DR. NÉGYESI IMRE

AZ ELEKTRONIKUS ALÁÍRÁS LEHETŐSÉGEI A MAGYAR HONVÉDSÉGBEN I.

Az informatika térhódítása a hétköznapi életben, így a haderőben is, sokszor a technológiától való függést okozhatja, amely bizony komoly kockázatot jelenthet egy-egy területen. A piacvezető megoldások csak hosszabb távon képesek bizonyítani létjogosultságukat, így az új technológiákkal szemben a bizalmatlanság egy ideig teljesen érthető. Az informatikai rendszerek területén jelentkező új megoldások gyakran még a felkészült szakemberektől is komoly erőfeszítéseket igényelnek, hogy ismereteiket naprakészen tudják tartani. Egy új feladat megoldása a részterület alapos ismeretét, megismerését követeli meg, s a részterületeket „átlátni" képes vezetőket, menedzsereket, akik a megfelelő projekteket koordinálni tudják.

Mindez azonban nem jelenti azt, hogy félni kellene az újtól. Alapos, átgondolt tervezéssel legalább olyan mértékben lehet csökkenteni a biztonsági kockázatokat, mint amilyen szinten a „biztonságot" a jelenlegi gyakorlat garantálja. Ezen publikáció témáját adó elektronikus aláírással kapcsolatos irodalmakat tanulmányozva akaratlanul is fölmerült bennem a kérdés, miért nem használjuk még ezt a szolgáltatást? Hiszen munkánk során elektronikus dokumentumokat készítünk, elektronikus leveleket küldünk, s mindeközben érezzük, hogy bár az informatikai rendszerünk „védett", valahogy mégsem tudunk bízni ebben a védelemben. A cikk megírásának egyik indokaként tehát azt kell mondanom, hogy bár tény, miszerint több cikk, dolgozat született már ebben a témában, de jelentős előrelépés a mai napig sem történt. A másik okot a megírásra az a tény szolgáltatta, hogy az eddigi publikációk a napi feladatok felől közelítették meg a kérdést (ami természetesen nagyon fontos szempont), ugyanakkor nem világítottak rá eléggé a technikai háttér kérdéseire, nem helyeztek hangsúlyt az alapfogalmak ismeretére és ezzel mintegy „megfoghatatlanná vált" és ezzel egy időben ellenérzést váltott ki ez az új, jövőbemutató lehetőség. Ennek az ellenérzésnek a feloldását tűzte ki elsődleges céljául ez a publikáció.

Az előzőekben leírtaknak megfelelően dolgozatomban összefoglalást szeretnék nyújtani a nyilvános kulcsú infrastruktúra (PKI — Public Key Infrastructure) alapú elektronikus aláírás szolgáltatásról, mely — bár nem új technológia — jelenleg, mint szolgáltatás nem érhető el a Magyar Honvédség

(MH) informatikai rendszereiben. Mindezek mellett összefoglalom mindazokat a jogszabályokat is, amelyek meghatározzák mindazokat a követelményeket, melyeket az elektronikus aláírás bevezetésének tervezései során figyelembe kell venni. Nem kívánok részletesen foglalkozni a felhasználó hitelesítés, vagy a titkosítás kérdésével, mindössze ezek PKI technológiához kapcsolódása miatt térek ki az adott területekre. Célom az is, hogy bemutassam, milyen lehetőségek állnak rendelkezésre az elektronikus aláírás szolgáltatás bevezetésére egy zártcélú hálózat esetében. Milyen követelményeknek kell megfelelnie az informatikai infrastruktúrának, hogy elegendő legyen — az egyébként is elektronikus formában keletkező — dokumentumainkat elektronikusan aláírni úgy, hogy azok bizonyos területeken jogi értelemben is kiválthassák a hagyományos papírformát.

DOKUMENTUMKEZELÉS A MAGYAR HONVÉDSÉGBEN

A sokszor elhangzó papírmentes iroda valóra váltásához jobban kell bíznunk az elektronikus dokumentumainkban, tehát ezt a bizalmat meg kell teremteni. Ellenkező esetben a számítógépeket és nyomtatókat továbbra is, mint profeszszionális villanyírógépeket fogjuk alkalmazni. Közhelyszerű, de sajnos igaz, hogy a szervezeti átalakulások (átalakítások) nem mindig a szervezeti folyamatok racionalizálásából adódnak, így a létszámcsökkentések néha komoly problémákat okozhatnak a mindennapi működésben, így például a belső iratforgalom lebonyolításában is. Dolgozatomban bemutatom, hogy milyen módon célszerű tervezni az elektronikus aláírás szolgáltatás bevezetését. Összehasonlítást teszek, milyen előnyökkel-hátrányokkal járhat, ha az elektronikus aláírás szolgáltatást „házon belüli” megoldással szeretnénk biztosítani.

Nagyvállalati rendszerekben a dokumentumok kezelésének módja alapvetően vagy tisztán papír alapú, vagy elektronikus alapú, vagy a kettő kombinációja oly módon, hogy az egyik domináns, és a rendszer alapvető jellemzőinek meghatározója. A nagyvállalati vállalatirányítási rendszerek (ERP — Enterprise Resource Planning) ma már több-kevesebb dokumentumkezelési funkcióval rendelkeznek, de eredendően nem erre a feladatra lettek kitalálva. A valódi dokumentumkezelő rendszerek (DMS — Document Management System) az ERP-hez hasonlóan moduláris felépítésűek, s a dokumentumkezelés minden területére kiterjednek. Az elektronikus adatcsere rendszerek (EDI — Electronic Data Interchange) terjedésével, a belső levelező rendszerek, intranet alkalmazások mind szélesebb körű terjedése elősegíti a dokumentumkezelés elektronikus formába történő átalakítását.

Nyilvánvaló, hogy mindezek a jelenségek új kihívásokat is teremtenek, mint például az elektronikus dokumentumok hiteles archiválásának problémája, amelyet nem csak technikai oldalról kell megoldani, de az iratkezelési szabályozást is át kell alakítani. Biztató lehet, hogy az iratfelhalmozódást sürgető belső intézkedések MH szinten is arra késztetik az ügyviteli területen dolgozókat, hogy tájékozódjanak az elektronikus aláírás témakörében, mely a belső — HM szintű — iratkezelési, ügyviteli szabályozás megfelelő átalakítása után alkalmazhatóvá válhat.

Mielőtt azonban mindezeket a problémákat részletesebben is áttekintenénk, egy kis összefoglalást kell tenni magáról az aláírásról — mind a hagyományos, mind az elektronikus változatról — s megvizsgálni, mennyire felelnek meg a hitelesség, sértetlenség, letagadhatatlanság alapvető biztonsági követelményeinek. Napi munkánk során ma már egyre gyakrabban fordul elő az, hogy az „irodai végtermékünket" — mindamellett, hogy kinyomtatjuk, és aláírva tovább adjuk feldolgozásra — elektronikus formában is felhasználjuk, vagy legalább eltároljuk (archiváljuk). Legyen szó akár egy egyszerű jelentésről, beszámolóról, amit a főnök kér, vagy a havi munkaidő nyilvántartásról, a belső hivatalos kommunikációban résztvevő „hivatalos", aláírt papírnak még mindig óriási a jelentősége. A legtöbb helyen ma már kialakított belső levelezési rendszerek ugyan valamelyest csökkentik a fölöslegesen kinyomtatott oldalak számát, használatuk azonban ma még igencsak korlátozott. Ez egyrészt abból is adódik, hogy az általános vélekedés szerint jogilag nincs bizonyító ereje egy ilyen „hagyományos" e-mailnek, szemben az aláírt papírral. Ez ma már szerencsére nem teljesen igaz, azért mert elektronikus formában létezik és elektronikusan aláírt, hitelesített a dokumentum, még el kell fogadni. A kérdés, hogy hol és milyen feltételekkel? De valóban az egyedüli megbízható és járható út, hogy a „fontos", esetenként jogi, pénzügyi vonatkozással járó, egyébként elektronikus dokumentumainkat kinyomtatjuk és aláírjuk? Hogy ebben a témában egy kicsit tisztábban lássunk, vizsgáljuk meg, miért is írunk alá egy dokumentumot. Majd nézzük meg, milyen kritériumoknak kell megfelelnie az aláírásnak (a hagyományos és elektronikus aláírásnak egyaránt), s ezeket kritériumokat hogyan teljesíti.

A vizsgálat tárgyát képező elektronikus dokumentumoknak az alábbi formáit különböztethetjük meg:

– az *elektronikus dokumentum*, bármely erre alkalmas eszköz útján érzékelhető adat, melyet elektronikus aláírással láttak el. Ez a hétköznapi fogalmaink szerint inkább tárgynak tekinthető, pl. egy térkép, tervrajz, fénykép. Ezeket is alá lehet írni elektronikusan, és az aláírás bizonyítani fogja, hogy az „elektronikus tárgy" az aláírás pillanatában milyen állapotban volt. Ez a hibás teljesítés körében jelentőséggel fog bírni. A hitelességet elősegíti az is, ha az elektronikus dokumentumhoz időbélyegző is kapcsolódik;

– az *elektronikus irat* funkciója az, hogy szöveget közöljön és más adat legfeljebb a szöveg azonosítását vagy könnyebb megértését szolgálja (pl. fejléc);
– az *elektronikus okirat* nyilatkozattételt illetőleg nyilatkozat elfogadását, vagy kötelező jellegének elismerését teszi lehetővé. Az elektronikus okiratot a törvény az eljárási törvényekben szereplő okirati bizonyítási eszközök virtuális megfelelőjeként hozta létre.

