**SPISÁK Andor**

# NYILVÁNOS KULCSÚ INFRASTRUKTÚRA ARCHITEKTÚRÁK

# PUBLIC KEY INFRASTRUCTURE MODELS

Abstract: A Magyar Honvédségen belül kialakítandó nyilvános kulcsú infrastruktúrával (Public Key Infrastructure – PKI) szemben támasztott nyilvánvaló követelmény többek között az, hogy illeszkedjen azokhoz a PKI architektúrákhoz, amelyekkel küldetéséből adódóan kapcsolódnia kell. Ide sorolhatóak többek között a Magyar Kormányzati PKI és a NATO-PKI, de feltételezhetően együtt kell működnie az EU majdan kialakítandó PKI rendszerével, valamint a külső beszállítók felé is el kell látnia feladatait. A cikk az ehhez szükséges a PKI architektúrák általános áttekintését követően a vonatkozó PKI architektúrák vizsgálja.

Abrstract: an obvious requirement of a Public Key Infrastructure to be established within the Hungarian Army is to be interoperable with the PKI-s of those institutions and organizations it is engagaed with due to its tasks and duties. Among these are the PKI of the Hungarian government, the NATO PKI, presumably the PKI of the EU and very likely certain PKI services will have to be provided to third partners. Following an overview of PKI infrastructure types the paper deals with the PKI-s of some relevant institutions and organizations.

## 1. PKI architektúrák

### 1.1. PKI összetevők és ezek feladatai [1]

#### 1.1.1. Regisztrációs Szervezet (Registration Authority - RA)

Az RA olyan hardver- és szoftver elemek, illetve személyzet összessége, amelynek feladata, hogy megbízható módon azonosítsa a felhasználókat, akik számára a CA a későbbiekben tanúsítványokat bocsát ki. Az RA feladata másrészről tevékenysége által megteremteni azt a PKI működéséhez szükséges bizalmat is, amelyet azok, akik a felhasználóval biztonságos módon kívánnak kommunikálni, a CA-ról feltételeznek. Egy CA-hoz több akkreditált RA is kapcsolódhat.

### 1.1.2. Hitelesítés Szolgáltató (Certification Authority - CA)

A CA alatt hardver- és szoftver elemek, valamint olyan személyzet összességét értjük, amelynek feladata, hogy a regisztrált felhasználók részére tanúsítványt bocsásson ki. Ebben szerepel a regisztrált felhasználó azonosítója (általában a neve), nyilvános kulcsa annak az algoritmusnak az azonosítójával, amelyet a titkosításhoz és a digitális aláírás készítéséhez a CA használ, a tanúsítvány verziója, a tanúsítvány sorszáma, a CA digitális aláírása, a kibocsátó neve, a tanúsítvány érvényességi ideje, valamint különböző opcionális azonosítók és bővítmények (pl.: használatra vonatkozó korlátozások). A tanúsítvány ajánlott felépítését, valamint a tanúsítvány létrehozásának ajánlott menetét az ITU-T által gondozott X.509-es ajánlás tartalmazza. A CA a létrehozott tanúsítványokat egy, a nyilvánosság számára hozzáférhető tanúsítványtárban tárolja. A CA felhasználóknak, illetve más CA-k részére is állíthat ki tanúsítványt.

### 1.1.3. Tanúsítványtár

A tanúsítványtár egy olyan címtár, amelyben a CA a kibocsátott tanúsítványokat, illetve visszavonási listákat tárolja és a nyilvánosság számára elérhetővé teszi. A tanúsítványtár célszerűen egy X.500 típusú címtár.

### 1.1.4. Visszavonási Listák

A CA az érvényüket vesztett tanúsítványokat Visszavonási Listák segítségével tartja nyilván, amelyeket egy X.500-as típusú könyvtárban hoz nyilvánosságra. A Visszavonási Listákat rendszeresen frissíteni kell. A Visszavonási Listákat tanúsítványként kezeljük, és az alábbiakban felsorolt listák közül valamelyik kategóriába tartoznak. A Visszavonási Listák tartalmazzák saját verzió számukat, a kibocsátó digitális aláírását, a kibocsátó nevét, a lista kiadásának időpontját, a visszavont tanúsítványokat (sorszám és visszavonási dátum alapján), valamint tartalmazhatnak különböző opcionális kiegészítéseket, mint például a visszavonás okát.

*Tanúsítvány visszavonási lista (Certification Revocation List - CRL)*

Ez a CA által digitálisan aláírt lista azoknak az érvényüket vesztett nyilvános kulcsú tanúsítványoknak a sorszámát, illetve visszavonási dátumát tartalmazza, amelyeket a CA az RA-nál regisztrált felhasználók számára bocsátott ki.

Egy tanúsítvány érvényét veszítheti, ha

- lejár az érvényességi ideje,

- a tanúsítványt birtokló felhasználó titkos kulcsa kompromittálódott,
- a tanúsítványt kiállító CA titkos kulcsa kompromittálódott,
- a regisztrált felhasználó törlését kéri akár az RA, akár a CA nyilvántartásából.

*Szervezeti Visszavonási Lista (Certification Authority Revocation List – CARL)*

A CARL egy CA által digitálisan aláírt visszavonási lista, amely olyan érvényüket vesztett tanúsítványok sorszámát illetve visszavonási dátumát tartalmazza, amelyeket a CA más CA-k számára bocsátott ki.

*Delta Visszavonási Lista (Delta Revocation List – dCRL)*

A dCRL egy részleges visszavonási lista, amely csupán azon érvényüket vesztett nyilvános kulcsú tanúsítványok sorszámát és visszavonási dátumát tartalmazza, amelyek a dCRL kibocsátását megelőző CRL (egy ilyen visszavonási listát bázis CRL-nek nevezünk) közzététele óta veszítették érvényüket.

