

Nyilvános Kulcs Infrastruktúra

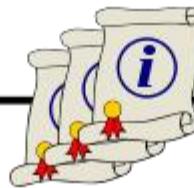
Nyilvános Kulcs Infrastruktúra Public Key Infrastructure (PKI)

Nyilvános Kulcs Infrastruktúra

azon hardver, szoftver, emberi erőforrások, szabályzatok, eljárások összessége, melyek szükségesek tanúsítványok létrehozására, kezelésére, terjesztésére, használatára, tárolására és visszavonására.

PKI

Hitelesítő hivatal



Tanúsítványtár



Regisztráló szervezet



From Wikipedia, the free encyclopedia

A PKI szolgáltatók felépítése

- **Regisztrációs hivatal** (RA – registration authority) feladata:
 - Az ügyfelek megbízható hitelesítése.
 - A tanúsítvánnykérés összeállítása és továbbítása.
 - Tanúsítvány visszavonási kérések fogadása.

A PKI szolgáltatók felépítése

- **Hitelesítő hivatal – CA** (certification authority) feladatai:
 - Tanúsítvánnykérések fogadása.
 - Kulcspárok generálása a különböző implementációk esetén.
 - A nyilvános kulcsú tanúsítványok kiállítása.
 - A kiadott tanúsítványok közzététеле a nyilvános tanúsítvántárban.
 - Korábban kiadott tanúsítványok és szükség esetén kulcspárok megújítása.
 - Tanúsítványok visszavonása.
 - A visszavont tanúsítványok listájának közzététеле (publikálása) a tanúsítvántárban.

CA jellemzői

- A CA védelme (fizikai, logikai) alapvető fontosságú.
- Egy CA kiadhat tanúsítványt felhasználók vagy más tanúsítványkiadók részére (akár mindkettő).
- Felhasználó tanúsítványok esetén szavatolja, hogy a tanúsítványban szereplő publikus kulcshoz tartozó privát kulcs a tanúsítványban szereplő entitás birtokában van. Egyéb információk (pl elérhetőség, eljárásrend, felhasználhatósággal kapcsolatos infók) feltüntetésével, azok helyességét is szavatolja.

CA jellemzői

- A CA minden tanúsítványban elhelyezi saját nevét és aláírja azt, ezáltal, ha a CA megbízható, akkor a tanúsítvány is.
- A CA titkos kulcsa az alapja az összes általa aláírt tanúsítványba vetett bizalomnak, ezért a CA legfontosabb feladata a saját titkos kulcsának védelme.

A PKI szolgáltatók felépítése

- **Tanúsítványtár**

- Speciális **adatbázis**, amely tartalmazza
 - a CA által kibocsátott tanúsítványokat,
 - a visszavont tanúsítványok listáját,
 - egyéb, a tanúsítványra vonatkozó adatokat.
- **Feladata:** bármely tanúsítvány állapotáról valós időben információt szolgáltasson.
- **Szolgáltatásai:**
 - Biztosítja az ügyfeleket egy adott tanúsítvány hitelességéről.
 - Biztosítja az ügyfeleket egy adott tanúsítvány érvényességéről.

A tanúsítványok életciklusa

- A tanúsítvány kiadása.
- A tanúsítvány használata.
- A tanúsítvány visszavonása.

A tanúsítvány használata

- A tanúsítványok szerepe: **egy adott személy, szervezet vagy szerver és egy publikus kulcs közötti kapcsolat igazolása.**
 1. Az alkalmazás működése közben olyan pontra ér, ahol valamelyik fél publikus kulcsára van szükség. (pl digitális aláírás, aszimmetrikus titkosítás, felhasználó hitelesítés)
 2. Az alkalmazás ekkor valamely szabvány segítségével elkéri a szolgáltató tanúsítványtárából a tanúsítványt. **Ellenőrzi a rajta lévő aláírást.** Ha az nem hiteles, vagy a tanúsítvány érvénytelen, akkor **az alkalmazás megakad, biztonsági intézkedés következik.**