A HAGYOMÁNYOS ALÁÍRÁS ISMÉRVEI

Az aláírás célja valaminek az igazolása, akár jóváhagyólag, akár tagadólag, például nyilatkozattétel, szerződéskötés vagy kötelezettségvállalás céljából. Ez egyaránt igaz a hagyományos és az elektronikus aláírásra is. Az aláírást általában egy irattal összefüggésben tesszük meg, s ez esetben az igazolás az irat *hitelesítését* jelenti. Leggyakrabban az irat származását, szerzőségét, a tartalom saját véleményünkként való elismerését, vagy csak az elolvasását jelzi az iraton elhelyezett aláírásunk. Az aláírással biztosítani kívánjuk az irat *sértetlenségét* is, vagyis azt, hogy az iratot az aláírás megtételét követően ne lehessen megváltoztatni, illetve ha mégis megtörténne egy ilyen változtatás, akkor az észlelhető legyen. Mind emellett az aláírás gondoskodik arról is, hogy a megtett igazolást utólag *ne tagadhassa le* az aláíró.

Így tehát az aláírás célja ezek alapján:
– hitelesség: az irat származásának igazolása;
– sértetlenség: az irat tartalmának biztosítása;
– letagadhatatlanság: az irat jogilag is bizonyító erejének biztosítása.

A következőkben vizsgáljuk meg, hogyan teljesíti ezen kitűzött követelményeket a hagyományos aláírás. A hagyományos aláírás a név egyedi formában történő papírra vetését jelenti. Ez az egyedi forma a kézjegy, vagy szignó.

Természetesen a kézjegy változik az életkorral, de befolyásolhatja a megtett aláírásunkat a pillanatnyi hangulatunk is. Így tehát egy embernek több kézjegye is létezhet, akár több célra külön-külön kialakított egyedi mintával. Az egyediség feladata minden esetben a *hitelesség* biztosítása. Az aláírás megtétele a *letagadhatatlanság* érdekében eltávolíthatatlan és megváltozhatatlan formában, vagyis tollal és tintával szokott történni. A sértetlenség garantálása végett az aláírás általában a dokumentum végén (vagy akár minden oldal alján megismételve) kap helyet. A hivatalos életben gyakran egészíti ki az aláírást egy pecsét, mely plusz tulajdonsága, hogy birtokolni kell. Plusz információként közölheti azt is, hogy az aláírás megtevője jogosult aláírni az iratot. (Pl. személyügyi, pénzügyi pecsét, stb.)

Az aláíráshoz tehát mindezek alapján nem kell más, mint egy golyóstoll és az írástudás képessége. Az aláírás ellenőrzéséhez pedig csupán az aláírás mintájának ismerete szükséges, aminek birtokában az aláírás eredetisége „könnyen" eldönthető. Látnunk kell tehát, hogy a hagyományos aláírás igen komoly kockázatokat rejt magában. Az aláírás a legtöbbször nem olvasható, így a tulajdonosa nem megállapítható, hacsak az külön nincs feltüntetve. Az aláírás hitelességéről is csak úgy tudunk meggyőződni, ha ismerjük az eredeti aláírásmintát (csak ennek ismeretében rendelhetjük össze az aláírást tulajdonosával). Így tehát minden egyes elfogadó előtt meg kell tenni a hiteles aláírást. (Például a bankok esetében a gyakorlati életben egy aláíró karton kitöltésével szokott erre sor kerülni.)

Ennek hiányában az aláírás hitelessége csak utólag tisztázható, rendszerint bírósági eljárás keretében, írásszakértő bevonásával. Tehát kijelenthető, hogy bizonyítás szempontjából elég problémás és sokszor már csak eső után köpönyeg. Az aláírások legtöbbje könnyen hamisítható, hiszen az aláírások egyedi mintája — legtöbbször egy másik aláírt dokumentumról — az esetek többségében nyilvánosan hozzáférhető. A köznapi életben pedig sajnos nem léteznek az aláírás kialakítására vonatkozóan általánosan követett biztonsági szabályok. Az az eset pedig, amikor valaki szándékosan nem az általánosan használt aláírását használja egy iraton, hogy később azt letagadhassa, szintén csak körülményesen tisztázható.

AZ ELEKTRONIKUS ALÁÍRÁS ISMÉRVEI, FAJTÁI

Az elektronikus aláírás tulajdonképpen bizonyos szempontból bármi lehet, amivel nevünket egy elektronikus irat végén elhelyezzük. Legyen az a dokumentum végére gépelt nevünk, vagy a beszkennelt aláírásunk, önmagukban ezek bizonyító ereje igencsak kétséges. Az elektronikus aláírás egy konkrétabb megfogalmazás szerint olyan bitsorozat, amely egy matematikai algoritmussal állítható elő, és nem értelmezhető másként, csak egy másik matematikai algoritmus által. A jogszabály szerint az elektronikus aláírás elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.

Fokozott biztonságú elektronikus aláírásnak a törvény azt az elektronikus aláírást tekinti, amely megfelel az alábbi követelményeknek:

- alkalmas az aláíró azonosítására és egyedül hozzá köthető;
- olyan aláíró eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll;
- a dokumentum tartalmához olyan módon kapcsolódik, hogy minden — az aláírás elhelyezését követően az iraton, illetve dokumentumon tett — módosítás érzékelhető.

Mindezeket is figyelembe véve az elektronikus aláírásnak a következő fajtáit különböztethetjük meg:

- *Egyszerű" elektronikus aláírás*: A törvény által használt elektronikus aláírás fogalmába beletartozik az a nem biztonságos eljárás is, ha az aláíró egy elektronikus szöveg végére odaírja a nevét. Ezt a kört nevezhetjük „egyszerű" elektronikus aláírásnak.
- *Fokozott biztonságú elektronikus aláírás*: Ez alkalmas az aláíró azonosítására és a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden, az aláírás elhelyezését követően az iraton illetve dokumentumon tett módosítás érzékelhető. A technika jelenlegi állása mellett ez már a nyilvános kulcsú aláírást jelenti. Az ilyen aláírást hitelesítés-szolgáltató cég tanúsítja.
- *Minősített elektronikus aláírás*: Ez fokozott biztonságú elektronikus aláírás, amely megfelel a fejlett technológiájú minősített hitelesítés-szolgáltatóval szembeni szakmai és megbízhatósági követelményeknek. Az ilyen aláírást minősített hitelesítés-szolgáltató tanúsítja.

A hagyományos és az elektronikus aláírás összehasonlítása

Amennyiben össze szeretnénk hasonlítani a hagyományos aláírást az elektronikus aláírással az aláírás létrehozása és ellenőrzési módja szerint — bár nyilvánvaló, hogy a két aláírás egymásnak nem lehet minden területen riválisa —, beláthatjuk, hogy bizonyos esetekben miért van létjogosultsága az elektronikus aláírásnak. Az összehasonlításhoz tekintsük a következő két táblázatot.

1. sz. táblázat

Az aláírás megtételi módszerek jellemzői

	HAGYOMÁNYOS ALÁÍRÁS	ELEKTRONIKUS ALÁÍRÁS
CÉL	Hitelesség, sértetlenség, letagadhatatlanság	Hitelesség, sértetlenség, letagadhatatlanság
ELJÁRÁS	Szignó lerajzolása	Matematikai algoritmusok
SZÜKSÉGES ESZKÖZ	Toll, tinta	Aláíró eszköz és környezet
SZÜKSÉGES TUDÁS	Aláírás minta ismerete	Aktivizáló adat (jelszó) ismerete
SZÜKSÉGES BIRTOK	—	Aláírás-létrehozó adat (magánkulcs)

2. sz. táblázat

Az aláírás ellenőrzési módszerek jellemzői

	HAGYOMÁNYOS ALÁÍRÁS	ELEKTRONIKUS ALÁÍRÁS
ELJÁRÁS	Szignó eredetivel történő vizuális összehasonlítása; az írás utólagos javításainak ellenőrzése	Matematikai algoritmusok
SZÜKSÉGES ESZKÖZ	—	Aláírás-ellenőrző környezet (pl. számítógép
SZÜKSÉGES ISMERET	Eredeti aláírás minta ismerete	Aláírás-ellenőrző adat (nyilvános kulcs) ismerete
EGYÉB KÖVETELMÉNY	—	Harmadik fél közreműködése (PKI esetén)

Az elektronikus aláírás készítéséhez és ellenőrzéséhez az alábbi feltételek teljesítése szükséges:

Az aláírás megtételéhez a következők szükségesek:

- az aláírandó elektronikus irat;
- személyes aláírás létrehozó adat (magánkulcs);
- aláíró eszköz és környezet (számítógép, mobiltelefon, intelligens kártya, stb.).

