GÁBOR DÉNES FŐISKOLA

A HITELESÍTÉS-SZOLGÁLTATÓKKAL SZEMBENI BIZALOM ERŐSÍTÉSE

sorszám: 732/2001

VÁRNAI RÓBERT

BUDAPEST

2001

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretnék köszönetet mondani azoknak a személyeknek, akik hozzájárultak szakdolgozatom elkészítéséhez:

Konzulensemnek, Dr. Tuzson Tibornak, aki szaktudásával és alapos munkájával, tanácsaival, véleményével és lelkes hozzáállásával segített e diplomamunka témájának kiválasztásában, a szakirodalom felkutatásában és a diplomamunka végleges formába öntésében.

Az Adatbiztonság, adatvédelem c. tárgy vezetőtanárának, Faragóné Ható Katalinnak, aki az informatika egy roppant érdekes területét ismertette meg velem, megalapozva ezzel a diplomamunka elkészítéséhez szükséges ismereteimet.

Szüleimnek a türelemért, a bátorításért és az anyagi áldozatvállalásért, amellyel lehetővé tették főiskolai tanulmányaim elvégzését.

Nélkülük nem jöhetett volna létre ez a szakdolgozat.

TARTALOMJEGYZÉK

ÁBRAJEGYZÉK

I. BEVEZETÉS

Az Internet felhasználók népes tábora napról napra növekszik, s ezzel párhuzamosan nő az elektronikus kereskedelem jelentősége. Az elektronikus kereskedelmet a hagyományos úton folytatott kereskedelemmel szembeni vitathatatlan előnyei teszik vonzóvá, többek között:

- gazdaságosság – járulékos költségek takaríthatók meg az üzletfelek közötti kommunikáció elektronikus útra való terelésével (pl.: utazási költség, üzlethelyiség fenntartásának költségei, munkaerő költségek stb.);
- rugalmasság – a nap 24 órájában, a hét minden napján rendelkezésre áll;
- hatalmas piac – a világ bármely részén élő ügyfeleket el lehet érni, ehhez csupán többnyelvű weboldalakat kell létrehozni, és nem szükséges külföldi kirendeltségeket fenntartani;
- könnyű elérhetőség – csupán egy hálózatra csatlakoztatható készülékre (számítógép, mobiltelefon stb.) van szükség a használatához;
- kényelmes használat – a vásárlónak nem kell kimozdulnia otthonról vagy a munkahelyéről, hogy időt és energiát nem kímélve felkutassa a megvásárolni kívánt árucikket, sőt a kereskedő a megtakarításai révén kedvezményesen kínálhatja a termékeit.

A bizalmat szándékosan hagytam ki a felsorolásból, ugyanis éppen a bizalmatlanság az, ami leginkább gátolja az elektronikus kereskedelem széles körű elterjedését. A megfelelő azonosítás nélkül a kereskedő nem lehet biztos benne, hogy megkapja az áru ellenértékét, a vevő pedig attól tarthat, hogy a kifizetett terméket nem kapja kézhez.

Az elektronikus kereskedelem jellegéből adódóan az üzleti partnerek az esetek többségében személyesen nem ismerik egymást, következésképp hitelt érdemlően meg kell bizonyosodniuk egymás személyazonosságáról és arról is, hogy a köztük folyó bizalmas kommunikáció biztonságos

csatornákon titkosítva történik. Ez utóbbi azért lényeges, mert az elektronikus kereskedelem nyílt hálózatokra épül, és emiatt a nyílt csatornán végbemenő kommunikációt illetéktelenek is megfigyelhetik.

A hitelesítés-szolgáltatók módosíthatatlanul és ellenőrizhetően megteremtik a kapcsolatot a nyilvános kulcs és annak tulajdonosa között. A hitelesítés-szolgáltató meggyőződik a felhasználó személyazonosságáról, egyedi kulcspárt hoz létre számára, majd meghatározott időre szóló tanúsítványt állít ki arról, hogy a létrehozott nyilvános kulcs egyértelműen a felhasználóhoz tartozik. Ezt követően a szolgáltató saját tikos kulcsával aláírja a tanúsítványt és felveszi a nyilvános kulcsot a kulcsadatbázisába. Ettől kezdve a felhasználó a tanúsítványával tudja igazolni a nyilvános kulcsa hitelességét a virtuális piacon.

A bizalom akkor lehet csaknem teljes, ha a hitelesítés-szolgáltatók tevékenységét törvények támasztják alá, és a szolgáltatók szabványos technológiát alkalmaznak, amelynek következtében a hitelesítés-szolgáltatók elismerhetik egymás tanúsítványait, a felhasználók pedig nyugodt szívvel használhatják ki az elektronikus kereskedelem minden előnyét.

Diplomamunkámban a hitelesítés-szolgáltatók tevékenységét elemzem az adatbiztonság szempontjából. Bemutatom azokat a tényezőket, amelyek – véleményem szerint – a felhasználók szemében megbízhatóvá teszik a hitelesítés-szolgáltatók által kibocsátott tanúsítványokat.

A fent leírtak szellemében szükségesnek tartom a tanúsítványkiadás alapját képező adatvédelmi technológiák rövid áttekintését, illetve az elektronikus aláírással kapcsolatos alapfogalmak tisztázását.

A technológiai tényezők mellett az egységes törvénykezés is a bizalmat növeli, így ennek általános ismertetése, illetve az elektronikus aláírásról szóló, 2001. szeptember 1-jétől hatályban lévő magyar törvény bemutatása is fontos részét képezi e diplomamunkának.

Az eddig említetteken kívül a szabványosítás kérdésével is foglalkozom. Elsősorban európai viszonylatban nyújtok áttekintést az elektronikus aláírással kapcsolatos szabványosítási folyamatokról, és rávilágítok a globális rendszerek fontosságára is.

A szabványosítás ismertetése után a valós életben működő NetLock hitelesítés-szolgáltató tevékenységét elemezve megvizsgálom a bizalmat növelő jellemzők érvényesülését. A vizsgálat eredményeképpen ismertetem egy általam biztonságosnak tekintett hitelesítés-szolgáltató felépítését és tevékenységét.

Végül összegezésképpen felvázolom a hitelesítés-szolgáltatók jövőbeni szerepét az információs társadalomban.

II. ALGORITMIKUS ADATVÉDELEM

A titkos kommunikáció tudománya a kriptológia, amelynek két ága a kriptográfia és a kriptoanalízis.

A kriptográfia nem új keletű tudomány, tudomásunk szerint már az ókori Egyiptomban is művelték 4000 évvel ezelőtt. A titkosítás tudománya folyamatosan fejlődött az emberiség történelme során, de az igazi áttörést a számítógépek megjelenése hozta.

A kriptográfia fő felhasználási területe a hadititkok és államtitkok védelme volt, emiatt elsősorban a hadvezérek, a diplomáciai testületek tagjai (kémek) és az uralkodók éltek vele.

A XX. század második felétől a számítógépek elterjedése következtében megnőtt az igény a személyes adatok védelmére, azaz megkezdődött a titkosítási algoritmusok polgári felhasználása.

A kriptográfia az olyan eljárások tudománya, amelyek révén biztosítható a tárolt és továbbított információ titkossága. Eszközei matematikai algoritmusok, melyek használatának leírását a kriptográfiai protokollok tartalmazzák [2 – 4.1. Kriptográfiai alapfogalmak, 113. o.].

A kriptográfia az alábbi információbiztonsági követelmények kielégítésének egyik leghatékonyabb eszköze:

1. A *bizalmasság* arra szolgál, hogy az információ csak az arra jogosultak számára legyen elérhető. Sokféle módszer létezik a megbízhatóság megvalósítására, a fizikai és logikai hozzáférés védelemtől kezdve az olyan matematikai algoritmusokig, melyek illetéktelenek számára érthetetlenné és elérhetetlenné teszik az adatfolyamot.
2. Az *adatsértetlenség* az adatok illetéktelenek által való megváltoztatását akadályozza meg. Ennek biztosításához észlelni kell

az illetéktelenek általi beavatkozást. Az adatok megváltoztatása jelentheti a törlést, új adatok beszúrását vagy a meglévő adatok mással való helyettesítését.

3. A *hitelesítés* vagy azonosítás a kommunikáló felek és az információ azonosítására szolgál. A kommunikáló felek egymást azonosítják. A továbbított információt a forrása, a keletkezési és küldési ideje, valamint a tartalma alapján lehet azonosítani. Az előbbiek miatt adat-, illetve adatforrás hitelesítésről beszélhetünk.
4. A *letagadhatatlanság* megakadályozza, hogy a kommunikáló felek letagadják régebbi elkötelezettségeiket vagy cselekedeteiket. Ha emiatt vita támad, szükség van egy mindenki által megbízhatónak tartott harmadik félre a probléma megoldásához.

A kriptoanalízis – a fentiekkel ellentétben – a titkok megfejtésére, feltörésére irányuló eljárásokkal foglalkozik.

A titkos kommunikáció során a küldő és a fogadó titkos üzenetváltása valósul meg. A küldő a nyílt szövegből titkosítás segítségével állítja elő a titkosított szöveget. Ezt a kommunikációs csatorna használatával juttatja el a fogadónak, aki azt visszafejti, és így megkapja az eredeti nyílt szöveget.

A titkosításnál az érthető nyílt szöveget érthetetlen karaktersorrá konvertáljuk, ezt a folyamatot rejtjelezésnek nevezzük. A megoldás (vagy visszaállítás) az a művelet, melynek segítségével a fogadó oldalán a karaktersorból visszanyerjük az eredeti nyílt szöveget.

A titkosított szöveg előállításához a titkosító algoritmuson kívül egy kulcs is szükséges, melyet ismernie kell a küldő és a fogadó félnek is. A megfelelő titkosító és megoldó kulcs nélkül általában nem lehetséges a titkosítás és megoldás műveleteinek elvégzése. A titkosító és megoldó kulcsnak nem kell feltétlenül megegyeznie. Ennek megfelelően a következőkben ismertetett két eljárást különböztetjük meg.

2.1. Kriptográfiai algoritmusok

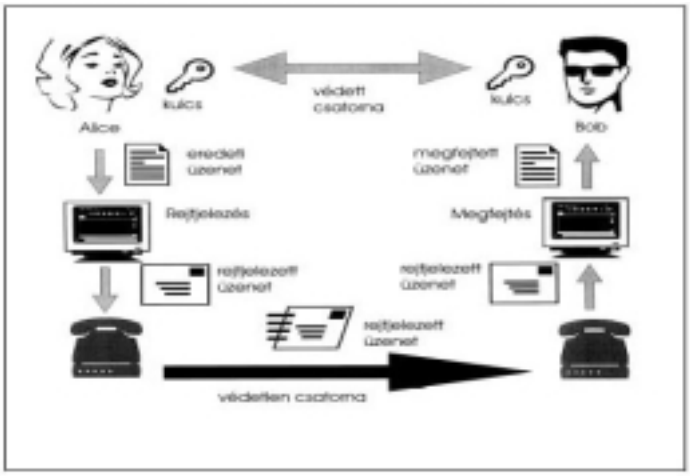
2.1.1. Szimmetrikus kulcsú titkosítás

Ha a titkosításnál és a megoldásnál is ugyanazt a kulcsot használjuk, szimmetrikus kulcsú titkosításról beszélünk.

A szimmetrikus titkosító algoritmusoknak két alaptípusa van [2 – 4.6. Technikák, 177. o.]:

- A *blokktitkosítás* a nyílt szöveget általában legalább 64 bites részekre vágja szét, és ezekre alkalmazza az algoritmust. Így ugyanaz a nyílt szövegblokk mindig ugyanazzal a kulccsal, ugyanarra a rejtjelezett szövegblokkra képződik le.
- A *folyó titkosítás* a titkosító algoritmust folyamatosan alkalmazza a nyílt szövegre. Egyszerre csak 1 bitet titkosít, így ugyanaz a bit mindig eltérő módon képződik le a rejtjelezett szövegre.

A szimmetrikus kulcsú rendszerekben a kulcsot valamilyen biztonságos úton el kell juttatni az üzenet címzettjéhez, hogy az visszaállíthassa a rejtjelezett szöveget. A rendszer jellegéből adódóan alapvető veszélyt jelent a kulcs illetéktelenek kezébe kerülése. Emiatt azt megfelelően védeni és rendszeresen cserélni kell.



***1. sz. ábra.* Üzenetküldés szimmetrikus kulcsú rendszerben**

Forrás: Sík Zoltán: Digitális aláírás, elektronikus aláírás c. cikke

2.1.1.1. A DES algoritmus

[2 – 4.7.1. A DES algoritmus, 186. o.] és [3 – 7.4.2 DES algorithm, 252. o.] alapján

A Data Encryption Algorithm (DEA) titkosító algoritmust 1977-ben szabványosították. Szabványos jellege miatt az algoritmust gyakran DES-nek (Data Encryption Standard) nevezik. A DES, mely a legismertebb szimmetrikus blokktitkosító algoritmus, 64 bites blokkméretet használ 56 bites kulcsméret mellett (a 64 bitből 8 paritásbit). Az IBM által kifejlesztett algoritmus Claude E. Shannon keverő transzformációját[1] használva biztosítja, hogy a blokkon belül a kimenet minden bitje függ a bemenet minden bitjétől. A DES-t mind üzenetek, mind fájlok titkosítására használni lehet.

A szabvány tartalmazza azt a kikötést, hogy csak az eljárás hardver implementált változata használható, és az USA kormánya megtiltotta, hogy ezt a hardver kivitelezést exportálják.

A DES megfejthetőségére utaló publikációk sorát Martin Hellman egy 1977-ben tartott előadása nyitotta meg, aki a teljes kipróbálást is kivitelezhetőnek tartotta. A DES halálához a döntő csapást Eli Biham és Adi Shamir munkássága adta meg, akik 1990-ben egy újonnan kifejlesztett módszer, a differenciál kriptoanalízis segítségével adtak meg egy fejtési eljárást. 1994-ben Mitsuru Matsui egy más típusú, ún. lineáris kripotanalízis módszert adott meg, amely lineáris közelítést alkalmaz, és eredményesen fejthető vele a DES algoritmus.

A fejtést gyakorlatilag kivitelezhetetlenné tevő eljárásként a DES kétszeres alkalmazását javasolták. Ehhez az algoritmust kétszer egymás után kellett alkalmazni két egymástól függetlenül választott kulccsal, ami a kulcs méretét 108 bit hosszúságúra növelte. Már 1992-ben Ralph Merkle és Martin

[1] Shannon javasolta először, hogy a nyelvi sajátosságok eltüntetéséhez keverjük össze úgy az üzenet karaktereit, hogy az már inkább zajnak tűnjön, mint valamilyen rejtjeles üzenetnek.

Hellman nyilvánvalóvá tette azonban, hogy ha az egyszerű DES fejthető, akkor a kétszeres DES (double DES) fejtése is kivitelezhető.

A DES jelenlegi legfejlettebb változata a háromszoros DES (triple-DES). Ez vagy kettő, vagy három 58 bites kulccsal dolgozik. Az üzenetet először az első kulccsal titkosítják normál DES módban, majd a második kulccsal a megoldó algoritmust alkalmazzák. Az így nyert közbülső szövegre alkalmazzák ismét az első, három kulcsos rendszerben a harmadik kulcsot. Az a tény, hogy a titkosítást megvalósító chip export tilalom alatt áll, alátámasztani látszik azt a vélekedést, miszerint az USA biztonsági köreiben ismerik a megfejtési algoritmust. Az exporttilalom miatt számos konkrét chip-megvalósítás található a piacon, és a pénzügyi szféra több nemzetközi szabványában található triple-DES elem.

2.1.1.2. Az IDEA algoritmus

[2 – 4.7.2. Az IDEA algoritmus, 189. o.] és [3 – 7.6 IDEA, 263. o.] alapján

Az elmúlt évtizedben számos megoldást javasoltak a DES kiváltására, helyettesítésére. 1990-ben Xuejia Lai és James Massey létrehozta a PES-t (Proposed Encryption Standard), ennek továbbfejlesztéséből született az IPES (Improved Proposed Encryption Standard), mely a differenciál és lineáris kriptoanalízis elleni védelmet is magában foglalta. A végső változat IDEA (International Data Encryption Algorithm) néven jött létre 1992-ben. A rendelkezésre álló szimmetrikus algoritmusok közül jelenleg az IDEA-t tartják a legbiztonságosabbnak.

Az IDEA gondosan választott alapvető, de kielégítő bonyolultságú matematikai műveletek speciális kombinációit használja fel. Ezeket a műveleteket 16 bites blokkonként alkalmazza 64 bites nyílt szöveg blokkokra, 128 bites kulcs felhasználása mellett. A blokkon belüli kimenő bitek mindegyike minden bemenő bittől függ. Bizonyítottan rendelkezik a Shannon által megkövetelt keverési és szétterjesztési tulajdonságokkal. A matematikai műveletek egyszerűsége gyors és egyszerű technikai megoldásokat tesz

lehetővé mind szoftver, mind pedig hardver szinten. Az IDEA eljárás szabadalommal védett Európában és az USA-ban is.

2.1.1.3. Az AES algoritmus

A DES ugyan még érvényben van, de már nem tekinthető korszerűnek, tekintettel arra, hogy napjainkban a blokkméretet nem tekintik megbízhatónak, ha az kisebb 128-nál, míg a kulcssorozat esetén az 512 bites hosszúság az irányadó.

A fenti okok miatt az amerikai National Institute of Standards and Technology (NIST) 1997. szeptemberében pályázatot hirdetett egy új amerikai (és nemzetközi) titkosítási algoritmus megalkotására, amely Advanced Encryption Standard (AES) néven lesz hivatott átvenni a korábban uralkodó DES szerepét. A szabvány elsődleges célja egy olyan titkosítási algoritmus kidolgozása, amellyel a bizalmas kormányzati információk megfelelő szintű védelme hosszú időre (akár 20 évre) biztosítható. Ebből következően a szabvány legfőbb haszonélvezői a kormányzati szervek lesznek, de természetesen – önkéntes alapon – a szabvány polgári használata is megengedett.

Az NIST által kidolgozott pályázati követelményrendszer blokktitkosító algoritmust ír elő 128 bites blokkmérettel és 128, 192 vagy 256 bites kulcsmérettel. A megkövetelt algoritmus erőssége kérdésessé teszi, hogy maga az állam képes lesz-e a megfelelő törvényes keretek között hozzájutni az üzenetek információtartalmához.

1998. augusztusában az első AES pályázati konferencián 15 jelölt algoritmust hirdettek ki, melyeket a világ legkülönbözőbb kriptográfiai szervezetei dolgoztak ki.

A második szakértői konferenciát 1999. márciusában tartották, ahol megvitatták az algoritmusokról a globális kriptográfiai szervezetek által

készített elemzéseket, illetve az algoritmusokkal kapcsolatos javaslatokat. Az ajánlások nyomán a NIST öt pályaművet választott be abba a körbe, melyből a győztes algoritmus kikerül. A döntőbe jutott algoritmusok között a következőket találjuk: MARS, RC6, Rijndael, Serpent és Twofish.

A benyújtott algoritmusok mögött elismert szakértők és multinacionális cégek sorakoztak fel: többek között az IBM, az RSA Laboratories, Joan Daemen, Eli Biham és Bruce Schneier.

A döntőbe jutott algoritmusokat egy újabb, még részletesebb vizsgálatnak vetették alá. Ezen kívül a NIST egy nem-hivatalos fórumot is nyitott, ahol az érdekelt felek megvitathatták a döntőbe jutott algoritmusokkal kapcsolatos észrevételeiket. A harmadik pályázati konferenciára 2000. áprilisában került sor. A végső vitában a pályázók válaszolhattak az algoritmusokkal kapcsolatban felvetett javaslatokra. A pályázat eredményét 2000. októberében hirdették ki, a győztes a Rijndael algoritmus lett. Megalkotói belga kriptográfusok: Dr. Vincent Rijmen, aki kutató a Leuven-i Katolikus Egyetem villamosmérnöki karán és Dr. Joan Daemen, a Proton World International munkatársa.

Ahogy ez a többi szabvány esetében is történik, a NIST figyelemmel kíséri a Rijndael algoritmus feltörésére irányuló kezdeményezések fejlődését és ennek fényében ötévente felülvizsgálja a szabványt.

A Rijndael algoritmus teljesítménye mind hardveres, mind szoftveres megvalósításban kiváló. S ugyancsak előnyössé teszi a rövid kulcskialakítási idő, a kis memóriaigény és a megfelelő védelem biztosítása a teljesítménycsökkenés legcsekélyebb jele nélkül. Az algoritmus változtatható blokk- és kulcsmérettel dolgozik, és ciklikus működése a párhuzamos utasítás-végrehajtásból eredő előnyök kihasználását is lehetővé teszi. Az algoritmus – rugalmasságának köszönhetően – mind hardvereszközökben, mind intelligens kártyákban kiválóan alkalmazható.

2.1.1.4. A szimmetrikus kulcsú titkosítás előnyei és hátrányai

Előnyök:

- A titkosítás sebessége meglehetősen nagy, hardveres úton pár száz MB/sec, szoftveres úton pedig pár MB/sec rejtjelzési sebesség érhető el.
- A rejtjelezési kulcsok viszonylag rövidek.
- A kulcsok összekapcsolhatók egy erősebb titkosítás megvalósításához. Az egyszerűen megfejthető átalakítások egymással összekapcsolva erős kulcsot eredményezhetnek.
- A szimmetrikus kulcsú titkosítás hosszú múltra tekinthet vissza, bár figyelembe kell venni, hogy az igazi áttörést a digitális számítógépek megjelenése és a DES algoritmus megalkotása jelentette.

Hátrányok:

- Két fél közötti kommunikációban a kulcsnak mindkét félnél titkosnak kell maradnia.
- Egy nagyobb hálózatban sok kulcspárt kell kezelni. Ebből következően a hatékony kulcsmenedzsment megkövetelheti egy megbízható harmadik fél közreműködését is, aki hozzáférhet a felhasználó titkos kulcsához.
- Két fél közötti kommunikációban a kulcsot gyakran kell cserélni, esetleg minden kommunikációhoz új kulcsot kell generálni.
- A szimmetrikus kulcsú titkosításon alapuló elektronikus aláírási eljárások vagy nagy kulcsokat igényelnek az ellenőrzési funkció ellátásához, vagy egy megbízható harmadik fél közreműködését.

2.1.2. Nyilvános kulcsú titkosítás

A nyílt hálózatok (mint például az Internet) felépítéséből adódóan az üzenetek különböző szolgáltatók által kontrollált rendszereken haladnak keresztül, így fennáll annak a lehetősége, hogy az üzenetekhez nem csak a címzett férhet hozzá. A biztonság növelésével az a cél, hogy a küldő és a

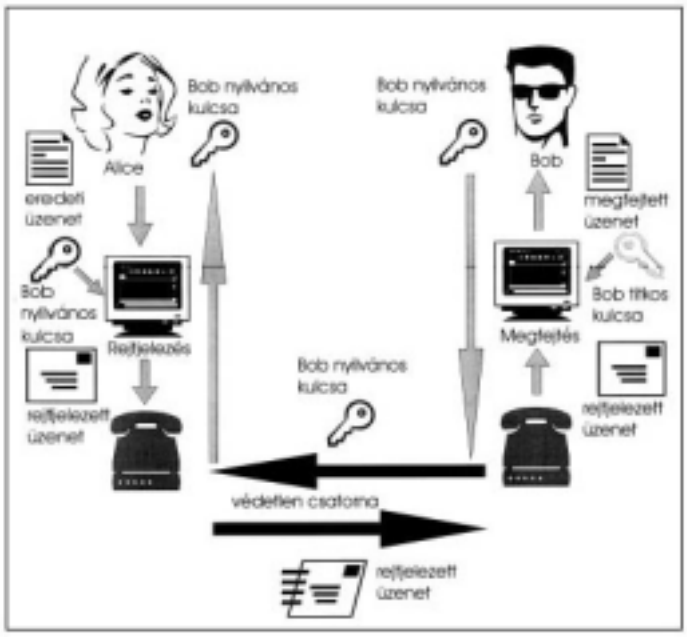
fogadó egyértelműen azonosítható legyen, az eredeti üzenet ne változhasson meg, illetve mások ne férhessenek az üzenet tartalmához.

Erre a problémára a mai legmodernebb technikai megoldás az aszimmetrikus, más néven a nyilvános kulcsú titkosítási eljárás, melynek alapjait 1976-ban Whitfield Diffie és Martin Hellman munkássága teremtette meg. A nyilvános kulcsú titkosítás előnye, hogy a küldő és fogadó félnek nem kell semmilyen titkos jelszót, kódot, kulcsot cserélnie egymással. Ehelyett minden résztvevő fél rendelkezik egy kulcspárral (egy nyilvános és egy titkos kulccsal), mellyel a biztonságos kommunikáció létrejöhet.

A kulcspár használata biztosítja azt, hogy az elektronikus üzeneteket csak az üzenet címzettje tudja megoldani. Az eljárás másik fontos tulajdonsága az, hogy az üzenetek feladói pontosan azonosíthatók, az üzenetek nem letagadhatók, bizonyító erővel bírnak. Erre szolgál az elektronikus aláírás.

A kulcspár egyik tagját nyilvános (vagy publikus) kulcsnak, a másikat titkos (vagy privát) kulcsnak hívják. A kulcsok elektronikus formában létező adatok, s segédprogramokkal könnyen előállíthatók. A nyilvános kulcsok mindenki számára hozzáférhetők az ún. kulcsadatbázisokból, míg a titkos kulcsok csak tulajdonosaik által elérhetők.

A nyilvános kulcsú titkosítás működése egy olyan lakat segítségével szemléltethető, amelynek két kulcslyuka van, egy-egy beleillő kulccsal. Ha a két kulcs közül az egyikkel zárjuk a lakatot, akkor az csak annak párjával nyitható ki, azaz még a bezárást végző kulccsal sem. Egy üzenet küldésénél a feladó levelét egy „ládába” teszi, a láda lakatját pedig a címzett nyilvános kulcsával bezárja. A bezárt láda – azaz a titkos üzenet – csak a záró kulcs párjával, azaz a címzett titkos kulcsával nyitható. Ezzel a módszerrel egymást nem ismerő személyek között is létrejöhet biztonságos kommunikáció.



***2. sz. ábra.* Üzenetküldés aszimmetrikus kulcsú rendszerben**

Forrás: Sík Zoltán: Digitális aláírás, elektronikus aláírás c. cikke

2.1.2.1. Az RSA algoritmus

[2 – 4.7.6. Az RSA algoritmus, 196. o.] és [3 – 8.2 RSA public-key encryption, 285. o.] alapján

Az alkotóiról elnevezett legismertebb nyilvános kulcsú algoritmus létrejöttét 1978-ban jelentette be Ronald Rivest, Adi Shamir és Leonard Adleman. Az RSA biztonsága a faktorizáció problémáján alapul. Egyaránt használható titkos kommunikációra és elektronikus aláírás generálására. Az algoritmus hamar népszerű lett egyszerű működése és közérthető matematikai apparátusa miatt. Ha az RSA paramétereit jól választják meg, a kriptoanalízis különféle módszereivel szemben megfelelő védelmet nyújt. Eddig sem bizonyítani, sem cáfolni nem tudták az algoritmus biztonságát, de a több éve folyó feltörési kísérletek eredménye alapján az RSA biztonságosnak tekinthető.

Ha az RSA paramétereinek választott prímszámok legalább száz jegyűek (ez előfeltétele a biztonságos használatnak), akkor a szükséges műveletek elvégzése – speciális szoftver használata nélkül – nagyon hosszú időt vesz

igénybe. Az RSA algoritmus hozzávetőleg 2000-szer lassabban működik, mint az IDEA, és 1000-szer lassabban, mint a DES. A legjobb kriptorendszert így egy olyan hibrid megoldás adja, amelyben az egyszeri kommunikációs kulcsot RSA-val küldik el a partnernek, az üzenetet pedig az IDEA vagy triple-DES alkalmazásával továbbítják.

Az RSA de facto szabvánnyá vált az egész világon. 1991 óta az ISO 9796 szabvány írja le. Az USA-ban szabadalmi védelem alatt áll.

Az RSA működése és matematikai háttere

Az RSA algoritmus *Fermat tételén* alapul, mely szerint ha p prímszám, és nem osztója egy a egésznek, akkor $a^{(p-1)}$-1 osztható p-vel.

A tétel alapján, ha p és q különböző prímszámok, és a-nak egyik sem osztója, akkor mind p, mind pedig q osztója $a^{(p-1)(q-1)}$-1-nek, ami képlettel leírva: $qp \mid a^{(p-1)(q-1)}-1$.

Ez nem más, mint a Fermat tétel, csak a tételbeli képletben a helyére egyszer a^{p-1}, egyszer pedig a^{q-1} kerül rendre a q-val, illetve p-vel való oszthatóságot felírva. Mivel p és q különböző prímek, ezért a szorzatukkal is osztható $a^{(p-1)(q-1)}$-1. Legyen $n = qp$. Ekkor $a^{(p-1)(q-1)+1}$ pont a maradékot ad n-nel osztva, ha $a < n$.

Legyen a kitevő $e*f = k*(p-1)(q-1)+1$ szorzat alakban felírva. Ekkor az $a^{ef} \bmod n = a$ egyenlethez jutunk, ahol a mod a maradékképzést jelenti. Legyen a nyilvános kulcs az e, n számpáros, a titkos kulcs pedig az f szám.

A rejtjelezés során az üzenetet először számokká alakítjuk olyan módon, hogy a számok mindegyike kisebb legyen, mint n. Ezután az egyes m számokat az $M = m^e \bmod n$ képlettel rejtjelezzük előállítva a titkosított M üzenetet, és ezt az üzenetet az $m = M^f \bmod n$ képlet alapján lehet visszaállítani.

A felhasznált számoknak olyan nagyoknak kell lenniük, hogy az n számot ne lehessen prímtényezőkre bontani. Ha ugyanis az *n* számot fel tudjuk bontani *n* = *qp* alakra, akkor *e* alapján egy osztással meg lehet határozni *f*-et.

A prímtényezős felbontásra pillanatnyilag nem áll rendelkezésre hatékony algoritmus, bár az sem bizonyított, hogy ilyen algoritmus nem létezik. Mivel az alapvető aritmetikai műveletek, mint szorzás, összeadás, hatványozás hatékonyan elvégezhetőek, ezért lehetséges olyan nagy *p* és *q* használata, amely esetén *n* nem bontható fel szorzattá.

A tipikus méret általában bithosszban van megadva, és többnyire kettő hatványa. Ha *n* 1024 bit hosszú, azt általában katonai célokra is megfelelőnek tartják.

2.1.2.2. A DSA algoritmus

[2 – 4.7.7. A DSA algoritmus, 201. o.] és [3 – 11.5.1 The Digital Signature Algorithm (DSA), 452. o.] alapján

A DSA (Digital Signature Algorithm) az RSA konkurense. Az USA-ban az elektronikus aláírásra vonatkozó DSS (Digital Signature Standard) szabvány részét képezi, amely 1994-ben jelent meg. A DSA az ún. diszkrét logaritmus problémán alapul és 1024 bites kulcsméret mellett megfelelő biztonságot nyújt. Ehhez az algoritmushoz is készültek gyors hardver- és szoftvermegoldások.

Az RSA-val összehasonlítva az alábbi eltéréseket tapasztaljuk:

- A DSA kizárólag aláírásra alkalmas. Nem használható titkosításra és a kulcsmenedzsment kivitelezésére.
- A DSA-t az NSA (National Security Agency, USA) fejlesztette, az ő szabadalma védi. Emiatt a felhasználók nem bíznak benne teljesen. Lehetséges, hogy az NSA beépített egy titkos feltörési algoritmust, amit csak ő ismer. Ezt a feltételezést sem bizonyítani, sem cáfolni nem lehet.

- A DSA lassúbb, mint az RSA. Az aláírás generálásában a két algoritmus azonos sebességű, de az ellenőrzésben az RSA átlagosan 25-ször gyorsabb.
- Az RSA de facto szabvánnyá vált, a felhasználók körében sokkal népszerűbb, mint a DSA.
- A DSA egy viszonylag új algoritmus, a felhasználók óvatosak a használatával.
- A DSA tartalmaz egy másik NSA tulajdonban lévő szabadalommal védett eljárást is, az SHA (Secure Hash Algorithm) egyirányú függvényt. Ez a tény is ellenérzéseket kelthet a felhasználókban.
- Az 512 bites kulcsméret nem ad elegendő biztonságot, ezért a szabadalom már az 1024 bites kulcsméret lehetőségét is tartalmazza.
- A DSA nagy erőssége, hogy a paraméteréül választott *p* és *q* prímszámokat nem kell titokban tartani, így kevesebb támadható pontja van, ezért biztonságosabbnak tekinthető az RSA-nál.

Az ANSI a bankok számára a DSA-t ajánlja, és a legelterjedtebb ingyenesen használható kriptorendszer, a PGP (Pretty Good Privacy) is támogatja ezt az elektronikus aláírási rendszert.

2.1.2.3. Elliptikus görbe alapú rejtjelezés

[18 – 3.5 Elliptic Curve Cryptosystems, 101. o.] alapján

Az elliptikus görbe alapú titkosítási rendszerek elmélete a nyolcvanas évek közepén született meg. Ezekben a rendszerekben a modulo aritmetika szerepét az elliptikus görbék pontjaival végzett műveletek töltik be. A kriptográfiában alkalmazott elliptikus görbéket véges számhalmazokon definiálják. A módszer biztonságát a görbék pontjaival végrehajtott műveletek számításigényes volta biztosítja.

Léteznek az RSA-hoz hasonló felépítésű rendszerek és olyanok, melyek a diszkrét logaritmus problémán alapulnak. Ez utóbbiaknál a következőkben foglalható össze a megfelelő védelmet nyújtó probléma lényege: egy

elliptikus görbén adott két pont, *G* és *Y* úgy, hogy *Y* = *kG* (azaz *Y G* önmagához *k*-szor hozzáadva), a feladat k egész érték megkeresése. Ezt a problémát elliptikus görbe diszkrét logaritmus problémának is nevezik.

A hagyományos diszkrét logaritmusokhoz viszonyítva az elliptikus görbe diszkrét logaritmusok kiszámítása sokkal számításigényesebb, ebből következően kisebb kulcsmérettel is biztosítható ugyanolyan szintű biztonság, mint a hagyományos aszimmetrikus rendszerek esetében. A kisebb erőforrásigény miatt az elliptikus görbe alapú titkosítás kiválóan alkalmazható a szűkös erőforrásokkal rendelkező intelligens kártyák rejtjelezési rendszereként.

A kisebb kulcsméret nagyobb hatékonyságot és gyorsabb működést tesz lehetővé, ezek a jellemzők várhatóan népszerűvé teszik a jövőben az elliptikus görbe alapú rendszereket.

2.1.2.4. A nyilvános kulcsú titkosítás előnyei és hátrányai

Előnyök:

- Csak a titkos kulcsot kell bizalmasan kezelni, bár a nyilvános kulcsok hitelességét is biztosítani kell.
- A kulcsok nyilvántartása a megbízható harmadik fél feladata, aki nem férhet hozzá a felhasználó titkos kulcsához.
- A kommunikáció módjától függően a nyilvános kulcsból és titkos kulcsból álló kulcspárt nem kell gyakran megváltoztatni, akár több éven keresztül is használhatóak.
- A nyilvános kulcsú titkosításon alapuló rendszerek hatékony elektronikus aláírási mechanizmusokat eredményeznek. Az ellenőrzéshez használt kulcs kisebb a szimmetrikus kulcsú rendszerekben alkalmazott kulcsnál.

Hátrányok:

- A népszerű nyilvános kulcsú titkosítási algoritmusok nagyságrendekkel lassúbbak szimmetrikus kulcsú társaiknál.
- Az aszimmetrikus kulcsok mérete nagyobb a szimmetrikus kulcsú rendszerekben használt kulcsok méreténél. Hasonló a helyzet a nyilvános kulcsú rendszerekben generált aláírások tekintetében is.
- A nyilvános kulcsú titkosítási algoritmusok egyike sem bizonyult abszolút biztonságosnak. A jelenleg használt leghatékonyabb aszimmetrikus eljárások biztonsága egy maroknyi számelméleti probléma feltételezett megoldhatatlanságán, illetve erőforrás-igényes megoldhatóságán alapul.
- A hetvenes évek közepén kidolgozott nyilvános kulcsú titkosításnak messze nincs olyan nagy múltja, mint a szimmetrikus kulcsú titkosításnak.

2.1.3. A két titkosítási rendszer kapcsolata

A jelenleg használatos hibrid kriptográfiai rendszerek egyesítik a szimmetrikus kulcsú és a nyilvános kulcsú titkosítás módszereit, így ezek előnyeit is. A nyilvános kulcsú titkosítási eljárások kulcscserére használhatók a szimmetrikus kulcsú rendszerekben. Ezáltal a kommunikáló felek egyszerre élvezhetik a nyilvános kulcsú eljárások által generált kulcspárok hosszú élettartamát és a szimmetrikus kulcsú rendszerek hatékonyságát.

A gyakorlat azt mutatja, hogy a nyilvános kulcsú titkosítás hatékony aláírási algoritmusokat és kulcsmenedzsmentet biztosít, míg a szimmetrikus kulcsú kriptográfia a titkosító és az adatintegritást biztosító alkalmazások területén nagyon hatékony.

2.1.4. A kriptográfia matematikai segédeszközei

A prímteszt

A prímteszt az az eljárás, melynek során megállapítjuk egy számról, hogy az prím-e. Ezt az eljárást általában kulcsok generálásához használjuk olyan

titkosítási rendszereknél, melyek a megfelelő prímszámok megválasztásán alapulnak, ilyen például az RSA algoritmus. A valószínűségi prím teszt segítségével egy számról nagy valószínűséggel eldönthető, hogy prím-e.

A véletlen prímek generálása úgy történik, hogy véletlenszám-generátorral számokat állítunk elő és végigfuttatjuk rajtuk a prímtesztet, melynek eredménye adja a véletlen prímszámokat.

A valószínűségi prímteszt jóval gyorsabb annál, mint hogy egy számról teljes bizonyossággal megállapítsuk, hogy prím-e.

Véletlenszám-generálás

A véletlenszám-generálást gyakran használják kulcsgenerálásra és protokollok ellenőrzésére. A véletlenszám-generátor egy függvény, ami 0-ákból és 1-esekből álló sorozatot állít elő úgy, hogy a sorozatban nem lesz olyan pont, ahonnan az addigi bitsorozat alapján ki lehetne következtetni a következő bit értékét. A számítógép determinisztikus jellegéből és véges komplexitásából adódóan a véletlenszám-generálást nehéz számítógéppel végezni. Emiatt ha kétszer egymás után futtatjuk ugyanazt a véletlenszám-generátort, hasonló eredményt kapunk.

Léteznek valódi véletlen-számokat előállító generátorok is. Ezek az eszközök a fizikai világból vett értéken alapulnak, ilyen lehet például egy radioaktív anyag neutron kibocsátásának az aránya, vagy az egérmozgatások száma egy meghatározott időintervallumban.

Az említett jellemzők miatt a számítógéppel végzett véletlenszám-generálást ál-véletlenszám generálásnak nevezzük. Az ál-véletlenszám generátor olyan bitsorozatot állít elő, amely véletlen számsorozatnak tűnik. Valójában egy ciklikusan ismétlődő számsorozatról van szó. Minél hosszabb a számsorozat ismétlődő része, annál jobban közelít az ál-véletlenszám az igazi véletlenekhez.

2.2. Kriptográfiai protokollok

A legbiztonságosabb kriptográfiai algoritmusok esetén is szükség van olyan rendszabályokra, amelyek biztosítják, hogy az adott alkalmazásban ezek az algoritmusok a megkívánt titkosságot, vagy hitelességet nyújtsák. Az ilyen előírások, rendszabályok összességét szokás kriptográfiai protokollnak nevezni.

A kriptográfiai protokollok által nyújtott szolgáltatások:

- Kulcsmenedzsment
- Üzenethitelesítés
- Partnerhitelesítés
- Elektronikus aláírás
- Titokmegosztás

Kulcsmenedzsment

A szimmetrikus kulcsú titkosítási rendszerekben a kulcskiosztás a titkosításhoz használt kulcs eljuttatását jelenti a rejtjelezett üzenet címzettjéhez. Tágabb értelemben véve kulcsmenedzsmentről beszélünk, melybe beletartozik a kulcsok létrehozása, hitelesítése és a lejárt kulcsok cseréje. A kulcsmenedzsment valójában a Shannon által definiált „abszolút biztos csatornát” valósítja meg, illetve próbálja megvalósítani.

A nyilvános kulcsú kriptorendszereknél a kulcsmenedzsment a nyilvános és titkos kulcs generálását, illetve a publikus kulcs nyilvános adatbázisban való közzétételét jelenti, ezek a tevékenységek a központi hitelesítés-szolgáltatók feladatkörébe tartoznak.

Üzenethitelesítés

Az üzenethitelesítéssel védekezhetünk az ellen, hogy illetéktelen személyek az adatátvitel során megváltoztassák az üzenet tartalmát. A módszer lényege, hogy az üzenetből egy ellenőrző összeget képeznek (Message Authentication Code, MAC), s amennyiben a fogadó oldalon az ellenőrzés során más összeg jönne ki, ez arra utal, hogy az üzenet tartalma

megváltozott. Az ilyen ún. ujjlenyomat képzését az Egyirányú és hash függvények c. pontban tárgyalom részletesebben.

Partnerhitelesítés

A partnerazonosítás kommunikációs környezetben vagy elektronikus levelező rendszerekben alkalmazott eljárás, amely arra szolgál, hogy a kapcsolat felvételekor a kommunikáló felek minden kétséget kizáróan megbizonyosodhassanak egymás személyazonosságáról a kommunikáció idejére.

Elektronikus aláírás

Az üzenet- és partnerhitelesítés csak a kommunikáció idejére és a kommunikáló felek számára nyújt hitelesítési lehetőséget. Az elektronikus aláírás azonban az üzenetváltás után és harmadik fél számára is lehetővé teszi a hitelesítést.

Az elektronikus aláírás protokollok feladatai:

- Az aláírás generálása (az üzenetküldő részéről);
- Az aláírás ellenőrzése (a fogadó részéről);
- A hitelességgel kapcsolatos viták tisztázása harmadik személy előtt.

Titokmegosztás

Minden algoritmus esetén szükség van valamilyen titkos adatra (titkos kulcs), amelyet már nem véd valamilyen újabb titkosító transzformáció. Ezért az ilyen titkos adat védelmét másfajta védelemre kell bízni. A fizikai védelem mellett lehetőség van a titok „feldarabolására” is. A módszer úgy igyekszik elosztani a titkot N személy között, hogy abból tetszőlegesen választott K személy együttesen tudja csak rekonstruálni az eredeti értéket, s ennél kevesebb személy erre sohase legyen képes. Ezt a módszert nevezzük titokmegosztásnak.

2.2.1. Egyirányú és hash függvények

[2 – 4.4.5. Egyirányú függvények, 141. o.] és [3 – 1.9 Hash functions, 33. o.] alapján

Az egyirányú függvény olyan függvénykapcsolat, ahol az $x \rightarrow f(x)$ hozzárendelést könnyű kiszámítani, de a fordított $f(x) \rightarrow x$ számítást gyakorlatilag lehetetlen elvégezni. Speciális egyirányú függvény a hash függvény (lenyomatkészítő függvény), amelyet szokás ujjlenyomatnak is nevezni.

A hash függvény változó hosszúságú nyílt szöveghez egy fix hosszúságú karakterláncot rendel, ennek hosszúságát nevezzük hash értéknek. Kriptográfiai szempontból a hash érték a bemenő karaktersorozattal összekötve annak lenyomataként szolgál.

A függvényt *ütközésmentes*nek tekintjük, ha nincs két olyan különböző szöveg, amelyek hash értéke megegyezik.

A hash függvényeket legfőképpen az *elektronikus aláírásoknál* használjuk. Az elektronikus aláírások esetében a küldendő üzenetet hash függvénnyel dolgozzuk fel és a kapott hash értéket írjuk alá. A fogadó fél is elvégzi az üzenet hash függvénnyel való feldolgozását és összehasonlítja a két hash értéket, ha egyeznek, akkor biztos lehet benne, hogy az aláírás hiteles. A hash érték az üzenetre jellemző. Ha az üzenet legalább 1 bitje módosul, a hash érték is megváltozik, ezt a jelenséget nevezzük *lavina hatás*nak.

Ezzel a módszerrel időt és helyet takaríthatunk meg szemben azzal, amikor magát az üzenetet rejtjelezzük és osztjuk blokkokra, majd minden blokkot külön-külön aláírunk.

A hash függvényekkel az adatintegritás követelményét is teljesíthetjük. A bemenő információ hash értékét megállapítjuk egy adott időpontban, majd egy későbbi időpontban újra elvégezzük ezt a vizsgálatot. A két érték

összehasonlításával megállapíthatjuk, hogy időközben megváltozott-e a bemenő információ. Ezt a módszert használja számos vírusvédelmi rendszer.

A hash függvényeket eredetileg adattárolásra és adatbankokban való keresésre dolgozták ki. Lényegében az ott elért eredményeket használják fel a kriptográfiában is.

A leggyakrabban alkalmazott hash függvény a Standard Hash Algorithm (SHA). Az algoritmus inputja egy tetszőleges hosszúságú (maximum 2^{64} bit) tetszőleges dokumentum, az outputja pedig egy 160 bit hosszúságú karakterlánc.

2.2.2. Az elektronikus aláírás létrehozása és ellenőrzése

Az elektronikus aláírás funkcionálisan ugyanúgy működik, mint a hagyományos, kézírásos aláírás, de annál többre képes.

Az elektronikus aláírással szemben támasztott elvárások:

- csak egyetlen személy tudja létrehozni a rá jellemző aláírást, hogy az ne legyen hamisítható és a későbbiekben ne lehessen letagadni,
- legyen könnyen létrehozható és ellenőrizhető,
- az aláírás olyan módon kapcsolódjon az aláírt dokumentumhoz, hogy az az aláírást követően már ne legyen észrevétlenül módosítható.

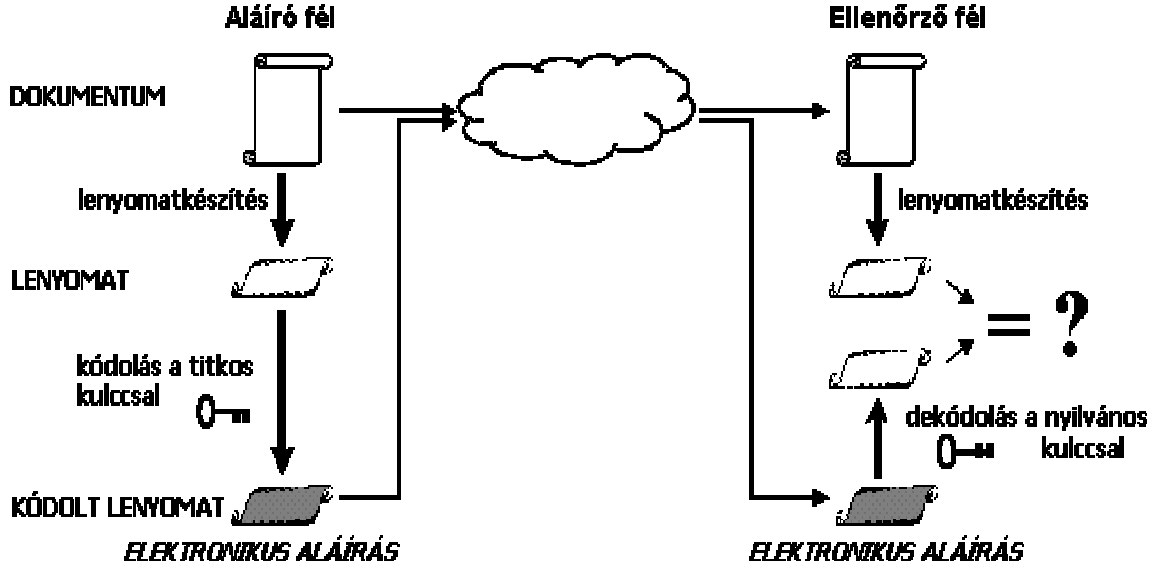
Az elektronikus aláírás módszere technológiailag a nyilvános kulcsú titkosítás elvén alapul. A nyilvános kulcsú algoritmusok bemutatásánál már említettem, hogy ez a fajta titkosítás egy kulcspárt igényel egy adott üzenet rejtjelezéséhez és megoldásához. Egy kulcsnak pontosan csak egyetlen párja létezik, amit a kulcspárt létrehozó eljárás garantál, mégis egyik kulcs a másikból gyakorlatilag kiszámíthatatlan.

A nyilvános kulcsot nyilvánosságra hozza a tulajdonosa, míg a titkos kulcsot szigorúan titokban kell tartania. Egy üzenetet rejtjelezésekor a saját titkos

kulcsát használja, így a titkosított üzenetet kizárólag az ő nyilvános kulcsának ismeretében lehet visszaalakítani, ezzel bizonyossá válik, hogy az aláíró csakis ő lehetett, tehát a letagadhatatlanság teljesül. Másvalaki a titkos kulcs birtoklása nélkül az üzeneten ugyanezt a transzformációt nem tudja elvégezni, vagyis az aláírás nem hamisítható.

Az aláírás a rejtjelezés eredményeként szorosan kötődik az aláírt dokumentum aláíráskori képéhez, hiszen annak a rejtjelezett megfelelője a dokumentum semmilyen módosított változatával nem feleltethető meg.

Az egyirányú hash függvények gyakorlati felhasználásának tárgyalásánál már írtam róla, hogy az elektronikus aláírás használatakor nem magát a dokumentumot szokták aláírni, hanem annak egy lenyomatát (hash érték), melyet a hash függvény segítségével állítanak elő belőle. Ha a dokumentum változik, akkor szükségképpen a lenyomata is, ha pedig a lenyomat változatlan, akkor biztosra vehető, hogy a dokumentumban sem történt változás.



***3. sz. ábra.* Az elektronikus aláírás létrehozása és ellenőrzése**
Forrás: [10]

Az elektronikus dokumentum lenyomatának titkos kulccsal rejtjelezett képe a dokumentum elektronikus aláírása. Ezáltal – a hagyományos aláírással

ellentétben – az elektronikus aláírás csak logikailag, és nem fizikailag kötődik a dokumentumhoz.

2.2.2.1. A hitelesítés-szolgáltatók szerepe

A fentebb vázolt rendszer biztonságos működésének persze számos feltétele van. Szükség van arra, hogy minden szereplő nyilvános kulcsát hitelt érdemlő módon mindenki más megismerhesse. A kulcscsere személyes találkozások során elvben megvalósítható, de ez az üzleti életben, ahol az összes piaci szereplő nem ismerheti egymást, elég nehezen kivitelezhető.

Van mód arra, hogy a felek elektronikus formában elküldjék egymásnak a nyilvános kulcsaikat vagy letöltsék azokat egy adatbázisból, de számolni kell azzal a veszéllyel, hogy a kulcsot útközben a nyílt kommunikációs csatornán egy támadó módosítja vagy esetleg illetéktelenül felhasználja (más nevében ír alá). A kulcs manipulációja ellen úgy lehet hatékonyan védekezni, hogy egy mindenki által megbízhatónak elfogadott harmadik fél (Trusted Third Party, TTP) elektronikus dokumentumba foglalja az adott személy nevét (illetve más azonosító jellemzőit) és a nyilvános kulcsát, majd ezeket együttesen saját titkos kulcsával aláírja, ezzel biztosítva, hogy észrevétlenül nem történhet változtatás a rögzített adatokban. Az ilyen kiadott dokumentum a *tanúsítvány* (certificate), a megbízható harmadik fél a *hitelesítés-szolgáltató* (**Certificate Service Provider, CSP**).

Amennyiben valaki elveszíti saját titkos kulcsát vagy feltételezhető, hogy az illetéktelen kezekbe kerül, a tulajdonos érdekében szükség van a kulcspár használatának azonnali letiltására, hiszen a titkos kulcsot birtokló személy az igazi tulajdonos nevében bármit aláírhat hitelesnek tűnően. Az elveszett kulcsokkal való visszaélések ellen a tanúsítvány visszavonásával lehet védekezni. Ez technikailag úgy oldható meg, hogy felveszik az elveszett kulcsot a tanúsítvány visszavonási listára (**Certificate Revocation List, CRL**). A visszavonási listán szereplő nyilvános kulcsokkal ellenőrizhető aláírás, mely a visszavonás időpontja után keletkezett, így nem érvényes. A visszavonást megelőzően készített aláírásoknak viszont a továbbiakban is

érvényesnek kell maradnia. Ebből is látszik, hogy alapvető fontosságú egyrészről, hogy a visszavonás időpontját pontosan rögzítsék, másrészről pedig, hogy amikor valaki elektronikusan aláír egy dokumentumot, az aláírás megtételének időpontját is rögzítse, hiszen adott esetben ettől az időponttól is függhet, hogy az aláírás érvényes-e vagy sem.

Az aláírás időpontjának rögzítése egy újabb problémát vet fel. Amennyiben az aláírás időpontját egyszerűen az aláírást végző személy írja bele a dokumentumba, fennáll a veszély, hogy akár jóhiszeműen, akár rossz szándékból helytelen időpontot rögzít: lehet, hogy egyszerűen csak „rosszul jár az órája", de az is előfordulhat például, hogy „vissza akarja dátumozni" az aláírást akkorra, amikor még érvényes volt az azóta már visszavont tanúsítvány. A megoldást természetesen megint egy megbízható harmadik fél, az *időbélyegző szolgáltató* (**Time Stamping Authority, TSA**) segítsége jelentheti.

Az időbélyegző szolgáltatót minden fél hiteles időforrásként fogadja el. Az általa kiadott *időbélyegző* (**Time Stamp, TS**) nem más, mint az időbélyegző szolgáltató órája szerinti pontos időt tartalmazó elektronikus dokumentum elektronikusan aláírva, vagyis hitelesítve a szolgáltató titkos kulcsával. Amennyiben a szolgáltató megbízhatóan működik, soha nem kerül kibocsátásra időbélyegző olyan időpontról, ami még nem múlt el. Így tehát ha az aláírás készítője egy időbélyegzőt tesz az elektronikus dokumentumomba az aláírás megtétele előtt, azzal bizonyítani tudja, hogy az aláírás ez után az időpont után történt. Azt, hogy a dokumentum az adott formában egy adott időpont előtt létezett, csak úgy lehet garantálni, hogy az aláírt dokumentumot be kell küldeni az időbélyegző szolgáltatónak, aki ehhez mellékeli az órája által mutatott pontos időt, és együttesen aláírja ezeket.

Látható, hogy a fentiekben vázolt, nyilvános kulcsú titkosításon alapuló rendszer működéséhez komoly háttérinfrastruktúra szükséges. Ezt az infrastruktúrát összefoglaló néven nyilvános kulcsú infrastruktúrának (**Public Key Infrastructure, PKI**) nevezzük, melynek elemei a mindenki által birtokolt nyilvános-titkos kulcspárok, a tanúsítványok, a hitelesítés-szolgáltató és

időbélyegző szolgáltató, a kulcsok létrehozásához és tárolásához valamint az elektronikus aláírás létrehozásához és ellenőrzéséhez szükséges szoftver és hardver eszközök, a kommunikációhoz szükséges hálózati elemek, az adatbázisok, valamint a biztonsági előírások és a jogi szabályozás is.

2.2.3. Egyszer használatos és vak aláírás

[3 – 11.6 One-time digital signatures, 462. o. és 11.8.1 Blind signature schemes, 475. o.] alapján

Az *egyszer használatos elektronikus aláírás* egyetlen üzenet egyszeri aláírására szolgál. Minden aláíráshoz új nyilvános kulcsot kell generálni. Az egyszer használatos aláírás ellenőrzéséhez szükséges nyilvános információkat érvényesítő paramétereknek nevezzük. Az egyszer használatos aláírás alkalmazása elsősorban az intelligens kártyáknál előnyös, ahol kis számítási teljesítmény is elegendő.

Az eddig bemutatott mechanizmusoktól eltérően a *vak aláírási mechanizmus* a küldő (A) és az aláíró (B) közötti protokollt jelenti. Az alapelv a következő: A elküldi az üzenetet B-nek, B ezt aláírja és visszaküldi A-nak. Az aláírásból A megfejtheti B aláírását, amely egy korábbi A által kiválasztott üzeneten (m) található. A protokoll lezárásakor B sem az m üzenetet, sem a hozzá kapcsolódó aláírást nem ismeri.

A vak aláírás célja éppen annak megakadályozása, hogy B, az aláíró beleláthasson az üzenetbe, amit aláír, illetve megvizsgálhassa az aláírást, ennek következtében a későbbiekben B nem tudja az aláírt üzenetet és a küldőjét egymáshoz rendelni.

Az elektronikus fizetési rendszerek jelentik a vak aláírások egyik alkalmazási területét. Ezekben a rendszerekben az üzenet egy pénzösszeget jelenthet, amit A, a küldő elkölthet. Amikor az üzenet és az aláírás megjelenik B-nél, az aláírónál (a banknál), B nem tudja kikövetkeztetni, melyik félnek küldte vissza

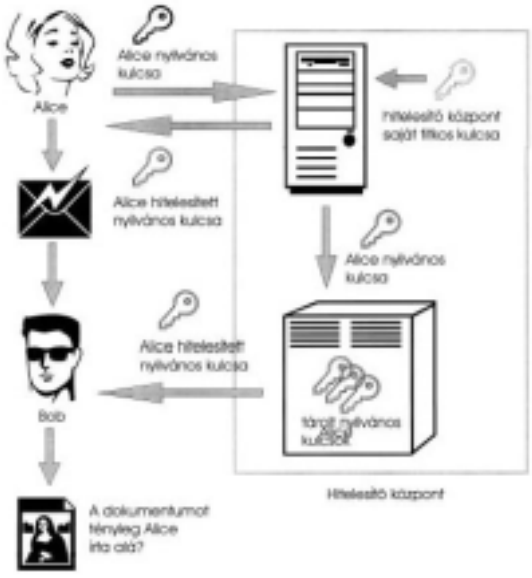
az aláírt értéket. Ezzel a módszerrel A inkognitóban maradhat, azaz nem lehet nyomon követni a költekezéseit.

2.2.4. A hitelesítés-szolgáltatók tevékenysége

A nyilvános kulcsú titkosítást használó rendszerek egyik fő eleme az a szolgáltatás, mely a kommunikációs feleket egymásnak „bemutatja", azaz amely segítségével a felek nyilvános kulcsai hitelt érdemlően megszerezhetők. Fontos, hogy garantálják a nyilvántartott felek (személyek, cégek, számítógépek) azonosságát, például közjegyzők közreműködésével.

Ezt a tevékenységet az intézményi formában működő hitelesítés-szolgáltatók végzik. A hitelesítés-szolgáltatók tevékenysége az alábbiakban leírt feladatokból áll.

A hitelesítés-szolgáltató azonosítja az aláírót annak személyi adatai alapján (az azonosító okiratok – személyi igazolvány, útlevél stb. – segítségével), ezután meggyőződik az aláíró és nyilvános kulcsa összetartozásáról, végül erről tanúsítványt állít ki, melyet saját elektronikus aláírásával hitelesít.



***4. sz. ábra.* A hitelesítés-szolgáltatók szerepe**

Forrás: Sík Zoltán: Digitális aláírás, elektronikus aláírás c. cikke

A hitelesítés-szolgáltató üzemeltet egy nyilvános elektronikus adatbázist, amely gyakorlatilag elektronikus telefonkönyvként üzemel. Mindenki számára elérhető, aki valamilyen módon meg akar győződni az aláíró elektronikus aláírásának valódiságáról. Ezek a megbízható adatbázisok többnyire az ISO/ITU X.509 v3-as szabványa szerint épülnek fel (ISO 9594-8, 1997). Az utóbbi időben ennek megjelent az internetes változata is PKIX névvel.

A hitelesítés-szolgáltató feladata még az érvénytelen elektronikus aláírásokról szóló tanúsítványok visszavonása, hogy a továbbiakban ne lehessen használni az érvénytelen aláírást. A visszavont tanúsítványokat a visszavont tanúsítványok listájában tartják nyilván.

2.2.4.1. A hitelesítés-szolgáltatók közötti kapcsolat

Maga a hitelesítés-szolgáltató más hitelesítés-szolgáltatókkal is kapcsolatban áll, és egymás aláírását is hitelesítik, hogy tudni lehessen, megbíznak egymásban.

Látszik tehát, hogy a hitelesítés-szolgáltatók többféle módon szerveződhetnek. Kölcsönösen egyenrangú kapcsolatba kerülhetnek egymással, hierarchikus kapcsolatban lehetnek (ekkor létezhet az úgynevezett gyökér vagy root CSP), vagy vegyes kapcsolódás is lehet köztük. Sőt, lehetnek olyan hitelesítés-szolgáltatók, amelyek csak kapcsolófunkciót látnak el (bridge CSP), illetve olyanok, amelyek elsők az egyenlők között abban a tekintetben, hogy ők kapcsolódnak ilyen kapcsolófunkciójú hitelesítés-szolgáltatókhoz (principal CSP-k).

A hitelesítés-szolgáltatóknál azonban szintén felmerül a kérdés, hogy ki az, aki a hitelesítők megbízhatóságát garantálja? Előfordulhat ugyanis, hogy a hitelesítés-szolgáltatók egész láncolata nem megbízható, ami a náluk regisztrált elektronikus aláírás-tulajdonosok szempontjából katasztrofális kimenetelű lehet. Ennek a problémának a megoldására találták ki a „hitelesítés-szolgáltatókat hitelesítő” intézményeket, amelyek sokszor állami hatóságként működnek. Ezek garantálják, hogy az adott hitelesítés-

szolgáltató megfelel a szabványoknak, módszerei és eljárásai olyanok, amelyek lehetővé teszik a megbízható működést.

2.2.5. A bizalmas kommunikációt fenyegető támadások

[2 – 4.1. Kriptográfiai alapfogalmak, 115. o.], [3 – 1.13 Classes of attacks and security models, 41. o. és 11.2.4 Types of attacks on signature schemes, 432. o.] alapján

A bizalmas kommunikációt kétféle támadás fenyegeti. A *passzív támadás* a kommunikációs csatorna lehallgatásában merül ki, lényege az észrevétlen megfigyelés. Ez a fajta támadás nem változtatja meg a kommunikáció tartalmát. Az *aktív támadás* ezzel szemben nem tartja be a protokoll szabályait, megváltoztatja a kommunikáció tartalmát. Az aktív támadó először passzív módszerekkel megszerzi a szükséges információt és ennek birtokában kezd az aktív támadáshoz.

A passzív támadások ellen megfelelő titkosító algoritmus alkalmazásával védekezhetünk, míg az aktív támadás okozta károkat a kriptográfiai protokollok használatával előzhetjük meg.

Ha a támadó jogosult felhasználó, azaz a protokoll egyik szereplője, akkor csalónak nevezzük. A passzív csaló betartja a protokoll szabályait, de több információt szerez, mint amennyi a protokoll szereplőjeként megilletné. Az aktív csaló nem tartja be a protokoll szabályait, így szerezve meg jogosulatlanul a többletinformációt.

Az alábbi kritériumok alapján lehet felmérni egy támadás súlyosságát:

- *Teljes feltörés*: A támadó vagy megfejti az aláíró titkos kulcsát, vagy a valódi aláírási algoritmust behelyettesíti egy azzal funkcionálisan egyenértékű algoritmussal.
- *Szelektív hamisítás*: A támadó képes arra, hogy egy üzenethez, vagy előre kiválasztott üzenetek csoportjához valódi aláírást generáljon. Az aláírás generálása nincs közvetlen hatással a törvényes aláíróra.

- *Egzisztenciális hamisítás*: A támadó képes legalább egy üzenet aláírásának hamisítására. Azonban nem tudja ellenőrzése alá vonni azt az üzenetet, amelynek megszerezte az aláírását, és a törvényes aláíró belekeveredhet a csalásba.

Az aláírási mechanizmusok elleni támadások célja a valódi aláírások hamisítása és mások nevében való felhasználása. Ezek a támadások egyben a titkosító algoritmusok ellen is irányulhatnak, veszélyeztetve ezzel a titkosított információ, súlyosabb esetben a titkos kulcs biztonságát.

A nyilvános kulcsú aláírási mechanizmusok elleni támadások:

- *Kulcs megszerzésén alapuló támadás*: A támadó csupán az aláíró nyilvános kulcsát ismeri.
- *Üzenet alapú támadás*: A támadó képes ismert vagy választott üzenetek aláírását analizálni. Az üzenet alapú támadásokat az alábbi osztályokba sorolhatjuk:
    - *Ismert üzenet alapú támadás*: A támadó számára ismert, de nem általa választott üzenetekhez tartozó aláírásokkal rendelkezik.
    - *Választott üzenet alapú támadás*: A támadó megszerzi az általa választott üzenetek aláírását, majd megkísérli az aláírási mechanizmus feltörését. Ez a fajta támadás nem-módosított abban az értelemben, hogy az üzenetek kiválasztása az aláírások vizsgálata előtt történik. A választott üzenet alapú támadások hasonlóak a nyilvános kulcsú titkosítási mechanizmusok elleni választott kriptoszöveg alapú támadásokhoz.
    - *Módosított választott üzenet alapú támadás*: A támadó megszerezheti az aláíró nyilvános kulcsától függő üzenetek aláírását, valamint az előzőleg megszerzett aláírásokon vagy üzeneteken alapuló üzenetek aláírását.

A módosított választott üzenet alapú támadást a legnehezebb megelőzni. Elképzelhető, hogy megfelelő mennyiségű üzenet és aláírás megléte esetén

egy támadó mintát készíthet és tetszés szerinti aláírásokat hamisíthat. Bár a gyakorlatban kivitelezhetetlen lenne egy ilyen támadás, egy jól megtervezett aláírási mechanizmusba célszerű bevenni az ilyen lehetőségek elleni védelmet is.

Az aláírási mechanizmusok biztonsági szintje az alkalmazásuk függvényében változhat. Például abban az esetben, ha a támadó csak egy kulcstámadás kivitelezésére képes, elegendő a szelektív hamisítás elleni védelmet beépíteni a mechanizmusba. Ha viszont a támadó az üzenet alapú támadást is meg tudja valósítani, akkor az egzisztenciális támadás elleni védelemre is szükség van.

A protokollokat is sokféle támadás fenyegeti, ezekből sorolok fel néhányat az alábbiakban:

- *Ismert kulcs alapú támadás:* A támadó néhány korábban használt kulcs birtokában új kulcsokat próbál megfejteni.
- *Visszajátszás:* A támadó rögzíti a kommunikáció tartalmát és egy későbbi időpontban visszajátssza az egészet, vagy a felvett anyag egy részletét.
- *Megszemélyesítés:* A támadó az egyik kommunikáló fél helyébe lép, azaz az ő nevében kommunikál.
- *Szótár:* Ez a támadás jelszavak ellen irányul. A jelszó általában egy számítógépes fájlban, egy hash függvény leképezéseként kerül tárolásra. Amikor a felhasználó belép és beírja a jelszavát, a beírt szónak képezik a hash értékét, amelyet ezután összehasonlítanak a tárolt értékkel. A támadó szerezhet egy listát a lehetséges jelszavakról, képezheti ezeknek a hash értékét és összehasonlíthatja az így kapott értékeket a titkosított jelszavak listájával, ha egyező értékeket talál, az adott jelszó a birtokába kerül.
- *Közbeékelődési támadás:* A támadó a kommunikáló felek közé ékelődve megváltoztathatja a kommunikáció tartalmát azáltal, hogy bármelyik felet meg tudja személyesíteni.

III. AZ ELEKTRONIKUS ALÁÍRÁS JOGI SZABÁLYOZÁSA

3.1. Miért van szükség az elektronikus aláírást szabályzó törvényre?

Két szerződő fél már a jogi szabályozás előtt is megegyezhetett, hogy az egymás közötti szerződéseket elektronikus formában is elfogadják, de ehhez előtte papír alapon hagyományosan hitelesített szerződést kellett kötniük erről. Ez külön törvény nélkül is működött. A törvényalkotással ezek a kétoldalú megegyezések egyszerűsödnek, bár a törvényben foglaltaktól a kétoldalú szerződésekben ezentúl is el lehet térni. A törvény megalkotásával azonban mód nyílik arra, hogy olyan területeken is bevezethetővé váljon az elektronikus iratok használata, ahol ezt a megelőző szabályozás nem tette lehetővé (pl. cégeljárások, adóhivatal, államigazgatás).

A törvény célja tehát, hogy az elektronikus aláírás alkalmazását bevezesse több, állami szabályozás alatt álló területre is. Ennek elengedhetetlen feltétele, hogy a kapcsolódó törvényeket is módosítani kell.

3.2. Az elektronikus aláírás szabályozása az Európai Unióban

Az Európai Parlament és a Tanács 2000. januárjában irányelvet adott ki az elektronikus aláírással kapcsolatban, melyben meghatározta az elektronikus aláírással kapcsolatos alapelveket, és elrendelte, hogy minden tagországnak 2001. júliusáig létre kell hoznia a közös elveken alapuló saját szabályozási rendszerét.

Az EU alapelvek között szerepel többek között, hogy az elektronikus aláírást minden szempontból egyenértékűnek kell tekinteni a hagyományos

aláírással, valamint hogy az Európai Közösség tagállamai elfogadják egymás elektronikus aláírásait és tanúsítványait, és támogatják a térség más államainak a rendszerhez való csatlakozását is. Egy ilyen több országra kiterjedő rendszer működőképességéhez természetesen nem csak a jogharmonizáció elengedhetetlen, hanem a technológiai hátteret is egyeztetni kell.

3.3. Az elektronikus aláírás jogi kereteinek kialakítása Magyarországon

Magyarországon már 1998-ban lefektették az elektronikus iratok szabályozásának alapelveit, ezt követően 1999-ben megalakult a szakminisztérium (Közlekedési, Hírközlési és Vízügyi Minisztérium) elektronikus aláírás munkacsoportja. 2000. augusztusában fogadták el az elektronikus aláírás bevezetéséről szóló kormányhatározatot, ebben rendelkeztek az elektronikus aláírási törvény meghozataláról.

Az elektronikus aláírásról szóló 2001/XXXV. sz. törvényt az Országgyűlés a 2001. május 29-i ülésnapján fogadta el. A törvény 2001. szeptember 1-jén lépett hatályba.

3.3.1. Az elektronikus aláírási törvény bemutatása

A magyar szabályozás kialakításánál alapvető szempont volt az EU irányelvek maradéktalan betartása. Emellett természetesen a hatályos hazai jogszabályokat is tekintetbe kellett venni. A kérdéssel legszorosabban összefüggő törvények módosítására a törvénytervezet záró rendelkezései tesznek módosító javaslatot, ezzel megteremtve az elektronikus aláírás és elektronikus dokumentumok felhasználásának alapeseteit is.

A törvény három lényeges témakört szabályoz:

- a törvény hatályát, mely egyszersmind meghatározza az elektronikus aláírás felhasználásának lehetőségét is

- az elektronikus aláírással kapcsolatos szolgáltatások szabályait
- a szolgáltatókat felügyelő és a szolgáltatókat nyilvántartó, illetve minősítő Hírközlési Főfelügyelet tevékenységére vonatkozó szabályokat

A törvénytervezet megalkotásánál szintén alapelv volt, hogy a jogi szabályozásnak technológia-függetlennek kell lennie. A használt jogi terminológiában az ismert műszaki fogalmak helyett azok funkciói szerinti elnevezésükre került sor.

A törvény a következő fogalmakat definiálja:

- egyszerű elektronikus aláírás, fokozott biztonságú elektronikus aláírás, minősített elektronikus aláírás
- elektronikus dokumentum, elektronikus irat, elektronikus okirat
- aláírás létrehozó adat (titkos kulcs), aláírás ellenőrző adat (nyilvános kulcs)
- aláírás létrehozó eszköz, biztonságos aláírás létrehozó eszköz
- tanúsítvány, minősített tanúsítvány
- időbélyegző
- elektronikus aláírás ellenőrzése, elektronikus aláírás felhasználása
- aláíró, elektronikus aláírás hitelesítés-szolgáltató

A törvény az elektronikus dokumentumok három fajtáját különbözteti meg:

- Az *elektronikus dokumentum* elektronikus eszköz útján értelmezett adat, mely elektronikus aláírással van ellátva.
- Az *elektronikus irat* olyan elektronikus dokumentum, melynek funkciója szöveg betűkkel való közlése.
- Az *elektronikus okirat* olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában.

Az elektronikus dokumentumhoz hasonlóan az elektronikus aláírásnak is három fajtáját határozza meg a törvény:

- Az *elektronikus aláírás* elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.
- A *fokozott biztonságú elektronikus aláírás* olyan elektronikus aláírás,
    - amely alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
    - melyet olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll, és
    - amely a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.
- A *minősített elektronikus aláírás* olyan – fokozott biztonságú – elektronikus aláírás, amely biztonságos aláírás ellenőrző eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

3.3.1.1. A törvény által meghatározott működési struktúra

A törvényben szabályozott, az elektronikus aláírással kapcsolatos szolgáltatások a következők:

- hitelesítés szolgáltatás (az elektronikus tanúsítványok kiadása és az ezzel kapcsolatos nyilvántartások vezetése)
- időbélyegző szolgáltatás
- aláírás létrehozó eszközön aláírás létrehozó adat elhelyezése

A fenti tevékenységek folytatását be kell jelenteni a Hírközlési Főfelügyeletnek, amely nyilvántartásba veszi az adott szolgáltatót és ettől kezdve folyamatos ellenőrzést gyakorol felette a törvényesség betartása, az üzletszabályzat és az általános szerződési feltételek betartása tekintetében. Amennyiben valamilyen rendellenességet észlel, akkor – akár azonnali hatállyal – intézkedéseket foganatosíthat, pénzbírságot szabhat ki, de akár kötelezheti is a szolgáltatót tevékenysége beszüntetésére.

Minősített tanúsítvány kiadását, illetve aláírás létrehozó eszközön aláírás létrehozó adat elhelyezését csak minősített hitelesítés-szolgáltatók végezhetik. A minősítést szintén a Hírközlési Főfelügyelet végzi, minősítés megszerzéséhez sokkal komolyabb feltételeknek kell eleget tenni (büntetlen előélet, szakképzettség, felelősségbiztosítás, pénzügyi erőforrás, biztonságos elektronikus aláírási termékek használata stb.). A minősített hitelesítés-szolgáltatónál a Hírközlési Főfelügyelet legalább évente egyszer átfogó helyszíni ellenőrzést tart. Amennyiben a minősített szolgáltató nem felel meg az előírt követelményeknek, és egyéb intézkedések nem vezetnek eredményre, akkor a Hírközlési Főfelügyelet visszavonhatja a minősítést.

A hitelesítés-szolgáltató végzi az elektronikus tanúsítványok kiadását. Ennek keretében először is azonosítania kell az igénylő személyét. Amennyiben ez sikerrel jár, az igénylő személy aláírás ellenőrző adatát, a személy azonosítására szolgáló egyéb adatokat, valamint a tanúsítvány készítésére és használatára vonatkozó egyéb paramétereket (pl. szolgáltató neve, felhasználási korlátozások, érvényesség kezdete és vége stb.) rögzíti a tanúsítványban, melyet saját aláírás létrehozó adatával ír alá. Nyilvántartást vezet a kiadott tanúsítványokról és azokról az adatokról, amelyek alapján a tanúsítványt kiadta. Fogadja és feldolgozza a tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról. Ez utóbbit, valamint saját szabályzatait és az aláírás ellenőrző adatokat közcélú távközlő hálózatok segítségével folyamatosan elérhető módon közzéteszi.

IV. AZ ELEKTRONIKUS ALÁÍRÁS SZABVÁNYOSÍTÁSA

4.1. Miért van szükség szabványosításra?

A hitelesség megállapítására szolgáló termékek és szolgáltatások fejlődése és használata még kezdeti szakaszban van. Léteznek ugyan kereskedelmi, kormányzati és közszolgálati azonosító rendszerek, de nincsenek mindenre kiterjedő ipari szabványok vagy műszaki specifikációk, amelyekkel szabályozni lehetne e rendszerek használatát. Az ilyen szabványoknak nemzetközi szinten is elismert, egységes biztonsági szintet kell meghatározniuk.

4.2. Szabványosítás az Európai Unióban

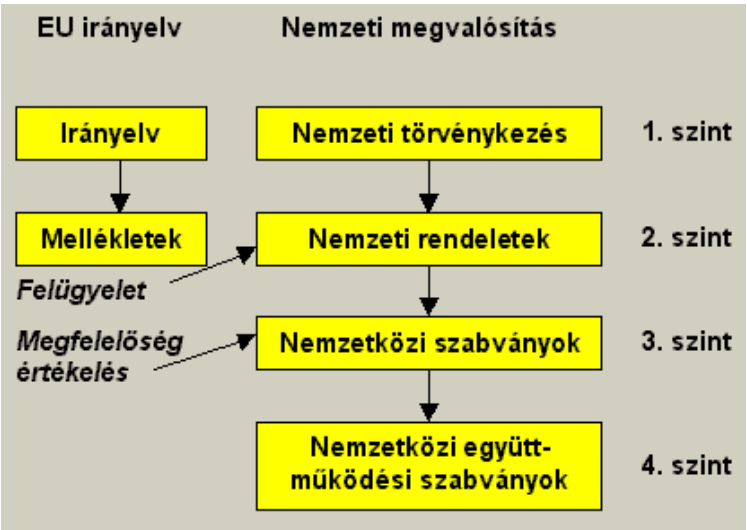
Az Európai Tanács felkérésére az Európai Bizottság egy irányelv kidolgozását indítványozta az elektronikus aláírás közösségi kereteinek szabályozására. Az irányelvnek nem az a célja, hogy lefedje a hitelesítési alkalmazások teljes skáláját, hanem az, hogy az elektronikus aláírás jogi kereteit megteremtse. Ezzel kapcsolatban az irányelv meghatározza a tanúsítványokkal, hitelesítés-szolgáltatókkal, valamint az aláírás létrehozó és ellenőrző eszközökkel szemben támasztott alapkövetelményeket.

Számos szabványosítási kezdeményezés van folyamatban országos, regionális és nemzetközi szinten. Említésre méltó a Nemzetközi Kereskedelmi Kamara (ICC), az Internet Law Policy Forum (ILPF), az Internet Engineering Task Force (IETF), a World Wide Web Consortium (W3C) és az American Bar Association (ABA) szabványosítási tevékenysége. Ezek azonban – a szabványosítás mai fázisában – nem elegendőek a jogi követelmények teljesítéséhez. Következetes szemlélet szükséges az elektronikus aláírás jogi kereteinek szabványokon és más önkéntesen elfogadott szabályokon keresztül történő megteremtéséhez,

abból a célból, hogy törvényesen elismert aláírás jöjjön létre, melyet nem csak Európában, hanem az egész világon elfogadnak.

A fentiek szellemében az Európai Bizottság felkérte az Információ- és Kommunikáció-technológiai Szabványosítási Tanács (ICTSB) keretében működő ipari és európai szabványosítási testületeket annak elemzésére, hogy az irányelvben meghatározott, az elektronikus aláírási termékekkel és szolgáltatásokkal kapcsolatos jogi követelmények teljesítéséhez milyen mértékű szabványosításra van szükség. A meglévő globális és regionális szintű szabványok és a jelenlegi folyamatok értékelése feltárja a hiányosságokat és a további szabványosításra való igényt, amely szabványok, specifikációk, megállapodások, vagy műhelyek formájában testesülhet meg.

Az ipari és az európai szabványosítási testületek feladata az irányelv által meghatározott jogi keretekkel összhangban a szabványosítási folyamat elindítása, amely kielégíti az üzleti szféra igényeit, és lehetővé teszi az elektronikus aláírás törvényi elismeréséből fakadó előnyök kihasználását az elektronikus kereskedelem fejlődése érdekében.



***5. sz. ábra.* A szabványosítás folyamata az Európai Unióban**

Forrás: [13]

4.3. Az Európai elektronikus aláírás szabványosítási kezdeményezés (EESSI)

Bár a hitelesítési rendszerek területén számos országos, regionális és nemzetközi szintű szabványosítási kezdeményezés indult, az általános tapasztalat az, hogy ezek nem eléggé összehangoltak és következetesek az irányelv által meghatározott ellenőrzési és kölcsönös-elismerési elvek követése tekintetében.

E probléma megoldásaként 1998. decemberében az Európai ICT Szabványosítási Tanács (European ICT Standards Board) az Európai Bizottság támogatásával elindította az Európai elektronikus aláírás szabványosítási kezdeményezést (EESSI), melynek résztvevői az ipar és az állami hatóságok képviselői, a téma szakértői és más piaci szereplők.

Az EESSI a résztvevők egységes szemléletét követve feltérképezi, hogy milyen területeken van szükség szabványosításra az irányelvben megfogalmazott követelmények teljesítése érdekében, és felügyeli az ilyen szükségletek kielégítése céljából megalkotott munkaprogram megvalósítását.

Az EESSI létrehozása három fő elven alapul:

- az elektronikus aláírás tárgykörében érdekelt felek hatékony bevonása a szabványosítási folyamatba;
- az alkalmazott mechanizmusok és a kezdeményezések nyitottá és átláthatóvá tétele;
- a globális, nemzetközileg elismert megoldások támogatása.

Két egyeztető megbeszélés után, 1999. júliusában született meg az EESSI zárójelentése, amely tartalmazza az alapvető ajánlásokat, áttekintést nyújt a szabványosítási tevékenységek követelményeiről, és részletes munkaprogramot fogalmaz meg e követelmények teljesítése céljából. A munkaprogramban három alapvető pontot döntő fontosságúként kezelnek, ezek az alábbiak:

- A hitelesítés-szolgáltatókra vonatkozó (CSP) minőségi és működési szabványok;
- Az aláírás létrehozó és ellenőrző termékekre vonatkozó minőségi és működési szabványok;
- Az elektronikus aláírást érintő szabványosítási követelmények.

Az alábbi tevékenységek különösen fontosnak minősülnek:

- Aláírási termékek biztonsági követelményei;
- Az elektronikus aláíráshoz kapcsolódó termékek és szolgáltatások megfelelőségének tanúsítása / nyilvántartásba vétele;
- Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatók biztonsági és hitelesítési politikája;
- Aláírás létrehozása és ellenőrzése;
- Az elektronikus aláírás szintaxisa és formája, az aláírási szabályzatok műszaki szempontjai;
- Az X.509 nyilvános kulcsú tanúsítványok minősített tanúsítványként való használatára vonatkozó szabvány;
- Protokoll az időbélyegző szolgáltatóval való együttműködéshez.

4.3.1. A megvalósítás folyamata

Egy irányító csoport felügyeli a munkaprogram megvalósítását. Az irányító csoport a piaci szereplők – a szakma, a szolgáltatók, a felhasználók / fogyasztók, az állami hatóságok és az érdekelt ICTSB tagszervezetek – képviselőiből áll.

Az európai szintű szabványosítási tevékenységet két elismert európai szabványosítási szervezet, az Európai Szabványosítási Bizottság (CEN) és az Európai Távközlési Szabványosítási Intézet (ETSI) más szervezetekkel együttműködve végzi. A CEN és az ETSI által végzett munka minden érdekelt fél számára nyitott. Mindkét szervezet külön erre a célra szakmai csoportot hozott létre.

Az EESSI részt vesz a globális vagy regionális szinten megvalósítandó kezdeményezésekben, és megoldásokat keres az elektronikus aláírási alkalmazások nemzetközi szintű összehangolásának elősegítésére.

4.3.1.1. Az ETSI SEC tevékenysége

Az ETSI műszaki testülete, az ETSI Security (SEC) felelős a távközlési szektorban a biztonsági infrastruktúráért és szolgáltatásokért. Az ETSI SEC-en belül működő Elektronikus aláírás infrastruktúra munkacsoport (ESI) felel az ETSI olyan tevékenységeiért, melyek kapcsolatban állnak az EESSI munkaprogramjával. Az ETSI SEC által megalkotott szabványtervezetek az ETSI műszaki specifikációk (TS). Ezekről szavaznak az ETSI tagszervezetei.

4.3.1.2. A CEN/ISSS tevékenysége

A CEN Információs Társadalom Szabványosító Rendszere (CEN/ISSS) az EESSI munkaprogram azon részéért felelős, amely az aláírás létrehozó és ellenőrző termékekre és a hitelesítés-szolgáltatókra vonatkozó minőségi és működési szabványokkal foglalkozik.

A gyors technológiai változások miatt a CEN/ISSS a hagyományos CEN műszaki bizottságok mellett nagy hasznát veszi a műhelyeknek. A CEN/ISSS létrehozott egy Elektronikus aláírási műhelyt (E-SIGN) a munkaprogram rá eső részének megvalósításához. A műhely az alábbi feladatokkal foglalkozik:

- Megbízható rendszerek és termékek biztonsági követelményei;
- Biztonságos aláírás létrehozó eszközök biztonsági követelményei;
- Aláírás létrehozási környezet;
- Aláírás ellenőrzési eljárás és környezet;
- Az elektronikus aláírással kapcsolatos termékek és szolgáltatások megfelelőségének értékelése.

Az E-SIGN CEN műhely megállapodások (CWA) formájában hozza nyilvánosságra a szabványosítási folyamat eredményeit. A CWA-k

bekerülnek a CEN tagszervezetek szabványkatalógusába, azaz nemzeti szabvánnyá válnak. A CWA-kat kétévente felülvizsgálatnak vetik alá. A vizsgálat eredményétől függően az alábbiak történhetnek:

- ha még működik, az eredeti műhely, vagy egy erre a célra felállított nyitott műhely újból elfogadhatja a megállapodást;
- a piaci fejlődésnek megfelelően módosítható a megállapodás;
- egy újabb európai vagy nemzetközi szintű szabványosítási folyamat részeként tárgyalható a megállapodás;
- a megállapodás visszavonásra kerülhet.

4.3.2. Az EESSI által kidolgozott szabványok és specifikációk

4.3.2.1. ETSI SEC szabványok

ETSI TS 101 465: A minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókkal szembeni követelmények

E szabvány meghatározza a minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatók működésével és biztonságával szemben támasztott követelményeket az elektronikus aláírásról szóló európai irányelvben (1999/93/EK) foglaltak alapján.

ETSI TS 101 862: Minősített tanúsítvány profil

Ez a szabvány a nyilvános kulcsú infrastruktúra piacon meghatározó X.509 nyilvános kulcsú tanúsítványnak az elektronikus aláírási irányelv szerinti használatát írja le. A szabványnak köszönhetően a hitelesítés-szolgáltatók közötti műszaki együttműködés, valamint az aláírás létrehozó és ellenőrző alkalmazások összehangoltsága jelentős mértékben javul, ezáltal is nyitottabbá téve az elektronikus piacot. Egy már széles körben elfogadott szabványra (X.509) építve ez a szabvány csökkenti a szolgáltatók költségeit, amelyek az irányelv rendelkezéseinek betartása miatt merülnek fel.

ETSI TS 101 861: Időbélyegzési profil

E szabvány azt írja le, hogy az időbélyegzésről szóló Internet specifikáció, amelyet már minden fontosabb szolgáltató elfogadott, hogyan alkalmazható a fokozott biztonságú elektronikus aláírásoknál a hosszú távú érvényesség fenntartása céljából. A szabvány elősegíti a hosszú távú érvényességű elektronikus aláírásokat kezelő alkalmazások és az időbélyegzési szolgáltatásokat nyújtó hitelesítés-szolgáltatók hatékony együttműködését. A szabvány – többek között – meghatározza az időbélyegző formáját és az időbélyegzéshez használt protokollt is.

ETSI TS 101 733: Elektronikus aláírási formák

A szabvány a fokozott biztonságú elektronikus aláírás formáját szabályozza az e-mail és iratbiztonsági piacot meghatározó szabványos forma alapján. Azt is meghatározza, hogy az időbélyegzési szolgáltatások és a megbízható archiváló szolgáltatások segítségével milyen módon lehet az elektronikus aláírás hosszú távú érvényességét biztosítani abból a célból, hogy a későbbiekben, vita esetén bizonyítékként szolgálhasson.

A szabvány mind a minősített tanúsítványokkal és biztonságos létrehozó eszközzel összekapcsolva használt minősített elektronikus aláírásokhoz, mind más formátumú elektronikus aláírásokhoz alkalmazható, melyek bizonyítékként szolgálhatnak a későbbiek során.

A szabvány meghatározza, hogyan alkalmazható a titkosított üzenetek szintaxisáról szóló RFC 2630 Internet specifikáció a fokozott biztonságú elektronikus aláírásokhoz és a hosszú távú érvényesség biztosítása érdekében további mezőket és eljárásokat definiál, melyek kompatibilisek a meglévő szintaxissal. Az ETSI formátum használata biztosítja, hogy az aláíró a későbbiekben ne tagadhassa le az aláírását, és hogy az aláírás a róla szóló tanúsítvány érvényessége lejárta után is ellenőrizhető legyen. E szabvány alkalmazásával az aláírás létrehozó és ellenőrző alkalmazások közötti együttműködés jelentősen javítható.

4.3.2.2. CEN/ISSS E-SIGN specifikációk

Az elektronikus aláírási tanúsítványokat kezelő megbízható rendszerekkel szemben támasztott biztonsági követelmények

Ezzel a témakörrel két specifikáció foglalkozik. Az egyik (CWA 14167-1) általános biztonsági követelményeket fogalmaz meg az egyszerű és minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatók által használt megbízható rendszerelemekkel szemben.

A rendszerbiztonsági követelmények azon funkciók strukturált modelljén alapulnak, amelyeket a hitelesítés-szolgáltató megbízható rendszere támogat. A specifikáció tartalmaz néhány általános biztonsági követelményt abból a célból, hogy a hitelesítés-szolgáltató megbízható rendszerének alapvető biztonsága garantálva legyen.

A másik specifikáció (CWA 14167-2) a hitelesítés-szolgáltatók által használt kriptográfiai modulokra vonatkozó követelményeket tartalmazza. A követelmények meghatározása az ISO 15408 nemzetközi szabvány rendelkezései alapján egy védelmi profil (PP) formájában történik. Ezt a védelmi profilt kell alkalmazni a kriptográfiai modulokra.

A biztonságos aláírás létrehozó eszközökkel szemben támasztott biztonsági követelmények

A specifikáció célja a biztonságos aláírás létrehozó eszközökre vonatkozó biztonsági követelmények egységesítése, valamint az EU irányelvnek való megfelelésük és kölcsönös együttműködésük biztosítása.

A biztonsági követelmények a specifikáció szerves részét képező védelmi profil formájában kerülnek meghatározásra. A követelmények – amennyire ez lehetséges – technológia-semlegesek. Ennek szellemében a specifikáció – a technológia jelenlegi állása szerint – annyi különböző megvalósítási módot tárgyal, amennyi csak lehetséges. A jövőbeni fejlesztések figyelembe vétele céljából a specifikáció rendszeresen frissítésre kerül.

Az e specifikáció szerint értékelt biztonságos aláírás létrehozó eszköz használatakor a felhasználó biztos lehet benne, hogy az eszköz biztonságos, és megfelel a minősített elektronikus aláírás létrehozására vonatkozó követelményeknek.

A szabványosítási folyamat során két védelmi profilt (CWA 14168 és CWA 14169) hoztak létre, melyek két különböző biztonsági szint szerint szabályozzák a termékek megfelelőségét.

Aláírás létrehozási és ellenőrzési eljárás és környezet

- Aláírás létrehozási eljárás és környezet (CWA 14170)
  Az irányelv nem határozza meg az aláírás létrehozási eljárásra és környezetre vonatkozó követelményeket. Ebből következően ez a specifikáció opcionális követelményeket fogalmaz meg az aláírás létrehozó rendszerekre vonatkozóan. A specifikáció az alábbiakat tartalmazza:
  - Az aláírás létrehozási környezet modellje és az aláírás létrehozó rendszer funkcionális modellje;
  - A funkcionális modellben meghatározott funkciókra vonatkozó általános követelmények;
  - A biztonságos aláírás létrehozó eszköz kivételével az aláírás létrehozási rendszerben meghatározott összes funkcióra vonatkozó biztonsági követelmények.

  A specifikációnak köszönhetően az aláírás létrehozási folyamat úgy építhető be az ezt használó alkalmazásokba és számítógéprendszerekbe, hogy a későbbiekben felmerülő vitás helyzetek minél nagyobb mértékben kiküszöbölhetők legyenek.

- Elektronikus aláírás ellenőrzési eljárások (CWA 14171)
  A specifikáció – az irányelv ajánlásainak megfelelően – előírásokat tartalmaz az aláírás ellenőrzési eljárásra vonatkozóan, beleértve az ellenőrzéshez használt termékeket és azok kezelését is.

A specifikáció az aláírás ellenőrzési rendszerek különböző elemeire vonatkozó követelményeket is meghatározza. Az ellenőrzési eljárás mellett foglalkozik a különböző interfészekkel, például az alkalmazás programozási interfészekkel (API) vagy az ember-gép interfésszel (MMI), amelyek szükségesek:

- az aláírt irat és az ellenőrzendő elektronikus aláírás kiválasztásához;
- az aláírt irat helyes formátumban történő megjelenítéséhez;
- az aláíró adatainak megszerzéséhez és az aláírás ellenőrzése után az állapot kijelzéséhez;
- a hosszú távú érvényesség ellenőrzése céljából további adatok kéréséhez; és
- különböző hitelesítés-szolgáltatóktól adatok gyűjtéséhez.

A specifikáció meghatározza azokat az adatokat, melyeket gyűjteni és archiválni kell abból a célból, hogy ha a későbbiekben vitás helyzet alakulna ki, akkor ezeket az adatokat fel lehessen használni ennek megoldására.

Megfelelőség-értékelési útmutató

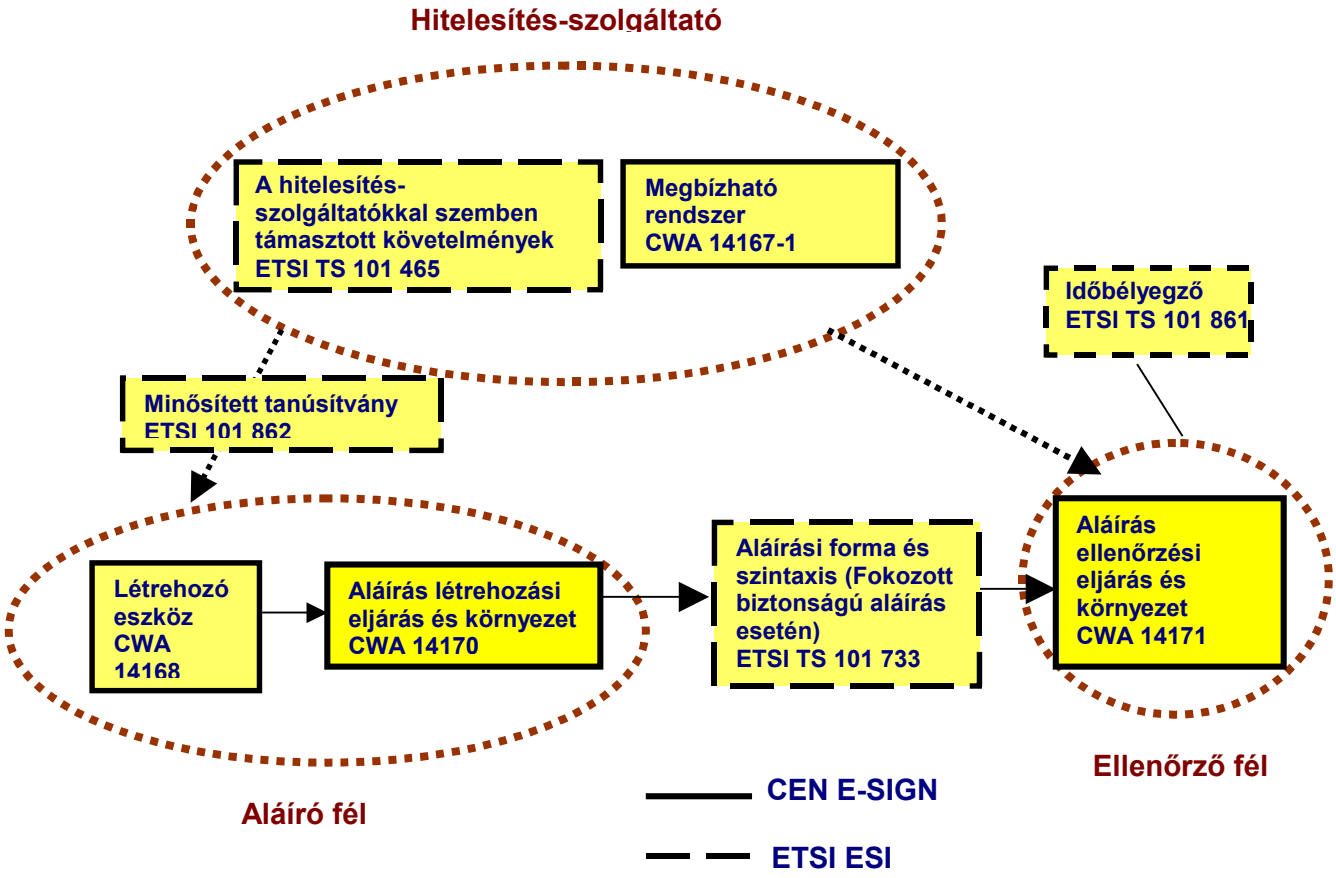
Ez a specifikáció útmutatást nyújt az elektronikus aláíráshoz kapcsolódó alábbi szolgáltatások, eljárások, rendszerek és termékek megfelelőség-értékeléséhez:

- a hitelesítés-szolgáltatók nyilvános kulcsú infrastruktúra és információbiztonság kezelési szolgáltatásai és eljárásai
- aláírás létrehozó rendszerek
- aláírás-ellenőrzés
- biztonságos aláírás létrehozó eszközök.

A specifikáció öt részből áll:

- 1. rész: Általános bevezetés a Megfelelőség Értékelési Útmutatóhoz (CWA 14172-1)

- 2. rész: Megfelelőség Értékelési Útmutató a hitelesítés-szolgáltatók szolgáltatásaihoz és eljárásaihoz (CWA 14172-2)
- 3. rész: Megfelelőség Értékelési Útmutató az aláírás létrehozási és ellenőrzési eljáráshoz és környezethez (CWA 14172-3)
- 4. rész: Megfelelőség Értékelési Útmutató az elektronikus aláírási tanúsítványokat kezelő megbízható rendszerek biztonsági követelményeihez (CWA 14172-4)
- 5. rész: Megfelelőség Értékelési Útmutató a biztonságos aláírás létrehozó eszközök biztonsági követelményeihez (CWA 14172-5)



***6. sz. ábra.* Az EESSI által meghatározott szabványrendszer**

Forrás: [8 – Annex 2]

4.3.3. Az EESSI irányító csoport ajánlása a kriptográfiai modulokról

Az elektronikus aláírásról szóló EU irányelvben foglaltak szerint a hitelesítés-szolgáltató köteles megbízható rendszereket üzemeltetni. Az általános gyakorlat az, hogy a megbízható rendszerek részeként a kriptográfiai tárolás és műveletek megfelelő védelem alatt állnak a hamisítás elleni kriptográfiai modulok használatának köszönhetően.

Az ajánlás az említett kriptográfiai modulokra vonatkozó szabványokkal és az ehhez kapcsolódó termékek és szabványok elfogadásával foglalkozik. A műszaki megvalósítás menetét a termékértékeléssel foglalkozó szervezetek – általában akkreditált laboratóriumok – határozzák meg.

A hitelesítés-szolgáltató által használt kriptográfiai modulok tekintetében az elsődleges fontosságú biztonság mellett a kapcsolódó szabványok és termékértékelési eljárások nemzetközi elismerése is lényeges. A jelenlegi értékelési és tanúsítási gyakorlatnak azonban alapvető hiányosságai vannak:

- A szabvány, amelyet a legtöbb gyártó figyelembe vesz (FIPS 140-1; Federal Information Processing Standards), nem kifejezetten a hitelesítés-szolgáltatók által használt kriptográfiai modulokkal foglalkozik, s emiatt számos követelmény hiányzik belőle.
- A szabvány európai alkalmazása elsősorban azért okoz gondot, mert ez egy észak-amerikai szabvány és a tesztelésére is kizárólag ott került sor. Ez hátrányos helyzetet okoz.
- Európában jelentős tapasztalat halmozódott fel a kriptográfiai modulok értékelésével kapcsolatosan az ITSEC (Information Technology Security Evaluation Criteria) alkalmazása nyomán. Ezek az értékelések azonban nem hasonlíthatók össze egymással, mivel nem létezik az ilyen kriptográfiai modulok biztonsági követelményeit tárgyaló szabványgyűjtemény.

A fenti okokból következően az EESSI szükségesnek látja a kriptográfiai modulokra és azok értékelésére vonatkozó nemzetközi szabvány

megalkotását. Az EESSI programon belül külön terület foglalkozik e szabvánnyal. A CEN/ISSS elektronikus aláírási műhely a munka felelőseként egy védelmi profilt dolgoz ki a közös kritériumok alapján. A NIST-tel (American National Institute for Standards and Technology) való szoros együttműködés a garancia arra, hogy kiváló és nemzetközileg elfogadott szabvány jöjjön létre.

A végső cél a kriptográfiai modulok minőségi szabványként szolgáló védelmi profiljának megteremtése. Ennek az az előfeltétele, hogy minden érintett fél (a szabványkészítők, felügyelők, auditorok, gyártók és a hitelesítés-szolgáltatók) ezt az új védelmi profilt használja.

4.4. Egy globális elektronikus aláírási hálózat

Az Identrus nevezetű profitorientált társaságot a világ legnagyobb pénzintézetei hozták létre 1999-ben abból a célból, hogy elhárítsák az üzleti partnerek közötti elektronikus kereskedelem fejlődését gátló akadályokat. Ezek a pénzintézetek felismerték, hogy az elektronikus kereskedelem fő akadályozó tényezője a bizalmatlanság: az üzletfelek nem bízzák az Internetre a nagy horderejű üzletkötéseket, mivel tudják, hogy nagyon könnyű más nevében e-mail-t írni, illetve az elektronikus úton terjesztett bizalmas iratokba beleolvasni.

Az Identrus alapítói – az ABN Amro Bank, a Bank of America, a Bankers Trust, a Barclays, a Chase Manhattan, a Deutsche Bank és a HypoVereinsbank – és a hozzájuk csatlakozó más pénzintézetek létrehoztak egy közös technológiai, kockázatelemzési és szerződéskötési szabályzatot annak érdekében, hogy az üzleti partnerek közötti elektronikus kereskedelem megbízható és biztonságos lehessen.

Az Identrus rendszerben résztvevő pénzintézetek Identrus hitelesítés-szolgáltatókként működnek, ennek következtében az ügyfeleik megbízható üzletfelekké válnak az összes Identrus tagszervezet számára. Az Identrus

hitelesítés-szolgáltatók egyedi azonosítót bocsátanak ki az ügyfeleik számára. Az azonosítók biztonságát a globális nyilvános kulcsú infrastruktúra garantálja.

A fent leírtak figyelembevételével kijelenthető, hogy az Identrus hitelesítés-szolgáltatók által hitelesített üzleti partner teljes bizonyossággal meggyőződhet bármely más Identrus üzleti partner megbízhatóságáról. Ez a globális rendszer lehetővé teszi az elektronikus kereskedelem terjedését gátló bizalmatlanság leküzdését, valamint elősegíti az Interneten történő banki műveletek és az internetes fizetés fejlődését is.

V. A HITELESÍTÉS-SZOLGÁLTATÓK TEVÉKENYSÉGE

5.1. A nyilvános kulcsú infrastruktúra szerepe

Az Algoritmikus adatvédelem c. részben már említett nyilvános kulcsú infrastruktúra (PKI) azoknak a tényezőknek az összességét jelenti, melyek megbízhatóvá teszik az aszimmetrikus titkosítási rendszerek hálózatban történő használatát.

A PKI fő célja a hálózati biztonság megteremtése, eszközök biztosítása a kommunikáló felek távolról történő azonosításához, valamint a kézírásos aláírás hasonmásának létrehozása és továbbfejlesztése a virtuális világban.

A PKI a biztonságot a dolgozatom elején általánosan bemutatott információbiztonsági követelmények kielégítésével teremti meg. A követelmények teljesítéséhez a PKI biztonsági szolgáltatásokat határoz meg, melyeket az elektronikus kereskedelmi rendszerek szempontjából mutatok be:

- *Azonosítás, hitelesítés*: a kommunikáló felek azonosítása a valós világban személyi okmányokkal történik (útlevél, személyi igazolvány stb.), míg a virtuális térben meg kell teremteni a távolról történő azonosítás lehetőségét.
- *A bizalmas jelleg megteremtése*: ez azt jelenti, hogy illetéktelenek ne kísérhessék figyelemmel a kommunikációt. A valós világban ezt a hangerő, a hely vagy éppen az időpont megválasztásával próbálják megoldani. A virtuális térben sokkal nehezebb megállapítani, hogy lehallgatja-e valaki a kommunikációt, s éppen emiatt a lehallgatást akadályozó szolgáltatások alapvető szerepet játszanak a bizalmasság megteremtésében.
- *Az adatok sérthetetlenségének biztosítása*: ez a szolgáltatás megakadályozza, hogy a kommunikáció tartalmát illetéktelenek

megváltoztassák. A valós világban a bélyegző használatával próbálják az ilyen jellegű beavatkozást meggátolni, míg a virtuális térben ezt a szerepet az elektronikus aláírás tölti be.

- *A letagadhatatlanság biztosítása*: ez a szolgáltatás azt segíti elő, hogy a kommunikáló felek cselekedeteit nyomon lehessen követni azért, hogy azokat később – vita esetén – ne lehessen letagadni. A papír alapú szerződéseknél ezt úgy próbálják kiküszöbölni, hogy mindkét fél által követhető módon az aláírás előtt feltüntetik a dátumot a szerződésen, amiből mindkét fél kap egy példányt, és egy későbbi jogvita esetén ez szolgál majd bizonyítékul. A virtuális térben is szükség van egy igazoló irat kiállítására, ami elsődlegesen a cselekedet megállapítására, illetve később ennek igazolására szolgál.

A PKI képezi az elektronikus kereskedelmi rendszerek alapját, azaz ez a háttér-infrastruktúra teszi lehetővé az elektronikus hálózatokon folyó kereskedelmi ügyletek bonyolítását, mind a vállalatok közötti, mind a nyilvános kereskedelmi hálózatok esetében. Tulajdonképpen a PKI szolgáltatásaira épülnek az elektronikus kereskedelmi alkalmazások, és az ezekkel bonyolított üzleti tranzakciók.

5.1.1. A PKI alapelemei

A PKI négy alapelemet tartalmaz a fent bemutatott szolgáltatások nyújtásához. Az alábbiakban ezeket mutatom be:

1. A hitelesítés-szolgáltató

- tanúsítványokat bocsát ki és von vissza;
- a felhasználó rendelkezésére bocsátja az igényelt tanúsítványt;
- a tanúsítványokat és a tanúsítvány visszavonási listákat egy tanúsítvány adatbázisban tartja nyilván.

2. A tanúsítvány adatbázis

- mind a felhasználók, mind az entitások számára lehetővé teszi a tanúsítványok és tanúsítvány visszavonási listák keresését.

3. A felhasználó

- tanúsítványt igényel a hitelesítés-szolgáltatótól;
- a tanúsítványt egy PKI kártyán (intelligens kártya) vagy egy hajlékonylemezen kapja meg;
- kiaknázza a megbízható azonosításból, adattitkosításból és letagadhatatlanságból eredő előnyöket a PKI szolgáltatásait támogató alkalmazásokban használt hitelesített kulcsok és tanúsítványok segítségével;
- tanúsítványokat és állapot információkat kereshet a tanúsítvány adatbázisban.

4. A szolgáltató

- tanúsítványt igényel és kap a hitelesítés-szolgáltatótól;
- PKI alapú szolgáltatásokat nyújt, melyek segítségével kiaknázhatók a megbízható azonosításból, adattitkosításból és letagadhatatlanságból eredő előnyök.

A hitelesítés-szolgáltató szerepe

A hitelesítés-szolgáltató bocsátja ki és vonja vissza a tanúsítványokat. Fő feladatai közé tartozik a hitelesített adatok valódiságának ellenőrzése, és annak vizsgálata, hogy az aláíráshoz használt kulcs és a tanúsítvány visszavonási listák nem kompromittálódtak-e.

A titkos kulcs tárolásához és alkalmazásához használt PKI intelligens kártya megköveteli azt, hogy biztonságos körülmények között kerüljön sor a szállítására a gyártótól a hitelesítés-szolgáltatóig, illetve a hitelesítés-szolgáltatótól a felhasználóig. További követelmény, hogy megbízható gyártónak kell előállítania a kártyát. Kibocsátó hatóságként a hitelesítés-szolgáltatónak kötelessége a tanúsítványkezelési rendszer megbízható kezelése és a tanúsítvány visszavonási listák elérhetőségének biztosítása.

A tanúsítvány adatbázis jelentősége

Az adatbázis feladata a tanúsítványok és a tanúsítvány visszavonási lista adatainak tárolása. Lényeges, hogy ehhez az adatbázishoz hozzáférjenek a felhasználók és az entitások. Ebből az adatbázisból nyerhető ki ugyanis a legfrissebb információ egy adott tanúsítvánnyal kapcsolatban. Akkor is ehhez az adatbázishoz fordulunk, ha egy titkosítani kívánt elektronikus levél címzettjének nyilvános kulcsát keressük.

Annak érdekében, hogy minél több felhasználót és entitást lehessen kiszolgálni, az adatbázis eléréséhez egy általánosan elfogadott interfészt kell biztosítani. Egy ilyen jól ismert interfész az LDAP (Lightweight Directory Access Protocol).

A felhasználó szerepe

A felhasználó általában egy olyan személyt jelent, aki az Interneten keresztül egy számítógép segítségével vesz igénybe olyan szolgáltatásokat, melyek a PKI-re épülnek. Az ilyen szolgáltatások köre a viszonylag új elektronikus banki szolgáltatásoktól a széles körben használt elektronikus levelezésig terjed. A felhasználó a szolgáltatón keresztül veszi igénybe a PKI alapú szolgáltatásokat.

A szolgáltató szerepe

A szolgáltató jelenthet egy banki alkalmazást, egy levelezési szervert vagy bármely más PKI szolgáltatást nyújtó alkalmazást. A szerver általában olyan háttérrendszerrel rendelkezik, amely biztosítja az adatbázishoz való hozzáférést. Az ilyen rendszert szükség szerint tűzfallal védik az illetéktelen behatolásoktól. Amikor a felhasználó kapcsolatba lép a szolgáltatóval, a felek azonosítják magukat. Az azonosítást követően az adatátvitel titkosított formában történik, biztonságossá téve ezzel a két fél között folyó kommunikációt.

5.1.2. A PKI alapszolgáltatásai

Tanúsítványok kibocsátása

A hitelesítés-szolgáltató tanúsítványt bocsát ki a felhasználók és entitások számára. Egy X.509 formátumú tanúsítvány kibocsátásával a hitelesítés-szolgáltató összeköti a hitelesített nyilvános kulcsot a tanúsítvány igénylőjével, s így logikailag a titkos kulcs is ehhez a felhasználóhoz vagy entitáshoz kötődik. Rendkívül fontos, hogy a tanúsítványban rögzített információ pontos legyen, hiszen a hitelesítés-szolgáltató a saját aláírásával ismeri el az információ valódiságát, s ezt egy független harmadik fél felülvizsgálhatja.

A felhasználó vagy entitás a tanúsítványt, illetve a kulcsot azonosításra és aláírásra használhatja. A tanúsítványokat általában meghatározott célra adják ki, például azonosításra, a bizalmasság megteremtésére vagy éppen a letagadhatatlanság biztosítására. A tanúsítvány érvényességi idejét a felhasználás célja határozza meg.

Tanúsítványok visszavonása

A tanúsítványt akkor kell visszavonni, ha elveszett a felhasználó vagy entitás titkos kulcsa, illetve felmerül annak gyanúja, hogy a titkos kulcs kompromittálódott. Ez a folyamat akkor zajlik le, amikor a titkos kulcs tulajdonosa a hitelesítés-szolgáltatóhoz fordul a visszavonás ügyében. A visszavont tanúsítványt a hitelesítés-szolgáltató felveszi a tanúsítvány visszavonási listába, s ezt a listát elérhetővé teszi az érdekeltek számára.

Miután egy tanúsítvány visszavonásra kerül, megszűnik a kapcsolat a volt tulajdonos és a kulcspár között. Természetesen a régi kulccsal létrehozott aláírás érvényben marad, de a visszavonás után ez a kulcs már nem használható hitelesítésre vagy aláírásra.

Akkor is megszűnik a tulajdonos és a kulcspár kapcsolata, amikor a tanúsítvány érvényességi ideje lejár. Ilyenkor mégsem visszavonásról beszélünk, noha a következmények ebben az esetben is hasonlóak, például

az érvényesség lejárta után a kulcsok nem használhatók azonosításra vagy a letagadhatatlanság biztosítására.

Azonosítás és ellenőrzés

Az egyik fél úgy tudja társát azonosítani, hogy kérést intéz hozzá, melyre választ vár. A választ a kérdezett fél a saját titkos kulcsával rejtjelezi, melyet a kérdező fél a kérdezett fél nyilvános kulcsával tud visszafejteni. Az azonosítás akkor sikeres, ha a megkérdezett fél nyilvános kulcsával valóban visszafejthető a válasz.

A folyamat természetesen a másik fél részéről is lezajlik. A gyakorlatban ez a felhasználó mint kliens és az entitás mint szerver között megy végbe, például egy banki tranzakció keretében.

Mindkét félnek rendelkeznie kell a tanúsítványokat kibocsátó hitelesítés-szolgáltató által használt titkos kulcs nyilvános párjával, s meg kell bízniuk a hitelesítés-szolgáltatóban. Ez a bizalom képezi a PKI alapját, ugyanis ennek megléte nélkül nem lehetne megvalósítani egy megbízható rendszert. Másképpen megfogalmazva a problémát: nem lehet megbízni egy tanúsítványban anélkül, hogy tudnánk, azt egy megbízható hitelesítés-szolgáltató bocsátotta ki.

Letagadhatatlanság és ellenőrzés

A letagadhatatlanságot az elektronikus aláírás segítségével lehet biztosítani. Az elektronikus aláírás úgy jön létre, hogy a letagadhatatlanság biztosítására kibocsátott titkos kulccsal titkosítjuk az aláírni kívánt adatot. Nyilvánvaló, hogy más alkalmazásoknál más célra kibocsátott kulcsot kell használni. A titkosított adat egyszerű szöveg, illetve hash algoritmussal készített lenyomat is lehet.

Az ellenőrző fél hasonló módszerrel győződik meg az aláírás hitelességéről. Az eljárás biztosítja a letagadhatatlanságot, mivel a fogadó fél képes a tanúsítvány érvényességi állapotának ellenőrzésére. A hosszú távú védelemhez szükség van egy általánosan elfogadott időbélyegző

szolgáltatásra, ezen kívül az időbélyegzőnek tartalmaznia kell az aláírt adat egy részét is a későbbi ellenőrzés miatt.

A letagadhatatlanság fontos szerepet játszik az elektronikus kereskedelmi rendszerekben, amikor például üzleti megállapodásokról vagy banki tranzakciókról van szó. Érdemes megjegyezni, hogy míg a kézírásos aláírás egyszerűen lemásolható, addig a megfelelően védett titkos kulcs szinte lehetetlenné teszi az elektronikus aláírás másolását.

5.1.3. Intelligens kártya alapú kulcstárolás

Tekintettel arra, hogy a PKI a nyilvános-titkos kulcspáron és a két kulcs között kapcsolatot teremtő algoritmuson alapul, egy fontos kérdést mindenképpen figyelembe kell venni. Ez pedig nem más, mint a titkos kulcs védelme a kompromittálódás ellen.

Az elektronikus kereskedelem színterét jelentő nyílt hálózatok nem tekinthetők biztonságosnak, védelmük pedig költséges és nehezítheti a hálózat használatát. Ennek tudatában az azonosításhoz, aláíráshoz és banki tranzakciókhoz használt titkos kulcsunkat a legjobb helyen akkor tudhatjuk, ha intelligens kártyát használunk.

A PKI rendszerek biztonsági szolgáltatásai a felhasználó egyedi titkos kulcsára épülnek. Ezt a titkos kulcsot nem ismerheti senki, még a felhasználó sem. Az ún. PKI kártya, amely egy RSA titkosítást végző kriptoprocesszorral felszerelt intelligens kártya, lehetővé teszi a kulcs használatát oly módon, hogy az ne kerüljön nyilvánosságra. A kulcsot egyszer kell letárolni a kártyába, ezt követően a kártya operációs rendszere gondoskodik a kulcs biztonságáról.

A tárolás után a kulcsot nem lehet kiolvasni, kitörölni vagy megváltoztatni, erre még a felhasználó sem képes. A felhasználó egy PIN kóddal férhet hozzá a kártya szolgáltatásaihoz. A PKI kártyák azért előnyösek, mert

használatuk könnyű, hordozhatóságuk megkérdőjelezhetetlen és sokféle alkalmazással képesek együttműködni. Ilyen alkalmazások például az internetes pénzügyi rendszerek, a biztonságos levelezés, a biztonságos webes szolgáltatások és a virtuális magánhálózatok használata.

Természetesen az intelligens kártyák sem egyformák. Vannak olyanok, amelyek nem támogatják az RSA algoritmust, vagy ha támogatják, a processzoruk teljesítménye nem megfelelő. Sok olyan megoldás létezik, amely egyszerű tárolóeszközzé fokozza le az intelligens kártyát. A felhasználók biztonsága érdekében ezen a téren is kívánatos lenne a technológiák egységesítése, illetve a kártyákra vonatkozó szabványok kidolgozása.

5.2. Nyilvános kulcsú infrastruktúra a NetLock Kft-nél

5.2.1. Néhány szó a NetLock Kft-ről

A NetLock Hálózatbiztonsági Kft. – szakdolgozatom írásának idején – Magyarország egyetlen PKI szolgáltatásokat nyújtó hitelesítés-szolgáltatója.

Az egyetlen hazai hitelesítés-szolgáltatóként fontos szerepet játszik a PKI működtetésében kulcsfontosságú tanúsítványkezelési eljárási rendek meghonosításában és a hazai jogi és kulturális környezetbe való adaptációjában.

A NetLock a szükséges eljárások bevezetése és felügyelete mellett az infrastruktúra technológiai fejlesztését és működtetését is feladatának tartja. A hitelesítés-szolgáltatói tevékenység mellett foglalkozik a tanúsítványok biztonságos kommunikációban való felhasználását lehetővé tevő titkosító eszközök telepítésével és folyamatos támogatásával, teljes, kulcsrakész rendszerek fejlesztésével, azok intelligens kártyákkal való kiegészítésével.

5.2.2. Tanúsítványok kezelése a NetLock Kft-nél

A NetLock által kibocsátott tanúsítványok megfelelnek a CCITT X.509v3 szabvány előírásainak. A szabvány alapján az alábbi mezők szerepelnek a tanúsítványban:

Alapmezők (Basic Certificate Fields):

Verzió (Version)

Sorozatszám (Serial number)

Aláírási algoritmus (Signature Algorithm ID)

Kiállító (Issuer Name)

Érvényesség (Validity)

Tulajdonos (Subject Name)

CN – Common Name (név)

E – E-mail (e-mail cím)

L – Locality (város)

C – Country (országkód)

O – Organization (szervezet)

OU – Organizational Unit (szervezeti egység)

Nyilvános kulcs (Public Key Information)

A kibocsátó elektronikus aláírása (Digital Signature)

Szabványos kiegészítő mezők (Standard Extensions):

Alapvető megkötések (Basic Constraints)

Kiadási feltételek (Certificate Policies)

Egyéb kiegészítő mezők (Private Extensions):

```
-----BEGIN CERTIFICATE-----
MIIDBzCCAnACAQAwczELMAkGA1UEBhMCSFUxCTAHBgNVBAgTADERMA8GA1UEBxMI
QnVkYXBlc3QxIzAhBgNVBAMeGgBWAOEAcgBuAGEAaQAgAFIA8wBiAGUAcgB0MSEw
BQADgY0AMIGJAoGBAK5Yz0XD5sDMtQ+dp0YOhUi2AezjzfMGwkDhQuBsUwxlOR8h
VtANKzPwGOsuNH10IMAD/V9lLDf09oCR1wOoLNzhg5YxzLcGaYgv0Swyd64Kcd0l
sIT7R4sSCRuSs2ghzJ1CnrCKDNTUHzvAPttWibIr/Zi+oC92huiZJUuiwUmlAgMB
AAGgggFSMB8GCisGAQQBgjcNAgMxERYPNC4xMC42Nzc2NjQ0Ni4xMDUGCisGAQQB
gjcCAQ4xJzAlMA4GA1UdDwEB/wQEAwIB8DATBgNVHSUEDDAKBggrBgEFBQcDAjCB
9wYKKwYBBAGCNw0CAjGB6DCB5QIBAR5UAE0AaQBjAHIAbwBzAG8AZgB0ACAAQgBh
AHMAZQAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABl
AHIAIAB2ADEALgAwA4GJACrHDhAGvqfN9fpmD4ajikFYx69u9cGSPfVWqIFILol8
BDZT42R5FjR96LCu1zzF63olLfK45PTyzZUL3U8KnycZtfZSFncBLPaumtN/v2oi
kWvz25MNHNIAtbgUHD6elHupjsaE9Sv6tZUApZWyZYwxGXcAzVtOkmjkQmYXtdST
AAAAAAAAAAAwDQYJKoZIhvcNAQEEBQADgYEAGLAK/tfmCwJuYoVQQ7DJRh7PifkS
Vrr1L7LoIxEdiiGNX1L61ALA+Cmhf9mp5IAUgWZxP7IFuRppx3FeSAXAUQPd6UAq
LuM44RAYhxqVkiRrBGVyaqbaM7h+vfSCrlCTmMl38u4on1V+tDQx3GtHUyYnHumm
VVA2eHO/56gKqlU=
-----END CERTIFICATE-----
```

7. sz. ábra. **Példa egy tanúsítványra**

5.2.2.1. Tanúsítványok osztályai és tulajdonságaik

A NetLock az alábbi osztályú tanúsítványokat kezeli.

Teszt osztályú tanúsítványok
A teszt tanúsítvány a hálózatbiztonsági szolgáltatások tesztelési céljaira kiadott tanúsítvány.

A teszt szinten a hitelesítés-szolgáltató nem nyújt, és nem vesz igénybe entitás-azonosító szolgáltatásokat. A teszt tanúsítvány kiadásának feltétele a beérkezett tanúsítványkérelem és a tanúsítványkiadás folyamán a kommunikációban használt elektronikus levelezési cím. A teszt tanúsítvány csak ezen elektronikus cím létezését bizonyítja az érintett felek számára; a tanúsítvány többi mezőjében található információt a hitelesítés-szolgáltató nem ellenőrzi.

„C" osztályú tanúsítványok
A „C" osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát korlátozott, részben emberi beavatkozással történt ellenőrzési lépéseken keresztül azonosította a hitelesítés-szolgáltató. Használata elektronikus levelezéshez, kisebb kockázatú tranzakciókhoz, internetes szolgáltatások igénybevételéhez, szoftver forrásának ellenőrzéséhez ajánlott.

„B" osztályú tanúsítványok
A „B" osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát szigorú ellenőrzési lépések során azonosította a hitelesítés-szolgáltató. Használata a fentieken túl közepes kockázatú tranzakciókhoz ajánlott.

„A" osztályú tanúsítványok
Az „A" osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát szigorú ellenőrzési lépések során azonosította a hitelesítés-szolgáltató. Használata nagy értékű

tranzakcióknál, pénzügyi utasítások és információk ellenőrzésénél, szerződéskötéseknél ajánlott.

5.2.2.2. Tanúsítványtípusok

Az „A”, „B” és „C” osztályokban a következő típusú tanúsítványok kiadását végzi a NetLock.

Személyes aláíró és titkosító tanúsítványok
Személyes tanúsítványokat természetes személy igényelhet a saját nevében.

A személyes tanúsítványok Country (C) és Locality (L) mezőjében az igénylő lakóhelyének országkódja és városa, az Organization (O) és Organization Unit (OU) mezőkben semmi, a Common Name (CN) mezőjében az igénylő neve és (opcionálisan) elektronikus levelezési címe szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat a kiegészítő mezőkben.

Meghatalmazásos aláíró és titkosító tanúsítványok
Meghatalmazásos (névjegykártyás) tanúsítványokat természetes személy igényelhet egy adott szervezet tagjaként. A szervezet – többek között – lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány. A tanúsítványban szerepel a személy szervezetben betöltött funkciója is.

A névjegykártyás tanúsítványok a személyes tanúsítványokhoz hasonlóan épülnek fel, de az ilyen tanúsítványok Country és Locality mezőjében az igénylő szervezete telephelyének országkódja és városa, az Organization mezőben szervezetének neve, az Organizational Unit mezőben funkciója szerepel. A Common Name mező a személyes tanúsítványnál már említett adatokat tartalmazza, azaz az igénylő nevét és (opcionálisan) elektronikus levelezési címét. A névjegykártyás tanúsítványokra is igaz, hogy a kiegészítő mezőkben egyéb ellenőrzött adatokat is lehet tárolni.

Szervezet aláíró és titkosító tanúsítványok

Szervezet tanúsítványokat szervezet vagy annak szervezeti egysége igényelhet saját nevében. A szervezet lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület vagy alapítvány.

A szervezet tanúsítványok mezőinek tartalma néhány eltéréssel mindenben megegyezik a névjegykártyás tanúsítványoknál említettekkel. Annyi a különbség, hogy az Organizational Unit mezőben a szervezeti egység neve, a Common Name mezőben pedig az Organization és az Organizational Unit mezők tartalma és opcionálisan a szervezeti egység e-mail címe szerepel.

Szerver tanúsítvány

Szerver tanúsítványt Internet címmel (ún. host névvel) rendelkező, szervert üzemeltető természetes személy vagy szervezet igényelhet.

A mezők tartalma:
Country és *Locality* mező: az üzemeltető székhelyének vagy lakóhelyének országkódja és városa
Organization mező: az üzemeltető neve
Organizational Unit mező: az üzemeltető szervezeti egység neve
Common Name mező: a szerver internetes elnevezése (ún. host neve)
Kiegészítő mezők: egyéb ellenőrzött adatok

WAP Gateway tanúsítvány

WAP Gateway tanúsítványt WAP Gateway eszközt üzemeltető természetes személy vagy szervezet igényelhet.

A WAP Gateway tanúsítvány mezőinek tartalma megegyezik a szerver tanúsítványoknál leírtakkal.

VPN tanúsítvány

VPN tanúsítványt VPN eszközt üzemeltető természetes személy vagy szervezet igényelhet.

A VPN tanúsítvány felépítése sem különbözik a szerver és WAP tanúsítványoknál tapasztaltaktól.

Láncolt hitelesítés-szolgáltató tanúsítvány
Egy adott szervezet számára, a szervezet alkalmazottai számára történő tanúsítvány-kibocsátást lehetővé tevő tanúsítvány.

A láncolt tanúsítvány Country és Locality mezőjében a szervezet székhelyének országkódja és városa, az Organization mezőben a szervezet neve, az Organizational Unit mezőben az üzemeltető szervezeti egység neve, a Common Name mezőben a hitelesítés-szolgáltató neve szerepel. Természetesen ebben az esetben is igaz, hogy a kiegészítő mezők egyéb ellenőrzött adatokat is tartalmazhatnak.

5.2.2.3. Tanúsítványok igénylése és kibocsátása

A NetLock szabályzata szerint tanúsítványt természetes személyek, szervezetek, web szerverek, valamint WAP Gateway és VPN eszközök tulajdonosai, üzemeltetői igényelhetnek. Az említett igénylőket összefoglaló néven entitásoknak nevezi a NetLock.

Az entitások adatait regisztrációs adatbázisban tartják nyilván, az adatszolgáltatás azonban önkéntes. Az igénylő kérésére a hitelesítés-szolgáltató törli az adatait az adatbázisból, ezzel egyidejűleg a kibocsátott tanúsítványok is érvényüket vesztik.

A tanúsítvány igényléséhez szükséges nyilvános-titkos kulcspárt az entitásnak kell létrehozni. A kulcspár létrehozása szoftver segítségével vagy biztonságos hardvereszközzel történhet. Az eszközök kiválasztása és használata a tanúsítványigénylő kizárólagos feladata és felelőssége.

A NetLock ajánlásokat fogalmaz meg a titkos kulcs védelmével kapcsolatban, melyben felhívja a figyelmet a jelszavas védelem gyengeségeire és az intelligens kártyák előnyeire.

A szolgáltató csak akkor fogadja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:

- az igénylő benyújtotta kérelmét a hitelesítés-szolgáltatónak,
- az entitás (akinek nevében az igénylő eljár) azonos a kérelemben szereplő alannyal,
- az igénylő jogosult a kérelemben szereplő alany nevében kérelmet benyújtani,
- az igénylő birtokában van a kérelemben szereplő nyilvános kulcs titkos párja,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak, kivéve a tájékoztató jellegű adatokat.

Teszt tanúsítvány kiadására irányuló kérelmek elfogadása

Teszt tanúsítványok kiadásához az igénylőnek érvényes elektronikus levelezési címmel kell rendelkeznie. A NetLock Teszt Hitelesítési Egység automatizált lépéseken keresztül biztosítja a teszt tanúsítvány kiadását. A lépések során a szolgáltató a megadott elektronikus levelezési címre továbbít utasításokat, és erről a levelezési címről várja a tanúsítvány kiadására vonatkozó kérelem megerősítését.

A teszt tanúsítvány kiadására irányuló kérelem akkor elfogadott, ha az elektronikus levelezési címmel az előírt kommunikáció lefolytatható.

A, B és C osztályú tanúsítvány kiadására irányuló kérelmek elfogadása

A szolgáltató akkor fogadja el a tanúsítvány kiadására irányuló kérelmet, ha az igényelt tanúsítvány osztályának és típusának megfelelő ellenőrzési lépések végrehajthatók és eredményesen befejeződtek.

Az „A” osztályú tanúsítványok esetében ez azt jelenti, hogy az adatokat közjegyzői dokumentumokkal és nyilatkozatokkal alátámasztva kell igazolni. A „B” osztályú tanúsítványok kiadásánál elegendő az, hogy a hitelesítés-szolgáltató a bemutatott dokumentumok és iratok alapján fogadja el az adatok hitelességét. A „C” osztályú tanúsítvány esetében pedig a nyilvános adatbázisokban elérhető adatokra támaszkodva ellenőrizhető az entitás által megadott adatok valódisága.

Ha az ellenőrzés hiányosságokat állapít meg, a szolgáltató elutasítja a tanúsítványkérelmet. Erről írásban értesíti az igénylőt és közli vele az elutasítás okát.

A kibocsátott tanúsítványokat a szolgáltató a honlapján elérhető publikus adatbázisban tartja nyilván, ugyanitt szerepelnek a visszavont tanúsítványok listái is.

A tanúsítvány attól az időponttól válik érvényessé, amikor a szolgáltató az általa aláírt tanúsítványt közzéteszi a fent említett adatbázisban.

A tanúsítványban szereplő nyilvános kulcs párja csak a tanúsítványban megjelölt időintervallumban használható elektronikus aláírások készítésére. A felhasználó felelős a tanúsítvány érvényességének ellenőrzéséért.

A tanúsítvány elfogadásakor, ami akkor történik meg, amikor a felhasználó belép a szolgáltató adatbázisába a tanúsítvány letöltése céljából, a tanúsítvány használója nyilatkozatot tesz többek között arról, hogy

- a szolgáltatóval közölt adatai megfelelnek a valóságnak, és azok az ő beleegyezésével kerültek bele a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről értesíti a szolgáltatót,
- titkos kulcsát megvédi a jogosulatlan hozzáféréstől,
- ismeri az elektronikus aláírás használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,

- minden egyes elektronikus aláírást, amely a tanúsítványban szereplő nyilvános kulcs párjával készült, a saját elektronikus aláírásának ismer el,
- tisztában van azzal, hogy a kulcs védelme és az elektronikus aláírás készítése kizárólag az ő felelőssége, s ezzel kapcsolatban a szolgáltatót semmiféle felelősség nem terheli,
- felhatalmazza a szolgáltatót a tanúsítvány nyilvánosságra hozatalára, és nyilvános tanúsítványgyűjtő helyeken történő elhelyezésére.

5.2.2.4. A tanúsítványok használata

Az aláíró tanúsítványok üzenetek integritásának ellenőrzésére, a titkosító tanúsítványok üzenetek titkosítására használhatók. Az elektronikus aláírás ellenőrzésével lehet meggyőződni arról, hogy az elektronikus aláírás a tanúsítványban szereplő nyilvános kulcs titkos párjával készült, és az aláírt üzenet nem változott meg az elektronikus aláírás elkészülte óta.

Az elektronikus aláírás létrehozása

Azért a folyamatért, amelynek végén az elektronikusan aláírt dokumentum megszületik, elsősorban az aláíró a felelős. Ő birtokolja a titkos kulcsot, ő az, akinek ismernie kell az aláírandó üzenet tartalmát, ő dönt az aláírási szándékról és általában ő az, aki az aláírást létrehozó technikai eszközt üzemelteti.

A NetLock az alábbi lépéseket határozta meg az elektronikus aláírás készítéséhez.

1. A titkos kulcs megőrzése

Az elektronikus aláírás csak akkor biztonságos, ha a titkos kulcs az előfizetőn kívül soha, senki más számára nem hozzáférhető. A kulcsot jelszavas vagy hardver védelemmel kell ellátni. A kulcsot idegen gépre átvinni védelem nélkül nem szabad. A kulcs elvesztéséből, véletlen vagy

szándékos nyilvánosságra hozatalából eredő károkért az előfizető felelős. A kulcs kompromittálódását a szolgáltatónak jelenteni kell.

2. Az aláírandó dokumentum tartalmának ellenőrzése

Míg hagyományos aláírásnál általában könnyen, addig számítógépes környezetben nem mindig egyszerűen tisztázható az aláírónak az aláírt dokumentumra vonatkozó aláírási szándéka.

Az egyszerűbben, észrevétlenebbül készíthető elektronikus aláírás alkalmazásának kockázata csökkenthető azzal, ha az aláíró csak a számára biztonságosnak tartott számítógépes környezetben, ismert és elfogadott elektronikus aláíró eszközöket használ. Ezen eszközök akkor alkalmasak feladatuk ellátására, ha az aláírás előtt biztonságosan megállapítható, hogy pontosan milyen üzenetre fog rákerülni az elektronikus aláírás.

Az aláírt dokumentum tartalmával kapcsolatos felelősségek elsősorban az aláírót terhelik. Amennyiben azonban nyilvánvalóan tévesen aláírt dokumentumról van szó, amit az érintett fél felismerhet, akkor az érintett felet is felelősség terheli.

3. Az elektronikus aláírás végrehajtása

Az aláírási folyamat során felmerülhetnek technikai hibák (pl. az aláíró szoftver hibás aláírást készít vagy megváltoztatja a dokumentum tartalmát aláírás előtt). Az elektronikus aláírás létrehozásakor csak olyan elektronikus aláíró eszközt szabad használni, amelyben az aláíró megbízik. Az aláíró döntési körébe tartozik a megfelelő aláíró berendezés kiválasztása és használata, ezért az aláírás hibátlan végrehajtásáért ő a felelős.

Az elektronikus aláírás ellenőrzése

Az elektronikus aláírás elfogadója csak akkor számíthat az elektronikus dokumentum jogi hatására és az azon alapuló előnyökre, ha az elektronikus aláírás elfogadásakor a törvényi előírások szerint jár el. Ezen lépésekről az

elektronikus aláírás készítőjének tájékoztatnia kell az érintett felet, de legalább utalást kell tennie a leírt követendő lépésekre. Az elektronikus aláírás ellenőrzésének a következő lépésekből kell állnia:

1. Tanúsítványláncok kialakítása és a megfelelő lánc kiválasztása

Az elektronikus aláírás ellenőrzéséhez a felhasználandó tanúsítványokat hitelesítéseik alapján láncba kell rendezni. Meg kell győződni arról, hogy a tanúsítványláncok közül a legmegfelelőbbet választjuk ki az elektronikus aláírás ellenőrzéséhez. Ha egy tanúsítvány ellenőrzésénél több tanúsítványlánc is található, amelyeken keresztül egy elfogadható gyökér tanúsítványhoz lehet jutni, akkor azt a láncot kell választani, amely a legmagasabb megbízhatósági szintű hitelesítés-szolgáltató tanúsítványánál ér véget.

2. Az üzenet aláírási időpontjának ellenőrzése

Az elektronikus aláírás ellenőrzéséhez meg kell állapítani az üzenet aláírásának időpontját. Csak az az elektronikus aláírás érvényes, amely a hozzá tartozó tanúsítvány érvényességi ideje alatt készült. Az időpont meghatározása az érintett fél felelőssége, legjobb módszer egy megbízható harmadik fél által kiadott időbélyegző alkalmazása, melynek érvényességét az elektronikus aláíráséhoz hasonlóan ellenőrizni kell.

3. A tanúsítványlánc tagjainak ellenőrzése a szolgáltató adatbázisa alapján

Az érintett félnek meg kell győződnie arról, hogy a láncban szereplő tanúsítványok mindegyike érvényes volt az aláírás időpontjában, azaz a bennük jelölt érvényességi időintervallumban történt az aláírás, és nem szerepelnek valamely visszavonási listán. A láncban szereplő egyes tanúsítványok ellenőrzéséhez célszerű a megfelelő hitelesítés-szolgáltató visszavonási listáját használni.

4. Az aláíró kulcs használatára vonatkozó korlátozások ellenőrzése

A hitelesítés-szolgáltató korlátozhatja az általa kiadott tanúsítványhoz tartozó titkos kulcs felhasználási körét. Az ilyen korlátozásokról, vagyis arról, hogy

mely esetekben nem tekinthető a kiadott tanúsítvány megbízhatónak, a tanúsítványban találhatunk információkat. Az elektronikus aláírást ellenőrző személynek meg kell győződnie arról, hogy a tanúsítványláncolatban nincs egyetlen olyan tanúsítvány sem, amely – az adott esetben – korlátozná a végfelhasználó elektronikus aláírását.

5. Az elektronikusan aláírt adatok pontos kiválasztása az üzenetből

Az elektronikus aláírás technikai ellenőrzéséhez pontosan kell tudni, mi az az üzenet, adat, amit aláírtak.

6. Az aláíró feltételezett vagy jelzett szándéka szerinti értelmezés meghatározása

Csak olyan elektronikus dokumentumtól várható jogi hatás, amelyen szereplő elektronikus aláírás elfogadásakor jóhiszeműen járt el az érintett fél.

Amennyiben a körülmények további ellenőrzési lépéseket tesznek szükségessé, az érintett fél a tőle elvárható legnagyobb gondossággal köteles ezeket végrehajtani. Az elektronikus aláírás elfogadója a körülmények mérlegelésekor – többek között – köteles figyelembe venni a tanúsítvány osztályát is.

7. Az aláírási jogosultság ellenőrzése

Elképzelhető, hogy az aláírt dokumentumon szereplő elektronikus aláírás minden technikai követelménynek megfelel: az üzenethez tartozik, érvényes, a hitelesítő tanúsítványlánc hibátlan, de az aláíró személynek nem volt joga, felhatalmazása az adott dokumentumot aláírni. Ugyanez a helyzet lehetséges a hagyományos aláírásnál is: az aláírás nem hamis, de az aláírónak nem volt joga az aláíráshoz. Az aláírási jogosultság ellenőrzése az aláírást elfogadó feladata.

8. Az elektronikus aláírás és az aláírt üzenet összetartozásának ellenőrzése

A tanúsítványban szereplő nyilvános kulcs és egy, az érintett fél által megbízhatónak tartott technikai eszköz (hardver, szoftver) segítségével

végre kell hajtani azon matematikai műveleteket, melyek során kiderül, hogy az aláírt üzenetrész és elektronikus aláírása összetartoznak-e.

5.2.2.5. A tanúsítványok visszavonása

A tanúsítványok visszavonásra kerülnek, ha kétely merül fel a kibocsátásuk feltételeinek teljesülésével kapcsolatban és a kétely alapja bizonyítható. A visszavonás oka lehet például

- a tanúsítványhoz tartozó titkos kulcs biztonságának sérülése,
- hibás vagy megváltozott adatokat tartalmazó tanúsítvány,
- a tanúsítvány alanyának visszavonási kérelme.

A visszavonást kérelmezni kell a szolgáltatónál, amely a visszavonási jogosultság és az indokok ellenőrzése után visszavonja a tanúsítványt. Általában a visszavonandó tanúsítvány biztonsági szintjének megfelelő ellenőrzést hajtják végre a visszavonáskor is.

A szolgáltató saját tanúsítványának visszavonása

Szélsőséges esetben előfordulhat, hogy magának a szolgáltatónak a tanúsítványát kell visszavonni. Ez esetben a szolgáltató tanúsítványa érvényét veszti, azonban ez nem befolyásolja automatikusan a szolgáltató által a visszavonást megelőzően kiadott tanúsítványok érvényességét.

Visszavonás hibás kibocsátás esetén

A szolgáltató visszavonja azokat a tanúsítványokat, melyekről kiderül, hogy nem az aktuális szabályzatokban, dokumentumokban leírt eljárási rend alapján vagy egyéb módon hibásan adták ki azokat.

Visszavonás az igénylő kérésére

A szolgáltató visszavonja azon tanúsítványokat, melyek visszavonását a tanúsítvány alanya vagy annak meghatalmazottja kéri. Ilyenkor a szolgáltató nem vizsgálja a visszavonás indokát.

A visszavont tanúsítványok listája

A visszavont tanúsítványok azonosítói a visszavont tanúsítványok listájára kerülnek. A listát a szolgáltató rendszeresen frissíti. A lista a visszavont tanúsítványok tárgy és sorszám mezőit, illetve a visszavonás okának kódját tartalmazza, mindezt a szolgáltató elektronikus aláírása hitelesíti.

A felfüggesztés és visszavonás következménye

A tanúsítvány érvényessége szünetel a felfüggesztés időtartama alatt, illetve a visszavonás pillanatától végérvényesen megszűnik. A szolgáltató tanúsítványának visszavonásakor a szolgáltató tanúsítvány aláírási joga is megszűnik, de ez nem érinti automatikusan a visszavonás előtt kibocsátott tanúsítványok érvényességét.

A titkos kulcs védelme visszavonás esetén

A titkos kulcs védelméről a felhasználó a tanúsítvány visszavonása után is köteles gondoskodni. A felhasználónak joga van a visszavont tanúsítványhoz tartozó titkos kulcs megsemmisítésére.

5.2.2.6. A tanúsítványok lejárata

Előzetes értesítés a tanúsítvány lejártáról

A lejáró tanúsítványokról annak felhasználója részére 30 nappal a lejárat előtt, elektronikus formában értesítést küld a szolgáltató.

A tanúsítvány lejártának következményei

A lejárt tanúsítvány érvénytelen. A lejárattal nem vesznek el azon kötelezettségek, melyek a tanúsítvány kérelmével, kibocsátásával, elfogadásával és használatával kapcsolatosak.

A tanúsítványok megújítása

A lejárt tanúsítvány kérelemmel megújítható. A kérelemhez csak a megváltozott adatokat kell csatolni, az igényelt tanúsítvány típusának és

osztályának megfelelő módon. Az új kérelemhez tartozó nyilatkozat aláírása után a szolgáltató új tanúsítványt állít ki az alany új kulcspárjához.

5.3. Észrevételek, javaslatok

A NetLock Kft. tanúsítvány-kibocsátási tevékenységének elemzése közben tulajdonképpen megerősödött bennem az a feltételezés, mely szerint a nyilvános kulcsú infrastruktúra leggyengébb eleme éppen maga a felhasználó, akitől elvárjuk, hogy megbízzon a szolgáltatóban.

A virtuális térben sem maradhat figyelmen kívül az emberi tényező. Hiába alkották meg a valós világban alkalmazott biztonsági tényezők (tanúk előtti aláírás, bélyegző, keltezés stb.) hasonmását (elektronikus aláírás, időbélyegző stb.) a virtuális térben is, ha a biztonság alapját képező titkos kulcs védelme a felhasználóra van bízva.

Érdemes megfigyelni, hogy a hitelesítés-szolgáltató, tudatában annak, hogy a felhasználó által elkövetett hibákért nem vállalhat felelősséget, a felhasználóra ruházza a kulcs létrehozásával és védelmével kapcsolatos feladatokat, kockáztatva ezzel a kibocsátott tanúsítvány hitelességét.

Véleményem szerint aggodalomra ad okot az, hogy a titkos kulcs védelmére egyes esetekben jelszavas védelmet alkalmaznak. Ez nem tekinthető megbízhatónak, még akkor sem, ha a szolgáltató előírásokat fogalmaz meg a jelszó megválasztásával kapcsolatban. Mindannyian hallottunk már olyan esetről, amikor a felhasználó a számítógépe monitorára ragasztott cetlin tartotta nyilván jelszavát, attól tartva, hogy esetleg elfelejti azt. Ennek természetesen egy ingyenes e-mail szolgáltatás igénybevételekor nincs nagy jelentősége, de az elektronikus aláírás használatakor gondolni kell annak jogi következményeire is.

Jelenleg az önálló memóriával, processzorral és operációs rendszerrel rendelkező intelligens kártya tűnik a legbiztonságosabb megoldásnak a titkos

kulcs tárolására. Az intelligens kártya használatával megelőzhető a titkos kulcs illetéktelen felhasználása, azaz a kulcs kompromittálódása. Ez nyilvánvalóan többletkiadással jár, hiszen a jelszavas védelemmel ellentétben, az intelligens kártyák használatához speciális hardvereszközökre is szükség van. A beruházás azonban megtérül, mivel olyan univerzális eszköz áll a felhasználó rendelkezésére, mellyel – ha a fényképét is tárolja a kártyán – mind a valós életben, mind a virtuális térben tudja magát igazolni.

Az elektronikus aláírás szabványosításához hasonlóan az intelligens kártyák területén is szükséges lenne a szabványos technológiák használata ahhoz, hogy a felhasználók szemében megbízhatóvá váljanak, és széles körben elterjedjenek.

A hitelesítés-szolgáltatók tevékenységével szembeni bizalom – nézetem szerint – akkor erősödhet meg, ha a felhasználókkal megismertetik a tanúsítványkezelés folyamatát. Nem tartom célravezetőnek azt a megoldást, hogy a felhasználóra hárul a hitelesítés alapját képező titkos kulcs védelme, hiszen ennek láttán a felhasználó jogosan gondolhatja: „ha éppen a legfontosabb tényező védelmét bízza rám a szolgáltató, akkor vajon mennyire bízhatok meg benne és az általa hitelesített partnereimben?”.

VI. EGY BIZTONSÁGOS HITELESÍTÉS-SZOLGÁLTATÓ FELÉPÍTÉSE

A NetLock Kft-ről szerzett, az előző részben ismertetett tapasztalataim alapján, *önálló munka keretében* az alábbiakban bemutatom egy általam biztonságosnak tekintett hitelesítés-szolgáltató felépítését és megbízható működésének feltételeit.

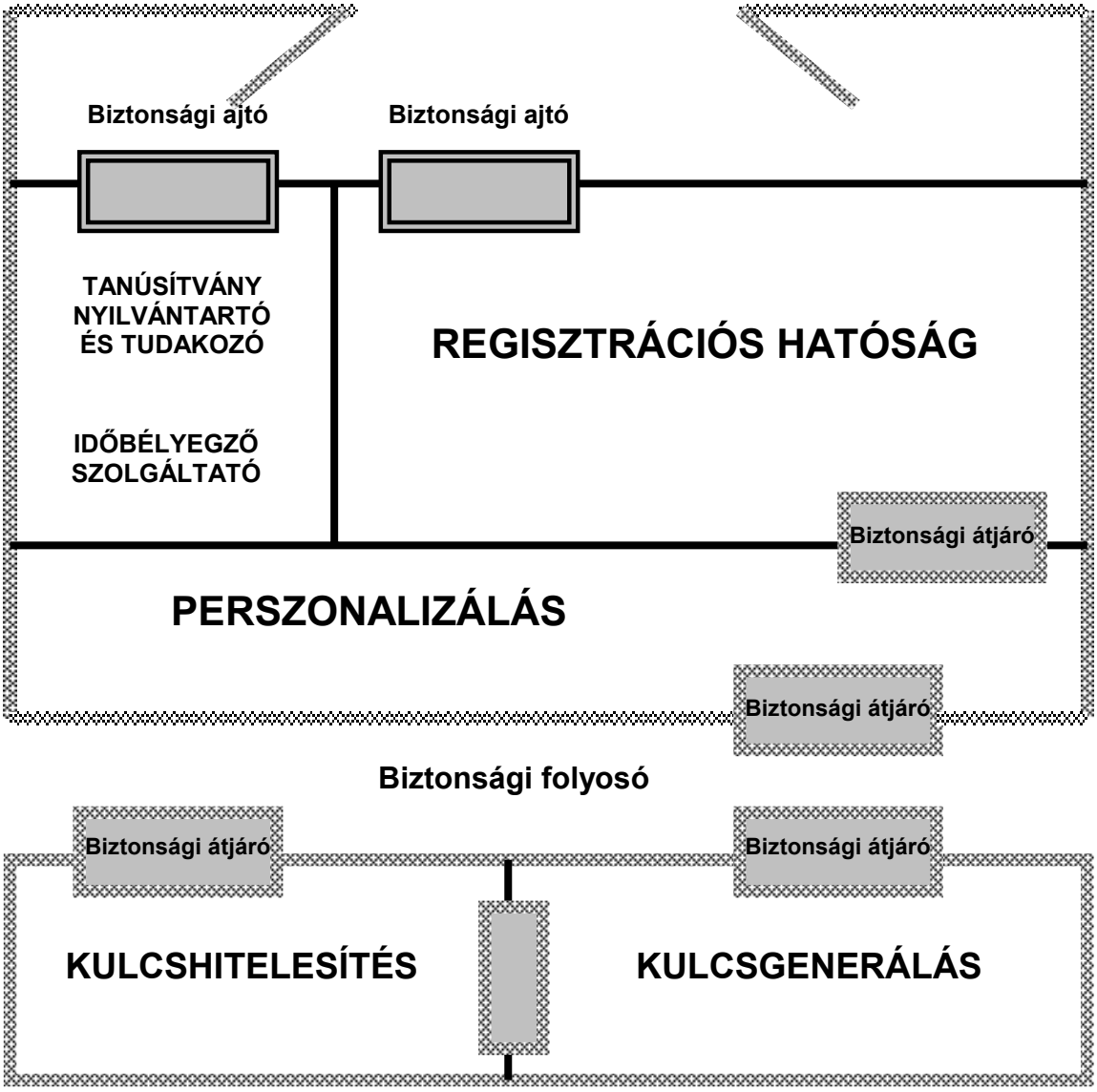
6.1. A hitelesítés-szolgáltató felépítése

A hitelesítés szolgáltatás során törekedni kell a tökéletes biztonság megteremtésére, csak így lehet biztosítani a tanúsítványok hitelességét. Ennek szellemében szigorúan el kell különíteni az egyes funkcionális egységeket az 5. ábra szerint.

6.1.1. A regisztrációs hatóság

A regisztrációs hatóság feladata a tanúsítványigénylések feldolgozása. A regisztráció során felveszik az ügyfél adatait és a személyazonosító okmányok alapján ellenőrzik azokat. Az ellenőrzés módja az igényelt tanúsítvány szintjétől függ. Minősített tanúsítvány esetén szükség lehet közjegyzői hitelesítésre vagy tanúk általi megerősítésre is.

Természetesen számolni kell azzal, hogy illetéktelenek mások nevében, hamis személyazonossággal igényelnek tanúsítványt, esetleg erőszakkal akarják elérni céljukat. Ennek megelőzésére a bankokban már megszokott biztonsági intézkedéseket kell bevezetni a regisztrációs hatóságnak helyet adó épületben. Fegyveres őröket kell alkalmazni, a biztonsági ajtót pedig úgy kell kialakítani, hogy zsilipszerűen működjön, azaz korlátozott számban engedje be az ügyfeleket, és közben ellenőrző funkciót is ellásson (pl. fémkeresővel felszerelve).



***8. sz. ábra.* A biztonságos hitelesítés-szolgáltató felépítése**

Forrás: Dr. Tuzson Tibor: Secure Electronic Business c. tanfolyam fóliakészlete

6.1.2. Kulcsgenerálás

A kulcsgenerálást nem kell feltétlenül a felhasználóra bízni, ezt egy külön részlegben maga a hitelesítés-szolgáltató is elvégezheti. Természetesen erre a tevékenységre vonatkozóan is rendkívül szigorú biztonsági intézkedéseket kell hozni.

A kulcsgenerálást a regisztrációtól hermetikusan elkülönítve kell végezni. Az egész folyamat személytelenül történik, a generált nyilvános kulcs ekkor még

nincs hozzákapcsolva az ügyfélhez. A kulcsgenerálás helyszínét el kell zárni a külvilágtól, nehogy a hitelesítés előtt illetéktelenek kezébe kerüljön az új kulcs. Az ideális az, ha a kulcsgenerálást két, egymást ellenőrző és tanúsító személy végzi, ők adják át a nyilvános kulcsot a kulcshitelesítő részlegnek. A biztonság szempontjából az a megoldás tűnik a legjobbnak, ha a kulcsgenerálást maga az intelligens kártya végzi, amiből csak a nyilvános kulcs nyerhető vissza, a titkos kulcs pedig még a felhasználó elöl is rejtve marad.

Az illetéktelen behatolást a biztonsági átjáró akadályozza meg. Az átjárón nem lehet átmenni, ez kizárólag a kulcs átadására szolgál.

6.1.3. Kulcshitelesítés

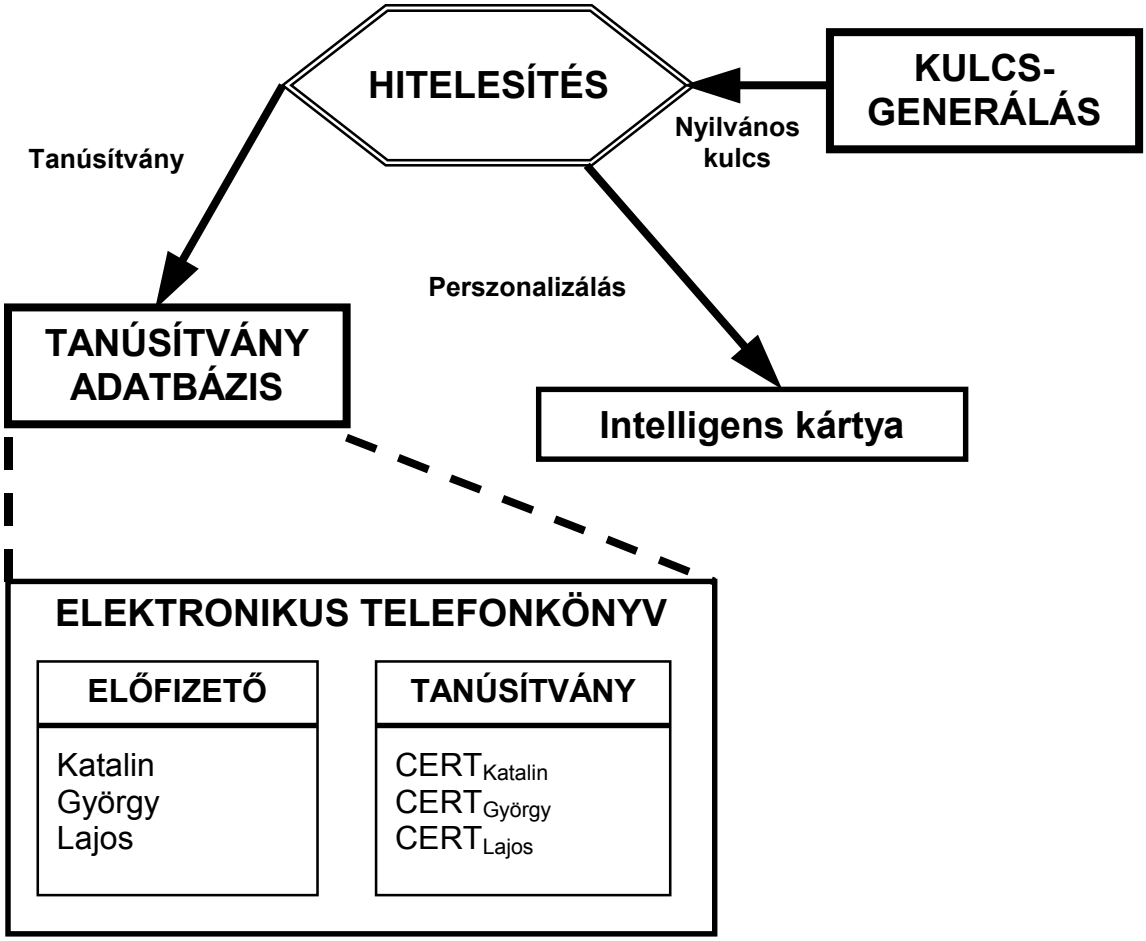
A kulcshitelesítés során logikailag az ügyfél személyazonosságához kötik a nyilvános kulcsot és erről a CCITT X.509v3 szabvány előírásainak megfelelő elektronikus tanúsítványt állítanak ki, melyet ellátnak a kibocsátó hatóság elektronikus aláírásával. A generáláshoz hasonlóan a hitelesítés is bizalmasan történik, itt is ügyelni kell a fizikai védelemre. Semmiféle hálózati kapcsolat nem megengedett a hitelesítés helyszínén.

6.1.4. Perszonalizálás

A perszonalizálás az aláíró eszköz „megszemélyesítését” jelenti. Azaz arról van szó, hogy az aláíró eszközt fizikailag az ügyfél személyéhez kötik. Az ügyféladatok aláíró eszközben való rögzítésén kívül ez még olyat is jelenthet, hogy dombornyomással rögzítik az ügyfél nevét az aláíró eszközön.

A perszonalizálás is a külvilágtól elzárva, bizalmasan történik, hiszen ilyenkor is fennáll annak a veszélye, hogy illetéktelenek beavatkoznak a folyamatba.

A perszonalizálás után a nyilvános kulcsot és az aláírt tanúsítványt a nyilvántartóban felveszik a tanúsítvány adatbázisba. Ez biztosítja a tanúsítvány ellenőrizhetőségét. A nyilvántartónak hálózati kapcsolattal kell rendelkeznie, hogy elérhetővé váljon az adatbázis. A fizikai védelmet azonban itt is biztosítani kell a szolgáltatás folyamatossága érdekében.



***9. sz. ábra.* A kulcsgenerálás és –hitelesítés folyamata**

Forrás: Dr. Tuzson Tibor: Secure Electronic Business c. tanfolyam fóliakészlete

6.2. Épületbiztonsági követelmények

Hiábavaló lenne minden erőfeszítés, amelyet a hitelesítés-szolgáltató funkcionális egységeinek szétválasztására javasolok, ha nem említeném meg az épületbiztonság jelentőségét.

Az eddig említett zsilipkapuk, biztonsági átjárók és fegyveres őrség alkalmazása mellett a lehallgatás elleni védelmet is meg kell oldani. Célszerű a különleges védelmet igénylő részlegeket – a kulcsgenerálást, a kulcshitelesítést és a perszonalizálást – a pinceszinten elhelyezni. A regisztrációs hatóságnak pedig tökéletes helyet lehet biztosítani a földszinten.

A számítógépes monitorokon megjelenő információ lehallgatását elsősorban a kisugárzás elleni védelemmel lehet megelőzni. Ennek érdekében a falakat réz- és vaslemezekkel kell borítani. Ezen kívül az egyes helyiségek hangszigetelését is el kell végezni.

A szigorú biztonsági intézkedések mellett biztosítani kell a megfelelő munkahelyi feltételeket az alkalmazottak számára. Ez azt jelenti, hogy például a teljesen elzárt részlegeket úgy kell biztonságossá tenni, hogy közben meg kell oldani a légkondicionálást is.

6.3. Egy másik megoldás

Mivel a javasolt biztonsági politika megvalósítása és fenntartása jelentős költségekkel jár, érdemes elgondolkozni azon, hogy a hitelesítés szolgáltatás hogyan valósítható meg decentralizált struktúrában.

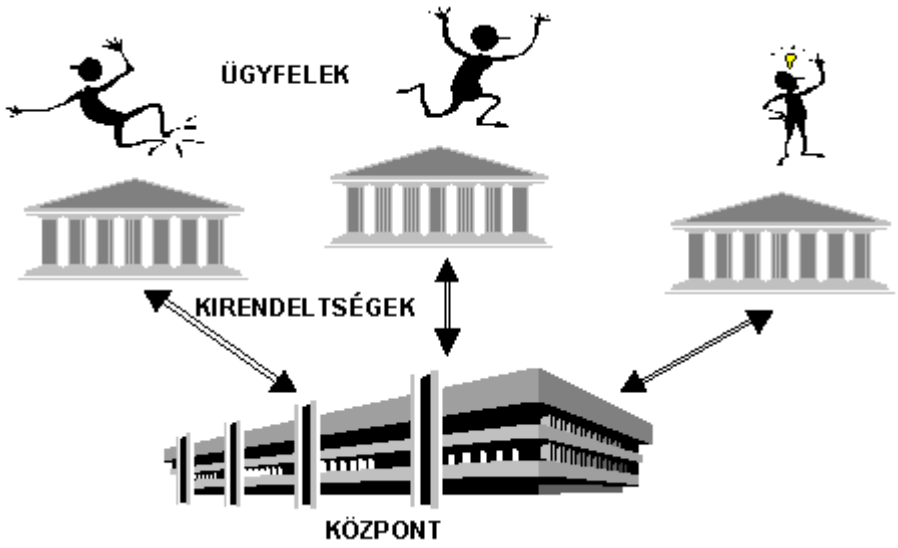
Tőkeerejük és kiépített fiókhálózatuk révén a nemzeti távközlési vállalatok és posták a legalkalmasabbak Európában a hitelesítés szolgáltatás ellátására, de éppen a felépítésükből adódóan ezeknek a társaságoknak nem érdeke egy központosított szolgáltatás beindítása. E társaságok célja az, hogy minden kirendeltségükön elérhetővé váljon a hitelesítés szolgáltatás. Számukra a különálló központok telepítése a tevékenységek felesleges párhuzamosításával és többletkiadással járna.

Az említett okok miatt regisztrációs kirendeltségeket és kulcsgeneráló központokat kell létrehozni. A kulcshitelesítést, a tanúsítványok

nyilvántartását, a perszonalizációt és az időbélyegző szolgáltatást pedig továbbra is a központ végezheti.

A decentralizált rendszer gyenge pontja a nyilvános kulcs eljuttatása a hitelesítés helyszínére, ezt biztonságos csatornán kell megvalósítani, esetleg egyszerre több – elektronikus és postai – úton is. Ha két úton jut el a kulcs a központba, feltételezhető, hogy egy esetleges megszemélyesítési támadás esetén, amely a kulcs kicserélésére irányul, csak az egyik „küldemény" kompromittálódik, s így megelőzhető a hamis kulcs hitelesítése.

A fentiekből kiderül, hogy a központosított rendszer biztonságosabb, a decentralizált rendszer pedig hatékonyabb működést tesz lehetővé. Valószínűnek tartom, hogy a jövőben a két rendszer előnyeit egyesítő hibrid megoldás fog elterjedni.



***10. sz. ábra.* A decentralizált rendszer modellje**

Forrás: Dr. Tuzson Tibor: Secure Electronic Business c. tanfolyam fóliakészlete

VII. ÖSSZEGEZÉS

7.1. A diplomamunka tartalmának összefoglalása

Diplomamunkámban a hitelesítés-szolgáltatók tevékenységét elemeztem az adatbiztonság szempontjából. Bemutattam azokat a tényezőket, melyek – véleményem szerint – a felhasználók szemében megbízhatóvá teszik a hitelesítés-szolgáltatók által kibocsátott tanúsítványokat.

A fent leírtak szellemében áttekintést adtam a tanúsítványkiadás alapját képező adatvédelmi technológiákról.

A technológia mellett – mint a bizalmat alátámasztó tényezők egyikét – bemutattam az elektronikus aláírással kapcsolatos európai jogi szabályozást, illetve az elektronikus aláírásról szóló magyar törvényt.

Az eddig említetteken kívül a szabványosítás kérdésével is foglalkoztam. Elsősorban európai viszonylatban tekintettem át az elektronikus aláírással kapcsolatos szabványosítási folyamatokat és világítottam rá a globális rendszerek fontosságára.

A szabványosítás ismertetése után a valós életben működő NetLock hitelesítés-szolgáltató tevékenységét elemezve megvizsgáltam a bizalmat növelő jellemzők érvényesülését. A vizsgálat eredményeképpen ismertettem egy általam biztonságosnak tekintett hitelesítés-szolgáltató felépítését és tevékenységét.

7.2. A hitelesítés-szolgáltatók jövőbeni szerepe

Az elektronikus kereskedelem olyan tényezővé vált az utóbbi néhány évben, amellyel a gazdasági szereplőknek számolniuk kell. A B2B, azaz a vállalatok közötti és a B2C, a cégek és az ügyfelek közötti kapcsolat részben már ma is elektronikus úton valósul meg. Van azonban még egy szereplő, az állam,

amely ugyancsak felismerte az elektronikus kereskedelem jelentőségét, és annak mintájára be kívánja vezetni az elektronikus közigazgatás intézményét. A cél a papírmentes ügyintézés biztosítása, azaz a papír nélküli társadalom megteremtése, melyre talán nem is kell annyit várni, mint ahogy azt ma gondoljuk.

Visszatérve a jelenbe, meg kell állapítanunk, hogy sorra születnek meg az elektronikus aláírásról szóló törvények[2], és az elektronikus aláírás használatának keretfeltételeit biztosító jogszabályok a világ számos országában, melynek alapján azt várhatnánk, hogy az elektronikus kereskedelem volumene is nő. A helyzet azonban az, hogy az elektronikus aláírás használatával kötött szerződések száma még világviszonylatban is alacsony. A legismertebb hitelesítés-szolgáltató, a Verisign 1998. óta több mint 25.000 szerver tanúsítványt adott ki pénzügyi intézményeknek, de mindössze 345 tanúsítványt bocsátott ki magánszemélyek számára, amiből az derül ki, hogy a nyilvános kulcsú kriptográfiát az esetek túlnyomó többségében a gépek közötti azonosításra használják.

Az Evans Data Corporation 2000-ben készített felmérése[3] szerint a mobil-alkalmazás fejlesztők harmada ugyan tervezi a nyilvános kulcsú infrastruktúra igénybevételét, de közülük csak kevesen látnak fantáziát az elektronikus aláírásban.

Szakértők abban látják a problémát, hogy a már működő rendszerek felkészítése a nyilvános kulcsú infrastruktúrára épülő szolgáltatásokra nagy költségekkel jár, és komoly szakértelmet igényel, ugyanakkor nincs biztosítva a befektetett pénz megtérülése, mivel a technológiák sokrétűsége miatt a különböző rendszerek közötti együttműködés sok esetben megoldatlan, ez pedig bizalmatlanságot szülhet a felhasználók körében.

[2] Erről átfogó elemzés olvasható a „Digital Signature Law Survey” c. honlapon a http://rechten.kub.nl/simone/ds-lawsu.htm címen.
[3] Ld. http://www.evansdata.com/pr103000.html

A cégek mellett a magánszemélyek, az ügyfelek számára is kiadásokkal jár az elektronikus aláírás használata. Az említett költségek – az aláírás létrehozó eszköz beszerzése és a tanúsítvány előfizetési díja – csak akkor térülnek meg, ha a felhasználó ki tudja használni az elektronikus aláírás használatából eredő előnyöket a mindennapi tevékenysége során.

Ez ördögi körnek tűnik: a nyilvános kulcsú infrastruktúrára épülő kereskedelmi rendszerek üzemeltetői nem lépnek addig, amíg a nem jelentkezik tömeges igény a PKI szolgáltatások igénybevételére, ugyanakkor a felhasználók azt várják, hogy a rendszerek megbízhatóbbá váljanak, és egységes technológiát alkalmazzanak.

A jövőben a pénzügyi intézményekre (bankok internetes szolgáltatásai) és a kormányzatra (elektronikus közigazgatás) hárul az a feladat, hogy megismertessék a felhasználók nagy részével a nyilvános kulcsú infrastruktúra előnyeit, hogy létrejöjjön az a kritikus tömeg, amely az e-kereskedelmi rendszerek rentábilissá tételéhez szükséges.

A hitelesítés-szolgáltatók szempontjából közelítve a problémát a fentiekből következően a magas költségekhez csekély bevétel párosul, ami azt jelenti, hogy azok tudnak majd talpon maradni, akik képesek a gazdaságos működéshez minimálisan szükséges ügyfélkör megszerzésére és megtartására. A piacon kevés szereplő marad, de éppen az előbb említett verseny miatt szolgáltatásaik megbízhatóbbá válnak majd a felhasználók szemében.

Nem mindenki ért azonban egyet a fentiekben megfogalmazottakkal, például Bruce Schneier, a kriptográfia neves szakértője épp ellenkezőleg úgy véli, hogy az elektronikus kereskedelem fejlődéséhez nincs szükség a nyilvános kulcsú infrastruktúra terjedéséhez, hanem ennek éppen a fordítottja igaz, azaz a kereskedelmi PKI virágzásának alapfeltétele az elektronikus kereskedelem széles körű elterjedése. Ebből látszik, hogy ez ma még erősen vitatott terület. A gyakorlat fogja eldönteni, hogyan tovább.

GLOSSZÁRIUM

Az alábbiakban közlöm a hitelesítés szolgáltatással kapcsolatos fogalmak magyarázatát.

Fogalom	Magyarázat
Aláírás ellenőrző adat	Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
Aláírás létrehozó adat	Olyan egyedi adat (jellemzően kriptográfiai titkos kulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.
Aláírás létrehozó eszköz	Szoftver vagy hardver, melynek segítségével az aláíró az aláírás létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
Aláíró	Az a természetes személy, akihez a hitelesítés-szolgáltató által közzétett aláírás ellenőrző adatok jegyzéke szerint az aláírás ellenőrző adat kapcsolódik.
Elektronikus aláírás	Elektronikus dokumentumhoz azonosítás céljából hozzárendelt vagy azzal logikailag összekapcsolt elektronikus adat, illetőleg dokumentum.
Elektronikus aláírások ellenőrzése	Az aláírt adat és az elektronikus aláírás összetartozását ellenőrző eljárás. Érvényes elektronikus aláírás esetén kijelenthető, hogy az aláírt adatot az ellenőrzéshez használt tanúsítvány tulajdonosa írta alá, s az aláírt adat az aláírás óta nem változott meg.
Entitás	A kommunikáló felek, illetve a tanúsítvány alanyok általános megnevezése. Entitás lehet természetes személy, társaság vagy szerver.
Hitelesítés-szolgáltató	Személy (szervezet), amely a hitelesítés szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait,

	valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás ellenőrző adatokat és a tanúsítvány visszavonási listát.
Időbélyegző	Elektronikus dokumentumokon a készítés időpontjának meghatározására alkalmas adat.
Intelligens kártya	Hitelkártya formájú és méretű számítógép. Fő alkalmazási területei a távközlés (telefonkártya), személyi azonosítás (digitális személyi igazolvány) és a hálózatbiztonság (digitális aláíró kártya).
Kompromittálódás	A biztonság sérülése. Titkos kulcs esetén például lehet jelszó nyilvánosságra kerülése.
Kulcs	Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
Kulcsadatbázis	Adatbázis, melyben a kibocsátó hatóságok által kiadott tanúsítványok elérhetők és letölthetők.
Kulcspár	Összetartozó nyilvános és titkos kulcs.
Nyílt hálózat	Hálózat, melyben a felhasználók által küldött üzenetek általuk nem kontrollált csomópontokon keresztül is haladnak.
Nyilvános kulcs **Publikus kulcs**	A kulcspár azon tagja, amelyet a küldendő üzenet titkosítására illetve a kapott üzenet elektronikus aláírásának ellenőrzésére használunk.
Nyilvános kulcsú infrastruktúra (PKI)	Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatásokat és eszközöket is.
Nyilvános kulcsú titkosítás	Rejtjelezési eljárás, mely olyan partnerek közti kommunikáció esetén is gyakorlati titkosságot nyújt, akik az üzenetküldést megelőzően soha nem találkoztak. Lényege az, hogy külön kulcsot használ a titkosításra és külön kulcsot az üzenetek megoldására.
Regisztrációs adatbázis	Adatbázis, melyben a PKI ügyfelek adatai találhatók. A tanúsítványkérelmek és tanúsítványok mindig egy, a

	regisztrációs adatbázisban szereplő felhasználóhoz kapcsolódnak.
Tanúsítvány	A hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás ellenőrző adatot az aláíró személyéhez kapcsolja.
Tanúsítvány alanya	Az a felhasználó, akinek adatai és nyilvános kulcsa a tanúsítványban szerepelnek.
Tanúsítvány elfogadása	A kibocsátott tanúsítvány adatainak ellenőrzése után a felhasználó kijelentése arról, hogy az a saját adatait tartalmazza.
Tanúsítványigénylés	Eljárás, mely során a felhasználó tanúsítvány kibocsátását kéri a hitelesítés-szolgáltatótól.
Tanúsítványlánc	Az elektronikus aláírás ellenőrzésekor használt tanúsítványok, melyek aláíróik alapján láncba szervezhetők.
Tanúsítványok osztályai	A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelőző ellenőrző lépések biztonságosságának jelzése.
Titkos kulcs **Privát kulcs**	A kulcspár azon kulcsa, amelyet a küldendő üzenet elektronikus aláírásának készítésére használunk. Fontos, hogy ehhez a kulcshoz csak tulajdonosa férjen hozzá.
Üzenetek integritása	Üzenetek sértetlensége, változatlansága.
Visszavont tanúsítványok listája (CRL)	Valamilyen okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a tanúsítványokat kiadó hitelesítés-szolgáltató saját elektronikus aláírása hitelesít.

RÖVIDÍTÉSEK JEGYZÉKE

Az alábbiakban közlöm a szövegben előforduló rövidítések magyarázatát, és ahol ez lehetséges, megadom az elnevezések magyar nyelvű megfelelőjét is.

Rövidítés	Angolul	Magyarul
ABA	American Bar Association	
AES	Advanced Encryption Standard	Tökéletesített titkosítási szabvány
ANSI	American National Standardization Institute	Amerikai Nemzeti Szabványügyi Intézet
API	Application Programming Interface	Alkalmazás programozási interfész
CA	Certificate Authority	Hitelesítő hatóság
CCITT	Comité Consultatif International de Télégraphique et Téléphonique	Nemzetközi Távíró és Telefon Konzultatív Bizottság
CEN/ISSS	European Committee for Standardization / Information Society Standardization System	Európai Szabványügyi Bizottság / Információs Társadalom Szabványosítási Rendszere
CRL	Certificate Revocation List	Tanúsítvány visszavonási lista
CWA	CEN Workshop Agreement	CEN műhely megállapodás
CSP	Certificate Service Provider	Hitelesítés-szolgáltató
DEA	Data Encryption Algorithm	Adattitkosítási algoritmus
DES	Data Encryption Standard	Adattitkosítási szabvány
DSA	Digital Signature Algorithm	Elektronikus aláírási algoritmus
DSS	Digital Signature Standard	Elektronikus aláírási szabvány
EESSI	European Electronic Signature Standardization Initiative	Európai elektronikus aláírás szabványosítási kezdeményezés
ESI	Electronic Signature Working Group	Elektronikus aláírási munkacsoport
E-SIGN	Electronic Signature Workshop	Elektronikus aláírási műhely
ETSI SEC	European Telecommunication Standardization Institute Security	Európai Távközlési Szabványosítási Intézet biztonsági testülete
FIPS	Federal Information Processing	Szövetségi információfeldolgozási

	Standards	szabványok
ICC	International Chamber of Commerce	Nemzetközi Kereskedelmi Kamara
ICTSB	Information and Communication Technologies Standards Board	Információ és Kommunikáció-technológiai Szabványosítási Tanács
IDEA	International Data Encryption Algorithm	Nemzetközi adattitkosítási algoritmus
IETF	Internet Engineering Task Force	
ILPF	Internet Law Policy Forum	Internet Jogpolitikai Fórum
ISO	International Standards Organization	Nemzetközi Szabványügyi Szervezet
ITSEC	Information Technology Security Evaluation Criteria	Információtechnológia-biztonság értékelési kritériumok
ITU	International Telecommunications Union	Nemzetközi Távközlési Unió
LDAP	Lightweight Directory Access Protocol	
MAC	Message Authentication Code	Üzenethitelesítési kód
MMI	Man–Machine Interface	Ember–gép interfész
NIST	American National Institute for Standards and Technology	Amerikai Nemzeti Szabványügyi és Technológiai Intézet
NSA	National Security Agency	Nemzeti Biztonsági Ügynökség
PES	Proposed Encryption Standard	Javasolt titkosítási szabvány
PGP	Pretty Good Privacy	Ingyenesen elérhető nyilvános kulcsú titkosítási rendszer
PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
PP	Protection Profile	Védelmi profil
RFC	Request for comments	Internet specifikáció
SHA	Standard Hash Algorithm	A legelterjedtebb hash algoritmus
SSL	Secure Socket Layer	Kriptográfiai protokoll
TS	Time Stamp	Időbélyegző
ETSI TS	ETSI Technical Specification	ETSI műszaki specifikáció
TSA	Time Stamping Authority	Időbélyegző szolgáltató
TTP	Trusted Third Party	Megbízható harmadik fél
W3C	World Wide Web Consortium	

IRODALOMJEGYZÉK

1. Könyvek:

[1] Faragóné Haló Katalin: *Adatbiztonság, a*datvédelem
Budapest, Számalk Kiadó, 2000.

[2] Ködmön József: *Kriptográfia*
Budapest, ComputerBooks, 1999., p. 113-202.

[3] Menezes, Alfred; van Oorschot, Paul, Vanstone, Scott: *Handbook of Applied Cryptography*
New York, CRC Press, 1997.

2. Jogszabályok:

[4] *2001. évi XXXV. törvény az elektronikus aláírásról*
In: Magyar Közlöny, 2001. 65. sz., p. 4137-4149.

[5] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*
In: Official Journal of the European Communities, 2000. L13 sz., p. 12-20.

[6] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*
In: Bundesgesetzblatt, Teil 1, 2001. 22. sz., p. 876-884.

3. Internetes publikációk:

[7] Savard, John: *A Cryptographic Compendium*
1999.
Forrás: *http://home.ecn.ab.ca/~jsavard/jscrypt.htm*
Letöltés dátuma: 2001. június 24.

[8] *EESSI Deliverable Description Document – First set of deliverables*
2001. április
Forrás: *http://www.ict.etsi.org/eessi/eessi-homepage.htm*
Letöltés dátuma: 2001. szeptember 3.

[9] *An Industry Initiative in Support of the European Directive on Electronic Signature* – EESSI introduction page
2001. január
Forrás: *http://www.ict.etsi.org/eessi/EESSI-intro.htm*
Letöltés dátuma: 2001. augusztus 27.

[10] Endrődi Csilla, Hornák Zoltán: *Az elektronikus aláírásról szóló törvény elemzése* c. előadásának összefoglalója
2000., BME Méréstechnika és Inf. Rsz. Tanszék
Forrás: *http://nws2000.iif.hu/ncd2001/docs/nevjegy/nj89.htm*
Letöltés dátuma: 2001. július 10.

[11] *Advanced Encryption Standard (AES) Development Effort – Overview*
2001. február, NIST
Forrás: *http://csrc.nist.gov/encryption/aes/index2.html*
Letöltés dátuma: 2001. szeptember 23.

[12] *AES: Questions and Answers*
2001., NIST
Forrás: http://www.nist.gov/public_affairs/releases/aesq&a.htm
Letöltés dátuma: 2001. szeptember 23.

[13] *Electronic Signatures in Europe*
2001., Sonera SmartTrust Ltd.
Forrás: h*ttp://www.smarttrust.com/legislation/europe.asp*
Letöltés dátuma: 2001. szeptember 10.

[14] Lannerstrom, Sten: *Basic elements of a PKI (White paper)*
2001., Sonera SmartTrust Ltd.
Forrás: h*ttp://www.smarttrust.com/whitepapers*
Letöltés dátuma: 2001. szeptember 23.

[15] Saliba, Clare: *EU Signs Off on E-Signature Initiative*
2001. augusztus 1., E-Commerce Times
Forrás: *http://www.ecommercetimes.com/perl/story/?id=12431*
Letöltés dátuma: 2001. szeptember 10.

[16] A. Greenberg, Paul: *E-Signatures: Unsigned, Unsealed, Undelivered*
2001. június 5., E-Commerce Times
Forrás: *http://www.ecommercetimes.com/perl/story/10247.html*
Letöltés dátuma: 2001. szeptember 23.

[17] Gócza Zoltán: *Elektronikus aláírás – alaptalan várakozások?*
2001. június 6., Dotkom Internet Consulting
Forrás: *http://www.dotkom.hu*
Letöltés dátuma: 2001. augusztus 23.

[18] *Frequently Asked Questions about Today's Cryptography*
2000. május, RSA Laboratories
Forrás: *http://www.rsalabs.com/faq/index.html*
Letöltés dátuma: 2001. szeptember 23.

4. Szakdolgozatok:

[19] Marty Zsolt: *Bizalom megteremtése kriptográfiai eszközökkel az elektronikus kereskedelemben*
Budapest, GDF, 2000.

[20] Róder Gábor: *Információvédelem kriptográfiai eszközökkel*
Budapest, GDF, 1999.

5. Egyéb kiadványok:

[21] *NetLock Ügyfél Tájékoztató*
Budapest, NetLock Kft., 2000.

[22] *NetLock Szolgáltatási Szabályzat tervezete*
Budapest, NetLock Kft., 2001.