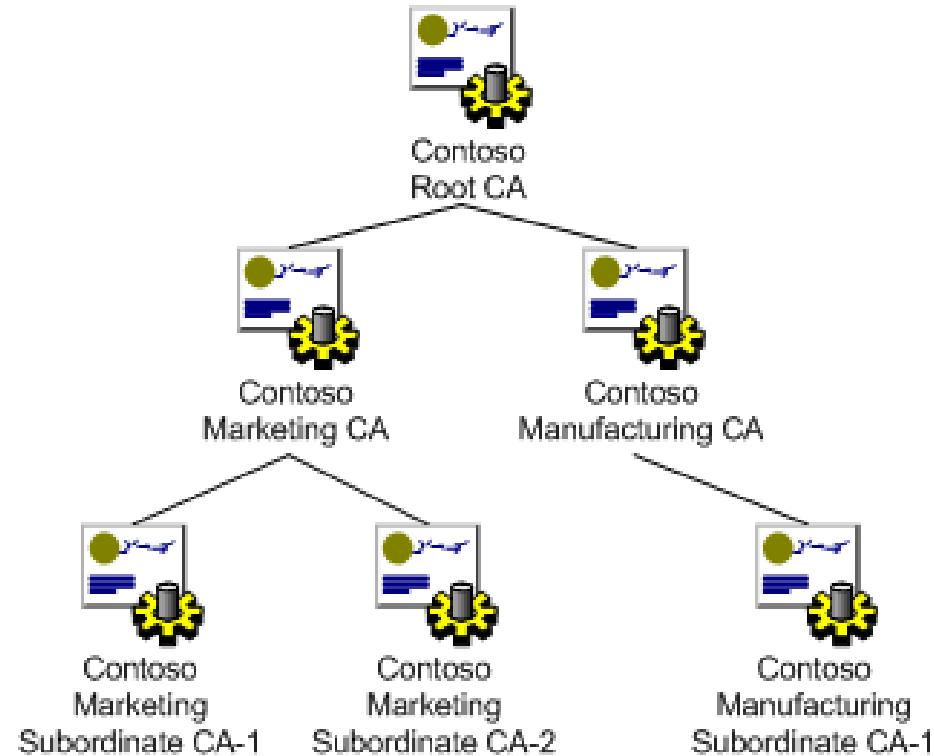
A tanúsítvány használata

3. Amennyiben a tanúsítvány hiteles és érvényes, az alkalmazás eldönti, hogy a kiállító hitelesítő szervezet megbízható-e vagy sem. A legtöbb PKI-t használó szoftver rendelkezik egy beépített listával a megbízhatónak megítélt hitelesítő szervezetekről. Ha a szolgáltató nincs benne ebben a listában, akkor az alkalmazás a hitelességszolgáltató aláíró tanúsítványának kiállítójához fordul.
4. Az alkalmazás mindaddig ismétli a 2. és a 3. lépéseket, amíg megbízható hitelességszolgáltatóhoz nem jut, vagy pedig óvintézkedésekre nem kerül sor.

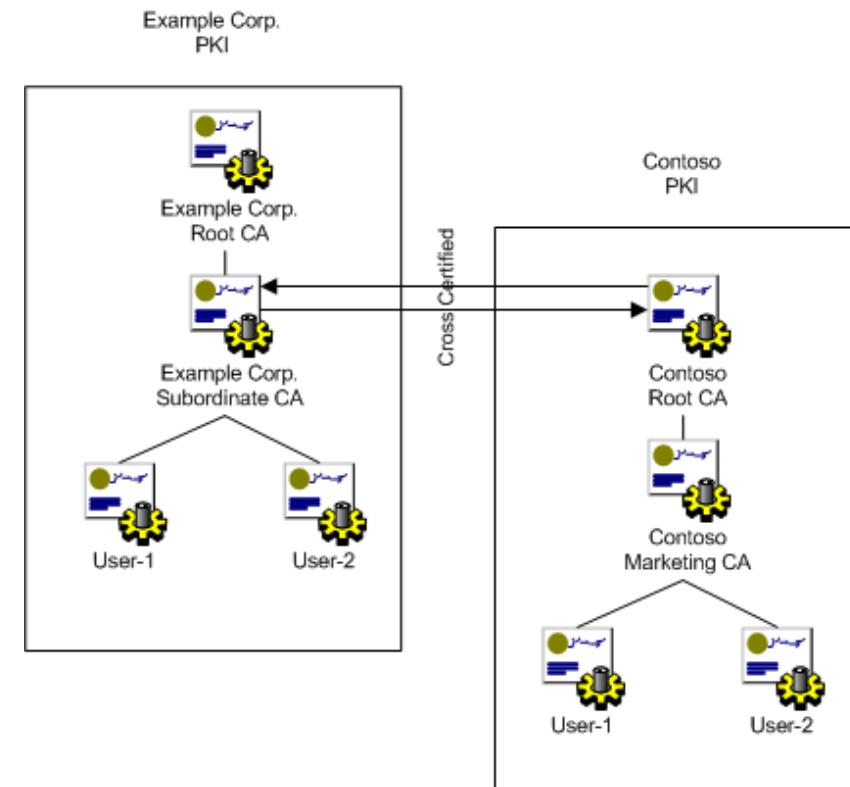
A tanúsítvány felépítése - szabványosítva

- Verzió
- Sorozatszám
- Aláírási algoritmus
- Aláírás-kivonatoló algoritmus
- Kiállító
- Érvényesség kezdete
- Érvényesség vége
- Tulajdonos
- Nyilvános kulcs
- Ujjlenyomat-algoritmus
- Ujjlenyomat

Hierarchia alapú hitelesítés



Kereszthitelesítés



Tanúsítványok visszavonása

Visszavonási lista (Certificate Revocation List):

A hitelesítés szolgáltató által kiadott tanúsítványok közül az - adott időpontban - visszavont tanúsítványokat tartalmazó, *aláírt* lista.

1. A szolgáltató előre meghatározott időközönként hozza nyilvánosságra .
2. A szolgáltató eseményvezérelten bocsát ki, azaz minden esetben, amikor változik egy általa kibocsátott tanúsítvány állapota új listát bocsát ki.