


Vad är ett certifikat?

Ett certifikat består av två delar

- En publik del med information om innehavaren
 - › Innehåller också en publik nyckel
- En privat del som består av den privata nyckeln.
 - › Vilken endast innehavaren av certifikatet ska känna till.

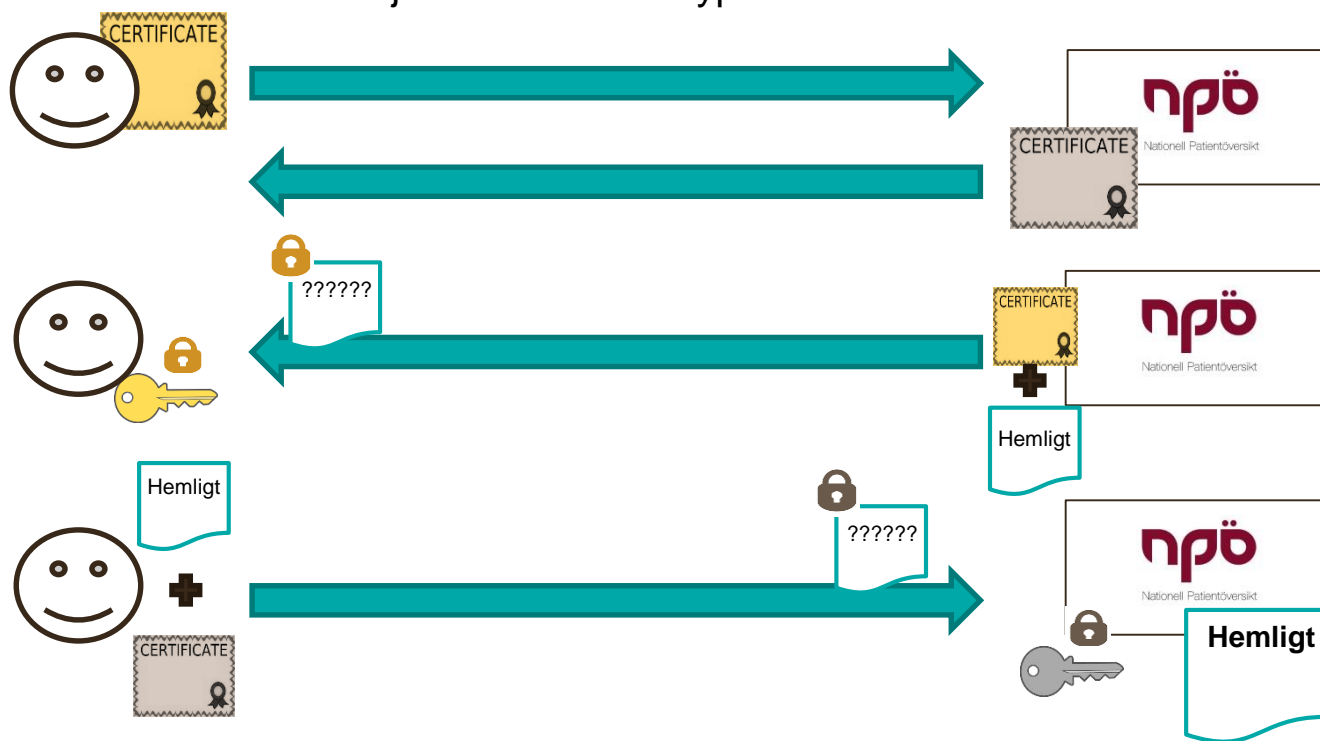


Attribut	
Serienummer	Slumpmässigt unikt värde
Subjekt/Certifikatobjekt	Namn, HSA-id, e-post etc
Publik Nyckel	 Matematiskt beräknad sträng
Utfärdare	SITHS Type 3 CA v1
Giltig från	Ex. 2013-01-01
Giltig till	Ex. 2017-12-01
Med mera...	UPN, e-post etc.



Identifiering med certifikat

- Tjänsten och nyckelinnehavaren utbyter sina publika nycklar
- Tjänsten krypterar information med innehavarens publika nyckel och skickar tillbaka till innehavaren
- Innehavaren dekrypterar informationen med hjälp av sin privata nyckel
- Innehavaren krypterar informationen med tjänstens publika nyckel och skickar tillbaka till tjänsten som dekrypterar den.



Vad är en CSR-fil?

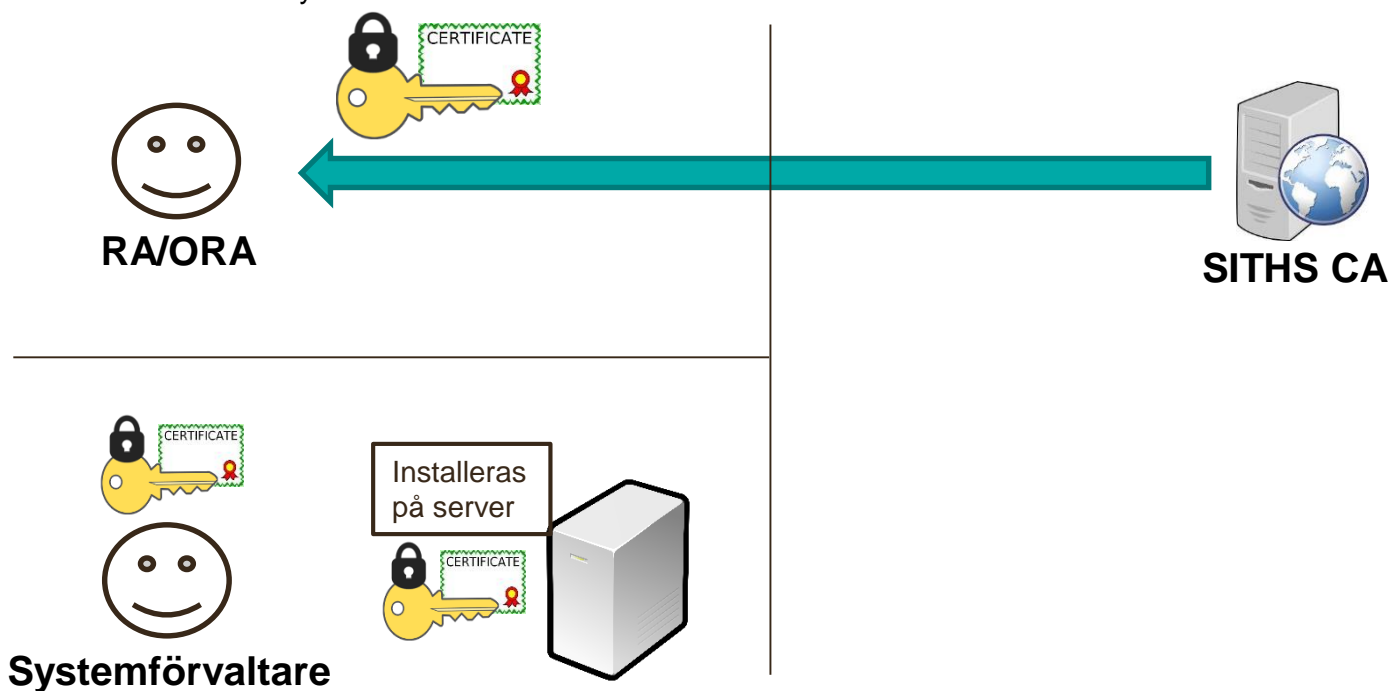
**Skillnader och likheter mellan
PKCS#10 och PKCS#12**

SITHS Type 2 CA v1 ersatt

- Från och med 2015-12-08 utfärdas alla nya SITHS Funktionscertifikat från **SITHS Type 3 CA v1** istället för **SITHS Type 2 CA v1**
 - › Man måste se till att systemen litar på den nya utfärdaren
- HASH-algoritmen blir då SHA-512
 - › Man måste se till att systemen har stöd för SHA-512
- Beställningsmetoden ändras från att även tillåta PKCS#12 till att bara tillåta **PKCS#10**
 - › Se kommande bilder för förklaring av vad detta innebär

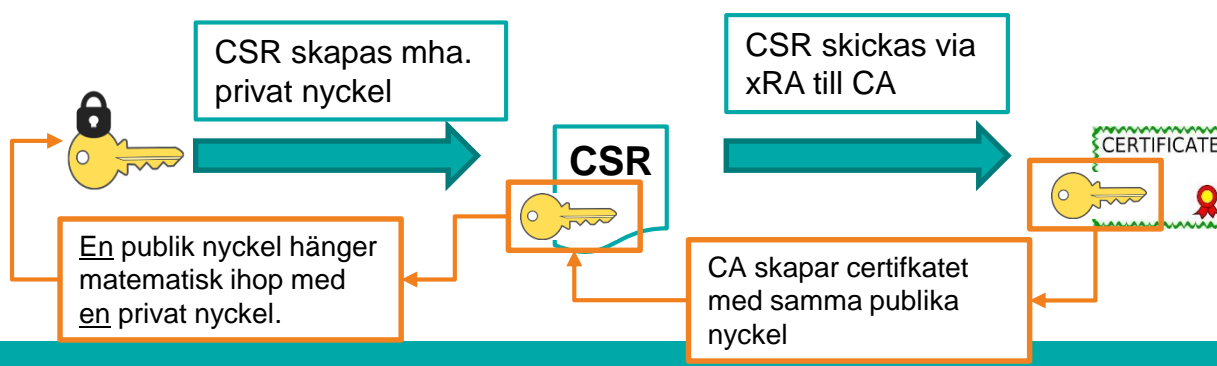
PKCS#12 - Distribution

- PKCS#12 kan ses som en zip-fil innehållande:
 - › Den privata nyckeln
 - › Certifikatet med den publika nyckeln
- Nackdelen är att den privata nyckeln hanteras av andra personer än den som förvaltar systemet den ska till:
 - › Skapas av CA:n
 - › Skickas till xRA
 - › Skickas till Systemförvaltare



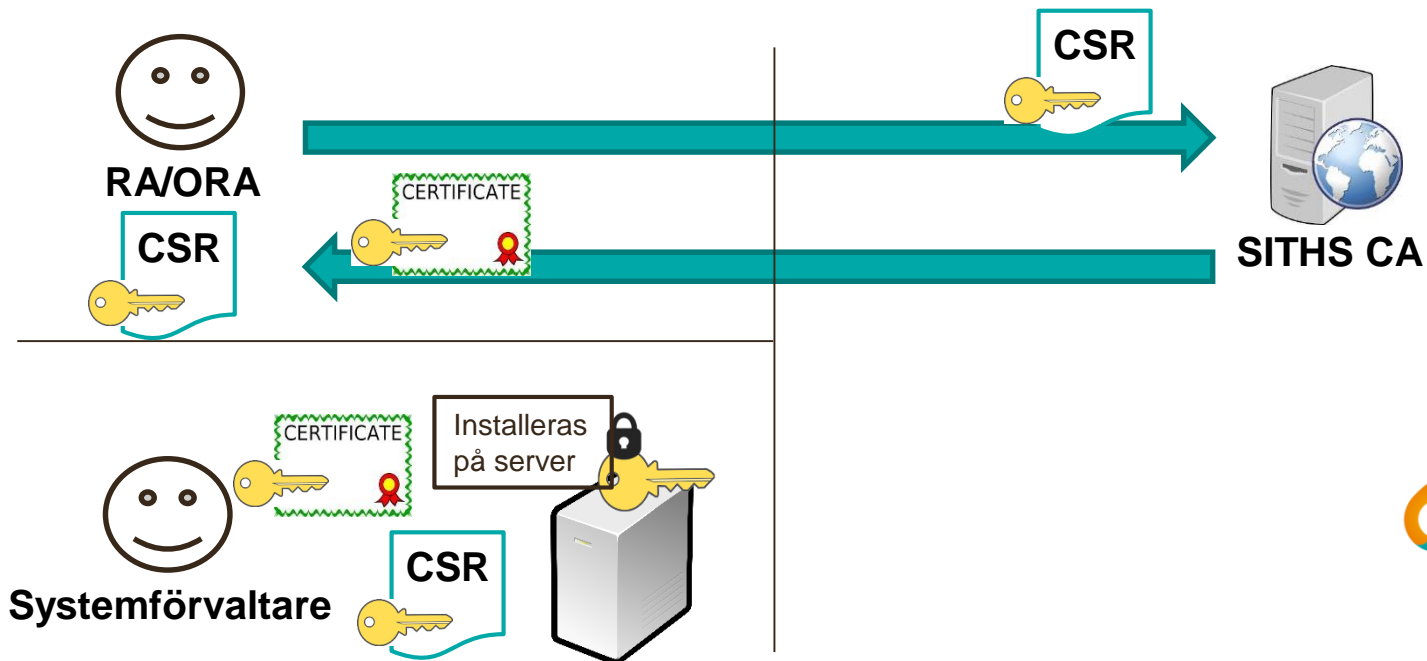
Vad är en CSR-fil

- En CSR-fil kan ses som en undertecknad beställning/förstadie av ett certifikat.
- CSR-filen innehåller samma publika nyckel som sedan används i certifikatet
- För att beräkna den publika nyckeln måste man använda den privata nyckeln
- CA:n tar den publika nyckeln från CSR-filen och skapar ett certifikat.
- Den publika nyckel som används i ett Certifikat passar alltså bara ihop med just den CSR-fil och privata nyckel som skapades i samband med beställningen



PKCS#10 - Distribution

- PKCS#10 är en standard för hur begäran om att signera ett certifikat (CSR-fil) ska se ut.
 - › Nyckelinnehavaren skapar en privat nyckel och en CSR inklusive publik nyckel
 - › CSR ges till xRA
 - › xRA skickar publik nyckel till CA
 - › CA signerar certifikatet inklusive den publika nyckeln
 - › xRA skickar tillbaka certifikatet till nyckelinnehavaren



Jämförelse PKCS#10 och PKCS#12

- P10 och P12 är olika beställningsmetoder inte olika typer av certifikat.
 - P10 – SITHS Admin skapar bara själva certifikatet baserat på den publika nyckeln i den CSR-fil organisationens xRA laddar upp i SITHS Admin.
 - Den privata nyckeln behöver aldrig lämna den egna organisationen.
 - P12 – SITHS Admin skapar den privata nyckeln och paketerar den tillsammans med certifikatet och den publika nyckeln.
- P10 – har ingen säkerhetskod som skickas med krypterad e-post
- P10 – Ansvar för den privata nyckeln hamnar helt hos beställare/nyckelinnehavare
- P10 – Beställaren har själv möjlighet att packa ihop certifikat och privat nyckel till PKCS#12/PFX eller annat format vid flytt.

Hur ser en PKCS#12 fil ut

Properties for 'monitor.test.basefarm.sjunet.org_autentisering.p12'

File: C:\Temp\Certifikat\Test\Interna\Drift\Inera-TSK-54867\monitor.test.basefarm.sjunet.org_autentisering.p12

Type: PKCS12

Provider: BC

Keys

Key Pairs

monitor.test.basefarm.sjunet.org

Private Key

- Algorithm: RSA
- Key Size: 2048 bits
- Format: PKCS#8
- Encoded: 0x30820...
- Public Exponent: 0x...
- Modulus: 0xB23F5...
- Prime P: 0xE0E6BF...
- Prime Q: 0xCAE51...
- Prime Exponent P: ...
- Prime Exponent Q: ...
- CRT Coefficient: 0x...
- Private Exponent: ...

Certifikat

CERTIFICATE

Certificates

monitor.test.basefarm.sjunet.org

- Version: 3
- Subject: SERIALNUMBER=T_SERVICES_SE165565594230-10DX,CN=monitor.test.basefarm.sjunet.org,O=Inera AB,DC=Nod1,DC=Services,C=SE
- Issuer: CN=SITHS Type 2 CA v1 PP,O=Inera AB,C=SE
- Serial Number: A0B9BCF743BCF5F0D9190099AE793831
- Valid From: 07/jan/2015 10:53:34 CET
- Valid Until: 07/dec/2016 23:58:00 CET

Public Key

- Signature Algorithm: SHA1WITHRSA
- MD5 Fingerprint: 3E:91:1B:03:FF:8D:B1:FB:71:DD:04:FA:34:B0:E1:04
- SHA-1 Fingerprint: 59:5D:73:B6:12:5E:5B:41:31:05:1E:7F:C9:56:5D:A4:AB:4D:B9

Hur ser en PKCS#10 fil ut

Properties for 'Untitled-1'

File: Untitled-1
Type: JKS
Provider: SUN

Keys ← ~~Ingen privat nyckel!~~

Key Pairs
None

Trusted Certificates

- type3.test.siths.se (siths type 3 ca v1 pp)
 - Last Modified: 15/jan/2016 16:18:55 CET
 - Version: 3
 - Subject: SERIALNUMBER=T_SERVICES_SE165565594230-108C,CN=type3.test.siths.se,O=Ptest1,DC=Nod1,DC=Services,C=SE
 - Issuer: CN=SITHS Type 3 CA v1 PP,O=Inera AB,C=SE
 - Serial Number: 29E05229143DD65C2C29340A9428D612
 - Valid From: 19/mar/2015 14:48:17 CET
 - Valid Until: 19/mar/2017 23:58:21 CET
 - Public Key ← Publik nyckel
 - Signature Algorithm: SHA512WITHRSA
 - MD5 Fingerprint: F9:CF:7C:6A:6E:E0:11:EB:F5:CA:BF:C1:80:BE:40:C3
 - SHA-1 Fingerprint: 52:98:5A:AE:7C:6B:A3:9E:79:CE:65:46:CB:BC:1C:CB:B2:8F:9A:95

Certifikat

Copy OK