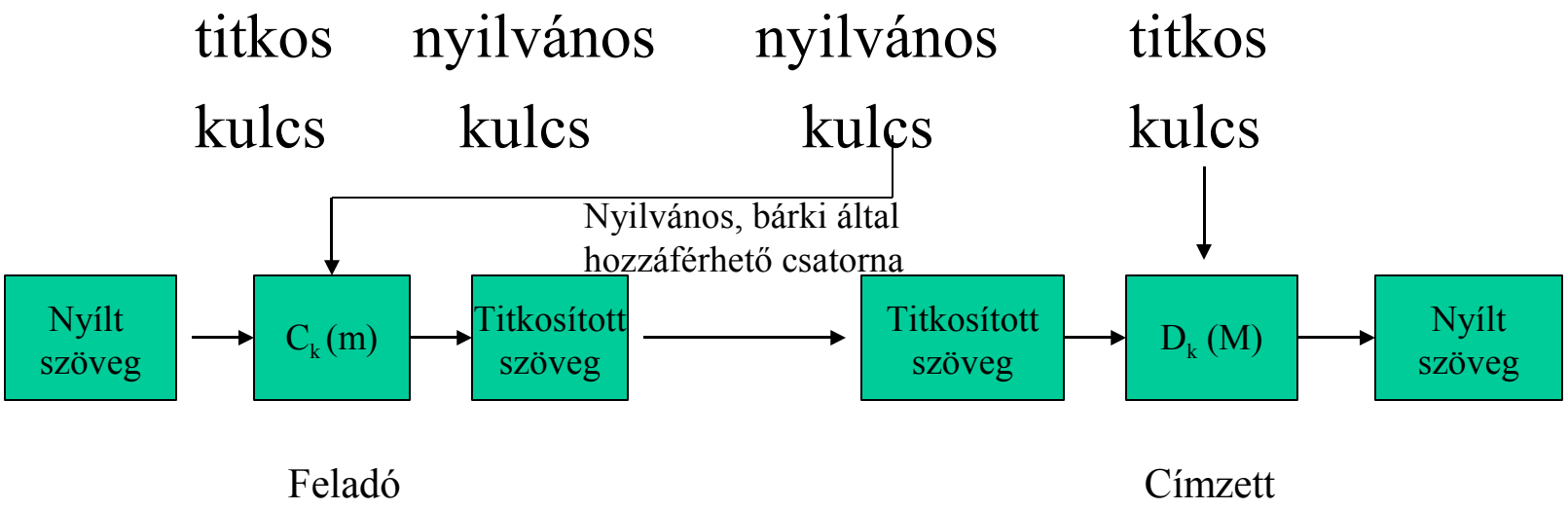
Titkosítás NetWare környezetben

Titkosítás NetWare környezetben

- Nyílt kulcsú titkosítás



Titkosítás NetWare környezetben

Nyílt kulcsú titkosítás

- A titkosítás és megfejtést az $M=C_e(m)$ és az $m=D_d(M)$ egyenletekkel adhatjuk meg. Ahol e és d titkosító ill. megfejtő kulcsok, C és D a megfelelő titkosító és megfejtő eljárások. Ezt az algoritmust és nyílt (e) kulcsot használva bárki tud titkosított üzenetet küldeni a címzettnek, de elolvasni csak a titkos (d) kulccsal rendelkező címzett tudja.

Titkosítás NetWare környezetben

Nyílt kulcsú titkosítás

Nyílt kulcsú titkosítás folyamata biztonsággal:

1. Küldés elött a feladó saját titkos kulcsával rejtjelezi a üzenetet
2. A feladó a címzett nyilvános kulcsával titkosítja az üzenetet
3. A címzett az üzenetet saját kulcsával kibontja
4. Nyilvános kulcstárból lekéri a feladó nyílvános kulcsát

Titkosítás NetWare környezetben
SSL

- A NetWare SSL kommunikációt (Secure Socket Layer) használ
- Az SSL egy titkosított kommunikációt biztosító protokoll
- Legelterjedtebb alkalmazása a HTTP

Titkosítás NetWare környezetben
NICI

- Novell International Cryptographic Infrastructure (NICI). A NICI egy alap titkosítási szolgáltatáskészlet a NetWare 5.x és újabb verzióihoz. Különféle biztonsági funkciókat szolgáltató modulokat és egy konzisztens felületet tartalmaz, amelyet az alkalmazásfejlesztők használhatnak fel. A NICI szolgáltatásokat használó alkalmazásokat vagy szolgáltatásokat fogyasztóknak hívjuk.

Titkosítás NetWare környezetben
PKI

- PKI (Public Key Infrastructure) szolgáltatások
- A PKI a NICI infratruktúra része
- Külső vagy NDS-en belüli CA használható
- NDS-ben tárolható kulcspár, felügyelhető a renszer
- Külső CA használata

Titkosítás NetWare környezetben
PKI

- PKI szolgálatások az NDS-ben új objektumok megjelenésével párosúl
- Új objektumok:
  - Security Container (NDS [root]-ban)
  - Certificate Authority Object (nyílt kulcs, saját kulcs, nyílt kulcs hitelesítés, hitelesítési lánc, konfigurációs információ az NDS CA számára)
  - Key Material Object (nyílt kulcs, saját kulcs, nyílt kulcs hitelesítés, hitelesítési lánc, külön minden alkalmazás számára, a saját kulcs titkosított formában található az objektumban)

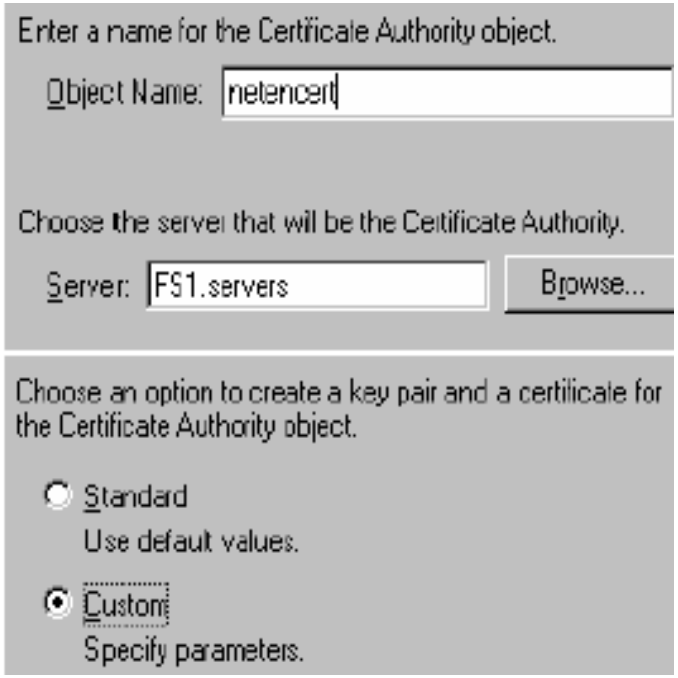
Titkosítás NetWare környezetben

Telepítés

- Telepíteni kell: SAS, PKI Services, NICI Cryptographic programokat
- SAS objektum (Secure Authentication Services) azonosítja az NDSPKI:Key Material objektumokat, amelyek egy adott szerverhez tartoznak

Titkosítás NetWare környezetben

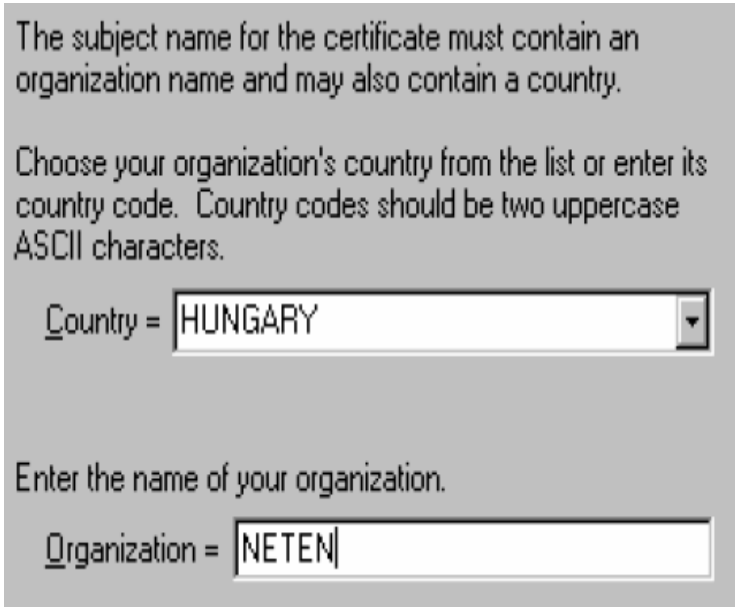
- CA objektum készítése:
  - Security konténerben kell létrehozni, ha nem külső CA-t akarunk használni.
  - Standard megadás esetén csak az objektum neve és a szerver kiválasztása szükséges, a többi automatikus.
  - Custom esetén objektum nevét, valamint a szervert kell kiválasztani.



Titkosítás NetWare környezetben

CA objektum készítése

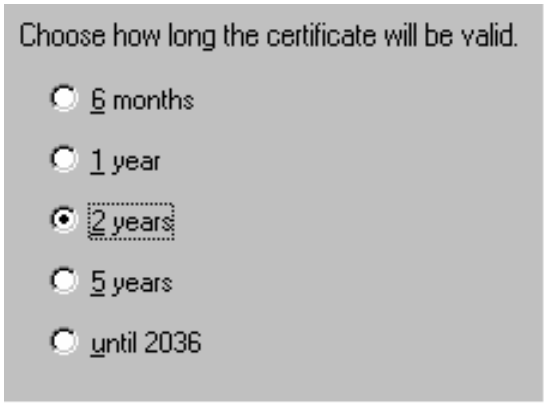
- Következő lépésben a meg kell adnia az ország azonosítót. A szervezet neve az NDS-ből automatikusan kitöltődik, de meg is változtathatjuk

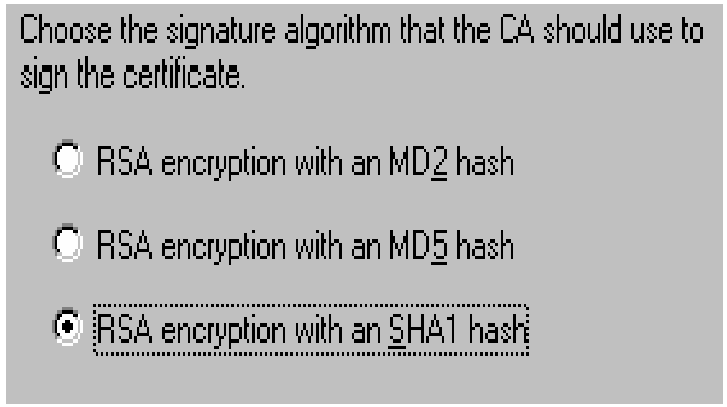


Titkosítás NetWare környezetben

CA objektum készítése

- Továbbiakban megadható a hitelesség érvényességi ideje, a következő lehetőség pedig a titkosítási algoritmus kiválasztása.





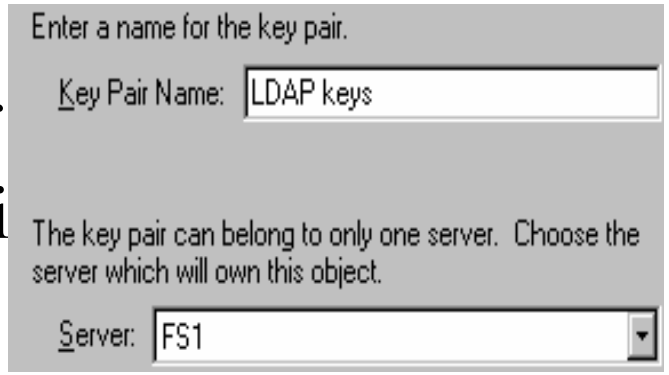
Titkosítás NetWare környezetben

CA objektum készítése

- MD5 (Message Digest 5) Egy olyan egyirányú hashfüggvény, amely egy tetszőleges hosszúságú üzenetből rögzített 128 bit hosszúságú bitsorozatot generál
- SHA1 (Secure Hash Algorithm) 160 bites pecsétet generál (előnye: műveletei száma sokkal több, hátránya: lassabb mint az MD5)

Titkosítás NetWare környezetben

- Key Material objektum készítése
- ha külső CA-t választottunk, akkor az ott kapott kulcsokat kell az objektum létrehozásához felhasználni.
- NDS alapú CA-nál az objektumot a szerverrel egy konténerbe kell létrehoznia.
- Meg kell adnunk a kulcspár nevét,majd ki kell választani a megfelelő szervert

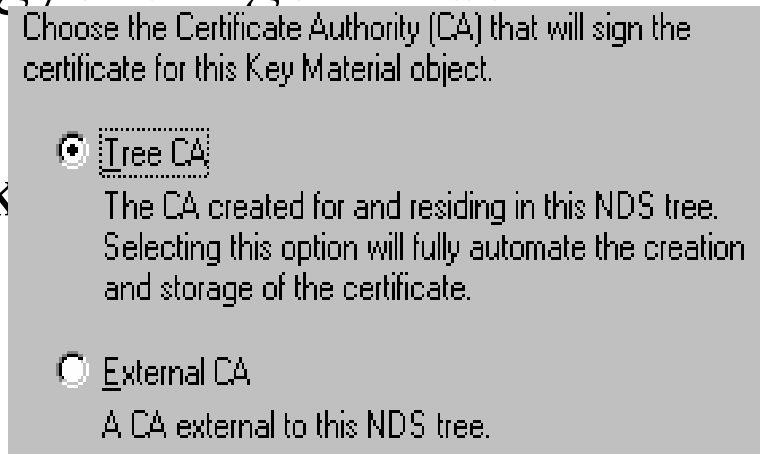


Titkosítás NetWare környezetben

Key Material objektum készítése

Ha NDS CA-t használunk itt megadhatjuk, ha külsőt, az External CA-t kell választanunk.

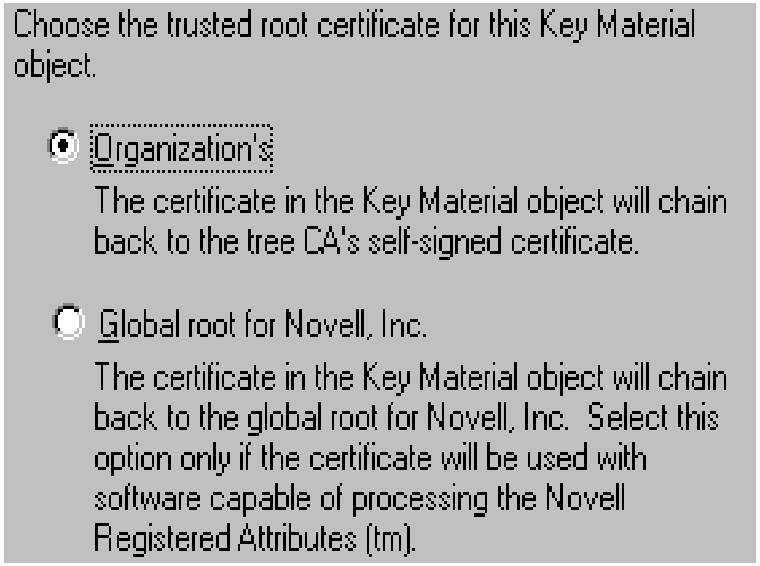
A következő a titkosítási algoritmus megadása, vigyázzunk a CA-val megegyező algoritmust használjunk.Ha külső CA-t választottunk, legenerálódik a kulcsunk, amit meg kell majd adnunk.



Titkosítás NetWare környezetben

Key Material objektum készítése

Ha az NDS a CA-nk, megadhatjuk, hogy a saját fában történjen a hitelesítés, vagy a Novell központi CA-ja segítségével. Ezután legenerálódik a kulcs, amelyet egy üzenet is mutat.



Titkosítás NetWare környezetben

Key Material objektum készítése

Fontos! Ha olyan fákat akarunk egyesíteni,
melyek Security konténerobjektumot tartalmaznak,
az egyiket törölnünk kell.