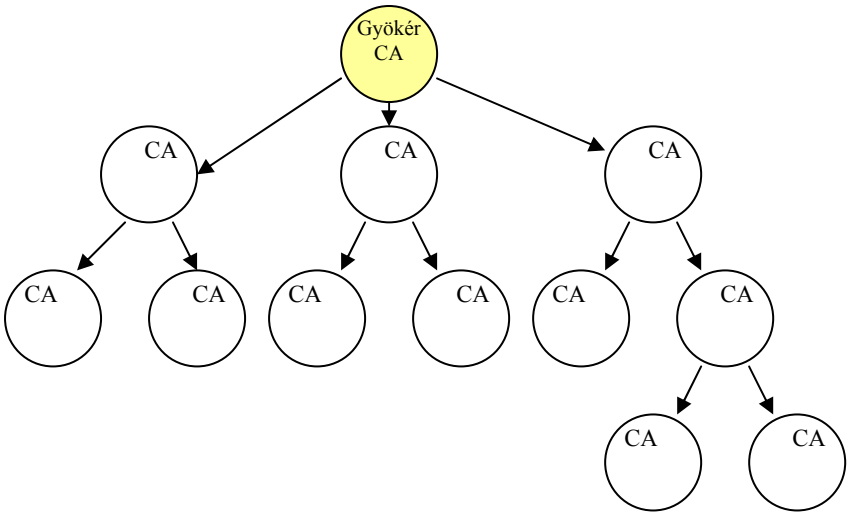
## 1.2. PKI architektúrák [2]

A PKI elemeit különböző architekturális felépítésben lehet elhelyezni.

### 1.2.1. Hierarchikus architektúra

A hierarchikus architektúra lényege, hogy létezik egy gyökér CA, amely minden alárendelt CA, illetve felhasználó bizalmát élvezi. A gyökér CA a hierarchiában alatta elhelyezkedő CA-k részére bocsát ki tanúsítványokat, akik részükről szintén, a hierarchiában alattuk levő CA-k részére állítanak ki tanúsítványokat, stb. Minden CA kiállíthat felhasználók számára is tanúsítványt. Az architektúra felépítését az 1. ábra szemlélteti.

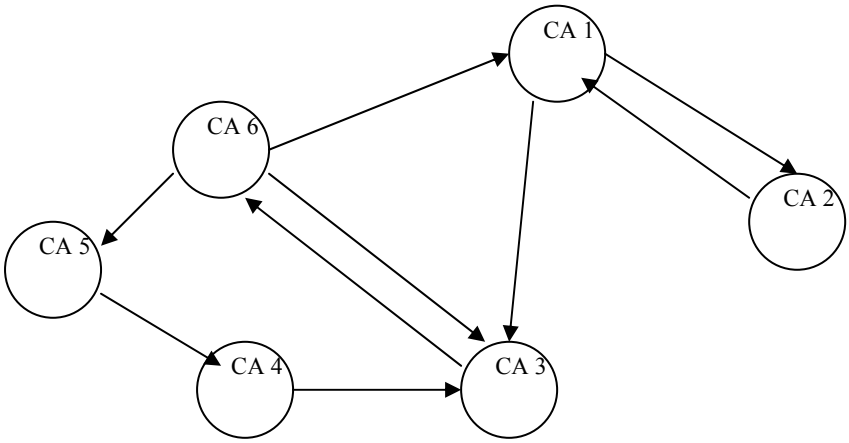
Amennyiben olyan felhasználók kívánnak egymással kommunikálni, akik különböző CA-k által kerültek tanúsításra, egy tanúsítvány lánc segítségével bizonyosodhatnak meg egymás tanúsítványának hitelességéről. Minden tanúsítvány lánc végén a gyökér CA van, amelyben a PKI minden felhasználója, illetve alárendelt CA-ja megbízik. Bármely köztes hierarchiai szinten fontos a CA-t úgy konfigurálni, hogy az általa kibocsátott tanúsítványokban a teljes tanúsítványlánc fel legyen tüntetve [3].




1. ábra. Hierachikus PKI architetktúra

### 1.2.2. Szövevényes architektúra

Ebben az esetben számos CA szövevényes vagy részben szövevényes módon lehet összekötve. A CA-k ekkor egymásnak állíthatnak ki (de nem szükségszerűen állítanak ki) tanúsítványokat. Amennyiben két CA egymás számára állít ki tanúsítványt, úgy kereszttanúsításról beszélünk.




2. ábra. Példa egy részben szövevényes PKI hierarchiára

Szövevényes esetben két felhasználó között több tanúsítvány lánc is létezhet. Ha például a 2. ábrában a CA5 egy A felhasználója a CA3 egy B felhasználójának a nyilvános kulcsának érvényességéről kíván meggyőződni, akkor a következő eljárást kell lefolytatni:

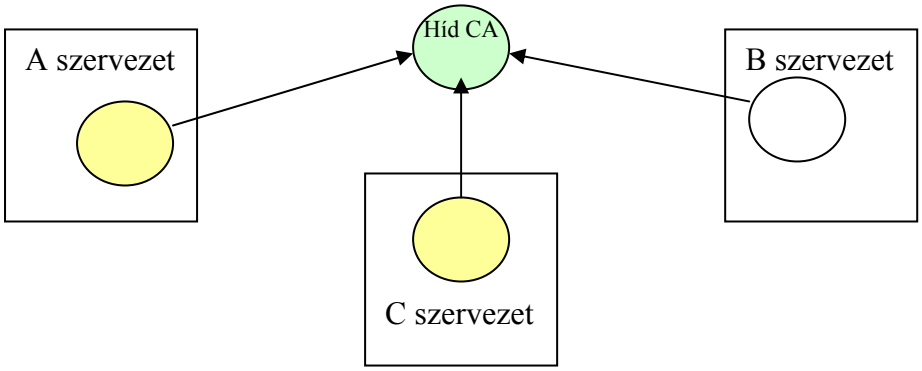
A megbízik CA5-ben, illetve mindenkiben, akit CA5 tanúsított, így például CA4-ben is, továbbá mindenkiben, akit CA4 tanúsított, így tehát CA3-ban is. Mivel B-nek CA3 által

kibocsátott tanúsítványa van, így A B-ben is megbízik, illetve hitelesnek ítéli meg a tanúsított nyilvános kulcsát.

