# Vad är ett certifikat?

# Ett certifikat består av två delar

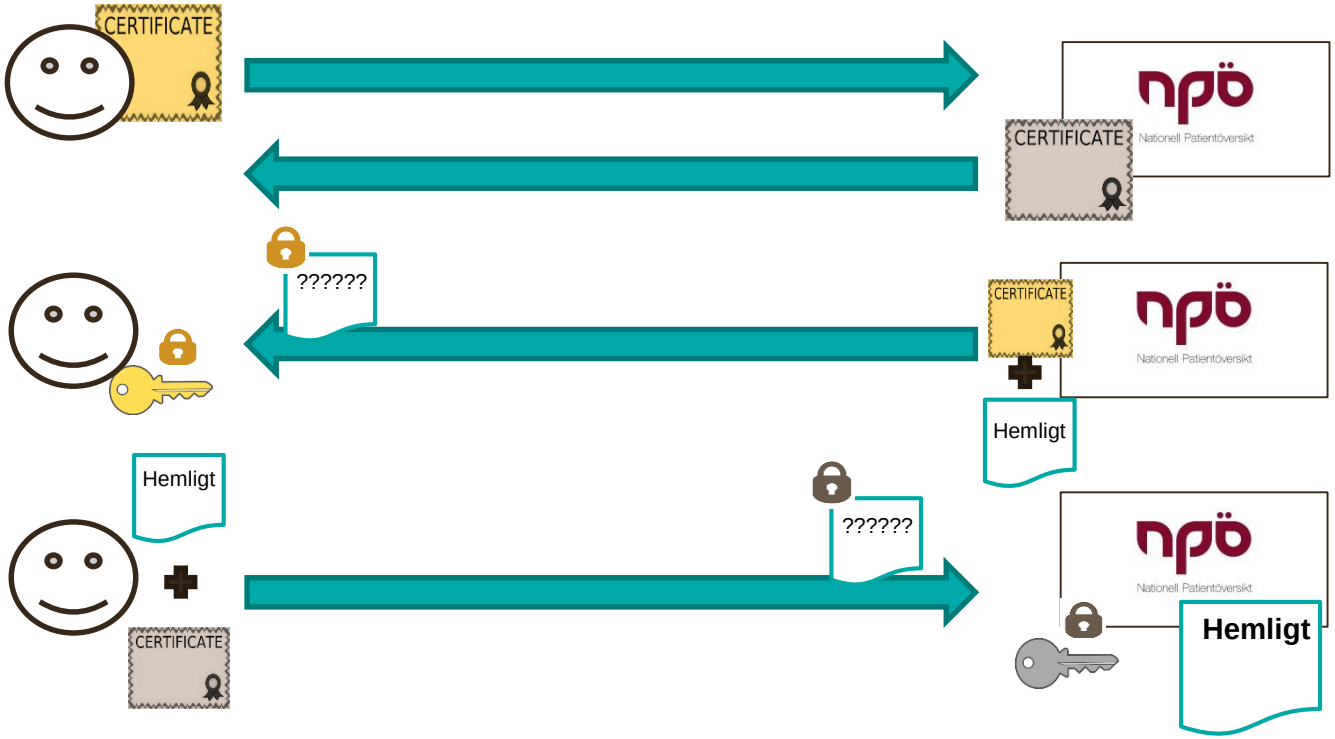
- En publik del med information om innehavaren
  - Innehåller också en publik nyckel
- En privat del som består av den privata nyckeln.
  - Vilken endast innehavaren av certifikatet ska känna till.

