comply with current legislation and follow the advice, instructions or decisions issued by the competent authorities/bodies. SignGuard Europe AB should use the technology and safety required. SignGuard Europe AB will have access to staff (its own or through other sources) with knowledge, experience and competence that is assumed to produce certification services. SignGuard Europe AB sets security on top of the agenda. SignGuard Europe AB shall monitor technological changes and always try to use the latest and safest technology.

2. Certificate Holders

The holder of a certificate answers for that the information given on the application is accurate. The holder of a certificate answers for the use of the certificate and the legal actions taken by the certificate; also their economic consequences. If the holder's smart card is lost or there is a possibility that the certificate is being misused, he shall immediately notify SignGuard Europe AB. SignGuard Europe AB has its business activities available 24 hours, through SignGuard Europe AB's website, for the certificate holders and third parties.

SignGuard Europe AB will not issue a certificate without having proved the reliability of the holder's identity.

2.1 Who can apply for qualified certificates

Only individuals can apply for qualified certificates by SignGuard Europe AB. The rights and obligations of the certificate applicant are specified in the application document which constitutes an agreement of the applicant of the certificate. The application document shows the contractual terms of SignGuard Europe AB. Information of the position and the authority of the individual or other information relating to the legal person and the certificate holder can be inserted in the certificate, provided that the person has completed the application with such data. SignGuard Europe AB reserves the right to refuse an application.

2.2 Criteria for application

The way of application for qualified certificates are set out on SignGuard Europe AB's website. If a legal person assists this shall be confirmed in writing to SignGuard Europe AB. Application forms are stored digitally by SignGuard Europe AB. SignGuard Europe AB requires the applicant to enter the full name, nationality, date of birth, registered address.

2.3 Identification of the applicant

Certificates shall be issued to the applicant only after that the identification process has been carried out in accordance with SignGuard Europe AB's conditions stipulated on SignGuard Europe AB's website.

Before the certificate can be issued, the applicant shall prove his identity with approved identity acts. To register a new user account with SignGuard Europe AB the applicant will need a Swedish ID-Card issued by the Swedish tax authority. With the identity card from the

Swedish tax authority the applicant creates a new user account with SignGuard Europe AB. User information like name, personal number, certificate number and validity for the identification issued constitutes the base in this procedure. An agreement with SignGuard Europe AB is signed using the existent signature certificate on the Swedish tax authority's id-card. Before the user receives permission to order a qualified certificate a revocation check is made with the issuer of the identification. Provided that the identification presented is valid the user can order a qualified signature certificate. Alternatively user accounts can be created where SignGuard Europe AB or a by SignGuard Europe AB authorized agent can carry out an identification of the applicant. The documents for identity control are then digitally stored with SignGuard Europe AB.

2.4 Validity of the certificate, et cetera.

The time of validity of the certificate is limited in accordance with the terms announced at the time of application. Other conditions are shown in the certificate. The certificate can be renewed online before the expiry under the conditions stipulated by SignGuard Europe AB's website.

When the applicant is identified and has received the certificate and when the identification base has reached SignGuard Europe AB, SignGuard Europe AB shall finally approve and register the issue. The certificate is considered as issued at the moment when SignGuard Europe AB registers the authorization. The certificate is valid during the time of the duration and terminates if not renewed in time or when SignGuard Europe AB withdraws the certificate.

2.5 Certificate Holder's duty of care

The certificate holder is responsible for that the smartcard and codes (keys) will not come in another person's possession. Codes (keys) and smart cards should never be stored together. The certificate holder should never reveal his private code (key), or let any one else use the certificate. The certificate holder is responsible that the certificate is used only by its holder.

2.6 Renewal of keys

Renewal of keys is not possible. A new application is required.

3. Third Party

SignGuard Europe AB shall, through its website, provide information of activities, certificate holders and revocation lists 24 hours a day. SignGuard Europe AB has by law a mandatory liability against third parties and has financial ability to secure any liability. SignGuard Europe AB's liability for damage is limited to 100,00 € per certificate.

4. Verification of certificates

SignGuard Europe AB provides a 24 hour opportunity to check the validity and identification of certificates issued. Control can only be done online on SignGuard Europe AB's website. SignGuard Europe AB issues also on request a certificate of licence and identity.

5. Revocation service

SignGuard Europe AB has a revocation service on its website which is available 24 hours a day. The holder of the certificate may revoke its certificate. The certificate holder shall revoke his certificate immediately if his smart card is lost or if it is suspected that this has occurred. SignGuard Europe AB can also revoke a certificate if it is suspected that the certificate is abused or if the smart card is lost. SignGuard Europe AB revocation service is available 24 hours a day. The revocation list is updated continuously and always one hour after the information is obtained at the latest.

6. Availability

SignGuard Europe AB has its website open 24 hours a day for authentication and revocation service.

7. Responsibility

The Swedish law, 2000:832, regarding qualified electronic signatures, directs that in some cases SignGuard Europe AB must compensate a relying party. The terms and conditions are listed in the Act § 14.

8. Safety and technology

SignGuard Europe AB uses hard- and software and other security procedures that are consistent with standards given by the European Commission and available with reference numbers in the Official Journal of the European Commission. SignGuard Europe AB aims at use the latest and safest technologies.

9. Competence

SignGuard Europe AB's requirements are that the staff performing services for SignGuard Europe AB shall be competent for their tasks and shall receive all appropriate education for the requirements.

10. Funding

SignGuard Europe AB has the financial ability to secure any claims that could be set against the company.

11. Terms

The terms of conditions between SignGuard Europe AB and a certificate holder is shown on SignGuard Europe AB's website. The special conditions which may have been stipulated are shown on the certificate holder's assigned user account.

12. Disputes

Swedish law and court is applied.