### 1.2.3. Híd architektúra

Híd architektúráról akkor beszélünk, ha egy kitüntetett CA (híd CA) több, önmagában zárt PKI-t köt össze azzal a céllal, hogy az egyes PKI-k által tanúsított felhasználók egymással hiteles módon kommunikálhassanak. A híd architektúrát a 3. ábra szemlélteti.

A híd architektúra esetén minden CA, amelyik a híd CA szolgáltatásait igénybe veszi, tanúsítványt bocsát ki részére. Ezzel biztosítja a saját felhasználói számára a hiteles kommunikációt. Amennyiben a szervezet PKI rendszere hierarchikus felépítésű (mint az A és C szervezetek esetében), úgy a híd CA a gyökér CA-val áll kapcsolatban, amennyiben szövevényes, úgy egy kitüntetett CA-val.

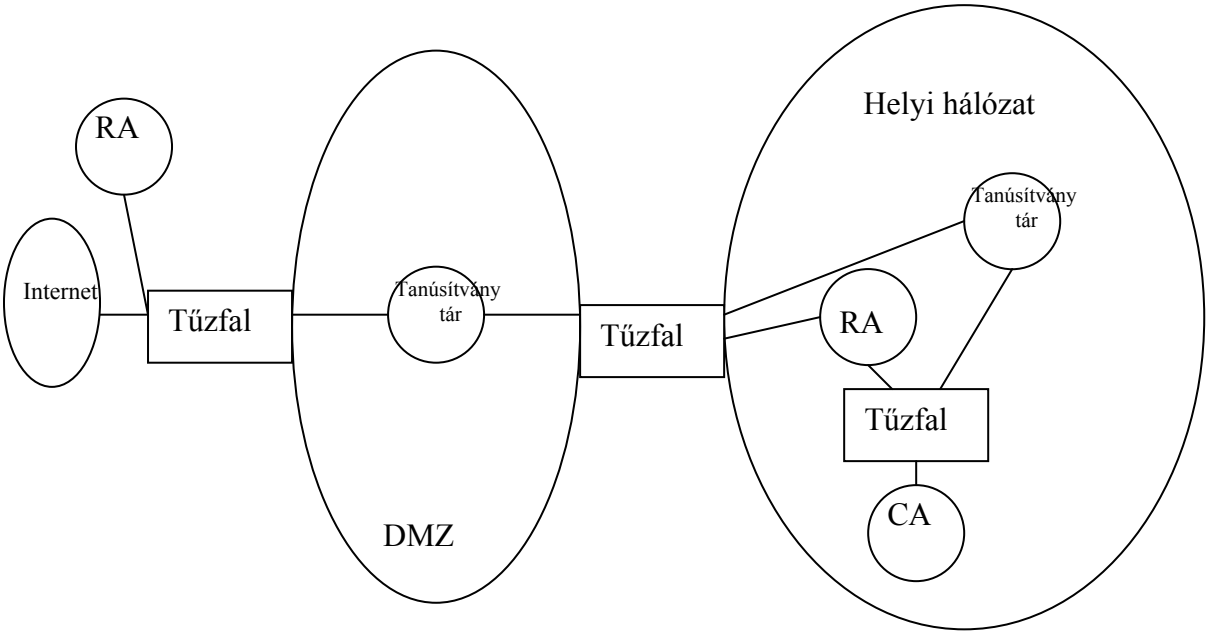



3. ábra. Híd architektúrájú PKI

### 1.2.4. Fizikai megvalósítás

Az eddigieket összegezve láthatjuk, hogy amennyiben egy PKI rendszert kívánunk létrehozni, szükség van egy CA-ra, egy tanúsítványtárra és egy vagy több RA-ra. A CA-t, a tanúsítványtárat és feltehetőleg egy RA-t egyazon helyi hálózaton kell működtetni. Amennyiben egy CA-hoz több RA is tartozik, úgy ezek között lehetnek olyanok, amelyek nem elemei az adott helyi hálózatnak, hanem valamilyen módon külső elemként csatlakoznak erre. A CA-t, az RA-t és a tanúsítványtárat mindenképpen célszerű a hálózat különböző szegmenseiben működtetni. Erre már csak azért is szükség van, mert a tanúsítványtárat minden külső csatlakozó számára elérhetővé kell tenni, a CA-nak viszont lehetőleg még a belső felhasználók számára is láthatatlannak kell lennie. Amennyiben a CA-hoz illetéktelen személy hozzáfér, a rendszerbe vetett bizalom megsérül, és ez megkérdőjelezi hitelességét.

Ezért célszerű a CA-t a belső hálózaton belül egy további tűzfallal védeni, elkerülendő, hogy a CA belső, illetéktelen személyek által elérhető legyen. A CA-nak közvetlen kapcsolatot kell biztosítani mindegyik RA-val és a tanúsítványtárral úgy, hogy az RA-k felől adatot fogadni és a tanúsítványtár felé adatot szolgáltatni tudjon. Ilyen tűzfal létrehozására különböző hardveres megoldások kínálkoznak, a legcélszerűbb azonban egy Linux alapú IPtables tűzfalat telepíteni, mivel konfigurálása igen egyszerű (alapvetően minden a CA felé irányuló, illetve a CA által generált forgalmat tiltani kell, kivéve a CA-tanúsítvány tár, illetve a több RA-CA forgalmat). További előnye más céleszközökkel szemben, hogy ezekhez viszonyítva olcsó.




4. ábra. PKI elemeinek fizikai elrendezése

Mivel a tanúsítványtárat egyrészről bárki számára hozzáférhetővé kell tenni, másrészről viszont folyamatos kapcsolatban áll a CA-val, célszerű két példányban létrehozni. Egy tanúsítványtár a helyi hálózatunk tűzfalán belül helyezkedik el, ezzel állhat kapcsolatban a CA, illetve ezt tekinthetik meg a belső felhasználók. A másik tanúsítványtárat, amelyiket a belső tanúsítványtár rendszeres időközönként frissít (a törvényi előírásoknak megfelelően legalább négy óránként) célszerű a hálózatunk demilitarizált zónáján (DMZ) belül elhelyezni. Ehhez férnek hozzá azok, akik kívülről kívánják a tárat megtekinteni. A helyi RA szintén a hálózaton belül, külön gépen van. A külső RA-k valamilyen titkosított csatornán keresztül csatlakoznak a helyi RA-hoz, amely egyedüliként áll közvetlen kapcsolatban a CA-val. Ilyen titkosított csatornaként egy virtuális magánhálózat (Virtual Private Network – VPN) csatorna tűnik a legbiztonságosabbnak, illetve egy különösen szigorú autentikációs protokollal ellátott

SSH (Secure Shell) csatorna. Amennyiben az autentikációra Kerberos protokollt használunk, architektúránkat további hardver elemekkel szükséges bővíteni. Az elrendezést a 4. ábra szemlélteti.

A CA-t, az RA-t, valamint a tanúsítványtárakat a NIST-FIPS 140-2-es szabványának megfelelő fizikai védelemmel ellátott, szeparált helyiségekben kell elhelyezni [4]. A két tanúsítványtárat egy helyiségben is el lehet helyezni (esetleg a hálózat üzemeltetéséhez használt egyéb szerverekkel együtt).

# 2. Magyar kormányzati PKI

## 2.1. A kormányzati PKI céljkitűzései

A kormányzati PKI szükségességének kérdése több aspektusból is vizsgálható. Egyrészről vizsgálandó, hogy az állampolgárok különböző állami, illetve önkormányzati szervekkel való (részben törvényileg előírt) elektronikus úton történő kapcsolattartását hogyan lehet egységesített formába öntve, hiteles módon megvalósítani. Másrészről felmerülhet az igény a kormányzat szereplőinek (minisztériumok, önkormányzatok, felügyelő hatóságok, stb.) egységes PKI rendszer alá vonása. Utóbbi hozzájárulna az Európai Bizottság által 2002-ben megfogalmazott E-Europe2005-höz történő csatlakozás megvalósításához is [5]. Harmadik szempontként említést kell tenni az üzleti szféra esetleges igényeiről, amelyek tükrében szükséges lehet egy egységes PKI rendszer kiépítése a gazdasági élet szereplői részére.

Az civil szféra részére nyújtott szolgáltatások terén azt kell megállapítani, hogy Magyarországon jelenleg nem létezik olyan egységes PKI-rendszer, amelyet az állampolgárok az összes általuk igényelt szolgáltatáshoz használhatnának. Felmerülhet a kérdés, hogy egy ilyen infrastruktúra kiépítése mennyiben kívánatos, hiszen ennek megvalósítását követően tartani lehet a meglévő, piaci hitelesítés szolgáltatók megnehezített helyzetéből fakadó ellehetetlenülésétől. Ez pedig ellentmondana az EU azon irányelvének, amely a monopóliumokkal szemben egyértelműen a szabad verseny megteremtésére helyezi a hangsúlyt.

A kormányzati szervek összefogásának érdekében létrejött az Egységes Kormányzati Gerinchálózat (EKG), amely a minisztériumok számára nyújt egységes szolgáltatásokat. Az EKG-t támogatandó létrehozták a Biztonsági Hitelesítés Szolgáltató Irodát (BHSz), amely

azoknak a közigazgatási szerveknek nyújt hitelesítés szolgáltatást [6,7,8], amelyek megállapodási szerződést kötnek vele.

2005 őszén megkezdte működését a Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda (KGyHSz), amely a 2001/XXXV, az elektronikus aláírásról szóló törvénynek (EAT), valamint a 194/2004 sz. kormányrendeletnek eleget tevő hitelesítés szolgáltatónak bocsát rendelkezésére az ő a tanúsítványát felülhitelesítő tanúsítványt [9].

## 2.2. A Kormányzati PKI Hitelesítés-Szolgáltatói

### 2.2.1. Biztonsági Hitelesítés Szolgáltató Iroda (BHSz)

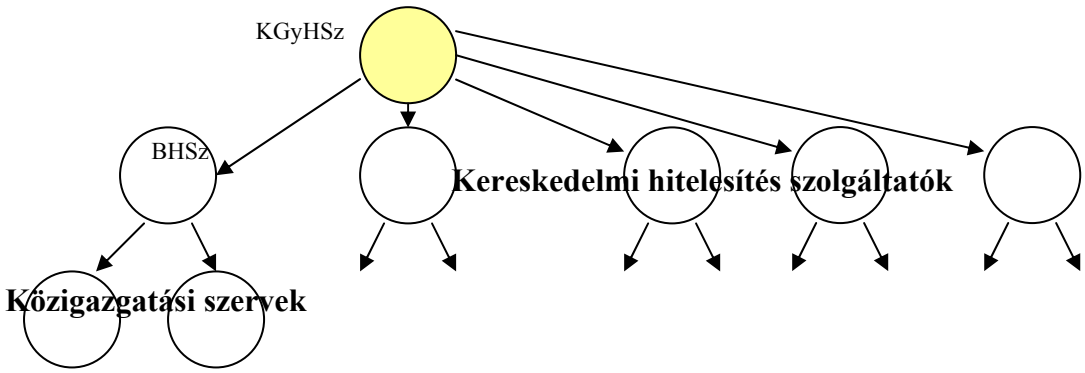
A BHSz 2006 februárjában kezdte meg működését. A hitelesítési rendjeinek [6,7,8] megfelelően olyan közigazgatási szerveknek nyújt hitelesítés szolgáltatást, amelyek együttműködési szerződést kötöttek vele. A BHSz kihelyezett regisztrációs szervezetet hoz létre a adott szervezetnél, ahol a felhasználók regisztráltathatják magukat. A hitelesítési rendekben foglaltak szerint a BHSz eleget tesz a NIST-FIPS 140-2-es szabványának, valamint az Nemzeti Hírközlési Hatóság (NHH) minősített tanúsítvány visszavonással és felfüggesztéssel kapcsolatos hatósági állásfoglalásának [10]. Visszavonási listáit 25 óránként frissíti. A BHSz által kibocsátott minősített kulcsok kizárólag digitális aláírás generálására használhatók [6], míg a fokozott biztonságú tanúsítványok a tanúsítvány „kulcshasználat", illetve „kiterjesztett kulcshasználat" mezőjében feltüntetett célokra használhatók fel. A BHSz tanúsítványának RSA kulcsa 2048 bit hosszúságú, az előfizetők számára kibocsátott RSA kulcsok hossza pedig 1024 bit. A digitális aláíráshoz hash algoritmusként az SHA-1 algoritmust használja.

### 2.2.2. Közigazgatási Gyökér Hitelesítés-Szolgáltató Iroda (KGyHSz) [9]

A KGyHSz azon az EAT hatálya alá eső, illetve az EAT hatálya alá nem eső közigazgatási és kereskedelmi hitelesítés szolgáltatókat hivatott felültanúsítani, aki vele együttműködési szerződést kötöttek, így többek között a BHSz-t is. A KGyHSz külön regisztrációs szervezettel nem rendelkezik, a regisztrációval kapcsolatos feladatokat az NHH látja el. Ez ésszerű, hiszen azokat a hitelesítés szolgáltatókat, akik felül kívánják magukat tanúsíttatni, az NHH már egyszer regisztrálta, valamint évente egyszer átesnek az NHH felülvizsgálatán, így azonosságukhoz, hitelesítési rendjük, illetve működésük megfelelőségéhez nem férhet kétség.

A KGyHSz a Magyar Köztársaság gyökérhitelesítőjeként működik, ezért csak fokozottan szigorú előírások segíthetik elő a társadalom által igényelt bizalom megteremtését. Ezek az előírások elsősorban a tanúsítványok visszavonásával és megújításával kapcsolatosak.

A KGyHSz saját tanúsítványát 20 évre, a közigazgatási hitelesítés szolgáltató(k) – egyelőre csak a BHSz ilyen – számára kibocsátott tanúsítványokat 15 évre, a kereskedelmi hitelesítés szolgáltatók számára kibocsátott tanúsítványokat legfeljebb 15 évre érvényesíti. Az NHH által minősített kereskedelmi hitelesítés szolgáltatók egyike sem rendelkezik a KGyHSz által kibocsátott gyökér tanúsítvánnyal [11,12,13,14]. A tanúsítványok visszavonását illetően a KGyHSz nem engedélyezi a lejárt tanúsítványok meghosszabbítását, a kulcscserét (csupán a tanúsítványban szereplő nyilvános kulcs, illetve a hozzá tartozó titkos kulcs kerül lecserélésre), illetve a tanúsítvány módosítását, valamint nem végez kulcsvisszaállítás szolgáltatást.




5. ábra. Magyar Kormányzati PKI és kapcsolata az egyéb hitelesítés szolgáltatókkal

A Magyar Kormányzati PKI két szereplője révén egy szigorúan hierarchikus struktúrában működik, amelyet az 5. ábra szemléltet.

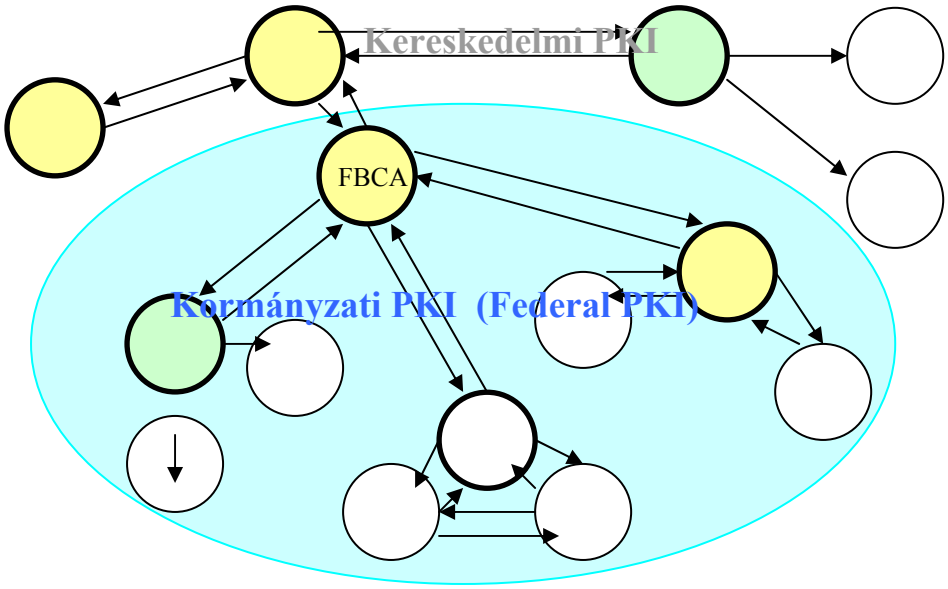
## 3. Az Amerikai Egyesült Államok Kormányzati PKI architektúra modellje [2]

Az USA kormányzati PKI architektúra modellje lényegesen eltér a magyar modelltől. A különbségnek feltehetően történelmi okai vannak. Amíg Magyarországon a kormányzati PKI létrejöttét megelőzően a közigazgatási szerveknek nagyrészt nem volt, vagy csak kezdetleges

stádiumban kiépített PKI rendszere volt, addig az USA közigazgatási szervei elég korán elkezdtek önálló PKI rendszereket működtetni. Ezen kívül lényegesen nagyobb igény merült fel a kereskedelmi hitelesítés szolgáltatókkal történő kereszttanúsításokra. Az USA kormányzati PKI elsődleges célja, hogy olyan tanúsítvány láncokat hozzon létre a közigazgatási szervek között, amelyek megteremtik a széleskörű és magas fokú bizalom légkörét. Ehhez – a magyar modelltől eltérően – a híd architektúra bizonyult célszerűnek. Létrejött tehát egy kormányzati híd-CA, amely a közigazgatási szervek CA-ival egymás részére kereszttanúsítványt bocsát ki. A Szövetségi Híd Hitelesítés Szolgáltató (Federal Bridge CA – FBCA) szintén egy kereszttanúsítvány segítségével teremti meg a kapcsolatot a kereskedelmi szolgáltatók egyikével (ez lehet gyökér hitelesítő, vagy egy másik híd hitelesítő).

Kormányzati oldalon az egyes közigazgatási szervek PKI architektúrájukat szabadon választhatják. Így azok a CA-k, amelyekkel az FBCA kereszttanúsítványt cserél, lehet gyökér hitelesítő, híd CA vagy egy a többi közül kitüntetett, attól függően, hogy az adott szerv hierarchikus vagy szövevényes felépítésű.

A közigazgatási szerveknek nem kötelező kereszttanúsítványokat cserélniük az FBCA-val, de azok, amelyek ezt kívánják tenni, többek között az ITU-T által gondozott X.509-es szabvány szerint kell kiállítaniuk a tanúsítványokat és a visszavonási listákat [15]. A használt algoritmusokat a NIST-FIPS 180-2 es szabványa [16], valamint a [17]-ben leírtak határozzák meg. Az USA kormányzati PKI architektúra modelljét a 6. ábra szemlélteti.




6. ábra. USA kormányzati PKI architektúra

Amennyiben az adott közigazgatási PKI hierarchikus felépítésű, úgy az FBCA a gyökér hitelesítővel (a 6. ábrán zöld színnel jelölve) hoz létre kereszttanúsítványokat egymás számára. Amennyiben a közigazgatási PKI híd felépítésű, úgy a híd CA-val (a 6. ábrán sárga színnel jelölve) teszi ugyanezt. Ha egy közigazgatási PKI szövevényes architektúrájú, úgy egy kitüntetett CA-val hoz létre kereszttanúsítványt (a 6. ábrán fehér színnel jelölve). Minden közigazgatási szerv, amely csatlakozni kíván az USA kormányzati PKI-hoz, kijelöli azt a hitelesítés szolgáltatóját, amellyel az FBCA majd létrehozza a kereszttanúsítványokat. Ezeket a hitelesítés szolgáltatókat Peer CA-nak hívják (a 6. ábrán vastagított széllel ábrázoltva). A Peer CA szerepét egy hierarchikus PKI-ban értelemszerűen a gyökér hitelesítő látja el, a híd architektúrájú PKI-ban a híd CA és a szövevényes architektúrájú CA-ban bármelyik CA elláthatja.

# 4. A NATO PKI referencia architektúrája [18]

## 4.1. A NATO PKI célkitűzései

A NATO PKI (NPKI) alapvető célkitűzése, hogy a szövetségeseknek egy olyan egységes biztonsági szolgáltatást nyújtson, amely megfelel a C/322-N/0780-as dokumentumnak.

Különösen kiemelt célként szerepelnek az alábbi biztonsági szolgáltatások nyújtása:

- Végpontok azonosítása és autentikálása
- Végpontok és folyamatok integritása
- Titkosítás
- Forrás letagadhatatlansága.

Ezen kívül a célkitűzések között szerepel még a kulcshelyreállítás és a titkosításra használt kulcsok archiválása. Az előzőekben tárgyalt PKI rendszerekkel ellentétben az NPKI támogatni kívánja a személyes és szervezeti elektronikus levelezést, a dokumentumok elektronikus publikálását, üzenetek titkosítását, a webes szolgáltatásokat, a periméter védelemhez használt eszközökhöz (pl. tűzfalak, IPS szenzorok, routerek, stb.) való hozzáférés védelmet és ezek távoli konfigurálását, az e-kereskedelmet, valamint bizonyos címtár szolgáltásokat. Ez azt jelenti, hogy az NPKI-nek támogatni kell a fent felsorolt szolgáltatások által használt protokollokat, mint az S/MIME, SSL/TLS, SNMP 3. verzióját, valamint IPSec-et, IPv6-ot. Ezek a célkitűzések lényegesen kiszélesítik az NPKI keretei között ellátandó

feladatok körét, hiszen sokkal szélesebb spektrumú hitelesítési, autentikálási és titkosítási folyamatokat kell lebonyolítani, mint egy olyan PKI rendszerben, amely mindezen szolgáltatásokat nem nyújtja. Ugyanakkor meg kell határozni azoknak az autentikációs protokolloknak a körét, amelyeket az NPKI egyes minősítési szintek (l. következő pont) esetén elfogadhatónak tartatnak.

### 4.2. Minősítési szintek

Az NPKI-n belül négy különböző biztonsági szintet kell kiépíteni:

- NATO titkos WAN
- NATO bizalmas WAN
- NATO korlátozott WAN
- NATO nem minősített WAN

### 4.3. Az NPKI architekturális elemei

Az NPKI hierarchikus felépítésű, és a fenti célok megvalósításához az alábbiakban felsorolt architekturális elemek kerültek meghatározásra. A leírásban kiemelt fonotossággal tárgyaljuk az egyes elemek esetében meghatározott biztonsági követelményeket.

#### 4.3.1. Gyökér hitelesítő

Mint minden hierarchikus architektúrájú PKI-nak, a NPKI legfelső szintjén is a gyökér hitelesítő áll, aki a NATO-CA-k részére tanúsítványokat és visszavonási listákat bocsát ki, valamint kereszttanúsítványokat hoz létre egyéb CA-kal. A megszokott szolgáltatásokon túlmenően, a gyökér hitelesítő hitelesítő visszavonási listákat (Authority Revocation List – ARL) is közzétesz. Ezek olyan listák, amelyek a visszavont, más CA-knak kibocsátott tanúsítványok listáját tartalmazzák.

Biztonsági okokból a gyökér hitelesítő semmilyen módon nem csatlakozik nagy kiterjedésű hálózathoz (WAN). A CRL-eket, ARL-eket, a tanúsítványok visszavonását és státuszát, illetve érvényességük lejártát off-line módban kezeli. A gyökér hitelesítőhöz egy kriptográfiai céleszköz társul, amely lehet dedikált hardver eszköz, de a szerverre telepített célszoftver is. Az eszköz – funkcionalitását és megbízhatóságát tekintve – NATO minősítése legalább EAL3 szintű, illetve ezzel ekvivalens szintű. Ez magába foglalja, hogy a kriptográfiai eszköz fizikai erőszakkal szemben ellenálló. A gyökér hitelesítőt fizikai

biztonságának érdekében egy olyan biztonsági zónában kell elhelyezni, amelyet legalább két személy felügyel.

### 4.3.2. NATO CA-k

A NATO CA-k az NPKI hierarchia második szintjén helyezkednek el, és feladatuk, hogy tanúsítványokat bocsássanak ki alacsonyabb szinten elhelyezkedő CA-k, illetve végfelhasználók részére, valamint visszavonási listákat publikáljanak. Ezen kívül hitelesítési szolgáltatásokat nyújtanak a hozzájuk tartozó RA-k részére. A NATO CA-kra vonatkozó biztonsági előírások egyeznek a gyökér hitelesítő esetén előírtakkal, azzal a különbséggel, hogy csatlakoznak WAN-ra. A NATO CA-kat szigorú perimétervédelemmel kell védeni a WAN felől érkező esetleges támadások ellen. Ez a védelem célszerűen egy olyan tűzfal alkalmazását jelenti, amely csak azokat a protokollokat, portokat és forgalmat engedélyezi, amelyek a CA működéséhez szükségesek (l. 1.2.4.). A referencia architektúra négy NATO CA-t javasol, amelyeket más-más földrajzi helyen kell elhelyezni. Ezek közül kettő csak az NGCS-en keresztül, kettő viszont Interneten keresztül is elérhető.

### 4.3.3. Regisztrációs egységek

Az RA-k feladata, hogy garantálják a regisztrált felhasználók azonosítását a CA részére, hogy az, az RA által szolgáltatott adatok alapján tanúsítványt állítson ki és írjon alá a végfelhasználó számára. Az RA-k biztonsági előírásai megfelelnek a CA-k biztonságára előírtakkal, nem rendelkeznek azonban önálló kriptográfiai céleszközzel, mivel nincs szükségük ilyenre.

### 4.3.4. Végfelhasználók


7. ábra. Végfelhasználók biztonsági követelményei

A végfelhasználók esetében meghatározott biztonsági követelmény réteges szerkezetű, amelyet a 7. ábán szemléltetünk.

A legalsó réteget az NPKI szolgáltatja úgy algoritmusok, mint kulcskezelés szempontjából.

A kriptográfiai céleszközt szintén az NPKI szolgáltatja a megfelelő biztonsági protokkollal együtt. Ezekre a felhasználónak nincs befolyása. A CAPI (Cryptographic Application Programming Module) elsősorban a szimmetrikus titkosítás szoftveres úton történő megvalósítására szolgál. Nagy adatmennyiségek esetén csupán a kulcscsere történik aszimmetrikus algoritmusok segítségével, maga az adat titkos átvitele a gyorsabb feldolgozás érdekében szimmetrikus algoritmusok segítségével valósul meg. Ezeket az NPKI nem kezeli központilag, nem is célszerű, hiszen a végfelhasználó lehet web-szerver, tűzfal vagy router is, amely az átvitelhez a kliensoldali alkalmazás függvényében választhatja a legmegfelelőbbnek tűnő szimmetrikus titkosítási algoritmust. A digitális aláírás, illetve aszimmetrikus titkosítás végrehajtása mindenképpen az NPKI által a felhasználó rendelkezésére bocsátott hardver céleszközben történik. Az operációs rendszer biztonsági beállításai részben adottak, sem a felhasználó, sem az NPKI nem képes a biztonságot fokozni, főleg, hogy a NATO-ban elterjedt Windows operációs rendszerek biztonsági beállításai meglehetősen merevek. Az alkalmazás, amelyet a felhasználó használ, mindenképpen erős autentikációt használ, amelyek az NPKI keretében kerülnek meghatározásra. Az NPKI alkalmazása a legfelső rétegben lehetőséget ad olyan nagy biztonságú hozzáférés korlátozásokra, amelyekre csak a NATO gyökér hitelesítő, illetve a NATO CA-k egyike által kibocsátott tanúsítvány ad lehetőséget.

A NPKI referencia modell nem tesz említést a tanúsítványtárak elhelyezéséről, illetve biztonsági követelményeiről. Erre részben nincs is szükség, hiszen a tanúsítványtáraknak a felhasználók, illetve az érintett felek által nyilvánosan hozzáférhetőnek kell lenniük. Másrészről viszont kapcsolatban kell állniuk a NATO CA-kal, amelyek biztonsági előírásairól a 4.3.1-es és 4.3.2-es fejezetekben már szó volt.

A felhasználók regisztrálása az alábbiak szerint történik:

1. A felhasználó azonosítja magát az adott RA felé.
2. RA digitálisan aláírja (a CA-tól kapott tanúsítvány és céleszköz segítségével) a felhasználó kérését, majd a kérést elküldi a CA-hoz. Egyidejűleg a felhasználó rendelkezésére bocsát egy egyszer használatos kriptográfiai céleszközt.

3. CA generálja az RA által továbbított kérés alapján a felhasználó tanúsítványát és kulcspárját.
4. A felhasználó az RA-tól kapott egyszer használatos céleszköz segítségével kikéri a CA-tól végleges céleszközét, rajta a titkos kulcsával.

# 5. Összegzés

A Magyar Honvédség kialakítandó PKI rendszerével szemben kiemelt követelmények fogalmazhatóak meg, főként a Magyar Kormányzati PKI, illetve a NATO nyilvános kulcsú architektúrájának (NATO PKI – NPKI) tükrében. Amíg a Magyar Kormányzati PKI-hoz történő csatlakozás feltételei világosak (nyilvánvaló, hogy a BHSz által kibocsátott tanúsítványra szüksége lesz egy majdani honvédségi gyökér hitelesítőnek, illetve híd hitelesítőnek), a NATO széleskörű PKI szolgáltatásai, illetve biztonsági követelményei szigorú feltételeket szabnak. Felmerülhet a kérdés, hogy a Magyar Honvédség PKI-ja az NPKI minden szolgáltatását igénybe kívánja-e venni, illetve ugyanezeket a szolgáltatásokat szolgáltatni kívánja-e. A felmerülő költségek tükrében feltehetően erős szelekcióra lesz szükség. Égetőbb kérdés azonban, hogy a Magyar Honvédség tudja-e vállalni azokat a biztonsági feltételeket, amelyeket az NPKI előír.

# 6. Felhasznált irodalom


[1] Benantar, Messoud: The Internet Public Key Infrastructure, IBM Systems Journal Vol 40, No. 3, 2001, 648-665

[2] Kuhn, Richard et al: Introduction to Public Key Technology and the Federal PKI Infrastructure, National Institute of Standards and Technology (NIST), 2001

[3] http://www.debian-administration.org/articles/284, 2006.04.07.

[4] National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, 2002

[5] European Commission: eEurope 2005: An Information Society for All, Bruxelles, 2002

[6] Informatikai és Hírközlési Minisztérium, Biztonsági Hitelesítés Szolgáltató Iroda, Biztonságos Aláírás-létrehozó Eszköz Használatát Megkövetelő, Aláírás Célú Tanúsítványokhoz Tartozó Minősített Hitelesítési Rend, Verzió: 1.0, 2006

[7] Informatikai és Hírközlési Minisztérium, Biztonsági Hitelesítés Szolgáltató Iroda, Kriptográfia Eszköz Használatát Nem Megkövetelő Egységesített Hitelesítési Rend, Verzió: 1.0, 2006

[8] Informatikai és Hírközlési Minisztérium, Biztonsági Hitelesítés Szolgáltató Iroda, Kriptográfia Eszköz Használatát Megkövetelő Egységesített Hitelesítési Rend, Verzió: 1.0, 2006

[9] Informatikai és Hírközlési Minisztérium, Közigazgatási Gyökér – Hitelesítés Szolgáltató Iroda, Hitelesítési Rend, Verzió: v1.0, 2006

[10] NHH Informatika Szabályozási Igazgatóság , Minősített Tanúsítvány Visszavonással és Felfüggesztéssel Kapcsolatos Hatósági Állásfoglalás, 2005

[11] http://eszigno.t-systems.magyartelekom.hu/eszignohitelesitokozpont/fokozotteszignoszolgaltatoitanusitvanyok.vm , 2006.05.28.

[12] http://www.mavinformatika.hu/ca/, 2006.05.28.

[13] http://www.netlock.hu/index.cgi?minositett&ca=mshea&lang=HU&tem=ANONYMOUS/kulcsjegyzok/adatok.tem 2006.05.28.

[14] http://www.e-szigno.hu/, 2006.05.28.

[15] ITU-T Recommendation X.509 (2000), Information Technology – Open Systems Interconnection – The Directory: Authentification framework.

[16] National Institute of Standards and Technology, Federal Information Processing Standards Publication 180-2, 2002

[17] National Institute of Standards and Technology, Federal Information Processing Standards Publication, Minimum Interoperability Specification for PKI Components, Version 1, 1997

[18] NATO C3 Board, NATO Public Key Infrastructure (NPKI) Reference Architecture, 2004, NATO Unclassified