| 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. |


inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

# 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.




inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

# Vad är en CSR-fil?

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

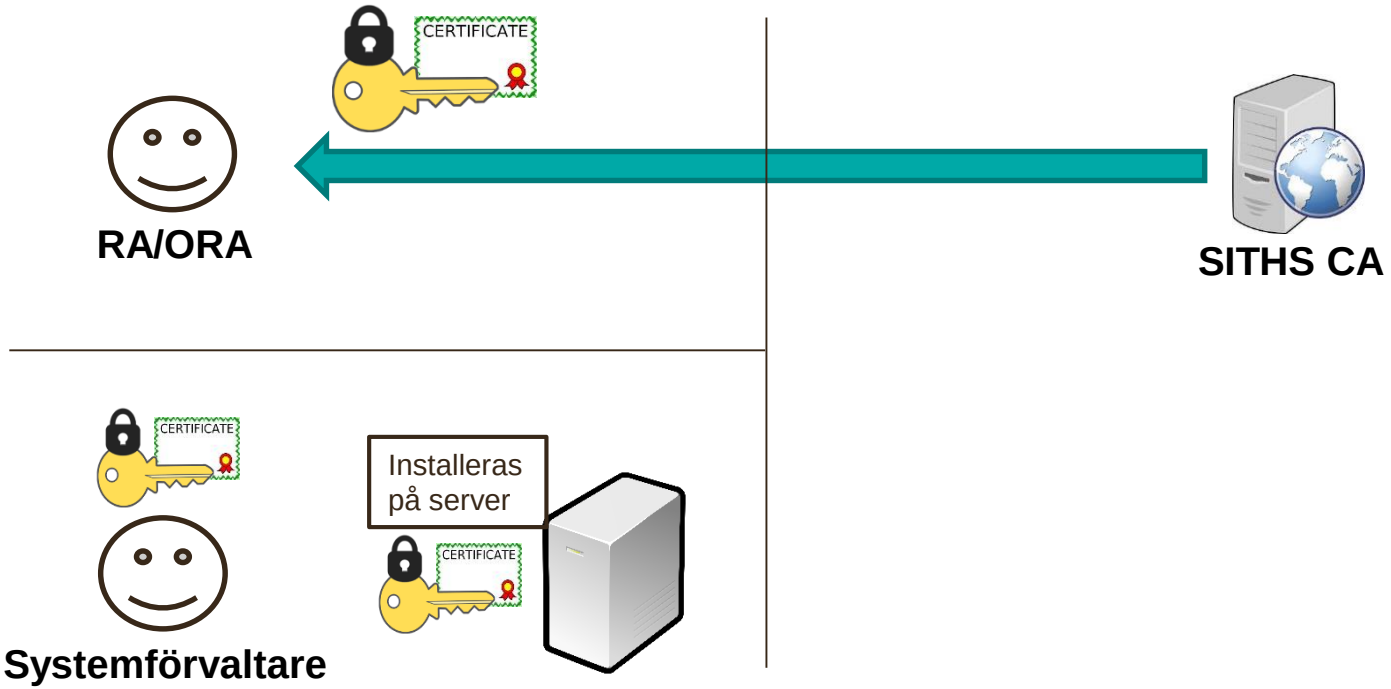
# SITHS Type 2 CA v1 ersatt

- 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

inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

# PKCS#12 - Distribution

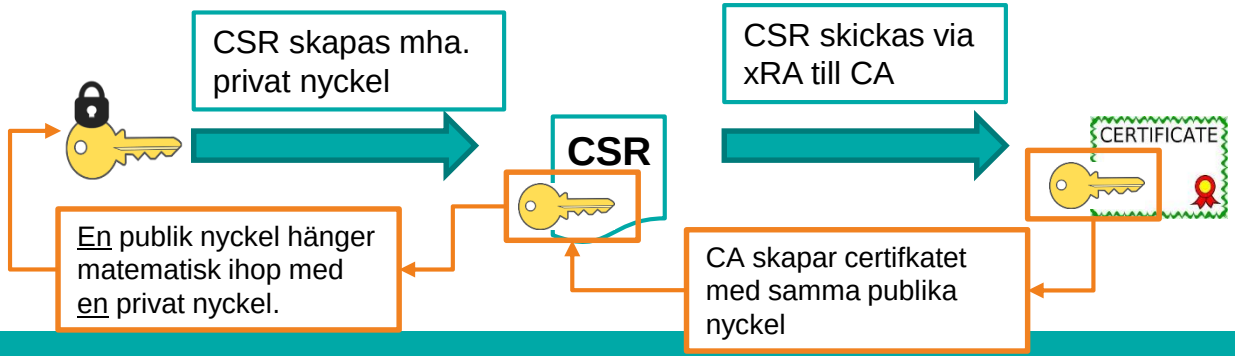
- PKCS#12 kan ses som en zip-fil innehållande:
  - Den privata nyckeln
  - Certifikatet med den publika nyckeln
- Nackdelen är att den privata nyckeln hanteras av andra personer än den som förvaltar systemet den ska till:
  - Skapas av CA:n
  - Skickas till xRA
  - Skickas till Systemförvaltare




inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

# Vad är en CSR-fil

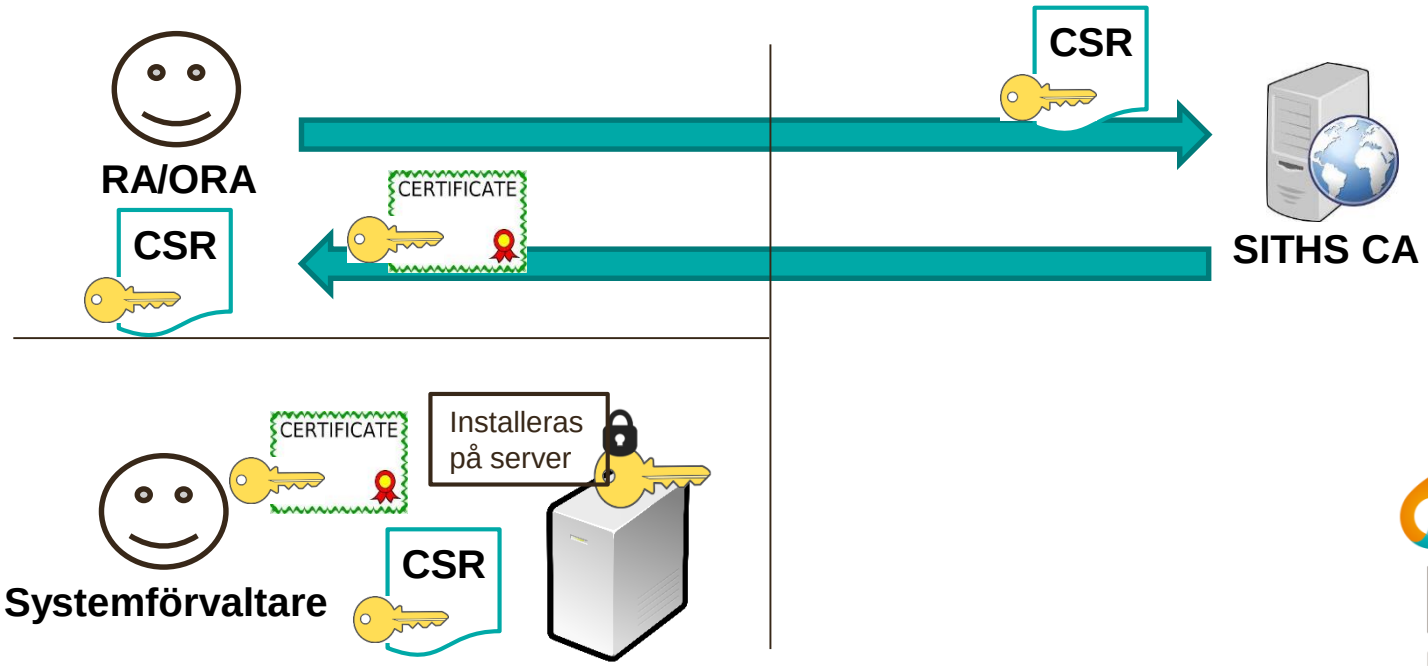
- En CSR-fil kan ses som en undertecknad beställning/förstadie av ett certifikat.
- CSR-filen innehåller samma publika nyckel som sedan används i certifikatet
- För att beräkna den publika nyckeln måste man använda den privata nyckeln
- CA:n tar den publika nyckeln från CSR-filen och skapar ett certifikat.
- 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




inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

# PKCS#10 - Distribution

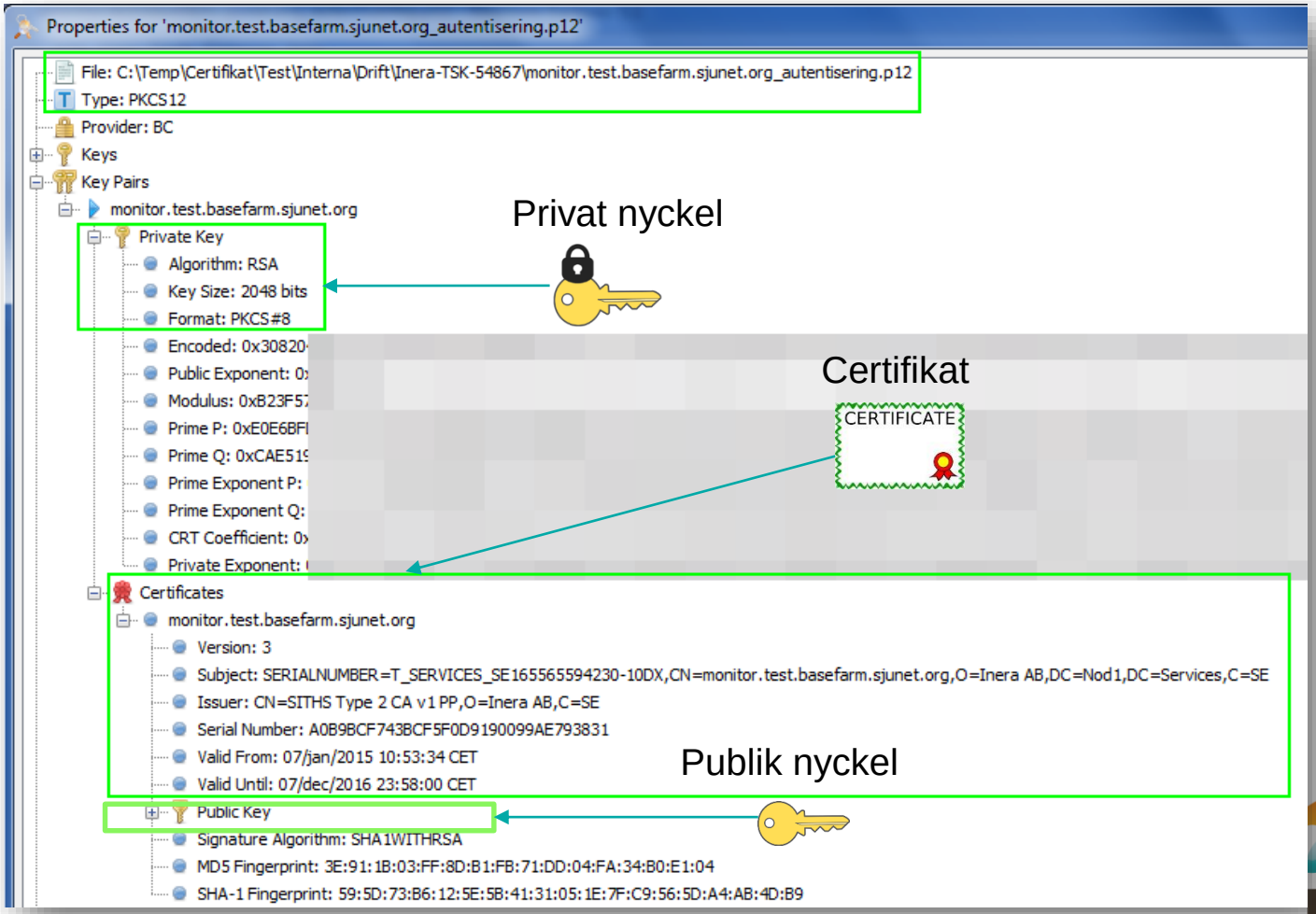
- PKCS#10 är en standard för hur begäran om att signera ett certifikat (CSR-fil) ska se ut.
  - Nyckelinnehavaren skapar en privat nyckel och en CSR inklusive publik nyckel
  - CSR ges till xRA
  - xRA skickar publik nyckel till CA
  - CA signerar certifikatet inklusive den publika nyckeln
  - xRA skickar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



# Hur ser en PKCS#10 fil ut