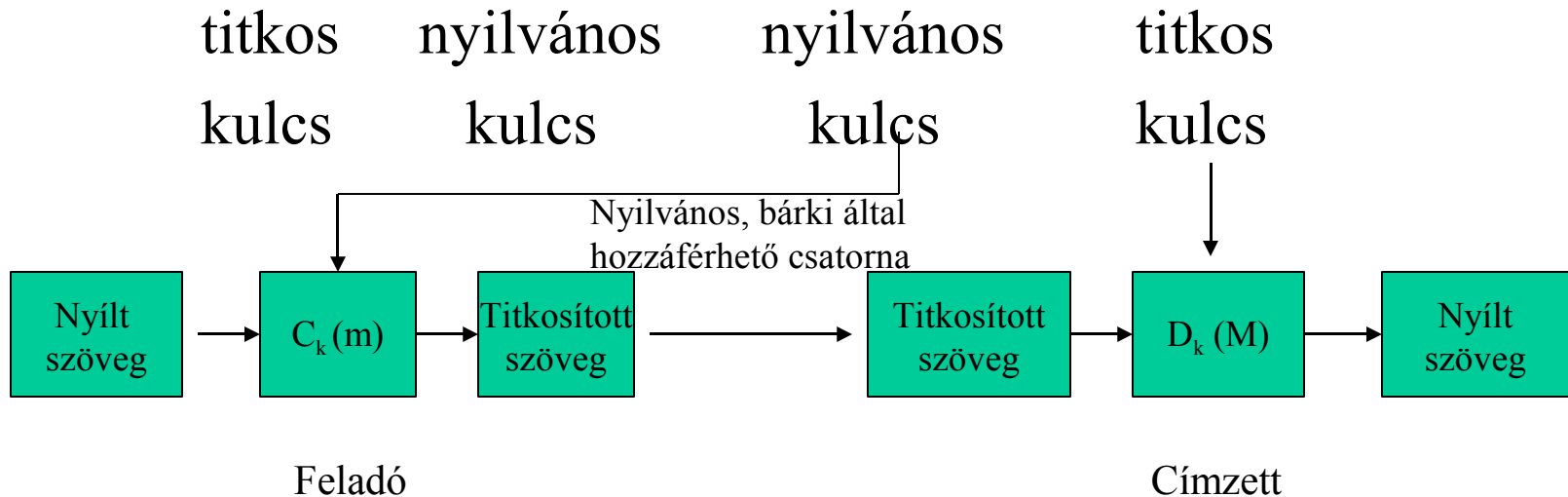


Titkosítás NetWare környezetben

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 előtt 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 nyilvános 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. Különbéféle 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 NDS infratraktúra része
- Külső vagy NDS-en belüli CA használható
- NDS-ben tárolható kulcspár, felügyelhető a rendszer
- Külső CA használata

Titkosítás NetWare környezetben

PKI

- PKI szolgáltatások az NDS-ben új objektumok megjelenésével párosul
- 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, NCI 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.

The screenshot shows a three-step configuration dialog for a Certificate Authority (CA) object in NetWare. The first step is titled "Enter a name for the Certificate Authority object." and contains a text field for "Object Name" with the value "netencert". The second step is titled "Choose the server that will be the Certificate Authority." and contains a "Server:" label, a text field with "FS1.servers", and a "Browse..." button. The third step is titled "Choose an option to create a key pair and a certificate for the Certificate Authority object." and contains two radio button options: "Standard" (with the instruction "Use default values.") and "Custom" (with the instruction "Specify parameters."). The "Custom" option is selected.

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

The subject name for the certificate must contain an organization name and may also contain a country.

Choose your organization's country from the list or enter its country code. Country codes should be two uppercase ASCII characters.

Country =

Enter the name of your organization.

Organization =

Titkosítás NetWare környezetben

CA objektum készítése

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

Choose how long the certificate will be valid.

- 6 months
- 1 year
- 2 years
- 5 years
- until 2036

Choose the signature algorithm that the CA should use to sign the certificate.

- RSA encryption with an MD2 hash
- RSA encryption with an MD5 hash
- RSA encryption with an SHA1 hash

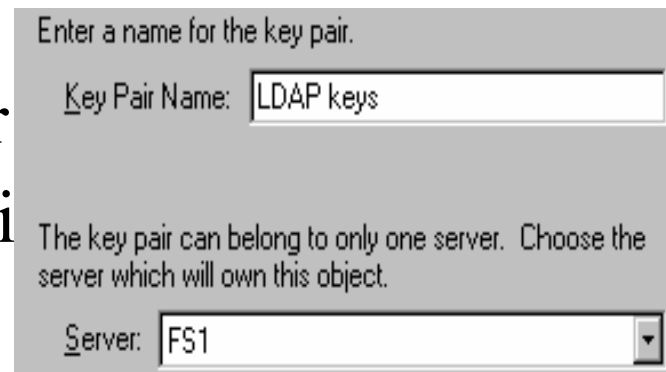
Titkosítás NetWare környezetben

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 létrehozni.
- Meg kell adnunk a kulcspár nevét, majd ki kell választani a megfelelő szervert



Enter a name for the key pair.

Key Pair Name:

The key pair can belong to only one server. Choose the server which will own this object.

Server:

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.

Choose the Certificate Authority (CA) that will sign the certificate for this Key Material object.

Tree CA

The CA created for and residing in this NDS tree. Selecting this option will fully automate the creation and storage of the certificate.

External CA

A CA external to this NDS tree.

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.

Choose the trusted root certificate for this Key Material object.

Organization's

The certificate in the Key Material object will chain back to the tree CA's self-signed certificate.

Global root for Novell, Inc.

The certificate in the Key Material object will chain back to the global root for Novell, Inc. Select this option only if the certificate will be used with software capable of processing the Novell Registered Attributes (tm).

Titkosítás NetWare környezetben

Key Material objektum készítése

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