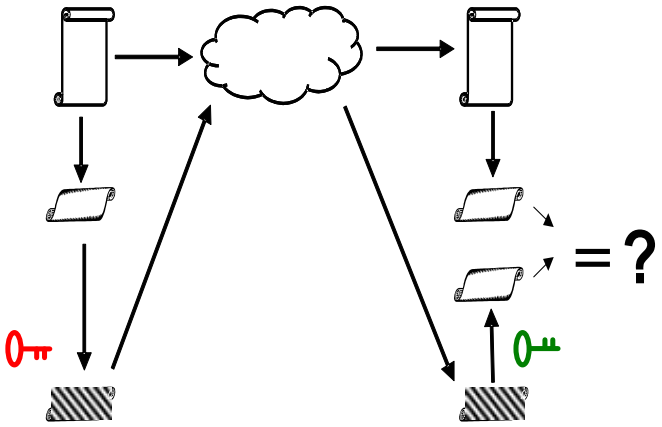
Az elektronikus aláírás ellenőrzéséhez pedig a következők kellenek:

- az aláírással ellátott elektronikus irat;
- az aláíráshoz tartozó aláírás-ellenőrző adat (nyilvános kulcs);
- aláírás ellenőrző környezet.

Ahhoz, hogy mindez ilyen „egyszerűen” egymást érteve együtt tudjon működni, szükségesek még algoritmusok, protokollok, alkalmazások, jogszabályok, szabványok és intézmények.

1. sz. ábra

Elektronikus aláírás elkészítése és ellenőrzése



A manapság elterjedt megoldások közül — bár a törvény kifejezetten technológia semleges e tekintetben — a nyilvános kulcsú infrastruktúrán (PKI) alapuló elektronikus aláírás elégíti ki a fenti követelményeket. A hagyományos aláírás kapcsán már áttekintettem, mi ellen kíván védelmet nyújtani az aláírás a köznapi életben. Az iratkezelés elektronikus formába történő átalakulása és még inkább az elektronikus kommunikáció kapcsán azonban a már korábban is létező veszélyek sokkal élesebben jelentkeznek, mint előtte. Nemcsak azért, mert manapság sokkal több információ áramlik elektronikusan, mint korábban bármikor papíron, hanem mert az adatok továbbításához használt kommunikációs csatorna mind a küldő és a fogadó fél számára gyakran észrevétlenül támadható (a személytelenné vált információtovábbító rendszer — megfelelő mechanizmusok nélkül — nem képes észlelni a támadást).

A hiteles kommunikációban résztvevő felek — jelen esetben a felhasználók — azonosítására elterjedt módszerek összehasonlítását az alábbi ábrán összefoglalva láthatóvá válnak az egyes módszerek közötti lényeges különbségek, valamint a PKI lehetőségei.

ALÁÍRÓ FÉL

DOKUMENTUM

Lenyomatkészítés
(Hash-algoritmus)

LENYOMAT

Kódolás a magánkulccsal

2. sz. ábra

Hiteles kommunikáció — PKI lehetőségek

A hiteles kommunikáció	Felh. név / Jelszó	Szimmetrikus kulcs	Hardver megoldások	PKI
azonosítás Identity Authentication	✓	✓	✓	✓
személyhez kötés Privacy / Encryption and decryption		✓	✓	✓
eredetiség Message integrity Temper detection		✓	✓	✓
letagadhatatlanság Nonrepudiation			✓	✓
"nemzetköziség" Global interoperability				✓

Forrás: Aberdeen Group

A már évtizedekkel ezelőtt is létezett egyedi, lokális és zárt hálózatok esetében ez a probléma kevésbé jelentkezett ilyen élesen, mert a hálózati forgalom csak a belső felhasználók által volt támadható. A külső „ellenségektől” igen magas műszaki ismereteket és kémfilmekbe illő módszereket kívánt ugyanez a feladat. A hálózatok egyre kiterjedtebbé, nyitottá és szabványossá válásával, a WAN, extranet és internet alapú infokommunikációs módszerek elterjedésével ugyanez a támadás már a külső felhasználóktól se kíván James Bond szintű felszerelést és tudást. Sőt az interneten könnyen elérhető kész vagy félkész hackerprogramok, amolyan instant „törjük meg könnyen és gyorsan” módszereket kínálnak az egyébként nem profi informatikus, „hobbihackerek” számára is.

JOGSZABÁLYI HÁTTÉR, SZABÁLYOZÁS

Mielőtt áttekintenénk az elektronikus aláírás létrehozásának elméleti alapjait, tisztáznunk kell azt is, hogy milyen törvényi, jogszabályi alapokon kell majd alkalmaznunk az elektronikus aláírással kapcsolatos szolgáltatásokat. Az Országgyűlés — felismerve és követve az egyetemes fejlődésnek az információs

társadalom felé mutató irányát, az új évezred egyik legfontosabb kihívásának eleget téve — törvényt alkot az elektronikus aláírásról annak érdekében, hogy megteremtse a hiteles elektronikus nyilatkozattétel, illetőleg adattovábbítás jogszabályi feltételeit az üzleti életben, a közigazgatásban és az információs társadalom által érintett más életviszonyokban. Az Országgyűlés által jóváhagyott két törvény a 2001. évi XXXV. törvény, amelynek egyes részeit az Országgyűlés a 2004. évi LV. törvényével módosított. A két törvény a módosításokkal együtt a következő fogalmakat tisztázza:

1. *Aláírás-létrehozó adat:* olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.
2. *Aláírás-ellenőrző adat:* olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
3. *Aláírás-létrehozó eszköz:* olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
4. *Aláíró:* Az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult.
5. *Biztonságos aláírás-létrehozó eszköz:* az e törvényben foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.
6. *Elektronikus aláírás:* elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.
7. *Elektronikus aláírás ellenőrzése:* az elektronikus dokumentum aláírás kori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, valamint a tanúsítvány felhasználásával.
8. *Elektronikus aláírás felhasználása:* elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése.
9. *Elektronikus aláírás hitelesítés-szolgáltató:* a 6. § (2) bekezdése szerinti tevékenységet végző személy (szervezet).
10. *Elektronikusan történő aláírás:* elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz.
11. *Elektronikus aláírási termék:* olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, valamint elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható.

12. *Elektronikus dokumentum:* elektronikus eszköz útján értelmezhető adat együttes.
13. *Elektronikus aláírás érvényesítése:* annak tanúsítása minősített elektronikus aláírás vagy e szolgáltatás tekintetében minősített szolgáltató által kibocsátott időbélyegző elhelyezésével, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegző elhelyezésének időpontjában érvényes volt.
14. *Érvényességi lánc:* az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás-ellenőrző adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató elektronikus aláírás ellenőrző adatára és annak visszavonására vonatkozó információk), amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt.
15. *Fokozott biztonságú elektronikus aláírás:* elektronikus aláírás, amely
    a) alkalmas az aláíró azonosítására,
    b) egyedülállóan az aláíróhoz köthető,
    c) olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak,
    d) a dokumentum tartalmához olyan módon kapcsolódik, hogy minden — az aláírás elhelyezését követően a dokumentumon tett — módosítás érzékelhető.
16. *Időbélyegző:* elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett.
17. *Minősített elektronikus aláírás:* olyan — fokozott biztonságú — elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.
18. *Minősített hitelesítés-szolgáltató*: az e törvény szabályai szerint nyilvántartásba vett, minősített tanúsítványt a nyilvánosság számára kibocsátó hitelesítés-szolgáltató.
19. *Minősített tanúsítvány*: az e törvényben foglalt követelményeknek megfelelő olyan tanúsítvány, melyet minősített szolgáltató bocsátott ki.

20. *Szolgáltatási szabályzat*: a 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.
21. *Tanúsítvány*: a hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot a 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

Az idézett két törvény természetesen további követelményeket, szabályokat is meghatároz, amelyek átfogó ismertetésére a terjedelmi korlátok miatt nincs lehetőség. Mindezek mellett további rendeletek is születtek ebben a tárgyban, amelyek közül megemlítést érdemel a 3/2005. (III. 18.) IHM rendelet „az elektronikus aláírással kapcsolatos szolgáltasokra és ezek szolgáltatóira vonatkozó részletes követelményekről" címmel, a 7/2005. (VII. 18.) IHM rendelet „ a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól" címmel, valamint a 9/2005. (VII. 21.) IHM rendelet „az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról" címmel. Ez e tárgyban további kutatásokat végzők számára ezek a rendeletek további információkkal szolgálhatnak.

A KRIPTOGRÁFIA ALAPJAI

A PKI jobb megértéséhez — miután az a kriptográfiára, mint tudományra „épül" — szólni kell néhány szót a kriptográfiáról röviden, valamint tisztázni néhány fogalmat.

A titkos kommunikáció klasszikus problémáival a kriptográfia foglalkozik, amely külön tudományterületté vált. A nyilvános kutatások az 1970-es évek közepétől egyre növekvő intenzitással folynak, ahogy a katonai és diplomáciai életen kívül (államtitok) az üzleti és magánéletben is egyre fontosabb kérdés a bizalmas információk védelme (üzleti és magán titok). Tágabb értelemben véve, a titkos, védett kommunikáció tudománya a *kriptológia*, amelynek két — egymással állandóan rivalizáló — ága a *kriptográfia* és a *kriptoanalízis*.

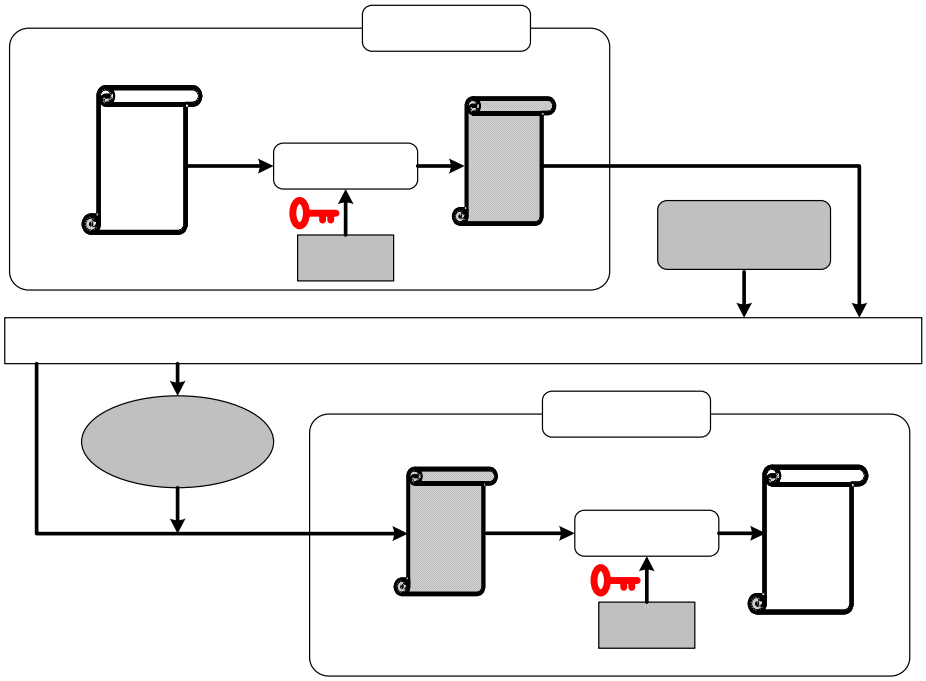
A *kriptográfia* olyan módszerekkel foglalkozik, amelyek biztosítják az üzenetek vagy tárolt információk titkosságát, védettségét, illetve hitelességét. Eszközei matematikai módszereket alkalmazó algoritmusok, amelyek használatának pontos leírását a *kriptográfiai protokollok* tartalmazzák. A kriptoanalízis pedig a titok — többnyire illetéktelen — megfejtésére, feltörésére irányuló eljárásokkal foglalkozik. A titkos kommunikáció folyamatában a küldő (sender) és a fogadó (reciever) titkos üzenetváltása valósul meg. A küldő rendelkezésére áll a nyílt szöveg (plain text), amelyből titkosítás

(encryption) segítségével állítja elő a kriptoszöveget (cypher text). Ezt a kommunikációs csatorna segítségével juttatja el a fogadónak, aki azt visszafejti (decryption), és így megkapja az eredeti nyílt szöveget.

A kriptoszöveg előállításához a titkosító algoritmuson kívül általában egy úgynevezett kulcs (key) is szükséges, amelynek ismerete mind a titkosításnál, mind pedig a visszafejtésnél szükséges. A megfelelő titkosító és visszafejtő kulcs nélkül általában az algoritmus ismeretében sem lehetséges a titkosítás és visszafejtés műveleteinek elvégzése. Az alábbi ábrán a titkos kommunikáció vázlata látható.

3. sz. ábra

A titkos kommunikáció általános sémája



A titkosító és visszafejtő kulcsnak nem kell feltétlenül megegyeznie. Az olyan titkosító algoritmust, amelyben a titkosításnál és visszafejtésnél is ugyanazt a K kulcsot kell használni, *szimmetrikus algoritmusnak* nevezzük. A nyilvános kulcsú — vagy más szóval *aszimmetrikus — algoritmus* pedig kulcspárt használ. Az egyik kulcs a *nyilvános kulcs* (public key), amellyel a titkosítást végezzük. A másik pedig a *magán kulcs* (private key), amit a visszafejtésnél használunk. A nyilvános kulcs bárki számára megismerhető — például egy publikus adatbázisból letölthető — míg a magán kulcsot csak tulajdonosa ismeri.

Titkosító algoritmusok

A továbbiakban néhány olyan algoritmusról lesz szó, amelyek egy részével minden bizonnyal találkozni fog az, aki elektronikusan szeretne dokumentumokat aláírni. Megbarátkozni nem kell minden rejtélyesnek tűnő rövidítéssel, de a legalapvetőbbek jelentésével jobb, ha tisztában vagyunk. Így talán kevésbé esünk abba a hibába, hogy a misztikum kategóriába soroljunk egy kijelentést, hogy a szolgáltatónk SHA-1 RSA 1024 bites nyilvános kulcsot bocsátott ki részünkre.

Bár az algoritmusok fontosságát sokszor túlzásba viszik maguk a gyártók is, való igaz, résen kell lenni, mit választ az ember, ha az elektronikus aláírás bevezetésén gondolkodik. Megfelelő algoritmust és kulcshosszt kell választani, hogy a kriptoanalízissel szemben „legalább" a tervezett időn belül védett legyen a rendszer. Itt ugyan nem foglalkozom részletesen azzal, hogy elméletileg mennyi idő kell az egyes algoritmusok feltörésére, s melyik a „jobb", hiszen ehhez mélyebben bele kellene menni az algoritmusok működésébe, ezt számos szakirodalomban megtaláljuk. A legismertebb DES, 3DES, IDEA, CAST, és AES algoritmusokról lesz szó röviden ebben a részben, a mélyebb matematika nélkül.

Minden idők legelterjedtebb szimmetrikus blokktitkosító algoritmusát 1977-ben szabadalmaztatták az USA-ban, mely 56 bites kulccsal 64 bites blokkokat kódol 64 bites blokkokká, s mivel igen gyors, hardveres megvalósítása eredményesen használható soros titkosítás céljára is (például kommunikációs berendezésekben). Bár az 56 bites kulcsméret feltörése mára elérhető közelségbe került, az algoritmus a kulcsméret növelésével máig használható. Bár a DES algoritmusnak számos változata létezik, melyek orvosolják az előbbi gyengeségeit (DESX, CRYPT(3), DES alternatív S boxal, GDES, RDES) mégsem ezek, hanem az izomból dolgozó 3DES (Triple-DES) terjedt el. Ennek egyrészt oka az is, hogy így a meglévő hardveres megoldások továbbra is használhatóak, csak többször kell megfuttatni az eszközöket.

Maga az algoritmus három egymást követő DES eljárás, természetesen három különböző kulccsal. Az algoritmust 1990-ben a DES kiváltására PES (Proposed Encryption Standard) néven hozták létre, majd 1992-ben IDEA (International Data Encryption Algorithm) néven nyerte el végső formáját. Sokak szerint ez az egyik legjobb és legbiztonságosabb szimmetrikus algoritmus. 64 bites blokkot és 128 bites kulcsot használ, azonos formában titkosításra és visszafejtésre is. Az IDEA szoftveres megvalósítása kb. kétszer gyorsabb, mint a DES-é, s hasonlóan eredményes hardveres megoldások is készültek.

A később bemutatásra kerülő PGP rendszer is a 3DES és IDEA algoritmusokat használja szimmetrikus titkosításra. Ezt az algoritmust 1993-ban, Kana-

dában fejlesztette ki Carlisle Adams és Stafford Tavares, akik nevének kezdőbetűikből adódik az elnevezés. Az eredeti CAST 64 bites blokkot és 64 bites kulcsot használ. Erősségét egy 8 bites bemenettel és 32 bites kimenettel rendelkező speciális S-boksz adja, amely nem kulcsfüggő, hanem alkalmazásfüggő. Így minden CAST implementációnál egyedileg kerül meghatározásra, milyen S-boxokat használ. A kanadai kormány ezt a szabadalommal is védett algoritmust új titkosítási szabványként kezeli.

A Northern Telecom használja a nagy biztonságot nyújtó szoftvercsomagjában a CAST algoritmust, természetesen nem publikált S-boksz szerkezettel. A PGP rendszer a CAST algoritmust használja a PGPdisk alkalmazásban a lemezek titkosítására. Az amerikai National Institute of Standards and Technology (NIST) 1997-ben pályázatot írt ki a DES leváltására alkalmas szabvány kidolgozására. A döntőbe jutott öt megoldás közül végül Joan Daemen és Vincent Rijmen „Rijandel" algoritmusa győzött. Az USA-ban 2001 óta szabványos algoritmus polgári felhasználásra is, mely támogatja a 128, 192, és a 256 bites kulcsok alkalmazását. A NATO nyilvános kulcsú infrastruktúra (NPKI) jelenleg 128 bites kulcsmérettel támogatja különböző célokra.

Aszimmetrikus algoritmusok

A nyilvános kulcsú algoritmusok közül a legismertebb az RSA, amely a feltalálók (Ronald Rivest, Adi Shamir, Leonard Adleman) nevének kezdőbetűiből kapta elnevezését. 1978-ban dolgozták ki az eljárást, mely a faktorizáció problémáján alapul. Két prímszám szorzatát kiszámítani meglehetősen egyszerű, ám ha ez a két prím szám megfelelően nagy, akkor az így előállt szorzatból az eredeti két számot (prímtényezőket) visszaszámolni már korántsem egyszerű. Gyakorlatban a problémát a megfelelő erősségű prímszámok megtalálása jelenti. Bár az eljárás ellen több támadás is ismert, ezek ellen lehet védekezni a prímszámok és a kulcsgenerálás egyéb paramétereinek gondos megválasztásával. Az eljárás blokkok rejtjelezésével működik, kulcs- és blokkméretként kettő hatványait felhasználva (512, 768, 1024, 2048 bit). A 2048 bit hosszú kulcsok akár katonai célokra is megfelelőek. (Lásd később.) Az RSA algoritmus mintegy ezerszer lassabb, mint a DSA.

A DSA algoritmus az RSA legnagyobb konkurense az elektronikus aláírás területén (az eljárás titkosításra és kulcsszétosztásra nem alkalmas). Az eljárást a National Security Agency (NSA) fejlesztette ki, és 1994-ben az USA digitális-aláírás szabványává vált[1]. A módszer az RSA-hoz hasonlóan a prímszámokkal dolgozik, de nem a faktorizálás, hanem a diszkrét logaritmus problémá-

[1] FIPS PUB 186-2 — Digital Signature Standard

ját alapul véve. A módszert az NSA szabadalma védi, ami miatt elég nagy a bizalmatlanság vele szemben. Való igaz, hogy a szervezet a lehallgatásban érdekelt, de az aláírás hamisításához nem fűződik nemzetbiztonsági érdek az USA-ban sem, így a módszer többnyire elfogadott. A módszer mintegy huszonötször lassabb az ellenőrzésekor az RSA-nál — az aláírás közel egyforma sebességű — ám kevesebb támadás ismert ellene.

Az ECDSA algoritmus a DSA egyik variánsa, mely az elliptikus görbék (innen az EC, Elliptic Curve) esetében fellépő diszkrét logaritmus problémáját hasznosítja. Az ECDSA algoritmus legnagyobb előnye a DSA-val és RSA-val szemben, hogy kisebb kulcsok felhasználásával is elérhető ugyanaz a biztonsági szint, és ezen eljárásoknál gyorsabb mind az aláírás elkészítése, mind pedig azok ellenőrzése. Megvalósítása így könnyebb lehet kis memóriával rendelkező eszközök, és nagy aláírási teljesítményt felmutatni képes hardverek esetében. Az IEEE és az ANSI pénzügyi szervezetek részére ANSI X9.62 néven szabványosította az eljárást. A DSA-val ellentétben titkosításra is alkalmazható.

A lenyomatkészítő eljárás egy egyirányú hash-függvényen alapszik. A hash-függvény tetszőleges hosszúságú szövegből olyan, fix hosszúságú bitsorozatot állít elő, amely egyértelműen jellemző az adott szövegre (az adott szöveg lenyomata mindig ugyanaz lesz). Ez a fix hosszúságú bitsorozat a lenyomat, más néven üzenetkivonat. Az alkalmazott hash-algoritmusok főbb jellemzői:

- *egyirányúak* (a lenyomatból képtelenség az eredeti dokumentumot visszaállítani, vagy annak tartalmára következtetni. Lehetetlen egy lenyomathoz olyan dokumentumot kreálni, amelyhez a transzformáció ugyanazt a lenyomatot rendeli);
- *ütközésmentesek* (lehetetlen két olyan dokumentum készítése, melyek azonos lenyomatot eredményeznének);
- *lavinahatásúak* (ha egy bitet megváltozatunk a dokumentumban, akkor a lenyomatok bitjei közel a felében különbözni fognak.).

A hash-függvény egyirányú volta miatt szükséges az elektronikus aláírás ellenőrzésekor újra előállítani a lenyomatot. Lavinahatása miatt észlelhető, ha az eredeti dokumentumban változás történt.

Az alkalmazott lenyomatkészítő függvények közül manapság az SHA-1 különböző változatai elterjedtek, de találkozhatunk még az MD-5 (Message Digest), és a RIPEMD-160 algoritmusok nevében is. Az NPKI jelenleg a Digital Signature Standard részét képező SHA 256 bites algoritmust támogatja, míg itthon a MÁV Informatika Kft. jelenleg 160 bites hash-függvényeket használ.

Mintegy összefoglalva az eddigieket álljon itt az NPKI jelenlegi és 2008-ig tervezett algoritmus és kulcstámogatásra kiadott táblázata.

3. sz. táblázat

NPKI algoritmusok használata — jelenlegi helyzet[2]

BIZTONSÁGI SZOGÁLTATÁS	FUNKCIÓ	ALGORIT-MUS	SZABVÁNY	PARAMÉ-TER SIZE
NPKI ROOT CA				
Sértetlenség, hitelesség	Hash	SHA-256	FIPS 180-2	256
	Aláírás	RSA	PKCS #1	4096
Bizalmasság	Titkosítás	AES	FIPS 197	128
Alárendelt NPKI CA-k				
Sértetlenség, hitelesség	Hash	SHA-256	FIPS 180-2	256
	Aláírás	RSA	PKCS #1	2048
Bizalmasság	Kulcs-csere	RSA	PKCS #1	2048
	Titkosítás	AES	FIPS 197	128
Végfelhasználó				
Sértetlenség, hitelesség	Hash	SHA-256	FIPS 180-2	256
	Aláírás	RSA	PKCS #1	2048
	Hash[3]	SHA-1	FIPS 180-1	160
	Aláírás	DSA	FIPS 186-2	1024
Bizalmasság	Kulcs-csere	RSA	PKCS #1	2048
	Kulcs-csere	Diffie-Hellman	—	2048
	Titkosítás	AES	FIPS 197	128

[2] Forrás: NATO Public Key Infrastructure Certificate Policy —ANNEX1

[3] A DSA és SHA-1 csak a DSA aláírások ellenőrzésére szolgál, nem aláírás készítésre!

4. sz. táblázat

NPKI algoritmusok tervezett használata — 2008-ig[4]

SECURITY SERVICE	FUNCTION	ALGORITHM	STAN-DARD	PARAM SIZE
NPKI ROOT CA				
Sértetlenség, hitelesség	Hash	SHA-512	FIPS 180-2	512
	Aláírás	ECDSA		512
Bizalmasság	Titkosítás	AES	FIPS 197	256
Alárendelt NPKI CA-k				
Sértetlenség, hitelesség	Hash	SHA-384	FIPS 180-2	384
	Aláírás	ECDSA		384
Bizalmasság	Kulcs-csere	MQV		384
	Titkosítás	AES	FIPS 197	256
Végfelhasználó				
Sértetlenség, hitelesség	Hash	SHA-256	FIPS 180-2	256
	Aláírás	ECDSA		256
Bizalmasság	Kulcs-csere	MQV		256
	Titkosítás	AES	FIPS 197	128

Amennyiben olyan rendszert szeretnénk létrehozni, amelynél már a tervezéskor figyelembe vesszük a későbbi interoperabilitási lehetőségeket, egy bonyolult kereszthitelesítési rendszert spórolhatunk meg a fenti paraméterek figyelembe vételével.

Kriptográfiai protokollok

Az eddigiekben szó esett a kriptográfia fontos területéről, az algoritmusokról. Ugyanilyen fontos azonban szót ejtenünk a kriptográfiai protokollokról, melyeken keresztül tulajdonképpen használjuk az algoritmusokat. Egyik nem létezik a másik nélkül. Kitűnő protokollt használva az algoritmus gyengeségei ronthatják az algoritmusos védelem hatásfokát. Lényeges hangsúlyozni, hogy egy nagyon jó algoritmus használata esetén egy rosszul kiválasztott protokoll teljesen hatástalanná teheti a védelmet.

[4] Forrás: NATO Public Key Infrastructure Certificate Policy —ANNEX1

A kriptográfiai protokoll tulajdonképpen véges számú lépések sorozata, mely két vagy több résztvevő között valósul meg. Amíg egy lépés nem fejeződött be, nem kezdődhet a következő. Célja egy feladat végrehajtása. A kriptográfiai protokolloknak három fő típusa ismert, amelyek eltérő helyzetekben alkalmazhatók.

A döntőbírós protokoll esetében a résztvevő felek mellett egy döntőbíró is helyet kap, aki a protokoll során valamit garantál. Az életben azok a helyzetek hasonlíthatók hozzá, amikor ügyvédet, vagy közjegyzőt veszünk igénybe. Ilyen például a lakásvásárlás esete, amikor az ügyvéd ellenőrzi, hogy a két fél közötti, szerződésben rögzített megállapodások teljesültek-e, s ekkor valósul meg az adás-vétel.

Mivel a döntőbíró a két személy „között" helyezkedik el, így alapvető jellemzője ennek a protokollnak, hogy:

- a döntőbíró valamilyen késleltetést fog okozni a rendszerben;
- lehet szűk keresztmetszet a kommunikációs csatornában (mondjuk az ügyvéd éppen nem ér rá);
- a közvetítő szerepéért fizetni kell (a HSz alkalmazhat átalány díjat is, az időbélyegzés szolgáltatás azonban általában eseti alapon fizetendő).

Ez a protokoll az életben leginkább a bíróságnak felel meg. Ebben az esetben a protokoll (gyakorlatilag a bírósági eljárás) azt biztosítja, hogy amennyiben a felek között vita merülne fel, akkor utólag képes tisztázni azt, kinek van igaza, s a felek elfogadják döntését.

A legideálisabb protokoll az önműködő protokoll, amely esetében a protokoll döntőbíró, vagy ítélkező bevonása nélkül képes garantálni a biztonságot. Ebben az esetben a „döntőbíró maga a kriptográfiai rendszer, amely egyértelművé teszi a résztvevő felek előtt, ha a protokollba valaki beavatkozna, vagy az nem fejeződne be.

A Diffie-Hellman kulcs-csere protokollja szimmetrikus kapcsolati kulcsokban történő megegyezésre használható. (Például, amikor az elektronikus aláírást DSA algoritmus végzi, vagy nincs rá szükség.) Tulajdonképpen nyilvános kulcsú algoritmusnak tekintik, itt viszont a kulcsok generálása és szétosztása közvetlenül kapcsolódik a kódolási és dekódolási lépésekhez.

Hardver és szoftver feltételek

Az elektronikus aláírás szolgáltatás megvalósításakor durván 1/3-ad részben meghatározók a technikai eszközök, mint például szerverek, kriptográfiai modulok, intelligens kártyák és kártyaolvasók, szoftverek, a fennmaradó rész szerződésekről, és a jogi szabályozásról szól. Az elektronikus aláírást kezelő szoftverek gyakran a nagy hardvergyártókhoz köthetők. A Windows 2000 operációs rendszer családtól a Microsoft már támogatja az elektronikus aláírás,

tanúsítványok használatát, valamint az Office alkalmazásokba is integrálta ezen szolgáltatások támogatását.[5]

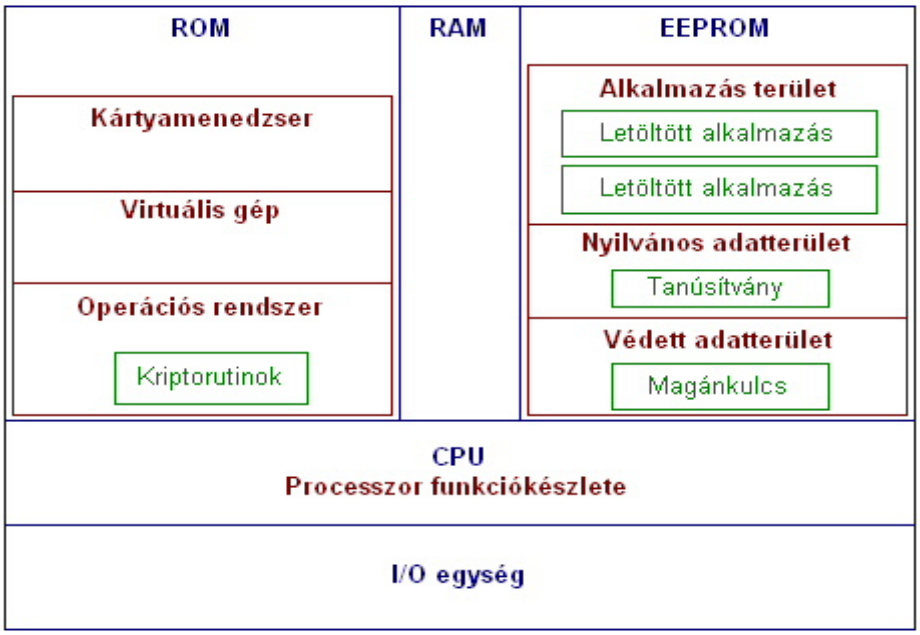
A hardver eszközök közül itt az intelligens kártyákról (chipkártyákról), mint a magánkulcs hordozó eszközről szeretnék néhány szót szólni. Míg a tanúsítványok arra szolgálnak, hogy nyilvános kulcsunk hitelesen jusson el partnerünkhöz, a chipkártyák — többek közt — abban nyújtanak segítséget, hogy a titkos kulcsunk valóban titokban maradjon. A chipkártyák bankkártya méretű műanyag kártyák, melyeken mikrochip helyezkedik el. Ez a chip csakis akkor enged hozzáférést a benne tárolt adatokhoz, ha megfelelően azonosította a felhasználót. A kártyán az adatok fájlba, a fájlok pedig fájlrendszerbe szerveződnek, ahol minden fájlhoz definiálhatjuk, hogy az egyes felhasználók milyen jelszó vagy titkos kulcs birtokában férhessenek hozzá. A kártyákat úgy alakítják ki, hogy a chip tartalmához semmilyen más módszerrel, még a kártya szétszerelésével, felboncolásával se lehessen hozzáférni (tamper-proof). A kártyák levilágítás ellen is védve vannak, így a memória területük nem sérülhet. A modern chipkártyák már biztonságos mikroszámítógépek. Azon túl, hogy tárolják a kriptográfiai kulcsokat, képesek velük kódolni is. Megoldható, hogy a titkos kulcsot tároló kártya senkinek, még a kártya birtokosának sem adja ki a kulcsot. Ugyanakkor, aki a kártyabirtokos jelszavát ismeri, az utasíthatja a kártyát, hogy kódoljon a titkos kulccsal. Így használhatjuk a kulcsot anélkül, hogy az egy pillanatra is elhagyná a biztonságos chipkártyát. Egyes kártyák képesek kulcsokat generálni is, így a kulcs teljes életciklusa (generálás, tárolás, használat, megsemmisülés) a kártyán zajlik le. Tipikus eset, hogy a felhasználó chipkártyán kapja meg a kulcspárját (nyilvános és titkos kulcsát) a HSz-tól.

Ha a felhasználó használni szeretné a titkos kulcsát, be kell helyeznie a kártyáját a számítógépéhez csatlakoztatott kártyaolvasóba. A felhasználó azonosítását követően, a számítógép elküldi a kártyának az üzenetet, az pedig — a titkos kulcs segítségével — előállítja a felhasználó digitális aláírását. Mivel a titkos kulcs soha nem hagyja el a kártyát, a felhasználó nevében digitálisan aláírni a kártya (és annak jelszava, PIN kódja) nélkül nem lehet. Ahhoz, hogy a kártyát a PC/SC Windows implementációja kezelni tudja, a kártyának meg kell felelnie az ISO 7816-1, az ISO 7816-2 és az ISO 7816-3 szabványoknak.

[5] A Windows 98/NT4.0 esetében még nem tartozott az operációs rendszer alapszolgáltatásihoz a tanúsítványok kezelése, de ezek a rendszerek is alkalmassá tehetők elektronikusan aláírt dokumentumok kezelésére

4. sz. ábra

Az intelligens kártya felépítése, aláíró eszközként való alkalmazása



A legtöbb kártya a kártyabeolvasó berendezésbe történő behelyezéssel aktiválható. Ezekkel a kártyákkal (melyek főként Európában terjedtek el), lehet telefonálni, fénymásolni könyvtárakban, kifizetni autópályadíjat vagy étel-ital automatáknál lehet vásárolni. Ugyanakkor lehetőség van a chipkártyák távoli érzékelésére/olvasására is, azaz a kártya nem kerül közvetlen fizikai kapcsolatba a leolvasóval. Az e-pénzzel való fizetésre tehát lehetőség nyílik akkor is, ha a kártya mozgásban van. A távoli érzékelésére is alkalmas kártyáknak két típusa van: a „közelség" (proximity) kártyák és a táv kártyák (amplified remote-sensing card). Az előbbit az olvasó berendezés 30 centiméter sugarú körében lehet aktiválni. A közelség kártyákat épületbe való bejutásra vagy tömegközlekedési eszköz díjának beszedésére alkalmazzák (Helsinki, Párizs). A táv kártyák 30 m-es körzetben érzékelhetők mozgó automatikus járművek díjfizetésére alkalmasak. Ilyet használnak az USA 91-es autópályáján, ahol így a pályadíj megállás nélkül is beszedhető. A leolvasók magas ára miatt és a szabványosítás hiánya miatt csak kevés kártya tölthető fel az Interneten keresztül.
A perszonalizáció az a folyamat, amikor a kártyára a leendő használójának személyes adatai rákerülnek. Ez kétféle módon történik meg, egyrészt a chipbe kell adatokat beírni, másrészt a kártya felületére kerülnek rá vizuálisan elér-

hető adatok. Ezt a folyamatot a Kártya Megszemélyesítő Központ szerepe végzi, ilyennek lennie kell minden kártyakibocsátás esetén. A Központ garantálja egyrészt a felírt adatok helyességét, másrészt a bekerült adatok bizalmas kezelését is. A perszonalizációs adatbázisból automatikusan kerülnek a kártyára az adatok, a megfelelő biztonsági előírások betartása mellett. A perszonalizációs adatbázisba bekerült adatok hitelességéért az adatrögzítő, regisztráló hatóság vállal garanciát, tehát a perszonalizációban is célszerű megkülönböztetni két folyamatot, ezek pedig a következők:

– regisztráció,
– adatfelírás.

A két funkció egymástól elválasztható, gyakran el is válik, de természetesen lehetséges az együttes elvégzésük is.

A kártyabirtokos jogosultságának ellenőrzése megtörténhet manuális úton is (pl. igazolvány), de megtörténhet elektronikus formában is (pl. PIN-kód, jelszó, biometria). A kártyabirtokos-ellenőrzési funkciót a fejlesztő a megrendelő igényeinek megfelelően implementálja a kártyára, ahol többek között azt is meghatározhatja, hogy mennyi egymás utáni sikertelen azonosítási próbálkozást toleráljon a kártya. A kártya — az inicializálástól függően — általában 3 sikertelen PIN-kód azonosítás után letiltja (zárolja) magát, azonban a blokkolt kártya újra használhatóvá válik a PUK kód megadásával.

A kártyaolvasók a szabványos perifériafelületekre (RS-232, PS/2, PCMCIA, USB) kapcsolódnak. Az olvasók kezelési szempontból olyanok, mint bármely szabványos Windows-os eszköz, tartalmaznak biztonsági leírót és Plug and Play azonosítót. Szabványos Windows eszközkezelők irányítják őket, telepítésüket és rendszerből való kivételüket a szabványos Hardver Varázsló irányítja. A kártyaolvasók könnyű kezelhetősége elősegítheti a kezdeti idegenkedést az elektronikus aláírás bevezetésekor az intelligens kártyák kezelésével kapcsolatban, így például érdemes elgondolkodni egy billentyűzettel kombinált kártyaolvasó megoldáson is. Class-1, 2 és 3-as olvasók vannak. Ezek különböző biztonsági szintnek felelnek meg. Áruk ezek tekintetében változnak. (PIN pad, Secure Messaging, stb.)[6]

ELEKTRONIKUS ALÁÍRÁS WINDOWS ALAPOKON

Az elektronikus aláírás szolgáltatás bevezetésekor felmerül a kérdés, vajon milyen új szoftvereket kell beszerezni, s mindez mennyibe fog kerülni. Az elektronikus aláírás létrehozását és ellenőrzését az MS Office alkalmazások

[6] A kártyaolvasók ára jellemzően az 5000Ft-40000Ft közötti tartományba esik, márkától és típustól függően.

támogatják. Amennyiben ezek a szolgáltatások valamilyen oknál fogva nem elégségesek, külön célszoftverek alkalmazhatóak dokumentumok aláírására és ellenőrzésére (Pl.: DSign, SDX, MultiSigno, stb.). A Microsoft ma már széleskörűen támogatja a PKI technológiát szoftvereiben, bár való igaz néha elég sajátosan implementálja az egyes szabványokat. Mivel a honvédségnél alkalmazott operációs rendszerek, valamint az irodai szoftvercsomagok zöme Microsoft termék, valamint a később bemutatásra kerülő hálózat is Microsoft szoftverekre épül, így az alfejezetben a Windows 2000 operációs rendszert, valamint az MS Office 2000 részét képező Outlook levelező klienst veszem górcső alá. Ezen vizsgálódás során röviden bemutatom azt is, hogyan néz ki egy tanúsítvány, s az milyen formában tárolódik. A Microsoft a Windows 2000-től kezdve beépítette a PKI alapú tanúsítványok kezelését az operációs rendszereibe.

A tanúsítványok tárolására és cseréjére a leginkább elterjedt kódolási forma az RSA Laboratories által kifejlesztett PKCS#7 (Cryptographic Message Syntax Standard) és a PKCS#12 (Personal Information Exchange). A PKCS#7 lehetővé teszi egy állományban több tanúsítvány összefogását is (egymástól független tanúsítványokat vagy egy tanúsítási lánc tagjait), és a tanúsítványok mellett különböző attribútumok tárolását is meg tudja oldani. A PKCS#12 képes a tanúsítvány mellett a magánkulcs tárolására is, valamint szintén magába tudja foglalni egy tanúsítási lánc minden tanúsítványát. A két tárolási forma így tulajdonképpen nem csak tanúsítványkódolási forma, de tanúsítványtár formátum is.

A Windows által kezelt tanúsítványtárak a tanúsítványbizalmi listaként fordítható CTL (Certificate Trust List), valamint a Microsoft Sterialized Certificate Store.Az előbbi a hitelesítés szolgáltatók önhitelesített gyökér tanúsítványának listája, melyet tipikusan egy szervezet felelős rendszergazdája állít össze a helyi szabályzatoknak megfelelően, ha szükséges korlátozva a benne szereplő tanúsítványok felhasználhatóságát. Az utóbbi a Microsoft saját formátuma, amely a PKCS#7 és a PKCS#12 formátumok tulajdonságait egyesítve több tanúsítványt is képes tárolni, azok magánkulcsaival együtt. A különböző tanúsítványformátumok eltérő kiterjesztésű állományok formájában öltenek testet: a PKCS#7 kódolásúak P7B, P7C vagy SPC kiterjesztést kapnak, a PKCS#12 kódolásúak P12 vagy PFX, a Certificate Trust List STL, a Microsoft Sterialized Certificate Store SST kiterjesztést. Ezeket a formátumokat (sőt többet is) kezeli és felismeri a Windows, exportálhatók és importálhatók a belső tanúsítványtárba, illetve onnan. A visszavonási listák szintén helyet kaphatnak PKCS#7 formátumú tárakban, illetve CRL[7] kiterjesztésű állományokban.

[7] Certificate Revocation List — tanúsítvány visszavonási lista

A Windows 2000 telepítésekor egy, a Microsoft által beépített „tanúsítványtár” kerül a gépre, melyet az mmc (Microsoft Management Console) egy beépülő moduljával tudunk megtekinteni. (Megfelelő jogosultság birtokában tudjuk a tanúsítványokat eltávolítani, illetve újakat hozzáadni. A „szűz” listát célszerű tüzetesen átnézni és megnyirbálni, és csak a szükségeseket meghagyni (pl. szoftveraláírás elfogadásához). A listában eleve vannak lejárt, vagy időközben visszavont tanúsítványok. A biztonsági felelősök eldönthetik, hogy megbíznak a listában (én nem javasolnám ezt), engedélyezik a lista automatikus frissítését az internetről (ezt is fenntartással kezelném), vagy személyesen kontrollálják, mely tanúsítványkiadókban bízik meg a hivatal.

Windows házi hitelesítő szerver —Active Directory

A Windows 2000 szerver termékcsalád beépített hitelesítő egységgel rendelkezik, mely a Microsoft Certificate Server nevet kapta. A belső működés ismertetése meghaladná a rendelkezésre álló terjedelmi kereteket, ezért csak egy-két gondolat ebben a témában.

A hitelesítő egységet két üzemmódban lehet működtetni:

1. Stand-alone módban, mely nem feltétlen integrált az Active Directoryval (AD), s a tanúsítvány visszavonási listák (CRL) szétosztására például a közös könyvtárban való közzététel szolgálhat. Csak weboldalon (intranet oldalon) keresztüli tanúsítvány menedzsment módszerek működnek. Ekkor a tanúsítvány igénylését, megújítását, visszavonását mind egy céges belső weboldalon kell intézni, amely oldalt a cég rendszergazdái készítenek el.
2. Enterprise módban, mely AD-vel integrált, s így összetettebb szolgáltatások nyújtására képes. A kibocsátott tanúsítványok és visszavonási listák, de az egység(-ek) helye és a velük kapcsolatos szabályzatok is mind a címtárban kerülnek közzétételre. Szintén használhatók a weben keresztüli menedzsment, valamint módunk van az mmc felületről történő tanúsítvány menedzsmentre is. Ekkor a tanúsítványkérelem egy tanúsítványvarázsló segítségével történik. A Windows XP esetén már lehetőség van a tanúsítványok megújításának automatizálására.

Tanúsítványok megjelenítése

A tanúsítványok tartalmának megjelenítését a Windows egy három-öt fület tartalmazó ablakban végzi. Az első fül alatt, a főoldalon a legfontosabb információk kivonata látható. A tanúsítvány felhasználási célja (a kulcshasználat, kiterjesztett kulcshasználat és Netscape tanúsítványtípus szabványos toldalékok alapján), a tanúsítvány tulajdonosának és kibocsátójának neve (az azono-

sítók Common Name mezője alapján), a tanúsítvány érvényessége és az, hogy a rendszer ismeri a tanúsítvány magánkulcs párját (saját tanúsítványok esetében általában igen, egyébként nem). A tanúsítvány bal felső sarkában megjelenő szimbólum kinézetet fontos jelentést hordoz. Alap formában (mint a fenti ábrán is) azt jelzi, hogy a tanúsítvánnyal nincs probléma. Egy piros körben megjelenő fehér kereszt feltűnése azonban arra utal, hogy valami nincs rendben (a tanúsítvány nem érvényes, mert például lejárt, vagy a kibocsátó szervezet nincs benne a megbízható hitelesítő szervezetek listájában).

Egy kis sárga háromszög jelzi, hogy a Windows nem képes a tanúsítvány ellenőrzésére (mert például nem rendelkezik a hitelesítő szervezet tanúsítványával). A kibocsátó nyilatkozata automatikusan megjeleníti a szolgáltató szabályzatát (melyre a Certificate Policies toldalék mutat) egy böngésző ablakban. A második fül alatt a tanúsítvány mezőinek részletes tartalma jelenik meg. Ha a tanúsítvány tulajdonosának, vagy kibocsátójának neve nem volt egyértelmű, itt a teljes azonosító megtekinthető. Ugyanígy részletesebb (óra, perc) adatokkal van feltüntetve a tanúsítvány érvényességének ideje, valamint itt lehet megtudni az algoritmus típusát és a kulcsméretre vonatkozó információt is.

A megjelenítés mezőben a legördülő listából választva szűrni is lehet, például csak a kritikus toldalékokat mutatva. Lehetőség van a tulajdonságok szerkesztésére (saját tanúsítvány esetében!), illetve a tanúsítvány fájlba történő másolására (Attól függően, hogy a magán kulcsunkat is bele szeretnénk e foglalni*.CER, vagy *.P7B fájlformátumban.) A harmadik fül a tanúsítási lánc felépítését mutatja, és a tanúsítvány állapotát jelzi, amelyen éppen állunk. (A tanúsítvány rendben van) A korábbi Office verziók ugyan nem tudják értelmezni az aláírást, az MS Office 2000 csomagnál már megoldották ezt a problémát. A leggyakrabban használt Exchange szerver — Outlook kliens levelező rendszerekben a tanúsítványok használata — a levelek automatikus aláírása, titkosítása, az aláírások ellenőrzése ma már könnyen megoldható. Az Outlookban a Beállítások, Biztonsági beállítások pontnál lehetőségünk van a tanúsítványunk kiválasztására, valamint automatikus csatolás beállítására a kimenő levelekhez. A megfelelő beállítások elvégzése után a leveleinket automatikusan aláírva, esetleg titkosítva küldhetjük el. Az elektronikusan aláírt levelekre hívja föl a figyelmet az üzenet megváltozott kis borítékja, mely kiegészül egy kis pecséttel.

Az itt bemutatott lehetőségek természetesen csak a „jéghegy csúcsát képezik”. Ennél részletesebb leírását az elektronikus aláírás folyamatának adott szoftver esetén a felhasználó dokumentációkban találhatunk. A különböző szoftverek más-más módon valósítják meg az e-mailek, fájlok aláírását, titkosítását.

A szerver operációs rendszerek (Windows 2000/2003 szerver) segítségével akár hitelesítő központokat is létrehozhatunk a hálózatunkban, s erre buzdít maga a Microsoft is.[8] Ám legyünk óvatosak. Az elektronikus aláírás szolgáltatásban meg kell bíznia minden érintett félnek. S itt most nem a szokásos „ez is egy stabil <<vindózos>> szolgáltatás" bizalmatlanságra gondolok. Egy egyszerű példa: ha a munkáltató kontrollálja az elektronikus aláírási infrastruktúrát — beleértve a hitelesítő szervereket -, a munkavállaló nem lehet száz százalékig biztos abban, hogy aláírásával adott esetben nem lesz „belső" visszaélés. Amit ugyebár motiválhat az is, hogy ártó szándékkal kompromittálni próbálják az adott munkavállalót, de előfordulhat a „jó szándékú" aláírom helyetted berögzött attitűd is. Ennek technikai lehetőségét nehéz tagadni, ha az aláírás-létrehozó adatot a rendszer szoftveresen tárolja, adott felhasználói fiókhoz párosítva! Az aláíró szoftverek esetében biztonsági kockázata van, ha a szoftver nem csak azt teszi a tanúsítványunkkal, amire a dokumentációja alapján hivatott. Ennek megállapítása, a szoftver biztonsági bevizsgálása komoly szakértelmet igénylő feladat. Amennyiben fontos az elektronikus aláírás szolgáltatásba vetett bizalom, érdemes megfontolni, hogy bár olcsónak tűnik egy operációs rendszerbe beépített szolgáltatás használata, az elektronikus aláírás szolgáltatás nem csak a hardver és a szoftver.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Egy hivatal tevékenységének elektronikus formában történő átalakításával elengedhetetlenné válik a pusztán szimmetrikus kriptográfián alapuló információs technológiai biztonsági szolgáltatások bővítése. A nyilvános kulcsú kriptográfia fontos szerepet játszhat a szükséges biztonsági szolgáltatások, így a bizalmasság kezelése, sértetlensége, hitelesítés és az elektronikus aláírás biztosításában is. A nyilvános kulcsú kriptográfia két elektronikus kulcsot, egy nyilvános és egy privát kulcsot használ. A nyilvános kulcsot bárki megismerheti, míg a privát kulcsot tulajdonosa titokban tartja. A nyilvános kulcsú kriptográfiát rendkívül egyszerű egy felhasználó pár és egyetlen alkalmazás esetében alkalmazni. A technológia egyszerűen méretezhető néhány alkalmazás vagy a felhasználók kis közösségének támogatására, de a közösség méretének növekedésével egyre nehezebbé válik a nyilvános kulcsok szétosztása és a hozzátartozó privát kulcs tulajdonosának figyelemmel kísérése.

A nyilvános kulcsú kriptográfia tág körben történő alkalmazásához a felhasználóknak szükségük van a nyilvános kulcsok kezeléséhez egy biztonsági infrastruktúra támogatására. A publikus (nyilvános) kulcsú infrastruktúra

[8]Microsoft Windows Server 2003 Deployment Kit

(PKI) lehetővé teszi a nyilvános kulcsú kriptográfia tág körben történő alkalmazását. A PKI segítségével, olyanok is részt tudnak venni igazolható tranzakciókban, akik sohasem találkoztak személyesen. Egy üzenet kezdeményezőjének azonossága visszavezethető a privát kulcs tulajdonosáig akkor, ha szoros kötődés van a tulajdonos és a tulajdonos nyilvános kulcsa között. A PKI biztosítja azt az eszközt, amely összeköti a nyilvános kulcsokat és tulajdonosaikat, és segíti a nyilvános kulcsok megbízható szétosztását nagy, heterogén hálózatokban. A nyilvános kulcsokat nyilvános kulcs tanúsítványok kötik tulajdonosaikhoz. Egy komplex hivatali PKI infrastruktúra kialakítása nagy kihívást jelent, részt kell vegyen benne több terület szakértője, mint például jogászok, informatikai szakemberek, személyzetisek, gazdálkodási szakemberek. Célszerű lenne a honvédségen belüli PKI bevezetési, kialakítási projekteket felsőbb szinten összefogni (HM), s már a kezdetekben a NATO PKI-val kompatibilis rendszer kiépítésében gondolkodni.

A cikkem második részében a lehetséges felhasználási területeket, valamint az elektronikus aláíráshoz kapcsolódó informatikai biztonsági kérdéseket, valamint részleteket tekintünk át a PKI modellekről és a PKG rendszerről. A továbbiakban a vizsgált elektronikus aláírás bevezetéséből adódó problémákat „rávetítem” egy képzeletbeli zártcélú hálózatra, ezzel is közelítve a napi életben történő bevezetés kérdésköréhez.

FELHASZNÁLT IRODALOM

1. ALMÁSI JÁNOS: Elektronikus aláírás és társai (Sans Serif, 2002, ISBN 963 202 744 2)
2. KÖDMÖN JÓZSEF: Kriptográfia (ComputerBooks, 2000, ISBN 963 618 224 8)
3. AC/322-D(2004)0024: NATO Public Key Infrastructure Certificate Policy
4. D. RICHARD Kuhn, VINCENT C. HU, W. Timothy Polk, Shu-Jen Chang: Bevezetés a Publikus (nyilvános) Kulcsú Technológiába és a U.S. Szövetségi Kormányzati PKI Infrastruktúrába, NIST SP 800-32, 2001. www.csrc.nist.gov/publications/nistpubs/index.html; Magyar fordítás: www.ihm.hu/tarsadalom/kutatasok/PKI_ismertetes.pdf)
5. IBM (Tanulmány): Kulcsvisszaállítás a magyar közigazgatáson belül (www.itktb.hu, 2004)
6. IAN MCLEAN: Windows 2000 Biztonság (Kiskapu Kiadó, 2001, ISBN 963 930 1221)
7. BERTA ISTVÁN ZSOLT — Dr. BERTA ISTVÁN: Hardver és Szoftver Biztonság II. (www.crysys.hu/publications/files/BertaB2003hwsw2.pdf)
8. ORVOS PÉTER: Elektronikus aláírások háttér-infrastruktúrája (Budapesti Műszaki és Gazdaságtudományi Egyetem, Diplomamunka, 2000, (http://home.mit.bme.hu/OrvosPeter.pdf)
9. GERENCSÉR ANDRÁS: Digitális aláírás szolgáltatások architektúrája (BKÁE előadás anyaga, 2002, nws.iif.hu/ncd2001/docs/eloadas/4/index.rtf)
10. 2001. évi XXXV. törvény
11. 2004. évi LV. törvény
12. 3/2005. (III. 18.) IHM rendelet „az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről”

13. 7/2005. (VII. 18.) IHM rendelet „ a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól”
14. 9/2005. (VII. 21.) IHM rendelet „az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról”