



# **Kundverifiering av SPs digitala signaturer**

**SP Sveriges Tekniska Forskningsinstitut  
SP IT**

## Versionshistorik

Författare	Utgåva	Datum	Kommentar
Fredrik Lorén	1.0	2010-08-12	Första versionen
Fredrik Lorén	2.0	2010-08-27	Uppdatering av automatisk installation
Fredrik Lorén	3.0	2010-09-30	Uppdatering av verifieringsinstruktion
Fredrik Lorén	4.0	2011-08-08	Uppdatering av Adobe version
Fredrik Lorén	5.0	2011-12-05	Uppdatering av kontroll mot spärrlista

## Innehåll

1	Inledning	4
2	Om SP-koncernens lösning för digitala signaturer	5
2.1	Vad är en digital signatur?	5
2.2	Vilka legala krav uppfyller SP:s digitala signaturer?	5
3	Vilka är fördelarna med ett digitalt signerat dokument?	5
4	Vad krävs för att verifiera SP:s dokument	5
4.1	Installationssätt	6
4.2	Automatisk installation via Internet Explorer	6
4.3	Manuell installation	6
4.3.1	Installation av rotcertifikat	6
4.3.2	Inställningar i Acrobat Reader	7
4.4	Installation på flera maskiner samtidigt	8
5	Validering av den digitala signaturen	9

## **1 Inledning**

Detta dokument är en sammanställning över de sätt som en mottagare av ett digitalt signerat dokument från SP-koncernen kan verifiera den digitala signaturen.

För att kunna genomföra en verifiering av SP-koncernens digitala signatur så behöver du göra ett par inställningar på din maskin. Innan du påbörjar detta så läs noga igenom detta dokument. Kontakta gärna även din IT-administratör på ditt företag om du känner dig osäker på något. För att förenkla denna process så har SP-koncernen tagit fram ett antal olika sätt som du kan göra inställningarna på.

## 2 Om SP-koncernens lösning för digitala signaturer

### 2.1 Vad är en digital signatur?

En digital signatur är en elektronisk signatur som kan användas för att styrka identiteten på avsändaren av ett meddelande eller den som har signerat ett dokument och för att säkerställa att det ursprungliga innehållet i meddelandet som har skickats är oförändrad.

### 2.2 Vilka legala krav uppfyller SP:s digitala signaturer?

SP-koncernens lösning för digital signering är standarprodukten CoSign från ARX (Algorithmic Research), [www.arx.com](http://www.arx.com). Lösningen är en traditionell PKI-lösning där varje person som kan signera dokument har ett eget certifikat utfärdat för sig, med en egen privat nyckel som enbart den enskilde certifikatsanvändaren kan använda.

Lösningen skapar rättsligt bindande digitala signaturer i enlighet med:

- UETA – Uniform Electronic Transactions Act - <http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm>
- 15 U.S.C. 7001 (E-Sign) - [http://www.law.cornell.edu/uscode/html/uscode15/usc\\_sec\\_15\\_00007001----000-.html](http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00007001----000-.html)
- EU Directives 1999/93/EC and 2001/115/EC - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:SV:PDF>

## 3 Vilka är fördelarna med ett digitalt signerat dokument?

Fördelarna för dig som kund är flera.

- Med en digital signatur i dokument så kan du styrka identiteten på den som har signerat och du kan även säkerställa att det ursprungliga innehållet i dokumentet är oförändrat.
- Vi har även möjlighet att ge dig en bättre läskvalité, då vi nu slipper att skanna in våra rapporter efter manuell underskrift. Detta är särskilt tydligt när dokumentet innehåller bilder, tabeller och diagram. Även filstorleken blir betydligt mindre än vid inskanning.
- Genom en rationellare hantering inom SP-koncernen kan vi också tillgodose att du får en snabbare och bättre tillgänglighet till dina dokument.

## 4 Vad krävs för att verifiera SP:s dokument

SP-koncernens digitalt signerade dokument är av filtypen PDF. För att verifiera en signerad PDF från SP-koncernen så behöver du ha Adobe Acrobat version 6 eller senare. Nedladdning av Adobe Acrobat kan du göra via länken <http://www.adobe.com/reader>.

En fördel med ett digitalt signerat dokument är att du alltid kan se om dokumentet förändrats efter signering. För att se detta krävs inga installationer.

För att kunna verifiera den som har skrivit under ett digitalt signerade dokument från SP-koncernen så behöver du installera vårt rotcertifikat, samt göra en inställning i din Adobe Acrobat Reader. Du behöver bara göra detta en gång.

För att underlätta detta så erbjuder vi två olika sätt att göra inställningarna. Enklast är att använda vår installationsguide som automatiskt gör installationen.

Beroende på vad du har för operativsystem och webbläsare på din maskin, samt vilka säkerhetsinställningar som du har i din webbläsare, så är det inte säkert att du kan använda den automatiska installationen. Följ då den manuella guiden som lotsar dig genom de olika installations- och konfigurationsstegen. Känner du dig osäker på installationen, så rådfråga din IT-avdelning.

## 4.1 Installationsätt

För att kunna verifiera att signaturen i ditt dokument är korrekt så behöver du göra ett par inställningar på din maskin. Läs först igenom de instruktioner som finns nedan. Känner du dig osäker på något så kontakta gärna din lokala IT-administratör för att rådfråga.

SP-koncernen erbjuder två olika sätt att genomföra installationen på:

- Automatisk installation via Internet Explorer
- Steg-för-steg guide för manuell installation.

De förändringar som genomförs på din maskin är:

- Installation av SP:s rotcertifikat.
- Ändring i Adobe Acrobat Readers inställningar så Acrobat Reader litar på alla certifikat som finns installerade i Windows certifikatarkiv på maskinen.

Beroende på din version av Windows, webbläsaren du använder eller på ditt företags säkerhetsinställningar så kan det hända att installationen inte går att genomföra eller att du saknar rättigheter att genomföra ändringarna. Kontakta i så fall i din IT-administratör för hjälp.

## 4.2 Automatisk installation via Internet Explorer

För att genomföra den automatiska installationen så skall du gå till sidan <http://www.sp.se/sv/digitalsignature/Sidor/verifier.aspx>. Följ där de anvisningar som visas på sidan.

## 4.3 Manuell installation

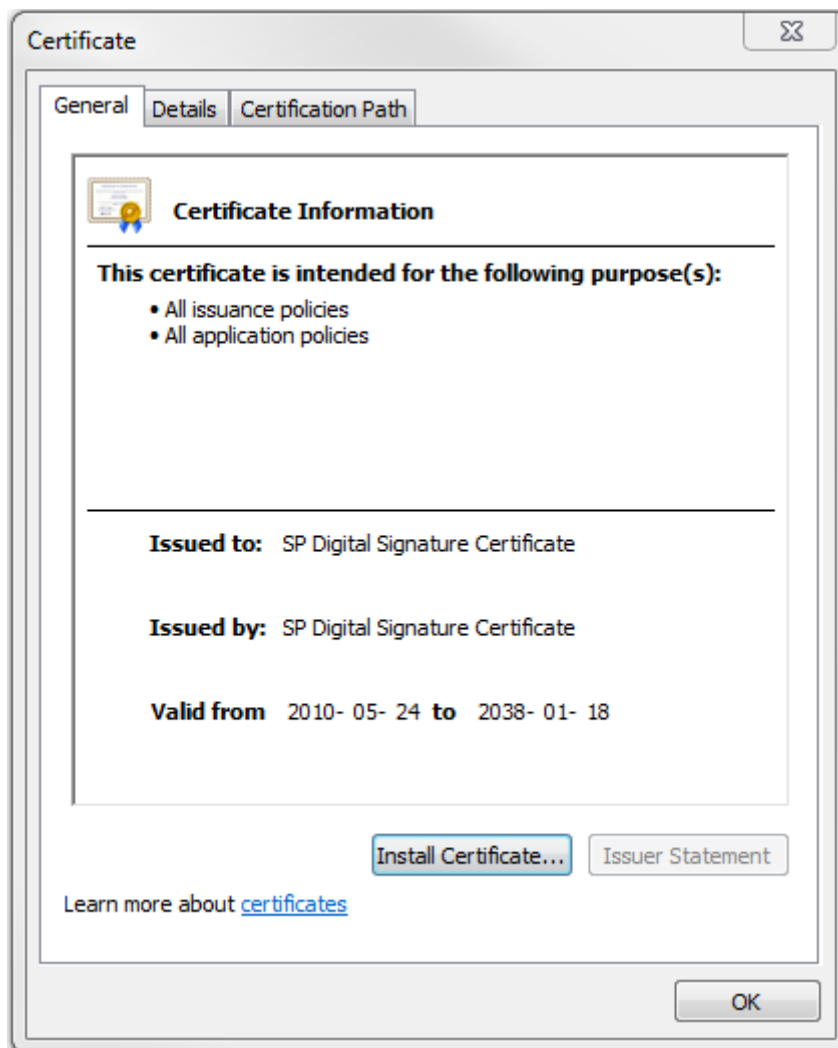
Följande steg visar vilka inställningar du behöver göra för att få det hela att fungera.

### 4.3.1 Installation av rotcertifikat

För att kunna verifiera signaturen korrekt på din maskin så måste du lita på det certifikat som är utställt till den eller de som har signerat dokumentet. Detta gör du genom att installera ett rotcertifikat som är utställt av SP-koncernen. Detta behöver göras en gång per maskin. Är ni flera som skall verifiera dokumenten och ni använder av ett AD (Active directory), kontakta din domänadministratör så kan installation ske för alla användare i domänen samtidigt.

Rotcertifikatet för SP-koncernen laddar du ner via adressen <http://aia.sp.se/SP.crt>

Välj att öppna eller spara ned certifikatet. Sparar du ner certifikatet får du därefter dubbelklicka på den nedladdade filen för att installera.



Tryck på knappen ”Installera certifikat...”

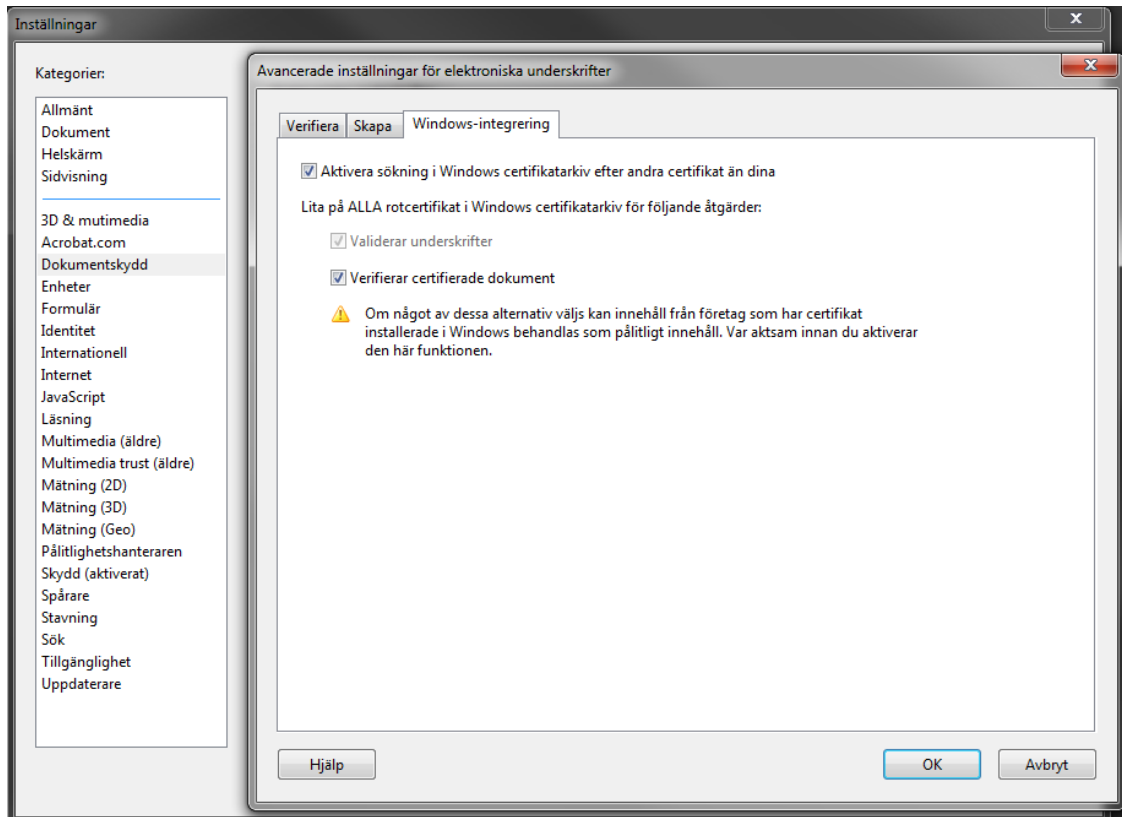
Klicka på Nästa, Nästa tills installationen är slutförd.

Detta slutför installationen av SP:s rotcertifikat i Microsoft Certificate Store på maskinen.

#### 4.3.2 Inställningar i Acrobat Reader

Ändra följande inställningar:

1. Starta Acrobat Reader och gå till Redigera -> Inställningar (Edit -> Preferences)
2. Från panelen till vänster välj ”Dokumentskydd” och tryck på knappen ”Avancerade inställningar” (”Security” och tryck ”Advanced Preferences”).
3. Klicka ur checkboxen ”Begär att spärrkontroll för certifikat ska lyckas när möjligt vid verifiering av underskrifter” (”Require certificate revocation checking to succeed whenever possible during signature verification”). I och med att SP-koncernen använder sig av en centraliserad lösning för signering så krävs ingen kontroll mot spärrlistan.
4. Tryck fliken Windows-integrering (”Windows Integration” tab)
5. Klicka i samtliga checkboxar.



Detta talar om för Acrobat Reader att lita på alla certifikat som finns installerade i Windows certifikatarkiv på maskinen.

#### 4.4 Installation på flera maskiner samtidigt

Är ni flera som behöver kunna verifiera dokument från SP-koncernen inom er organisation, ta kontakt mer IT-administratör och se vilka möjligheter som finns för en gemensam installation via er organisations automatiska installationsrutiner.

1. Installation av Adobe Acrobat Reader 6.0 eller senare, <http://www.adobe.com/reader>.
2. Installation av SP:s rotcertifikat, laddas ner från <http://aia.sp.se/sp.crt>.
3. Anpassningar av inställningar i Adobe Acrobat Readers inställningar att lita på certifikat som finns installerade i Windows certifikatarkiv.

##### Registerinställningar för Acrobat Reader 6.0

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\6.0\Security\cPPKMS]
"bCertStoreImportEnable"=dword:00000001
"iWinTrust"=dword:00000003
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\6.0\Security\cPubSec]
"bReqRevokeCheck"=dword:00000000
```

##### Registerinställningar för Acrobat Reader 7.0

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\7.0\Security\cPPKHandler] "bCertStoreImportEnable"=dword:00000001
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\7.0\Security\cASPKI\cMSCAPI_DirectoryProvider]
"iMSStoreTrusted"=dword:00000062
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\7.0\Security\cASPKI\cASPKI\cVerify]  
"iReqRevCheck"=dword:00000000
```

#### Registerinställningar för Acrobat Reader 8.0

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\8.0\Security\cASPKI\cMSCAPI_DirectoryProvider]  
"iMSStoreTrusted"=dword:00000062
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\8.0\Security\cPPKHandler]  
"bCertStoreImportEnable"=dword:00000001
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\8.0\Security\cASPKI\cASPKI\cVerify]  
"iReqRevCheck"=dword:00000000
```

#### Registerinställningar för Acrobat Reader 9.0

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\9.0\Security\cASPKI\cMSCAPI_DirectoryProvider]  
"iMSStoreTrusted"=dword:00000062
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\9.0\Security\cPPKHandler]  
"bCertStoreImportEnable"=dword:00000001
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\9.0\Security\cASPKI\cASPKI\cVerify]  
"iReqRevCheck"=dword:00000000
```

#### Registerinställningar Acrobat Reader 10.0

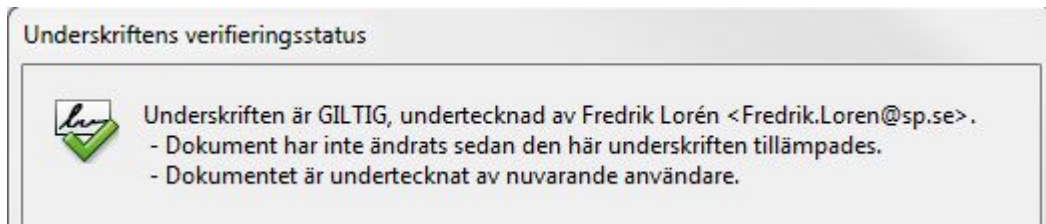
```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\10.0\Security\cASPKI\cMSCAPI_DirectoryProvider]  
"iMSStoreTrusted"=dword:00000062
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\10.0\Security\cPPKHandler]  
"bCertStoreImportEnable"=dword:00000001
```

```
[HKEY_CURRENT_USER\Software\Adobe\Acrobat  
Reader\10.0\Security\cASPKI\cASPKI\cVerify]  
"iReqRevCheck"=dword:00000000
```

## 5 Validering av den digitala signaturen

Öppna PDF dokumentet. Högerklicka på signaturfältet i PDF dokumentet och välj "Validera underskrift". Ser du den gröna bocken så är dokumentet oförändrat efter signering och underskriften giltig.



Om Adobe indikerar att signaturen inte är giltig så kontrollera följande:

- **Är du ansluten till internet?** Vid verifiering av signaturen såg görs en automatisk kontroll mot vår revokeringslista, <http://crl.sp.se/sp.crl>. Du kan även stänga av den här kontrollen i Adobe Acrobat genom att göra följande:
  - o Starta Acrobat Reader och gå till **Redigera -> Inställningar**
  - o Från panelen till vänster välj **Dokumentskydd** och tryck på knappen **Avancerade inställningar**
  - o Under fliken **Verifiera** så checka ur alternativet **Begär att spärrkontroll för certifikat ska lyckas när möjligt vid verifiering av underskrifter.**
- **Har du SP-koncernens rotcertifikat installerat?**
  - o Öppna **Internet Explorer -> Verktyg -> Internetalternativ.**
  - o Välj fliken **Innehåll.**
  - o Klicka på knappen **Certifikat.**
  - o Under fliken **Betrodda rotcertifikatutfärdare** så skall certifikat utfärdat av **SP Technical Research Institute of Sweden** finnas med.

Om certifikatet saknas, så följ instruktionerna under avsnitt 4.3 i detta dokument.