

---

## Information – Beställning funktionscertifikat

Västra Götalands län (Kommun, VGR)

---

### Ansökan gällande SITHS Funktionscertifikat PKCS10

Funktionscertifikat är en elektronisk legitimation för funktioner och servrar giltig upp till 2 år. De finns som legitimeringscertifikat och som signeringscertifikat.

Certifikaten skapas utifrån **befintliga** HSA-objekt för funktionen.

Certifikaten kan beställas som PKCS#10 SHA512.

Certifikaten beställs enligt PKCS#10 och levereras som en DER-kodad certifikatsfil.

Rotcertifikat är publika och hämtas från <http://www.siths.se>

Ansvarig mottagare är den som skriftligt kvitterar ut certifikatet. Den ansvarige mottagaren ska förvara nycklar och koder på fysiskt åtskilda platser. Nycklar och/eller koder får inte kopieras, arkiveras eller på annat sätt dupliceras med undantag för backuptagning.

### Förutsättningar

- Funktionen/Servern skall finnas som serverobjekt i HSA innan certifikat kan skapas. Certifikatets namn blir som HSAobjektet
- SITHS Funktionscertifikat kan enbart ges ut till av SITHS validerade och godkända domännamn. Organisationens RA ansvarar för denna validering. Nedanstående är godkända per automatik, skall annan domänadress användas blir du kontaktad av RA som validerar domännamnet tillsammans med organisationens domänansvarig
- CSR-fil måste sändas ihop med beställning av PKCS#10
- Lista på [Godkända domäner](#)

## Ansvar

**Behörig beställare** är den som äger eller förvaltar en funktion och därigenom har mandat att begära certifikat till denna. Behörig beställare ansvarar för funktionens identitet samt att certifikatet spärras om behovet upphör eller vid misstänkta oegentligheter.

Vid misstanke om missbruk skall certifikatet omgående begäras spärrat till TjänsteID Service. Revision av certifikatshantering sker enligt RAPS och Rutinbeskrivning TjänsteID av SITHS PA Västra Götalands RA eller Västra Götalandsregionens säkerhetschef.

- För Västra Götalandsregionen kan revision initieras av Säkerhetsdirektör och Säkerhetsstrategiska Enheten
- För kommuner enligt respektive kommuns interna regelverk

Västra Götalandsregionen och personer inom Västra Götalands RA-organisation ansvarar inte för följder av:

- att någon nyckel ändras på otillbörligt sätt
- att NI använder certifikat på otillbörligt sätt
- felaktigheter i CA:s certifikatsutfärdande

## Beställningsflöde

PKCS#10

Behörig beställare fyller i ansökan och skickar till TjänsteID Service. I ansökan anges personen som skall kvittera ut certifikatet – Nyckelinnehavaren (NI). NI bifogar en CSR-fil<sup>1</sup> – certifikatsbegäran – till TjänsteID Service vilken laddar upp denna till CA – certifikatutfärdaren och kan därefter skriftligt kvittera mottagande av certifikat. Privata nycklar utväxlas inte vid PKCS#10 då dessa hanteras av systemet som skapade CSR.

TjänsteID Service administrerar och utför:

Säkerhetsansvarig och revisionspart är säkerhetschef i Västra Götalandsregionen

<sup>1</sup> kodat i binär form (DER-kodning) eller i textform (binär Base64-kodning). Vid Base64-kodning ska 7-bit ASCII användas för text, inte Unicode. Även s.k. PEM format är tillåtet.

---

## Villkor för användning av SITHS funktionscertifikat

Dessa bestämmelser för utfärdande av SITHS Funktionscertifikat omfattar de krav som varje organisation vilka utfärdar SITHS funktionscertifikat till egen eller annan organisation, eller beställaren av SITHS funktionscertifikat via ett ombud, måste förhålla sig till, det vill säga beställning och utgivning av elektroniska funktionscertifikat enligt SITHS-konceptet.

### 1. UTGIVNING AV FUNKTIONCERTIFIKAT

- 1.1. Vid utgivning av funktionscertifikat ska ombudet säkra att beställaren av funktionscertifikatet är införstådd med CA/RA-områdets användarvillkor
- 1.2. Kontroll av domännamn samt kontroll av äktheten i certifikatsbegäran skall göras av utfärdaren vid varje tillfälle då funktionscertifikat utfärdas
- 1.3. Inga andra parter än beställaren av funktionscertifikatet får arkivera den privata nyckeln.
- 1.4. Beställaren av funktionscertifikatet skall efter leverans av funktionscertifikatet kontrollera dess innehåll
- 1.5. Beställaren av certifikatet skall garantera att certifikatet endast installeras på servrar som är tillgängliga på den plats som anges i intyget, och att certifikatet enbart används i överensstämmelse med alla tillämpliga lagar och endast i enlighet med SITHS regelverk samt gällande användarvillkor

### 2. ÅTERKALLANDE/REVOKERING AV CERTIFIKAT

- 2.1. Utgivaren av funktionscertifikat skall säkra att beställaren omgående har en kontaktväg till utgivaren för att hos denne begära återkallande (revokering) av certifikat med tillhörande privat nyckel, i händelse av att funktionscertifikatet har eller misstänks ha används felaktigt eller på annat sätt har missbrukas. Det skall finnas möjlighet att revokera certifikatet inom rimlig tidsperiod

### 3. UPPSÄGNING AV AVTAL

- 3.1. CA (Inera AB) eller RA-ombud har rätt till att omedelbart säga upp samarbetsavtal mellan ombud och tredjepartsansluten organisation samt mellan CA och RA-organisation
  - a) om utgivaren och beställaren skulle bryta mot regelverken för Identifieringstjänst SITHS och/eller
  - b) om CA/RA-områdets användarvillkor för utfärdande av funktionscertifikat bryts, eller
  - c) om CA/RA upptäcker att certifikat används för att göra det möjligt för kriminella aktiviteter såsom nätfiskeattacker, bedrägeri eller distribution av skadlig kod.