2016-04-07

Beställning av certifikat v 3.0

Riksgäldskontoret
ORG.NR.
202100-2635

POSTADRESS POSTAL ADDRESS
SE-103 74 Stockholm
Sweden

BESÖK VISITORS
Norrlandsgatan 15

TELEFON TELEPHONE
NAT. 08 613 52 00
INT. +46 8 613 52 00

TELEFAX
NAT. 08 21 85 53
INT. +46 8 21 85 53

INTERNET
riksgalden@riksgalden.se
www.insattningsgarantin.se

Innehållsförteckning

Inledning 3
Undvik vanliga problem 3
Generell information 3
Ordlista 3
Certifikatsansökan 4
Beställningsblankett: 4
    Information om organisationen: 4
    Godkännare 5
    Certifikatssökande 5
    Validering 5
    Att översända ansökan 5
Skapa en Certificate Sign Request (CSR) 6
    CSR med OpenSSL: 6
Exempel på hur man hanterar svaret från certifikatsutfärdaren. 6
    Med OpenSSL: 6
Support 7

Inledning

Observera att Riksgälden inte kan ta ansvar för några produkter som nämns i detta dokument. Inte heller kan vi garantera att de exempel som ges är kompletta eller korrekta. De är bara tänkta som en översiktlig hjälp för att komma igång med tekniken.

Riksgälden rekommenderar alla institut att noga läsa och förstå dokumentationen till de produkter de väljer att använda sig av.

Undvik vanliga problem

Det vanligaste problemet är att ett datorbyte sker under processen och den privata hemliga delen av nyckelparet går förlorat. Det är alltså viktigt att slutföra processen på en och samma dator och helst, som en och samma användare.

Det händer också att certifikaten förkommer. När processen är klar och ett komplett certifikat har skapats ska det därför säkerhetskopieras och förvaras på ett säkert ställe.

Se till att både den privata och den publika delen kommer med och testa att återläsa certifikaten på en annan dator för att verifiera att säkerhetskopiorna är kompletta och läsbara.

Generell information

Certifikaten utfärdas av Buypass AS (”Buypass”). Buypass avgifter för att utfärda certifikatet bekostas av Riksgälden. Dessa certifikat ska inte användas för något annat ändamål än att signera filer enligt Riksgäldens föreskrifter RGKFS 2011:2. Endast de institut som tillhör den svenska insättningsgarantin är berättigad till ett certifikat.

Ordlista

Till följd av att Buypass är ny certifikatsleverantör och på grund av förändrade processer har vissa begrepp som tidigare använts ändrats. Följande beskrivning avser sådana begrepp där andra benämningar använts i tidigare instruktioner.

Beställningsblankett: Den pdf-mall där instituten ansöker om certifikat. Beställningsblanketten finns tillgänglig på insättningsgarantins hemsida: https://www.riksgalden.se/sv/Insattningsgarantin/For-anslutna-institut/Foreskrifter/ . Beställningsblanketten benämndes tidigare Certificate Enrollment Request (CER)

Godkännare: Förekommer i beställningsblanketten och är den person som Buypass kontaktar för att bekräfta certifikatsbeställningen. Godkännaren måste följaktligen vara bemyndigad att godkänna certifikatsbeställningen för institutets räkning. Godkännarens bemyndigande kommer att valideras av Buypass. Godkännare motsvarar i stort den person som i tidigare instruktioner benämndes Corporate Contact (CC).

Certifikatssökande: Förekommer i beställningsblanketten och är den person som hanterar beställningen och erhåller certifikatet från Buypass. Certifikatssökande kan vara den samma som godkännaren. Certifikatssökande motsvarar i stort den person som i tidigare instruktioner benämndes Technical Contact (TC).

Certifikatsansökan

Instituten ska ansöka om ett certifikat hos Riksgälden. Ansökan ska bestå av en CSR och en beställningsblankett. I ansökan ska också anges upp till maximalt fem IP-adresser eller ett nätobjekt från vilka institutet kommer att anropa Riksgäldens sida för uppladdning av signerade och krypterade filer. För det fall institutet redan meddelat IP-adresser behöver detta ***inte*** ske igen såvida inte institutet önskar ändra tidigare angivna IP-adresserna. Ansökan ska e-postas till ig@riksgalden.se.

Om *inte* kontaktpersoner för filleverans tidigare angivits ska dokumentet för kontaktuppgifter för filleverans bifogas ansökan. Notera att med kontaktpersoner för filleverans avses *inte* de samma som anges i beställningsblanketten för certifikatet. Notera också att institutet är skyldigt att vid behov uppdatera information om kontaktpersoner. Blanketten för kontaktuppgifter för filöverföring finns på insättningsgarantins hemsida: https://www.riksgalden.se/sv/Insattningsgarantin/For-anslutna-institut/Foreskrifter/

Riksgälden säkerställer att ansökan inkommit från ett institut som är anslutet till insättningsgarantin och vidarebefordrar denna till Buypass som inleder processen med att verifiera, skapa och slutligen sända ut certifikatet.

För det fall ansökan innehåller felaktigheter eller är ofullständig kommer Buypass att kontakta den som står angiven som certifikatssökande i ansökningsblanketten och begära rättning eller komplettering.

Buypass validerar informationen i beställningsblanketten och CSR mot EBRs bolagsregister (www.ebr.org). Buypass använder organisationsnummret för att söka i registret varför det är viktigt att detta anges korrekt. Vid mindre felaktigheter kan Buypass rätta utifrån registerdata. Större felaktigheter kräver en rättning i beställningen.

Buypass stämplar och skickar certifikatet till i första hand certifikatssökaren eller, för det fall ingen certifikatssökare angivits, till godkännaren. Riksgälden tar *inte* del av detta certifikat.

Beställningsblankett:

Beställningsblanketten finns på insättningsgarantins hemsida:

https://www.riksgalden.se/sv/Insattningsgarantin/For-anslutna-institut/Foreskrifter/

Information om organisationen:

Detta fält avser information om institutet. Buypass kommer kontrollera bolagets namn och organisationsnummer mot relevant register. Buypass kommer kontrollera att telefonnumret tillhör det ansökande institutet.

Organisationsnummer: Ska avse institutets organisationsnummer. Detta kommer att kontrolleras mot tillämpligt register.

Organisationsnamn: Ska vara bolagets officiella namn så som det framgår av exempelvis bolagsverkets register. Vid tveksamhet kan namnet kontrolleras genom att söka på Riksgäldens hemsida över anslutna institut. Institutens officiella namn framgår där.

Telefonnummer: Ska vara ett telefonnummer till institutet. Buypass kommer kontrollera att telefonnumret går till institut. Telefonnumret kommer användas för att kontrollera godkännarens behörighet att beställa ett certifikat i institutets namn.

Godkännare

Detta fält avser information om certifikatbeställaren. Beställaren måste vara anställd på bolaget och vara behörig att beställa ett certifikat i institutets namn. Buypass kommer validera följande:

- Att beställaren faktiskt beställt ett certifikat.
- Att beställaren är anställd hos bolaget
- Kontrollera att beställaren är behörig att beställa ett certifikat i institutets namn.

Certifikatssökande

Detta fält avser information om den som certifikatet ska skickas till. Godkännare och certifikatssökande kan vara samma person. I så fall lämnas fältet certifikatssökande tomt.

Validering

Validering sker genom att Buypass kontaktar godkännaren för att verifiera att vederbörande beställt ett certifikat och för det fall en certifikatssökande angivits, att certifikatet ska levereras till denna. Buypass kommer också att efterfråga godkännarens chef.

Buypass kommer därefter kontakta godkännarens chef för en bekräftelse om godkännarens behörighet att beställa ett certifikat för institutets räkning. Godkännarens chef bör därför vara medveten om denna process.

Utfärdat certifikat kommer skickas till antingen till godkännarens eller till certifikatssökande om en sådan angivits.

Att översända ansökan

Beställningsblanketten ska fyllas i elektroniskt (inte scannas in) och skickas till ig@riksgalden.se tillsammans med CSR:en. För det fall kontaktpersoner för filleverans och ip-adresser inte tidigare meddelats Riksgälden ska dessa också bifogas ansökan.

Skapa en Certificate Sign Request (CSR)

Se http://en.wikipedia.org/wiki/Certificate_signing_request

Följande information skall vara specificerad i CSR:en:

Email Address: Institutets E-Post adress
CN=Institutets Namn
L=Institutets Stad t.ex. Stockholm,
OU=Insattningsgarantiv2,
O=Samma som i CN,
C=Institutets landskod t.ex.: SE

Key Type: RSA
Key Strength: 2,048 bits
Certificate Usage: Sign, Encrypt

Observera att det är särskilt viktigt att ”CN” (institutets namn) anges korrekt. Det ska skrivas exakt som det står i Bolagsverkets register.

CSR med OpenSSL:

```
openssl genrsa -aes256 -out institut.key 2048

openssl req -new -sha256 -key ./institut.key -out institut.csr -subj
"/C=SE/O=InstitutNamn/OU=Insattningsgarantiv2/L=Stockholm/CN=InstitutNamn/emailAdd
ress=driftansvarig@institut.se"
```

Det första kommandot skapar den privata nyckeln. Det andra skapar CSR:en.

Allt i det andra kommandot ska skrivas på en rad med mellanslag mellan de olika delarna.

CSR:en hamnar i filen institut.csr och den privata, hemliga nyckeln hamnar i filen institut.key. Byt ut de grönmarkerade fälten mot för er relevanta uppgifter.

Exempel på hur man hanterar svaret från certifikatsutfärdaren.

Den fil som kommer i retur som svar på er CSR innehåller den signerade publika nyckeln och de certifikat som är intressanta för att verifiera signaturen. Filen har filändelsen p7b.

Med OpenSSL:

Konvertera svaret till pem-format med följande kommando:

```
openssl pkcs7 -in institut.p7b -inform DER -print_certs -out institut.pem
```

Editera filen och radera Buypass intermediate-CA-certifikat ur filen men behåll ert eget.

Konkatenera sedan den publika och privata delen genom att kopiera ihop dem till en fil (signeringscert.pem)

```
copy institut.pem + institut.key signeringscert.pem
```

Support

Kontaktvägar vid problem eller frågor:

- Riksgälden besvarar frågor runt certifikatsansökan, filformat, lagkrav etc.
- Instituten förväntas huvudsakligen själva besitta eller på annat sätt ordna kompetens att hantera certifikatet men Riksgälden kan i viss uträckning vara behjälplig med frågor runt implementering och användning. Kontakta då Avdelningen för finansiell stabilitet och konsumentskydd på:
    - ig@riksgalden.se
    - 08 – 613 52 00