Gara Péter, senior technikai tanácsadó

2007. április 22.

SYNERGON

Nyilvános kulcsú hitelesítés napjainkban

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

Az előadás tematikája

- A nyilvános kulcsú infrastruktúra (PKI) alapfogalmai
- A kriptográfia üzleti felhasználási területeinek bemutatása esettanulmányokon keresztül
- A PKI szabványosítása és jogi szabályozása
- A PKI rendszerek létrehozása során szerzett tapasztalatok

Alapfogalmak

Informatikai biztonsági alapfogalmak

- Bizalmasság (Confidentiality)
- Sértetlenség (Integrity)
- Hitelesség (Authenticity)
- Letagadhatatlanság (Non-repudiation)

Kriptográfiai alapfogalmak

- Rejtjelezés
  - algoritmusok, kulcsok
  - szimmetrikus rejtjelezés
  - aszimmetrikus rejtjelezés
- Titkosítás
  - szimmetrikus vs. aszimmetrikus (előnyök és hátrányok)
- Elektronikus aláírás
  - hashképzés
  - digitális aláírás

PKI alapfogalmak

- Tanúsítvány (Certificate)
- Tanúsítvány hitelesítő központ (Certificate Authority)
  - a hitelesítés logikája
  - CA-k hierarchiája (gyökérhitelesítés, köztes CA-k)
  - Kereszthitelesítés
- Visszavonási lista (Certificate Revocation List; CRL)
- OCSP (Online Certificate Status Protocol) szolgáltatás
- Kulcsarchiválás
- Időpecsét (Timestamp) szolgáltatás

Gyakorlati példák

Esettanulmány: PKI kialakítása vállalaton belüli felhasználásra

- Az ügyfélnél Microsoft Windows alapú hálózatot alakítottak ki, Active Directory címtár megoldással.
- A levelezéshez Outlook klienseket használnak.
- A következő igények merültek fel:
  - erős (két faktorú) azonosítás a felhasználók AD tartományba történő bejelentkezésekor
  - digitális aláírás biztosításának lehetősége elektronikus levelezéshez kötődően
  - titkosított üzenetek küldésén alapuló levelezés biztosítása

Kliensoldali megoldás kérdése

- Az erős azonosítás bevezetésénél feltétlenül szükséges tokenes/smartkártyás vagy biometrikus azonosításra. A digitális aláírás és a titkosítási igények kielégítése, továbbá a vállalaton belüli felhasználás és költséghatékonyság miatt smartkártyás megoldás javasolt.
- Smartkártyás megoldások esetében ügyelni kell arra, hogy elegendő memória legyen a kártyán a kulcspárok és a tanúsítványok tárolására.
- Fontos, hogy a kártyának megfelelő szoftveres támogatása legyen a kívánt platformon. Windows környezetben ez alapvetően CSP támogatást jelent.
- A Windows támogatja a smartkártyás beléptetést, az Outlook lehetővé teszi az üzenetek digitális aláírását és titkosítását is.

Tanúsítványok beszerzésének kérdése

- Érintett felhasználók száma néhány száz.
- Egy helyi CA környezet előnyösebb lehet, mint a szükséges számú tanúsítvány megvásárlása, illetve a későbbi megújításuk utáni rendszeres fizetés.
- Saját CA esetén a munkaerő változásának kezelése is egyszerűbb.
- Fontos kérdés: van-e olyan CA megoldás, amely árban kedvezőbb a tanúsítványvásárlásnál, és kielégíti a vállalat igényeit.
- Választás: a Microsoft CA megoldása az ügyfél egyéb Microsoft licenszeinek birtokában ingyenes, és az alapigényeknek fejlesztés nélkül is eleget tesz.

A tanúsítványok kiosztása

- A Windows a belépéskor a smartkártya ún. default konténerében lévő tanúsítványt (és kulcspárt) használja.
- Microsoft CA környezetben a más nevében („on behalf of”) történő tanúsítványkérés esetében mindig a default konténerbe kerül az új tanúsítvány.
- Ezek után elég körülményes ugyanazon kártyára, más nevében generálni a Smart Card belépési, a digitális aláírási és a titkosítási tanúsítványokat.
- Áthidaló megoldásként a következő munkafolyamatot javasoljuk:
  - Smart Card belépési tanúsítvány generálása „on behalf of” módon, a CA operátora által
  - A felhasználó az operátori gépen már a Smart Card tanúsítványával lép be
  - Saját maga számára igényli az aláíró tanúsítványt
  - Saját maga számára igényli a titkosító tanúsítványt

„Extra” igény

- A vállalat igényt tart arra, hogy szükség esetén (például egy alkalmazott távozásakor) belenézhessen dolgozói levelezésébe. Ehhez a titkosított levelek esetében szükségük van a címzett privát kulcsára.
- Lehetséges megoldások:
  - kulcsarchiváló használata
  - szoftveres titkosító kulcsok használata, amelyeket praktikus okból (közös helyről használat) utólag tárolnak el a smartkártyán

További igények kezelése Microsoft CA környezetben

- Az ügyfél kiépített Microsoft CA környezettel rendelkezik. A rendszer működésével kapcsolatban a következő igényeket támasztja:
  - az előre gyártott tanúsítvány sablonokban nem szereplő mező jelenjen meg a kész tanúsítványban
  - a felhasználó csak akkor kaphasson tanúsítványt, ha a HR adatbázisban aktív, belső alkalmazottként szerepel
  - az aktuális visszavonási listákat egy adatbázisban tárolják le, hogy később visszakereshető legyen, adott időpontban érvényes volt-e egy tanúsítvány vagy nem.
- Bár a Microsoft CA moduláris felépítésű, kisszámú modul fedi le a feladatokat, így egyedi igények kielégítése jelentős többletfejlesztést eredményezhet.
  - Entry modul: A tanúsítványkérések fogadására szolgál, nem változtatható.
  - Policy modul: Eldönti, hogy a tanúsítvány kiadható-e. Csak egyetlen policy modul lehet aktív.
  - Exit modul: Közzéteszi az elkészült tanúsítványokat. Egyidejűleg több exit modul is használható.
- Az első két feltétel teljesítéséhez policy modul, az utolsóhoz exit modul fejlesztése szükséges. A policy modult kompletten kell cserélni.

Technikai korlátok

- AD-n kívüli tanúsítvány és CRL publikálás (exit modul fejlesztést vagy állandó kézi beavatkozást igényel)
- Nagy rendszerek (több ezer tanúsítvány) kezelésére alkalmatlan a Microsoft CA
- Tömeges tanúsítványkérés feldolgozást nem támogat

Esettanulmány: Szolgáltatói PKI rendszer kialakítása

SYNERGON

- A szóban forgó vállalat alapszolgáltatása révén ideális kapcsolatokkal rendelkezett egy bizonyos piaci szegmens szereplőihez.
- Reális lehetőségek kínálkoztak a PKI szolgáltatás értékesítésében.
- Feladatunk egy jól védett, viszonylag magas rendelkezésre állást biztosító, sokoldalú és rugalmas PKI rendszer létrehozása volt.
- A rendszernek több 10 000 tanúsítványt kellett kezelnie.

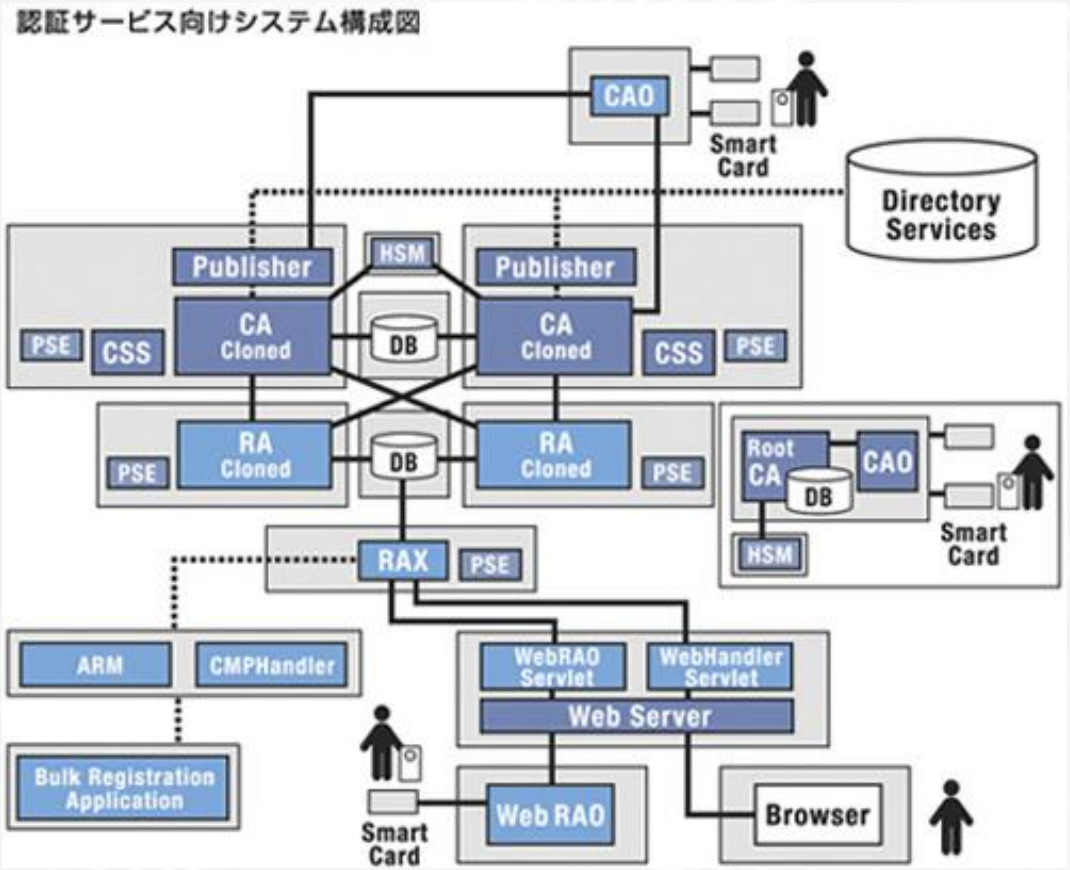
Mit jelent a „jól védett” jelző?

- A központi rendszer fizikai védelmének biztosítása:
  - többszintű beléptető rendszer
  - váltott őrök
  - központi riasztás
  - Faraday kalitka
  - megfelelő páratartalom és hőmérséklet biztosítása
  - tűzvédelem
- Helyi hozzáférés védelem:
  - erős (több faktorú) azonosítás
  - privát kulcsok Hardware Security Module-ban (HSM) tárolása
- Távoli hozzáférés védelem:
  - mélységi védelem (Defense of Depth) kialakítása a számítógépes hálózatban (tűzfalrendszer, behatolás megelőzés, központi naplózás)
  - szigorúbb esetben teljes hálózati szeparáció (a tanúsítványkéréseket kézzel másolják be, a tanúsítványokat kézzel továbbítják)

Egy összetett PKI rendszer alkotóelemei

- Tanúsítványhitelesítő központ részei
  - Certificate Authority (CA)
  - Certificate Authority Operator (CAO)
  - Certificate Status Server (CSS)
- Regisztrációs központ részei
  - Registration Authority (RA)
  - Registration Authority Operator (WebRAO)
  - Registration Handlers (WebHandler, EmailHandler, CMPHandler)
  - Registration Authority eXchange (RAX)
  - Advanced Registration Module (ARM)
- Publikus címtárszolgáltatás részei
  - Publisher
  - Directory Services

Egy komplex PKI rendszer felépítése



Forrás: www.betrusted.co.jp

Programozhatóság

- Microsoft CA
  - Entry modul
  - Policy modul
  - Exit modul
- UniCERT ARM
  - Inicializáció
    - ABL_StartUp
    - ABL_LogOn
    - ABL_InitComplete
    - ABL_StartRun
  - Induló ciklus
    - ABL_Pulse
    - ABL_PublishTemplates
    - ABL_PublishTemplatesComplete
    - ABL_ReadRequest
    - ABL_Idle
  - Regisztráció (14 callback fv.)
    - ABL_VerifyRequest
    - ABL_SaveRequest
    - ABL_RequestComplete

Szabályozási kérdések

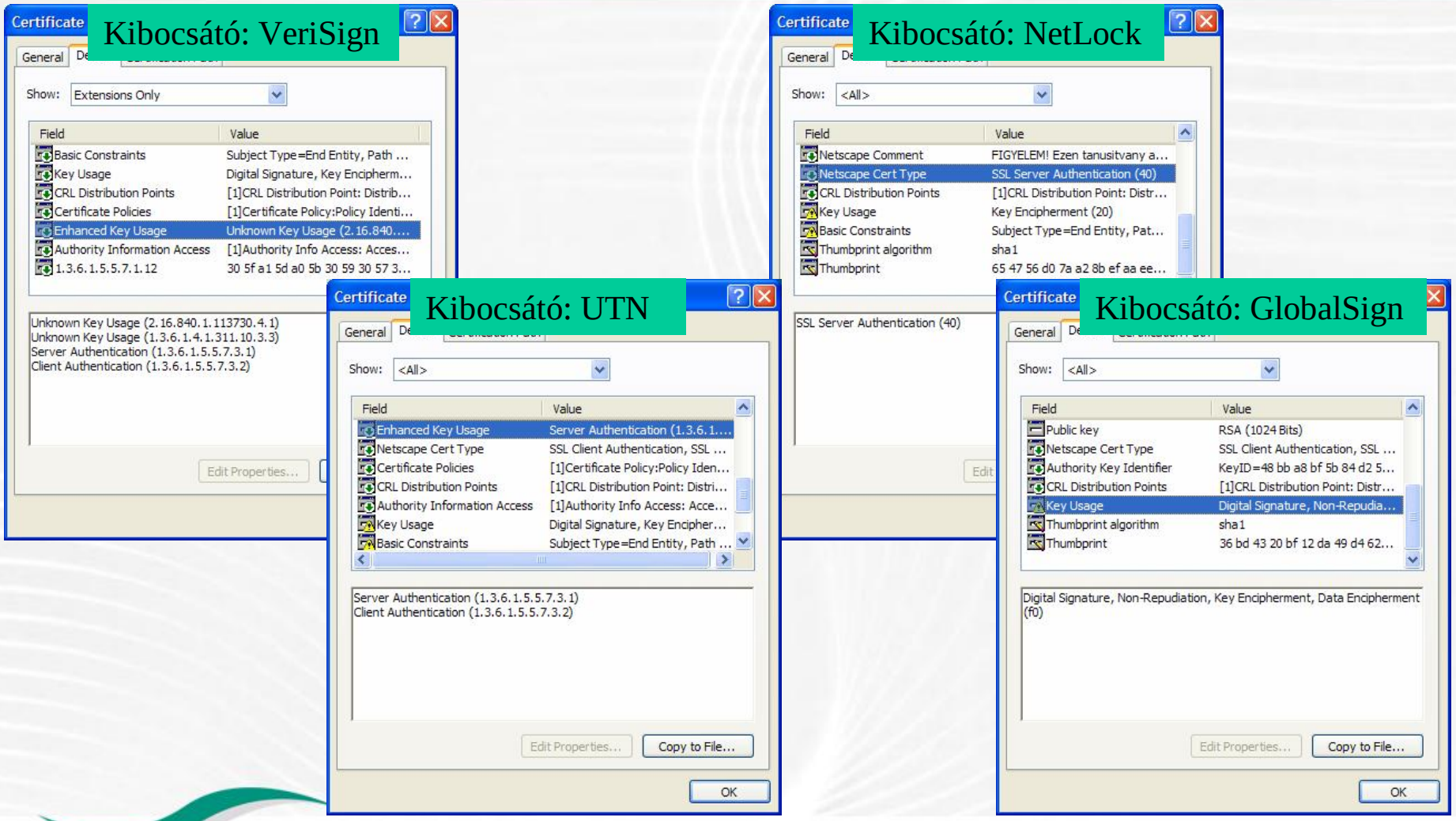
Tanúsítvány felépítése

- Lényeges alkotóelemek:
  - Kibocsátó (Issuer)
  - Tulajdonos (Subject)
  - Kulcshasználat (Key Usage)
  - Kiterjesztett kulcshasználat (Extended Key Usage)
  - Netscape tanúsítvány típus (Netscape Certificate Type)
  - Visszavonási lista helye (CRL Distribution Point; CDP)

Esettanulmány: SSL szerver tanúsítványprofil kialakítása

- A szerveroldali tanúsítvánnyal szembeni megkötés (Forrás: OpenSSL.org):
  - Key Usage: vagy hiányzik, vagy tartalmazza a Digital Signature és a Key Encipherment legalább egyikét.
  - Extended Key Usage: vagy hiányzik, vagy tartalmazza a Web Server Authentication és/vagy legalább egy Server Gated Cryptography OID értéket.
    - Microsoft SGC: 1.3.6.1.4.1.311.10.3.3
    - Netscape SGC: 2.16.840.1.113730.4.1
  - Netscape Certificate Type: vagy hiányzik, vagy tartalmazza az SSL Server beállítást.
- Kiegészítő beállítások:
  - Extended Key Usage: Client Authentication
  - Netscape Certificate Type: SSL Client

Ahány CA, annyi szokás?



SSL szerver tanúsítványprofilok

Key Usage Digital Signature, Key Encipherment			Extended Key Usage Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC					Netscape C. T. SSL Server, SSL Client		
-	DS	KE	-	SA	CA	MS	NS	-	S	C
-	VS	VS	-	VS	VS	VS	VS	VS	-	-
-	U	U	-	U	U	-	-	-	U	U
-	-	NL	NL	-	-	-	-	-	NL	-
-	GS	GS	GS	-	-	-	-	-	GS	GS
VS = VeriSign, U = UTN, NL = NetLock, GS = GlobalSign										

Jogi szabályozás Magyarországon

- Az elektronikus aláírásról szól a 2001. évi XXXV. törvény és több rendelet is.
- Az alábbi rendeletek szabályozzák a szolgáltatók működését:
  - 45/2005. kormányrendelet
    - szolgáltatók nyilvántartásba vétele, törlése
    - változások bejelentése
    - szolgáltató tevékenységének befejezés
  - 3/2005. IHM rendelet
    - a szolgáltatásokra és a szolgáltatókra vonatkozó részletes követelmények (szolgáltatói kulcspár kezelése, fizikai és környezeti biztonság, naplózás, archiválás, időszinkronizáció stb.)

Egyéb rendelkezések

- Az elektronikus ügyintézéssel kapcsolatos rendelkezések:
  - 193/2005. kormányrendelet
    - az elektronikus ügyintézés részletes szabályozása
    - viszontazonosítás
  - 194/2005. kormányrendelet
    - a közigazgatási hatósági eljárásokban használt elektronikus aláíráshoz kötődő követelményekről szól
  - 195/2005. kormányrendelet
    - az elektronikus ügyintézést lehetővé tevő rendszerek biztonságáról, egységes használatáról szól

Szakmai egységesítési törekvés

- Az elektronikus aláírásra vonatkozó egységes MELASZ formátumokról a következő weboldalon találnak további részleteket:
  - http://www.melasz.hu/documents/MMM_formatum_v1_0.pdf

Esettanulmány: Elektronikus számlázás

- Elektronikus számlát előállító és ellenőrző alkalmazás fejlesztése projekt.
- Feladat: elektronikus dokumentumok digitális aláírása és időbélyeggel ellátása.
- Az első verzióban egy régebbi szabvány, a PKCS#7-es szolgált alapul a számla formátumának meghatározásában.
- A dokumentumok digitális aláírását smart kártyával teszteltük. (Egy konkrét projektben a számlák tömegesen állítódnak elő, így biztosítani kellett, hogy a PIN kód beütésére egy előállítási folyamatban egyszer kerüljön sor.)
- Az elektronikus számlát kézhez kapó ügyfelektől nem várható el, hogy smart kártyával rendelkezzenek. Windows operációs rendszert használata esetén Microsoft kriptográfiai provider-t használhatunk a digitális aláírás ellenőrzésére.
- A digitális aláíráshoz RSA Cryptoki-t, az ellenőrzéshez Microsoft CryptoAPI-t használtunk.

Microsoft CAPI vs. RSA Cryptoki

- Microsoft CAPI (CryptoAPI): Windows alkalmazások kriptografikus funkciói valósíthatóak meg ezen az API-n keresztül.
- RSA Cryptoki: Kriptográfiai tokenekhez hozzáférést biztosító API.
- Összehasonlítás:
  - CryptoAPI-val mind szoftveresen tárolt, mind hardveren tárolt kulcsokkal tudunk dolgozni. A Cryptoki kifejezetten tokenekkel, smart kártyákkal foglalkozik.
  - A CryptoAPI egy-egy függvényhívása mögött több Cryptoki függvényhívás bújik meg.
  - Paraméterezhetőség tekintetében a Cryptoki jóval rugalmasabb mint a CryptoAPI.

CryptoAPI vs. Cryptoki

SYNERGON

- CryptoAPI
  - CPAquireContext
- Cryptoki
  - C_Initialize()
  - C_GetSlotList()
  - C_GetSlotInfo()
  - C_GetTokenInfo()
  - C_OpenSession()
  - C_Login()
  - C_FindObjectsInit() (4 hívás)

A „kihívás”

SYNERGON

- A projekt egyik kihívása a következő probléma megoldása volt:
  - Milyen paraméterezéssel kell meghívni a Cryptoki függvényeket, hogy CryptoAPI-val ellenőrizhető legyen a digitális aláírás?
  - Nem találtunk dokumentumot ebben a témában.
  - Néhány nap alatt kikísérleteztük a helyes paraméterezést.

A MELASZ és az elektronikus számla

- A MELASZ a XAdES-EPES formátum használata mellett tette le a voksát.
- El kellett vetni a PKCS#7-es kivitelezést, és elkészíteni az XML változatot.

Gara Péter, senior technikai tanácsadó

2007. április 22.

SYNERGON

Köszönöm figyelmüket!

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON