



## **Beställning av Förlitandepart-certifikat**

**Version 3.0**

**2016-11-16**

---

---

## Innehållsförteckning

<b>1</b>	<b><i>Bakgrund</i></b> .....	<b>3</b>
1.1	<b>Versioner</b> .....	<b>3</b>
<b>2</b>	<b><i>FP-certifikat för test</i></b> .....	<b>3</b>
<b>3</b>	<b><i>Systemkrav för produkten</i></b> .....	<b>4</b>
3.1	<b>Installera JCE</b> .....	<b>4</b>
<b>4</b>	<b><i>Beställ FP-certifikat för produktion</i></b> .....	<b>5</b>
<b>4.1</b>	<b>BankID Keygen grafisk version</b> .....	<b>5</b>
4.1.1	Starta BankID Keygen på en säker dator .....	5
4.1.2	Påbörja en beställning.....	5
4.1.3	Fyll i informationen om ditt företag .....	6
4.1.4	Skicka certifikatbegäran till banken: .....	8
<b>4.2</b>	<b>Console Applikation</b> .....	<b>9</b>
4.2.1	Starta BankID Keygen på en säker dator .....	9
4.2.2	Påbörja en beställning.....	9
4.2.3	Skicka certifikatbegäran till banken: .....	10
<b>5</b>	<b><i>Installation av FP-certifikat</i></b> .....	<b>10</b>
<b>5.1</b>	<b>BankID Keygen grafisk version</b> .....	<b>10</b>
5.1.1	Färdigt certifikat levererat av bank.....	11
5.1.2	Skapa din PKCS#12 fil .....	11
<b>5.2</b>	<b>Console Applikation</b> .....	<b>12</b>
5.2.1	Färdigt certifikat levererat av bank.....	12
5.2.2	Skapa din PKCS#12 fil .....	12

---

---

# 1 Bakgrund

Detta dokument beskriver hur en förlitande part i Bankernas ID-tjänst kan använda verktyget BankID Keygen för att beställa ett förlitandepartcertifikat (FP-certifikat) för produktionsmiljön. Detta certifikat behövs för att kunna använda BankID-tjänsten för företag som integrerat BankID-tjänsten. Certifikatet används för att identifiera förlitande part och för att användaren skall kunna se vilken tjänst som hen håller på att logga in till eller signera information från.

## 1.1 Versioner

Datum	Version	Beskrivning	Författare
2003-02-14	1.2		BankID
2009-10-23	2.0	Uppdaterat för att återspegla att BankID Keygen skall användas istället för KeyMan	BankID
2009-12-01	2.1	Java version 1.6.0_11 fungerar inte. Beskrev vilka versioner vi testat med.	BankID
2009-12-02	2.2	Java version 1.6.0_11 fungerar visst om sökvägen inte innehåller mellanslag.	BankID
2009-12-08	2.3	Version 1.2 av programvaran är nu släppt för att hantera tidigare problem med Java 1.6.0_1 till 1.6.0_13 då mellanslag i sökvägen till applikationen fanns. Dokumentationen återspeglar nu att det fungerar igen	BankID
2010-09-15	2.4	Uppdaterat med instruktion för installation av Java JCE	BankID
2011-01-25	2.5	Klargjort instruktion för löpnummer	BankID
2011-02-28	2.6	Förlitande part ersätter begreppet Köpare. Lagt till information om "display name".	BankID
2011-04-27	2.7	Längdbegränsning för display name (max 30 tecken).	BankID
2011-10-31	2.8	Förtydligande om display name	BankID
2014-12-31	2.9	Små justeringar.	BankID
2016-11-16	3.0	Ändrat krav för antal tecken i "display name" till 40 samt uppdaterat länkar och Java version.	BankID

## 2 FP-certifikat för test

För testmiljöer så skall man inte beställa certifikat. Instruktioner för hur du hämtar FP-certifikat för test finns på <https://www.bankid.com/rp/info> och i dokumentet "BankID Relying Party Guidelines".

## 3 Systemkrav för produkten

För att kunna köra produkten så krävs det att följande är installerat

- Java Runtime 1.8
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8.
- <http://www.oracle.com/technetwork/java/javase/downloads/index.html> (under Additional Resources)

Applikationen fungerar på de flesta plattformar. BankID har testat på följande:

- Windows Windows 8
- Windows Server 2008
- Ubuntu Desktop 9.04
- MacOSX 10.10

Java versioner som testats är:

- 1.8.0\_73-b02

### 3.1 Installera JCE

På grund av restriktioner för import av krypto behöver Java uppdateras med stöd för ”obegränsad” kryptering.

1. Först måste du ladda ner JCE, det kan du göra här:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

Längst ned på sidan under ”Additional Resources” finns ”Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8”. Ladda ner det.

2. Packa upp och extrahera den nedladdade filen.

Detta kommer att skapa en underkatalog kallad JCE. Den här katalogen innehåller följande filer:

- README.txt
- COPYRIGHT.html
- local\_policy.jar
- US\_export\_policy.jar

3. Installera JAR filer.

Installationen görs genom att ersätta två befintliga filer med de två jar-filerna du laddat ner. Standardplatsen för filerna som skall ersättas är:

För Unix: <java-home> / lib / security. T.ex: /home/user1/jdk1.8.0/

För Windows: <java-home> \ lib \ security. T.ex: C:\Program Files\Java\jre1.8.0\lib\security

För Mac: /Library/Internet\ Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/

Gör först en kopia av de ursprungliga JCE policy filerna (US\_export\_policy.jar och local\_policy.jar) om du senare vill återgå till de ursprungliga versionerna. Nästa steg är att ersätta de två JAR filerna med dem du laddade ner i steg 1.

---

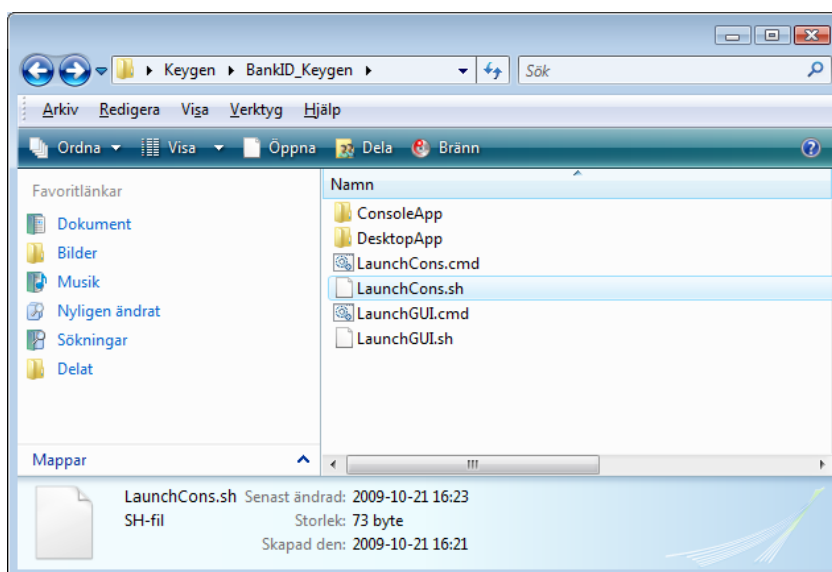
---

## 4 Beställ FP-certifikat för produktion

### 4.1 BankID Keygen grafisk version

#### 4.1.1 Starta BankID Keygen på en säker dator

Packa upp filen ”BankID\_Keygen\_banknamn.ZIP” i en egenvald katalog. BankID Keygen kräver ingen installation utan kan köras från t.ex. ett USB-minne. *banknamn* skall stämma överens med den bank ni har tecknat avtal med. Du skall då ha ett kataloginnehåll enligt nedan:



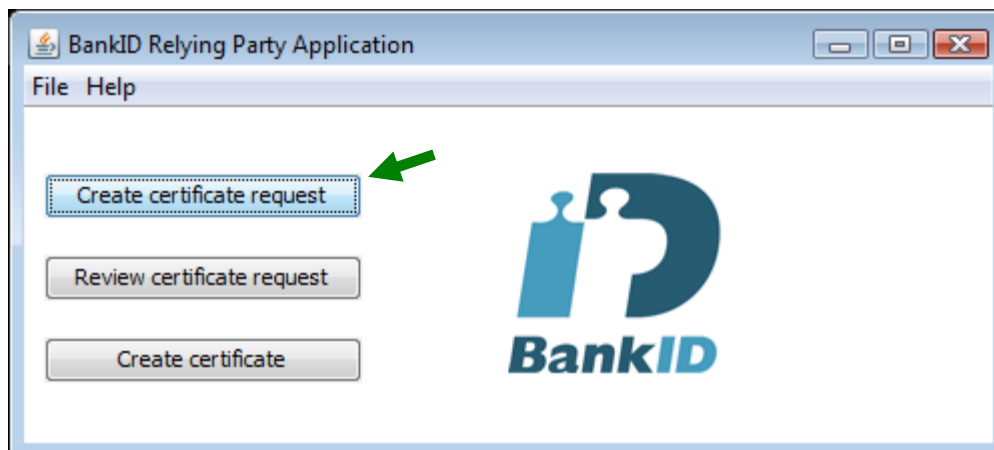
#### 4.1.2 Påbörja en beställning

**Windows:** Dubbelklicka på LaunchGUI.cmd för att starta beställningsprocessen.

**Linux:** Sätt rättigheterna på filen LaunchGUI.sh så att du får köra den ./LaunchGUI.sh

*Om du har problem att starta Keygen kan det bero på att du saknar java-stöd i din dator. Se kapitel 3.*

Klicka sedan på ”Create certificate request”



### 4.1.3 Fyll i informationen om ditt företag

**Ange ”Company name” följt av ev. Tjänstenamn + ev. Löpnummer** : Företagsnamn skall för svenska organisationer vara enligt Bolagsverkets register.

*Tjänstenamn* : Valfritt fält som kan användas för att särskilja olika tjänster hos FP som använder BankID.

*Löpnummer* : börjar på 01 och stegas sedan uppåt. Det används för att särskilja beställningar som ligger nära varandra i tiden och i övrigt är identiska.

Exempel : ”Internetshoppen AB (publ) Webbutiken 01”

**Ange ”VAT number” enligt Bolagsverket eller motsvarande**: Ange ditt företags organisationsnummer enligt Bolagsverket eller motsvarande utan bindestreck eller blanksteg (10 siffror).

**Kontrollera att ”Name of the Bank” är korrekt**: Banknamn skall ange den bank du har tecknat BankID-avtal med.

**Password**: Måste vara minst 12 tecken långt och innehålla minst 4 bokstäver och 1 siffra.

**Display name (max 40 tecken)**: Visas endast för användaren vid legitimering och underskrift och är obligatoriskt. Välj ert registrerade bolagsnamn eller ett mer känt namn som förknippas med er tjänst eller organisation på högst 40 tecken.

Exempel:

**Finansiell ID-Teknik BID AB** är mer känt som **BankID** och kan då använda det i Display name för att visas för användare.

**Telefonaktiebolaget LM Ericsson** är mer känt som **Ericsson** och kan då använda det i Display name för att visas för användare.

En sida för **Windows-support** från **Microsoft** skulle kunna använda **Microsoft Windows Support** som Display name.

***OBS – det är mycket viktigt att du kommer ihåg lösenordet.***

Om du förlorar det finns det inget sätt att återskapa lösenordet.

***Om inte alla dessa uppgifter är helt rätt så kan inte beställningen genomföras. Banken som ni har avtal om BankID med kommer att kontrollera innehållet i beställningen.***

**Tips**: Om du klickar på ”Browse” så kommer applikationen föreslå ett filnamn åt dig.

---

---

**Create Certificate Request**

User Information

Company name: Finansiell ID-Teknik BID AB 01

VAT number: 5566304928

Display Name: BankID

Password: .....

Repeat password: .....

Request file path: orlitande\_cert\_for\_FinansiellID-TeknikBIDAB\_20110415.p10 [Browse]

Private key file path: orlitande\_cert\_for\_FinansiellID-TeknikBIDAB\_20110415.key [Browse]

[Help] [Create certificate request]

Bank Settings

Name of the bank: Bankens namn

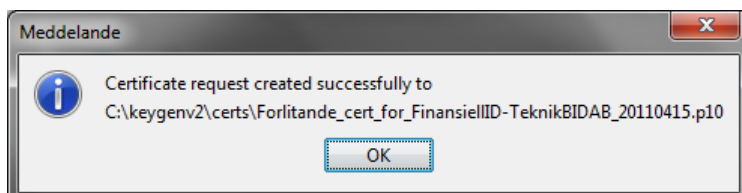
Country code: SE

Key length: 1024

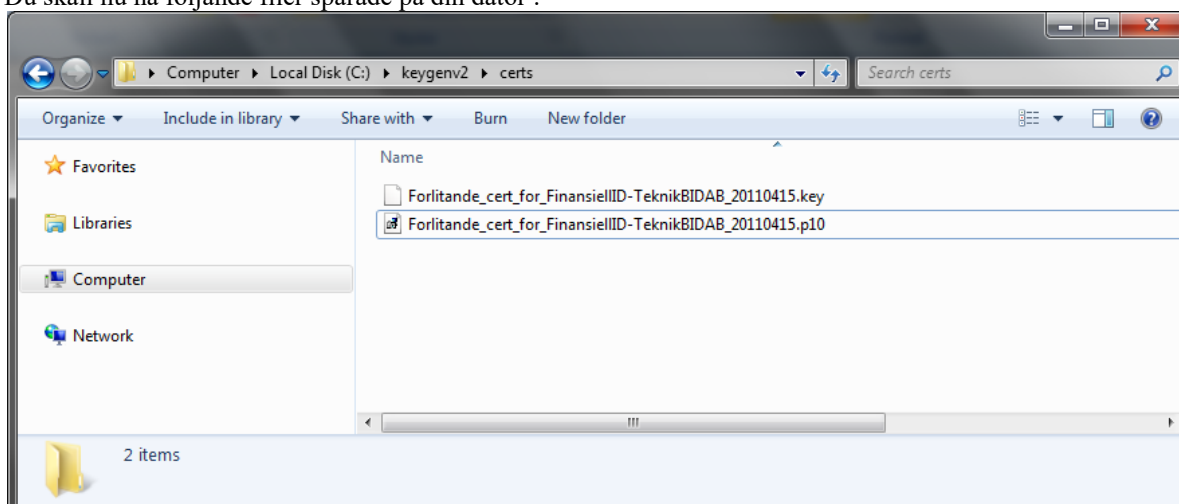
Signature algorithm: sha1WithRSA

Key usage: nonRepudiation

När du är klar klickar du på "Create certificate request". Om allt går bra får du en bekräftelse liknande den nedan.



Du skall nu ha följande filer sparade på din dator :



#### **4.1.4 Skicka certifikatbegäran till banken:**

Du skall nu ge filen med certifikatbegäran (exempel "Forlitande\_cert\_for\_FinansiellID-TeknikBIDAB\_20110415.p10" ) till banken, som du har tecknat BankID avtal med. Du skall ha fått information om mottagare och leveranssätt då du fick programmet och denna instruktion levererad.

När du sedan får tillbaka certifikatet från banken ska du starta med instruktionerna under avsnitt 5.

---

---



## 4.2 Console Applikation

### 4.2.1 Starta BankID Keygen på en säker dator

**Packa upp filen "BankID\_Keygen\_banknamn.ZIP"** i en egenvald katalog. BankID Keygen kräver ingen installation utan kan köras från t.ex. ett USB-minne. Banknamn skall stämma överens med den bank ni har tecknat avtal med.

### 4.2.2 Påbörja en beställning

**Windows:** Från en kommandotolk kör

```
LaunchCons.cmd -createrequest privatekey.key certrequest.txt
```

**Linux:** Sätt rättigheterna på filen LaunchCons.sh så att du får exekevera den och kör sedan

```
./LaunchCons.sh -createrequest privatekey.key certrequest.txt
```

*Om du har problem att starta Keygen kanske du saknar java-stöd i din dator. Se kapitel 3.*

**Ange "Company name" följt av ev. Tjänstenamn + ev. Löpnummer:** Företagsnamn skall för svenska organisationer vara enligt Bolagsverkets register.

*Tjänstenamn* : Valfritt fält som kan användas för att särskilja olika tjänster hos som använder BankID.

*Löpnummer* : börjar på 01 stegas sedan uppåt. Det används för att särskilja beställningar som ligger nära varandra i tiden och i övrigt är identiska.

Exempel : "Internetshoppen AB (publ) Webbutiken 01"

**Ange "VAT number" enligt Bolagsverket eller motsvarande:** Ange ditt företags organisationsnummer enligt Bolagsverket eller motsvarande utan bindestreck eller mellanrum (10 siffror).

**Kontrollera att "Name of the Bank" är korrekt:** Banknamn skall ange den bank du tecknat BankID avtal med.

**Password:** Måste vara minst 12 tecken långt och innehålla minst 4 bokstäver och 1 siffra.

**Display name (max 40 tecken):** Visas endast för användaren vid legitimering och underskrift och är obligatoriskt. Välj ert registrerade bolagsnamn eller ett mer känt namn som förknippas med er tjänst eller organisation på högst 40 tecken.

Exempel **Finansiell ID-Teknik BID AB** är mer känt under **BankID** och kan då använda det i Display name för att visas för användare.

***OBS – det är mycket viktigt att du kommer ihåg lösenordet.***

Om du förlorar det finns det inget sätt att återskapa lösenordet.

***Om inte alla dessa uppgifter är helt rätt så kan inte beställningen genomföras. Banken som ni har avtal om BankID med kommer att kontrollera innehållet i beställningen.***

---

---

```
C:\Windows\system32\cmd.exe
Usage:
To create a certificate request:
ConsoleApp.jar -createrequest privatekey.key certrequest.txt
ConsoleApp.jar -validatecert certrequest.txt
ConsoleApp.jar -createp12 privatekey.key certificate.cer output.p12

C:\keygenv2\ConsoleApp>LaunchBankID.cmd -createrequest Forlitande_cert_for_FinansiellID-TeknikBIDAB_20110415.key Forlitande_cert_for_FinansiellID-TeknikBIDAB_20110415.p10

BankId Relying Party Certificate application
(C) 2009 BankId
Version: 1.3

Your choice: Create Certificate Request

Enter your organizations official name (max 64 characters):
Finansiell ID-Teknik BID AB 01

Enter your organizations official registration number without dash:
5566304928

Enter your display name that will be displayed in "BankID på App":
BankID

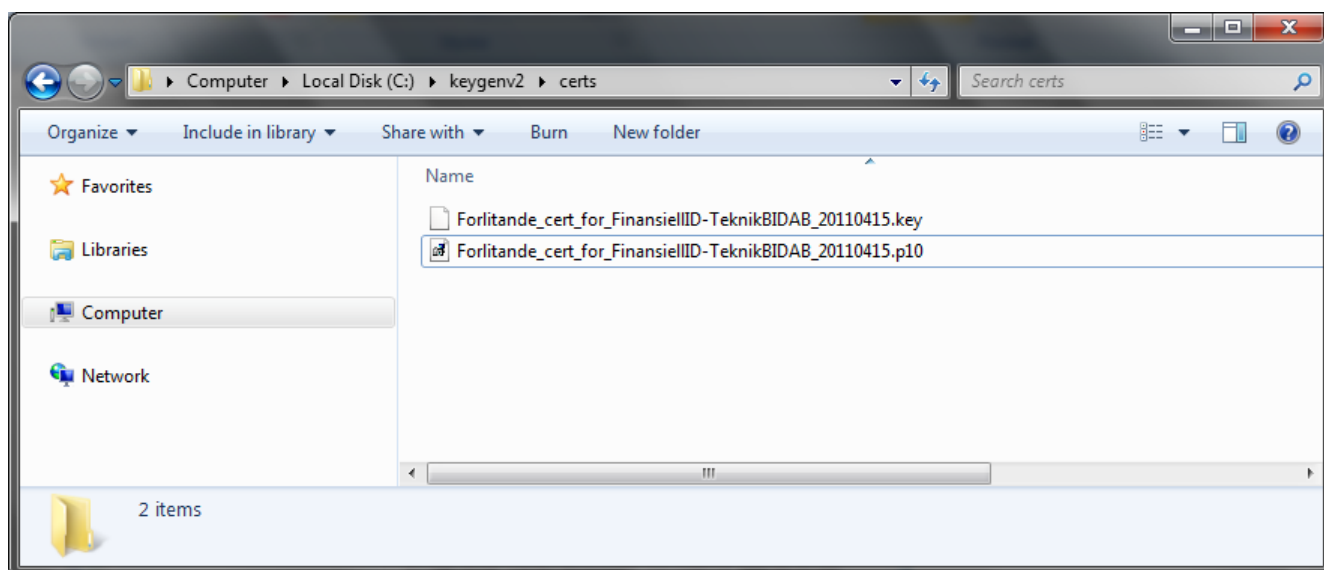
Enter the password that will protect your private key:
123456qwerty
Re-enter the password that will protect your private key:
123456qwerty

The following information will also be used for generating the request:
The name of the bank: Bankens namn
Country code: SE
RSA Key Length: 1024
Signing Algorithm: sha1WithRSA
KeyUsage: nonRepudiation

To continue, press return.

Generating key, please wait
Key generated. Writing request to file "Forlitande_cert_for_FinansiellID-TeknikBIDAB_20110415.p10"
Encrypting private key and writing to file "Forlitande_cert_for_FinansiellID-TeknikBIDAB_20110415.key"
C:\keygenv2\ConsoleApp>
```

Du skall nu ha följande filer sparade på din dator :



#### 4.2.3 Skicka certifikatbegäran till banken:

Du skall nu ge filen med certifikatbegäran (" Forlitande\_cert\_for\_FinansiellID-TeknikBIDAB\_20110415.p10") till banken du tecknat BankID avtal med. Du skall ha fått information om mottagare och leveranssätt då du fick programmet och denna instruktion levererad.

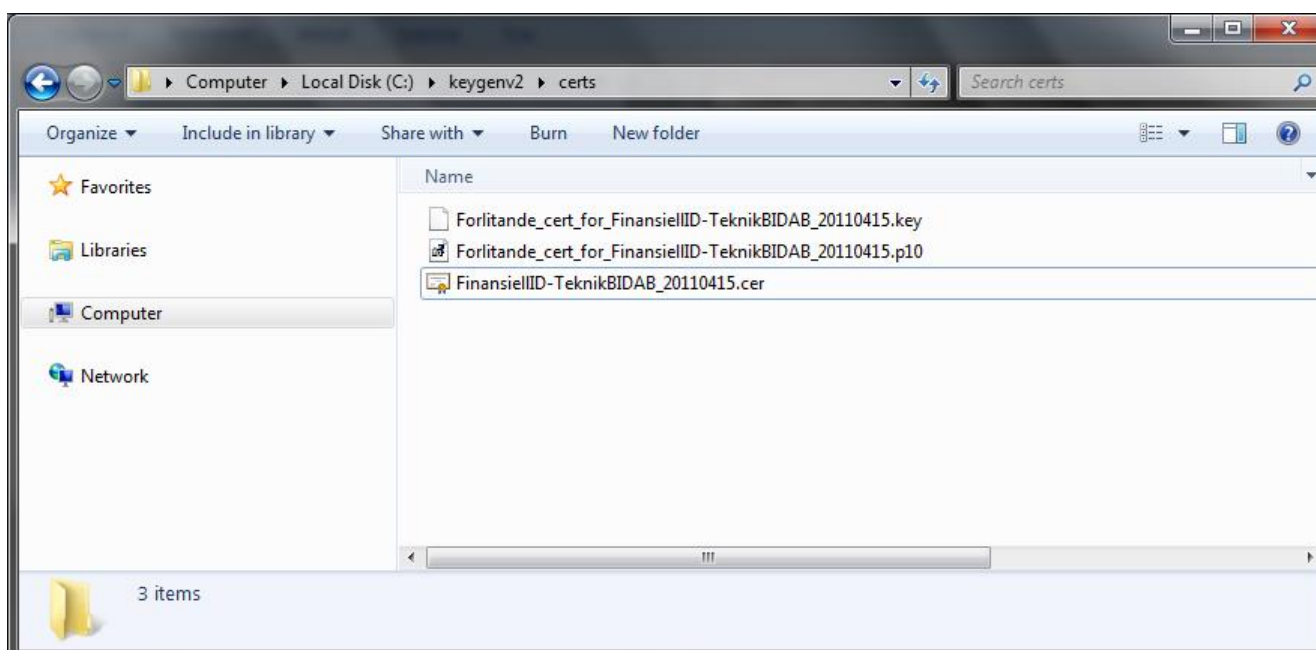
När du sedan får tillbaka certifikatet från banken ska du starta med instruktionerna under avsnitt 5.

## 5 Installation av FP-certifikat

### 5.1 BankID Keygen grafisk version

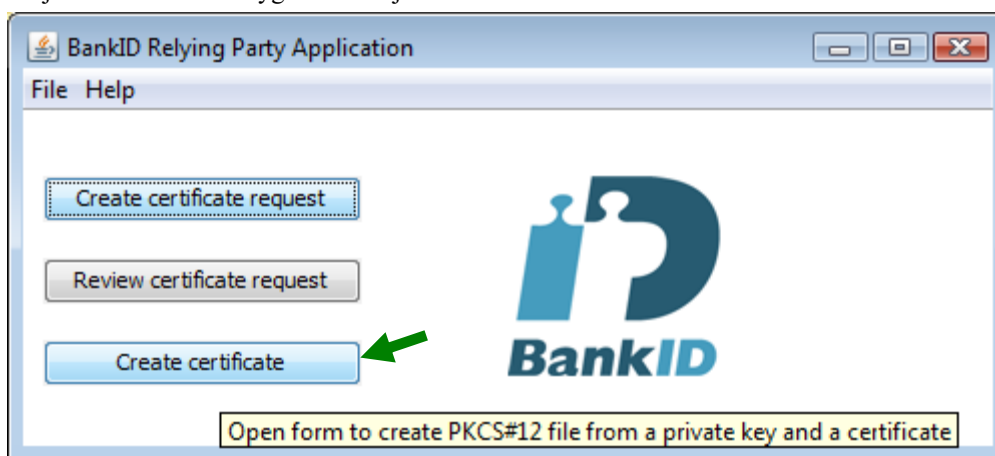
### 5.1.1 Färdigt certifikat levererat av bank

Du kommer att få ett certifikat levererat av din bank.

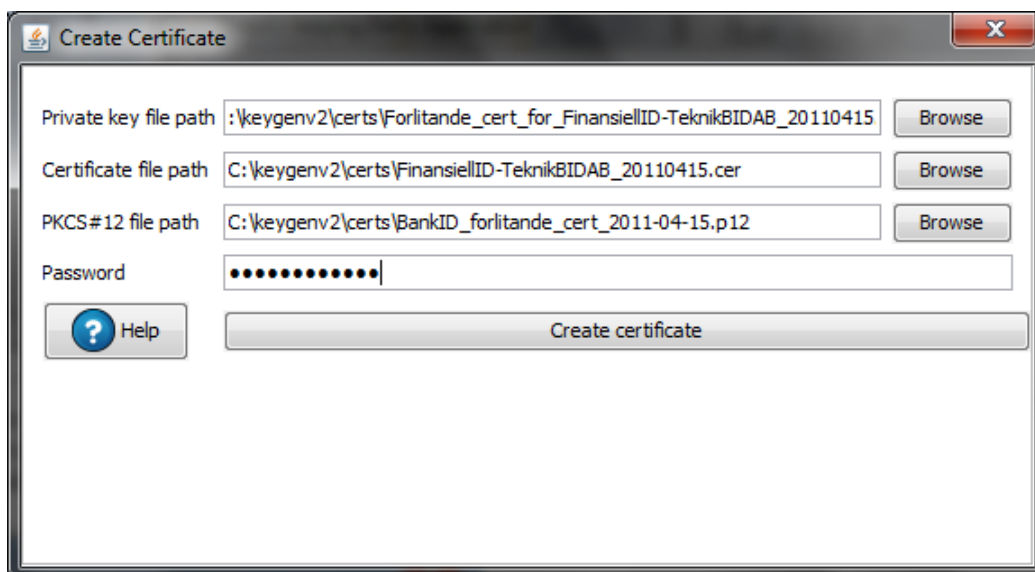


### 5.1.2 Skapa din PKCS#12 fil

Börja med att starta Keygen och välj sedan "Create certificate"



Ange nu sökvägarna till din privata nyckel och till det certifikat du har fått från banken. Ange sedan sökvägen och filnamn till den fil du vill ska skapas. Lösenordet du anger är samma som du angav när du skapade din certifikatsansökan. (Om du inte kommer ihåg detta måste du göra en ny ansökan). Det lösenordet kommer också att vara det nya lösenordet på PKCS#12 filen.



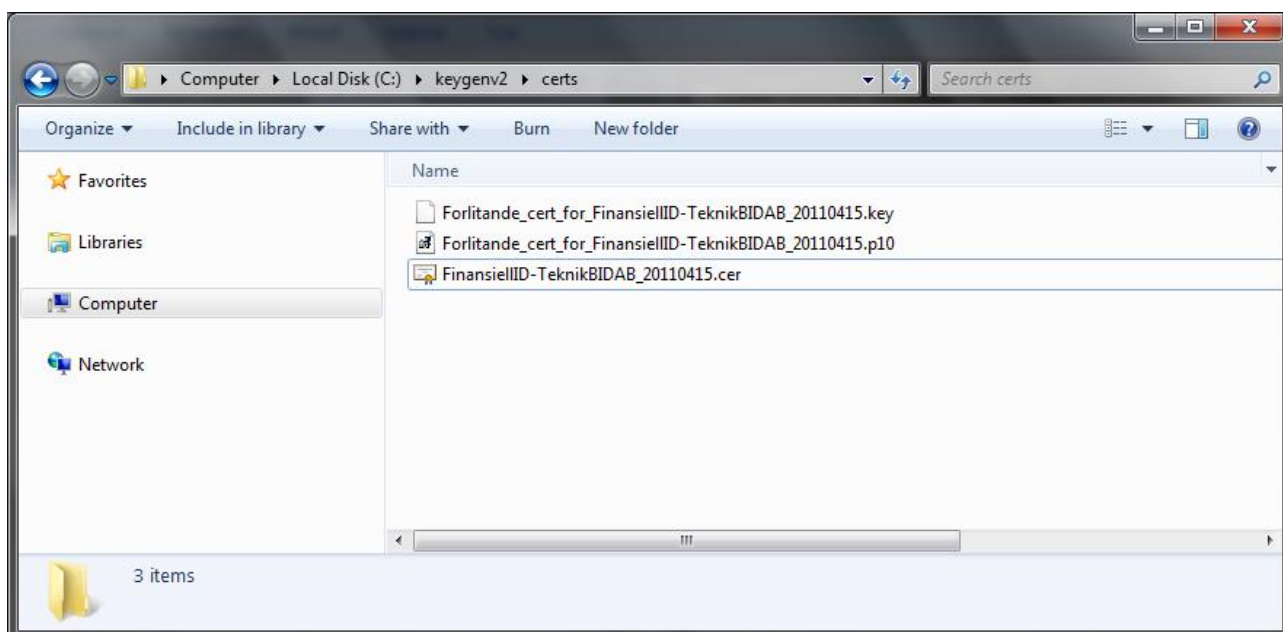
Nu har du ett färdigt FP-certifikat som kan användas i BankID-tjänsten. Se dokumentation för din programvara för att använda certifikatet. Kopiera det från PKCS#12 file path till den plats du önskar.

## 5.2 Console Applikation

### 5.2.1 Färdigt certifikat levererat av bank

Efter en tid kommer du få ett certifikat levererat av din bank. bi

Exempel : "Förlitande\_part\_AB\_(publ)\_webbutiken\_01\_Banknamn\_AB\_20030114-152349.der" där datum och tidpunkt är då certifikatet har skapats.



### 5.2.2 Skapa din PKCS#12 fil

**Windows:** Från en kommandotolk kör

LaunchCons.cmd -createp12 privatekey.key certificate.cer output.p12

**Linux:** kör

./LaunchCons.sh -createp12 privatekey.key certificate.cer output.p12

Kommandot för detta exempel blir alltså:

```
LaunchCons.cmd -createp12 .\certs\Forlitande_cert_for_FinansiellID-  
TeknikBIDAB_20110415.key.\certs\Forlitande_cert_for_FinansiellID-  
TeknikBIDAB_20110415.p10.\certs\  
FinansiellID-TeknikBIDAB_20110415.p12
```

Lösenordet du anger är samma som du angav när du skapade din certifikatsbegäran. (Om du inte kommer ihåg detta måste du göra en ny begäran). Det lösenordet kommer också att vara det nya lösenordet på PKCS#12 filen.

Nu har du ett färdigt FP-certifikat som kan användas i BankID-tjänsten.

---

---