Elektronikus ECDL jegyzet

Hogyan oldjam meg az ECDL Elektronikus Hitelesség, Elektronikus Aláírás vizsgamodul feladatait?

Verzió 1.0

Készítette:

Erdősi Péter Máté, CISA

NJSZT információrendszer-ellenőrzési szakértő

2010. október 11.

EPM

Elektronikus Aláírás & Hitelesítés Szakértő

Készült az ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv szövegeinek és ábráinak felhasználásával.

Szerkesztette és írta: Erdősi Péter Máté, CISA

Kiadó: OTY Startel Kft. 1025 Budapest, Nagybányai út 8.

Ügyvezető igazgató: dr. Rátai Balázs

ISBN: 978-963-08-0181-2

Tartalomjegyzék

1 Bevezetés

A világ változásai szinte követhetetlenül gyorsan történnek az orrunk előtt, alig van időnk felocsúdni és a helyes ösvényt megtalálni. Folyamatosan kutatnak a tudósok is a megfelelő jövő megteremtése érdekében, bizonyság erre az utóbbi évek számtalan találmánya és új technológiai megoldása. Vannak azonban régóta megoldatlan problémák is, például egyik ilyen az, hogy az ipari társadalom mellett megjelent az információs társadalom fogalma. Az információs társadalom – az 1980-as években meghatározott definíciók szerint – szimbiózisban él a természettel, a környezetével, erősen információtermelő és -fogyasztó, emiatt a gépesítési rátája magas, az oktatás perszonalizált, fő valutája az időérték, és az összjólét megvalósítása helyett a társadalmi cél az összelégedettség elérése. Az elektronikus kommunikáció hitelessége alapvető eleme az információs társadalomnak az erős informatika-függése miatt.

Idekívánkozik továbbá korunk új stratégiájának rövid ismertetése, a Kék Óceán Stratégia (Blue Ocean Strategy), mely szerint a versengő „Vörös Óceán" ütközeteiből kilépve a „Kék Óceán" mindenkinek biztosít elegendő teret ahhoz, hogy működjön – természetesen csak akkor, ha stratégiáját, szemléletét átalakítja az itt leírt módszereket követve. Egyébként ennek az a lényege – nagyon leegyszerűsítve, hogy ha valaki – szakítva az eddigi hagyományos módszerekkel – olyan új módon kínálja termékét, mely az igénybe vevő igényét (és csak azt) elégíti ki felesleges sallangoktól mentesen és kedvező áron, akkor rövid idő alatt tömeges érdeklődői táborra szert téve megalapozottan működhet abban a szegmensben versenytársak nélkül. De mi köze van ennek az elektronikus aláíráshoz? Három tényt ismertetünk ezzel kapcsolatban.

1. Az elektronikus piacon egy termékhez potenciálisan másfél milliárd internetező férhet hozzá egy időben – sávszélességtől függően, ezt a jelenséget egyetlen hagyományos bolt sem tudja produkálni, és a média is csak akkor, ha összehangoltan veszik át egymástól a híreket, tudósításokat – erre viszont nincs még sok példa.

2. Matematikailag bebizonyítható tény, hogy a Földön bármely két ember egymástól legfeljebb hét (6,23) kézfogásnyi távolságra van, azaz az ismerős ismerősének az ismerősének az ismerősének az ismerősének az ismerősének az ismerőse a célszemély lesz – de az esetek többségében még ennyi ismerős sem szükséges bármely két ember közötti ismeretségi alapú kapcsolati lánc felépítéséhez – elegendő megnézni a közösségi portálok gombamód szaporodását és statisztikai adatait.

3. Az ember saját szükségleteinek kielégítéséhez más emberek tevékenységét, szolgáltatását, termékét használja fel az esetek többségében, egyszer az igénybe vevői, másszor a felajánlói oldalon. Embertípustól – és időszaktól – függ, hogy mikor melyik van túlsúlyban, de „egyedül nem megy".

Mindezekhez amennyiben hozzá tudjuk tenni a hiteles elektronikus igényjelzés, számlázás, ügyfélkezelés, kommunikáció módszerét, akkor nagyságrendekkel megnövekedik bárkinek a lehetősége arra, hogy a saját életminőségét a megfelelő szintre felemelje és ott meg is tartsa. Ehhez kínál széles körben elfogadott és jogilag is elismert segítséget, eszközöket az elektronikus aláírás és technológiái.

Az új évezred első évtizedeiben már sok helyen ismert és alkalmazott ez a technológia az elektronikus cégeljárásban, ügyvédi tevékenységben, közjegyzői szolgáltatásokban, APEH

elektronikus adóigazolások kiadásakor, közüzemi és mobiltelefónia számlák kibocsátásánál, közbeszerzéseknél és láthatóan egyre inkább terjed az elektronikus aláírás alkalmazása az üzleti területeken is, belső és külső kommunikációban egyaránt. Mindez azt jelenti, hogy az elkövetkezendő időben a ma még csak 1,2 millió magyarországi számítógépes munkahelyen dolgozó ember számára az elektronikus aláírás ismerete a közeljövőben vélhetően létfontosságú lesz a hatékony, gyors és minőségi munkavégzésben – annál is inkább, mert a felmérések a számítógépes munkahelyek számának növekedését prognosztizálják az elkövetkezendő 20 évre, a munkahelyek 80-90%-áig, más szóval az információs társadalom növekedése beindult. Tekintettel arra, hogy erre a tudásra szükség van és szükség lesz a jövőben is, felmerült az igény, hogy tanúsíthatóan meg lehessen szerezni az ezzel kapcsolatos tudást. Ezt az igényt hivatott szolgálni az ECDL új elektronikus hitelességre vonatkozó modulja, amelynek gazdája a Neumann János Számítógép-tudományi Társaság, és mely az ECDL-től megszokott módon modulvizsgával bizonyítható, hogy ezt a tudást valaki elsajátította és képes a mindennapi gyakorlatban ezt használni.

Az elektronikus aláírással kapcsolatos ECDL vizsgakérdések megválaszolásához kíván ez a szabadon hozzáférhető könyv alapszintű segítséget nyújtani, mely az ECDL Elektronikus Hitelesség, Elektronikus Aláírás modultankönyv [1] kérdésekre fókuszáló átdolgozott kivonata. Hozzá kell azonban tenni, hogy a digitális írástudásnak ez a szintje azok számára javasolható jó szívvel, akik az alapszintű informatikai jártasságot (pl. ECDL Start, Select) már megszerezték. A modultankönyv olvasása és a benne foglaltak felhasználói szintű elsajátítása természetesen szintén ajánlott a vizsgára való sikeres felkészülés érdekében, mert a modultankönyv több alapvető információt tartalmaz, mint ez a – csupán a vizsgakérdésekre fókuszáló – kiadvány.

Remélhetőleg sokaknak fog a közeljövőben hathatós segítséget nyújtani az – úgy tűnik, hogy – mindenképpen bekövetkező életviteli és gazdasági változások, elektronizálódások sikeres átélésében, a saját és a közösségi élet minőségének fenntartásában, az összelégedettség megteremtésében, az információs társadalom kialakításában, más szóval az „áramlat”, a „flow”, avagy akár a hétköznapi boldogság fenntartásában az ECDL Elektronikus Hitelesség, Elektronikus Aláírás modulvizsgán igazolhatóan elsajátítható új informatikai írástudási képesség, készség, tudás és gyakorlat.

Erdősi Péter Máté, CISA

http://www.erdosipetermate.hu
NJSZT információrendszer-ellenőrzési szakértő
Elektronikus aláírással kapcsolatos szolgáltatási szakértő
Magyar Elektronikus Aláírás Szövetség alelnök (MELASZ)
Oktatási és Terjesztési Bizottsági tag, Education and Dissemination Committee (EDC 2010-11), ISACA

Erd»si P®ter M§t®

Digitally signed by Erd»si P®ter M§t®
DN: cn=Erd»si P®ter M§t®c=HU l=Budaº rs e=perdosi@upcmail.hu
Reason: I am the author of this document
Location:
Date: 2010-10-28 11:49+02:00

2 Tudásanyag az elméleti és gyakorlati kérdésekhez

A tudásanyag három részből tevődik össze:

1. elméleti kérdések felsorolása
2. elméleti ismeretek a kérdések megválaszolásához
3. gyakorlati útmutató a gyakorlati feladatok megoldásához.

A kérdések strukturálása megegyezik az ECDL Elektronikus Hitelesség, Elektronikus Aláírás modultankönyv szerkezetével.

2.1 Elméleti kérdések

2.1.1 Információ és információs társadalom

2.1.1.1 Az információ fontossága

Kérdések
1. Mi az információ általános definíciója?
2. Az információ mérhetőségére mi igaz?
3. Mi az információ mértékének alapegysége?
4. Miért számít kiemelt alakzatnak a „világkép” az információtörténetben?
5. Melyik kommunikációs problémával foglalkozik a híradástechnika?
6. Mi a híradástechnikai rendszerek feladata?
7. Az információtartalomra mi igaz?
8. A redundanciamentes üzenet milyen tulajdonsággal rendelkezik?
9. Az információfizika szerint az információt mi jellemzi?
10. Az információ archiválása mit jelent?
11. A nyílt archiválási rendszerek mit csinálnak?
12. A biztonságtechnikai szabványok szerint mi az adat?
13. Egy adott társadalomban milyen bonyolultságú rendszereket lehet működtetni?
14. Mi az információs társadalom alapértéke?

Kérdések
15. Időérték alatt az információs társadalom mit ért?
16. Az oktatásban az információs társadalom mit preferál?
17. Az információs társadalomban az ember társadalomban elfoglalt helyének megőrzéséhez mi szükséges?
18. A digitális világban mit lehet az információ-forrásokról megállapítani?
19. A digitális világban mi igaz a digitális források elérhetőségére?
20. Az internetes keresőprogramok milyen eredményeket adnak?

2.1.1.2 Hiteles és nem hiteles információ

Kérdések
21.Melyik biztonsági követelmény foglalkozik a hitelességgel?
22.Melyik üzleti követelmény foglalkozik a hitelességgel?
23.Mikor lesz egy információ hiteles?
24.Mire vonatkozik a sértetlenség?
25.Mi a hitelesség definíciója?
26.Mi a hitelesítés definíciója?
27.Mikor tekinthető valami hitelesnek?
28.Milyen műszaki eljárások biztosíthatják az üzenetek tartalmának hitelességét?
29.Mi a feladata a digitális aláírásnak a biztonsági intézkedések között?
30.Ha egy tartalomhoz kapcsolt digitális aláírás ellenőrzése fél évvel ezelőtt sikeres volt, akkor mit lehet megállapítani?
31. Egy számítógépes bejelentkezés folyamatában mit lehet megállapítani az azonosítás, hitelesítés és feljogosítás műveletekről?
32. A letagadhatatlanság teljes körű biztosítása mit jelent?
33. A digitális aláírás mit biztosít?

Kérdések
34. Az üzenethitelesítő kód mit biztosít?
35. A hitelesség megállapítása mikor szükséges?
36. A sértetlenség megállapítása hogyan viszonyul a hitelesség megállapításához?
37. A letagadhatatlanság mivel valósítható meg?
38. Az adatsértetlenséget mivel lehet biztosítani?
39. A nyílt infrastruktúrák biztonsági szolgáltatások alatt mit valósítanak meg?
40. A visszajátszás elleni védelmet melyik intézkedés valósítja meg?

2.1.2 Az elektronikus aláírás az Európai Információs Társadalomban

2.1.2.1 Az elektronikus aláírás fogalmai

Kérdések
41.Mi az elektronikus aláírás definíciója a 93/1999 irányelv szerint?
42. Az elektronikus aláírás fogalmát hol határozták meg?
43. Az elektronikus aláírás jogi szabályozására miért volt szükség?
44. A beszkennelt kézi aláírás elektronikus dokumentum végére való beillesztése mire alkalmas?
45. Az aláírás-létrehozó adat jogi értelemben mit jelent?
46. Elektronikus aláírás létrehozásához szükséges-e tanúsítvány?
47.Melyik adat nem szerepel az ITU X.509 v3 tanúsítványokban?
48. Az aláírási fogalmak közül melyik nem műszaki fogalom?
49. Az aláírási fogalmak közül melyik műszaki fogalom?
50. A PKI magánkulcs és a PKI nyilvános kulcs milyen tulajdonsággal rendelkeznek?
51. A titkos kulcsok generálására alkalmas intelligens kártyák milyen tulajdonsággal rendelkeznek?

Kérdések
52. A titkos kulcsok generálására alkalmas USB-eszközök (tokenek) milyen tulajdonsággal rendelkeznek?

2.1.2.2 Az EU céljai és az elektronikus aláírás jogi szabályozásának helyzete

Kérdések
53.Mi volt a célja az EU elektronikus aláírással kapcsolatos szabályozásának?
54.Mely témakörökre vonatkoznak a legfontosabb uniós szabályozások?
55. Az elektronikus aláírásról szóló irányelv mire kötelez és kiket?
56. A hitelesítésszolgáltatások szabad piacra lépésének követelménye mit jelent?
57. Lehet-e kötelező az önkéntes akkreditáció egy hitelesítésszolgáltató számára?
58.Mire kötelezi az irányelv a tagállamokat a bírósági és hatósági eljárásokban?
59.Miért felelnek a minősített tanúsítványt kibocsátó szolgáltatók?
60.Mi nem vonatkozik egy unión kívüli szolgáltató által nyújtott szolgáltatások unión belüli elismerésére?
61. Az elektronikus aláírási uniós irányelv tagállami implementációja hogyan valósult meg?
62. A magyar elektronikus aláírási fogalmi szabályozás jogszabály struktúrában elfoglalt helye hol van?
63. Az elektronikus aláírások jogi elismerésével kapcsolatos fontosabb előírásokat mi tartalmazza?
64. Melyek az elektronikus aláírásokkal kapcsolatos szolgáltatások az elektronikus aláírás törvény szerint?
65. A hitelesítésszolgáltatás keretében az elektronikus aláírás törvény szerint a hitelesítésszolgáltató mit végez?
66. Az elektronikus aláírással kapcsolatos szolgáltatásokat végző szolgáltatókra milyen követelmények vonatkoznak?
67. Mely tevékenységet nem végzi egy hitelesítésszolgáltató?
68. Az időbélyegző jogi értelemben minek felel meg?

Kérdések
69. Az aláírás-létrehozó adat aláírás-létrehozó eszközön való elhelyezése során a szolgáltató milyen tevékenységet végez?
70.Kinek a jogszabályi kötelessége figyelemmel kísérni a kriptográfiai algoritmusok fejlődését?
71.Mely elektronikus aláírástermékekhez szükséges a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolás?
72.Mely elektronikus aláírási termékekhez nem szükséges a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolás?
73. Az elektronikus aláírási termékekre vonatkozó terméktanúsítványokat ki állítja ki?
74. Az időbélyegben milyen idő szerepel?

2.1.2.3 Az elektronikus aláírás működése

Kérdések
75.Melyik állítás igaz a digitális aláírás tulajdonságára vonatkozóan?
76.Melyik lépés nem tartozik a digitális aláírás elkészítéséhez?
77.Melyik lépés nem tartozik a digitális aláírás ellenőrzéséhez?
78. A digitális aláírás sikeres ellenőrzéséből milyen állítás nem következik?
79. A digitális aláírás ellenőrzésének sikertelenségéből milyen állítás következhet?
80.Mikor tekinthető egy tanúsítvány megbízhatónak?

2.1.3 Publikus Kulcsú Infrastruktúra, PKI

2.1.3.1 Kriptográfiai háttérismeretek

Kérdések
81.Mi jellemzi a kétkulcsos titkosítást?
82. A digitális aláírás során ki a titkos kulcs birtokosa és ki használja a nyilvános kulcsot?

2.1.3.2 A PKI elemei

Kérdések
83.Melyik elem nem a PKI eleme?
84.Melyik PKI-elem végzi a tanúsítványt igénylő személy azonosítását?

2.1.4 Digitális tanúsítványok

2.1.4.1 A tanúsítványok fogalmi rendszerei

Kérdések
85.Mi a gyökér tanúsítvány-kibocsátó feladata?
86.Mi a digitális tanúsítvány?
87.Meddig érvényes egy tanúsítvány?

2.1.4.2 A tanúsítványok használata

Kérdések
88. A tanúsítványigénylés során megadott adatokból mi nem szerepel a tanúsítványban?
89.Melyik számít a legbiztonságosabb regisztrációnak?
90. A tanúsítványigénylés során mely adatokra nincs szükség?
91.Mi a tanúsítvány előállítás első lépése?
92.Ki töltheti le a tanúsítványokat a hitelesítésszolgáltatótól?
93.Mi az aláíró magánkulcs szerepe a tanúsítvány igénylésekor?
94.Mire való az aláírás-aktivizáló adat?
95.Mit nem írnak alá általában elektronikusan?
96.Mi az a tanúsítási lánc?
97.Mi áll a tanúsítási lánc tetején?
98.Mi a teendő, ha megváltozik a tanúsítványban szereplő e-mail cím?

Kérdések
99. Milyen adat nem szerepel a tanúsítványtárban?
100. Melyik adat nem titkos az alábbiak közül?
101. Melyik állítás hamis az alkalmazások tanúsítványtárával kapcsolatban?
102. Ki írja alá a felhasználói tanúsítványt?
103. Milyen adat szerepel a tanúsítványban?
104. Mely esetben lehet a tanúsítványt megújítani?
105. Melyik művelet nem megengedett a tanúsítvánnyal kapcsolatban?
106. Mikor szükséges a személyes megjelenés?
107. Melyik lépés nem része a tanúsítvány elkészítésének?

2.1.4.3 Digitális tanúsítványok a mai rendszerekben

Kérdések
108. Milyen tanúsítványokat tartalmazhatnak a telepített rendszerek tanúsítványtárolói?
109. Hogyan szegmentálódnak a tanúsítványok a tanúsítványtárban?
110. Miért kell vigyázni a felhasználói profilra?
111. Miért jelent nagyobb kockázatot a vándorló profil alkalmazása a tanúsítványok használata szempontjából a helyi profil alkalmazásánál?
112. Mit kell tennie több különböző célú tanúsítvánnyal rendelkező felhasználónak aláírás előtt?
113. Melyik tanúsítvány hibás?
114. Mi a célja a szoftvertanúsítványoknak?

2.1.4.4 Visszavonási listák, a visszavonási állapot ellenőrzése

Kérdések
115. Mit tesznek egy tanúsítvány visszavonásakor?

Kérdések
116. Melyik tény nem okozza egy tanúsítvány érvénytelenségét?
117. Hol van a tanúsítvány visszavonási lista feltalálási helye?
118. Mi a kivárási idő?
119. A tanúsítvány visszavonási lista mely adatokat tartalmazza?

2.1.5 Az elektronikus aláírások osztályozása és készítése

2.1.5.1 Az elektronikus aláírások osztályozása

Kérdések
120. Mit jelent a „beágyazott aláírás” fogalma?
121. Mit jelent a „különálló aláírás” fogalma?
122. Mit jelent a „beágyazódó aláírás” fogalma?
123. Mit jelent a „párhuzamos aláírás” fogalma?
124. Mit jelent a „szekvenciális aláírás” fogalma?
125. Mit jelent az „ellenjegyző aláírás” fogalma?
126. Mi nem tartozik az elektronikus aláírási irányelv előírásai közé?

2.1.5.2 Az elektronikus aláírások készítése

Kérdések
127. Melyik állítás igaz az aláíró alkalmazások együttműködésére vonatkozóan?
128. Mi igaz az aláíró programokra?
129. Mely programokkal nem lehet digitális aláírásokat készíteni?
130. Mi az aláírási politika?
131. Az aláírási politika szabályrendszere mit biztosít?

2.1.6 Kormányzati és hivatali ügyintézés elektronikusan

2.1.6.1 Az elektronikus aláírás és a kormányzás kapcsolata

Kérdések
132. Melyik a legfejlettebb ügyintézési szint az Alapvető közszolgáltatások egységes listája szerint?
133. Kötelező-e a közigazgatási ügyekben az elektronikus ügyintézés?
134. Van-e működő példa az elektronikus aláírás használatára Magyarországon?

2.1.6.2 Elektronikus aláírás és internetbanking

Kérdések
135. Ha jogszabály a szerződés érvényességéhez írásbeli alakot rendel, melyik forma nem alkalmazható?
136. Mi az elektronikus pénz?
137. Hogyan biztosítja a pénzintézet a bankszámla feletti rendelkezési jog elektronikus gyakorlása esetén a hitelességet?

2.1.6.3 Az e-adózás és e-számla

Kérdések
138. Mit jelent az elektronikus adóbevallás és adatszolgáltatás?
139. Mit neveznek e-számlának?

2.2 Válaszok az elméleti kérdésekhez

2.2.1 Információ és információs társadalom

2.2.1.1 Az információ fontossága

Az információnak nincs általánosan elfogadott definíciója annak ellenére, hogy számos helyen különböző megfogalmazásokkal találkozhatunk, mint például:

- minden információ, ami továbbítható – ez csak a katonai célú definíció,
- az információ értelmezett adat – a klasszikus információ fogalmi definíciója,
- az információ ismeretterjesztés, tudásbővítés – ez az Értelmező Kéziszótár definíciója.

Az információ mérhetőségére vonatkozó állítások közül hamis az, hogy az információ nem mérhető, mivel az információ mérhetősége annak valószínűségével függ össze. Az is igaz továbbá, hogy az információ átalakítható energiává – az információfizika szerint, de ennek nincs köze a mérhetőséghez. Továbbá fontos tudnunk azt is, hogy az információ mérhetősége nem a közlés hosszával függ össze, a hossztól nem feltétlenül függ az információtartalom (pl. ismétlődő hosszú üzenet), hanem a váratlansággal.

Az információ mértékének létezik alapegysége, mégpedig az információ mértékének alapegysége egy kétkimenetelű esemény valószínűségi értéke, a bit. Helytelen megfogalmazás, hogy az információ mértékének alapegysége az események valószínűsége, mert a bit nem az események, hanem egyetlen kétértékű esemény valószínűsége, továbbá az sem igaz, hogy az információ mértékének alapegysége az 1, 0 számjegyek segítségével előállítható számok, mivel ezek a bináris számok. Ugyanígy helytelen a kilobájtot alapegységnek tekinteni, mivel a kilobájt a digitális adatok egyik mértékegysége, hasonlóan a gigabájthoz, a terrabájthoz stb., nem pedig alapegysége.

A „világkép” az információtörténetben kiemelt alakzatnak számít, mert nem transzformálódik. Hibás az a megfogalmazás, hogy a világkép magában foglalja az összes többi alakzatot, mivel ez a „minden halmazok halmaza” filozófiai képződmény. Az sem igaz, hogy a világkép másként transzformálódik, mint a többi, hiszen egyáltalán nem transzformálódik. Információfizikai szempontból természetesen igaz, hogy az információ kívül esik az ember központú vizsgálódási területein, azt fizikai lényegűnek tekinti, de a világkép az információtörténet fogalmi rendszerébe tartozik, onnan kiemelni nem szerencsés.

A híradástechnika azzal a kommunikációs problémával foglalkozik, hogy milyen pontosan vihetők át az adott hírközlési szimbólumok. Nem foglalkozik az értelmezés problémájával – hogyan lehet a közlés jelentését a lehető legpontosabban átvinni, és azzal sem, hogy hogyan lehet nagy hatótávolságú kommunikációs berendezéseket építeni – hiszen ez az átviteltechnika feladata, továbbá az sem a híradástechnika problémája, hogy a fogadó milyen cselekvésre lesz képes az üzenet hatására, azaz az átvitt üzenet mennyire hatásos.

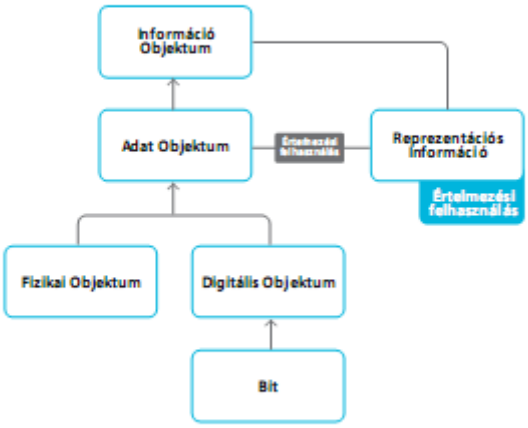
A híradástechnikai rendszerek feladata nem egy adott, maximális hosszúságú közlés átvitele, mert több közlés átvitele a cél. De nem feladat minden közlés átvitele, hiszen egyszerre minden közlést nem lehet átvinni, hanem a lehetséges közlések összességéből véletlenül kiválasztott bármelyik

közlésnek az átvitelét kell egy híradástechnikai rendszernek megoldania. Éppen ezért azt sem vállalhatja fel, hogy a kommunikációs rendszereket folyamatosan működteti az egész világon, hiszen ez üzemeltetési feladat.

Az információtartalomra az igaz, hogy egy „képtelenség” és egy „nagy jelentéstartalmú üzenet” információtartalma lehet teljesen egyenértékű, mivel a váratlansággal van az információtartalom összefüggésben, nem pedig a közlés hosszától vagy az üzenet jelentésétől függ. Továbbá az sem igaz, hogy az információtartalom mérhetetlen, emiatt reláció is felállítható az információtartalmak között.

A redundanciamentes üzenetre nem jellemző, hogy a legtömörebb érthető formában tartalmazza a közlést, mivel a tömörség igaz, de annyira tömör ez már, hogy értelmezhetetlen, érdektelen a fogadó számára. Éppen ezért katonai célokra is alkalmatlan. Azért van ez így, mert a redundanciamentes üzenet ismétléseket nem tartalmazhat, így a megértés lehetetlen.

Az információfizika szerint az információ nemcsak az emberi agyban létezik – ez az információtörténet megközelítése, hanem embertől független fizikai mennyiség. Az információ mennyisége nem a hőmennyiség közlésével, hanem a rendezettséggel függ össze. Fizikai mennyiségként kémiai úton nem előállítható anyag, és nem is anyag a szó szoros értelmében, hanem az anyag és energia mellett egy harmadik független jellemző mennyisége a világegyetemnek.



Az információ archiválása azt jelenti, hogy információobjektumokat őriz meg értelmezési adatokkal együtt, technológiaváltástól, adatformátumoktól és felhasználói közösségek változásától független módon. Ebben nincs az benne, hogy mennyi ideig kell azt megőrizni, hogy archiválásnál az információobjektumokat legalább száz évig őrzik, vagy hogy archiválórendszereket kell kiépíteni és működtetni, mert megőrizni nem csupán archiválórendszerekben lehet. Az igaz, hogy össze kell gyűjteni az információobjektum mindenkori értelmezéséhez szükséges adatokat, de ez csupán szükséges, de nem elégséges feltétele az archiválásnak, más szóval ez nem az archiválás, hanem annak egy részeleme.

A nyílt archiválási rendszerek tehát információobjektumokat őriznek meg hosszú távon. Nem igaz az, hogy csak fizikai objektumok megőrzésére vonatkozó szabályokat rögzítenek, hiszen digitális objektumokat is őrizhetnek. Nem írhatják le az információ száz évre történő megőrzési formáját, ha az időtartamtól független a megőrzési forma leírása.

A biztonságtechnikai szabványok szerint az adat tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás, illetve távközlés céljára. Vannak más megfogalmazások is, de nem a biztonságtechnikában, ilyen például az, hogy az adat értelmezett információ – ez egy klasszikus megközelítés. Az sem igaz, hogy információ az információk megszerzésével, tárolásával és feldolgozásával összefüggő ismeretek összessége, ez kibernetikai megközelítés, és csak a katonai célú információ-fogalom mondja azt ki, hogy az információ olyan ismeretanyagot jelent, amelyet bármilyen formában továbbítani lehet.

Egy adott társadalomban olyan bonyolultságú rendszereket lehet működtetni, amennyire szabad információáramlást biztosítanak a társadalmi folyamatok, hiszen a megfelelő üzemeltetéshez a tapasztalatok összeadása és szabad hozzáférése alapvető követelmény. Ebből kifolyólag nem lehet igaz a rendszerek bonyolultságára, hogy olyanok lehetnek, amelyek működtetését jogszabályok előírják, hiszen ha nincs meg a képesség, hiába van előírás, és hiába vannak társadalmi szervezetek, amelyek önkéntesen működtetnek rendszereket, a rendszerek nem működnek. Az önkéntesség egyébiránt nem jelent működtetési alapot. Az sem jelent garanciát egy rendszer bonyolultságára, hogy melyek működési költségeit finanszírozza a társadalom, hiszen a bonyolultság alapesetben nem függ a költségtől, példa rá a nyílt rendszerek.

Az információs társadalom alapértéke az időérték. Ez változást jelent a korábbi szemlélethez képest, mivel az időérték nem egyezik meg az anyagi javakkal. Az anyagi javak az ipari társadalom alapértékének számított. A számítógép sem alapérték, mert a számítógépesítés megléte szükséges, de nem elégséges feltétele az információs társadalomnak. Továbbá az információ része az időértéknek, de nem fedi le teljesen azt.

Időérték alatt az információs társadalom azt érti, amit valamely idő alatt az ember az erőforrások céltudatos felhasználása révén hoz létre. Ha meg kellene fogalmazni az időértéknek a mértékét, akkor azt lehetne mondani, hogy az egységnyi idő alatt létrejövő időértéket nevezhetjük az időérték mértékének. Az időérték nem az, ami az összjólétet magasabb szintre emeli, az összjólét az egyik célkitűzése a jóléti ipari társadalomnak.

Az oktatásban az információs társadalom erősen preferálja a személyes jellegű oktatás bevezetését. Nem cél, legfeljebb következmény lehet az oktatás és nevelés teljes számítógépesítése. Nem oktatási célja az információs társadalomnak a környezetszennyezés visszaszorítása, de azért ez kimondottan a céljai közé tartozik. Továbbá a tanultak mielőbbi termelésben történő hasznosítását sem tűzte az információs társadalom a zászlajára, mert a termelés az ipari társadalom központi célja.

Az információs társadalomban az ember társadalomban elfoglalt helyének megőrzéséhez hiteles, pontos, aktuális információ szükséges. A pénzügyi információ szükséges, de nem elégséges, a jótékony megnyilvánulások inkább erkölcsi kötelesség és nem információs társadalom-függő tevékenység, hasonlóan a társadalmi munkavégzéshez, mert ez is belső késztetés és nem információs társadalom-függő előírás.

A digitális világban nem igaz, hogy minden információforrás egyenértékű, mert lehetnek elsődleges és másodlagos információforrások, de ugyanúgy vannak ismeretközlő és ezekről tájékoztató

dokumentumok, mint a papír alapú világban. Szintén nem igaz, hogy a hiteles digitális információ három ezreléke a teljes információnak, de a papír alapú információra – összehasonlítva az elektronikus információval, ez már igaz állítás lesz. Az sem fedi a valóságot, hogy egyik információ sem számít hitelesnek, mert létezik hitelesnek számító információ a jogi szabályozás szerint.

További igaz állítás, hogy a digitális források elérhetőségét és változatlanságát sok esetben nem garantálják, de léteznek olyan források, ahol igen – ezek vannak kevesebben. Ebből következően nem helyes az, hogy a digitális források elérhetőségét és változatlanságát minden esetben garantálják, az sem, hogy a digitális források elérhetőségét és változatlanságát legtöbbször garantálják – habár a változatlanságot egyre többször garantálja digitális aláírás, az elérhetőséget továbbra sem garantálják. Az is hamis állítás, hogy a digitális források elérhetőségét és változatlanságát soha nem garantálják, mivel vannak jogszabályi előírás alapján működtetett rendszerek, melyek elérhetőségét előírás és műszaki intézkedés is garantálja.

Az internetes keresőprogramok működésére különböző állítások fogalmazhatók meg. A keresők általában nem összehangoltan működnek és nem egészítik ki egymás hiányosságait, hanem versenyben állnak és az indextáblájuktól függően adnak eredményeket, valamint a dinamikus webet nem tudják keresni. Különböző keresők eltérő kérdésre eltérő eredményt is adnak általában, nehéz olyan egymástól különböző keresőket találni, melyek lényegesen eltérő keresési kérdésekre ugyanazt az eredményt adják válaszul. De az is nehezen képzelhető el, hogy különböző keresők ugyanarra a keresési kérdésre ugyanazt az eredményt adják, mivel eltérő keresők ugyanazon kérdésre eltérő eredményt is adhatnak, az indextáblájuktól – azaz a látószögüktől – függően. Ezért az egyetlen igaznak tűnő állítás a keresők esetében az, hogy különböző keresőprogramok különböző eredményeket adhatnak ugyanarra a keresési kérdésre is.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 17-36. oldal

2.2.1.1 Hiteles és nem hiteles információ

A hitelességgel foglalkozó biztonsági követelmény a sértetlenség. A bizalmasságnak nincs köze hozzá. A sértetlenség biztonsági követelménynek a letagadhatatlanság ugyanolyan része, mint a hitelesség. A megbízhatóság nem biztonsági követelmény, hanem üzleti.

A hitelességgel foglalkozó üzleti követelmény a biztonság. Emlékeztetőül, három üzleti követelményt ismer a szakirodalom, minőség – ez a minőséggel foglalkozik, megbízhatóság – ez a működéssel foglalkozik és biztonság. Lehetne még megfelelőségről is beszélni a hitelesség kapcsán, de a megfelelőség nem üzleti követelmény, hanem egy információ-kritérium a CobiT[1]-ban – a szervezetek vezetőségei számára készített IT irányítási segédletben – megfogalmazott hétből.

Egy információ akkor lesz hiteles, ha ha az eredeti állapotának megfelel és teljes. Nem tévesztendő össze azzal, amikor ismert a küldője és digitálisan is alá van írva, mert ez egy megvalósulása a hitelességnek, és nem nevezünk hitelesnek egy információt akkor sem, ha az információhoz csatolt digitális aláírás érvényes, ugyanis az aláírás érvényessége szükséges, de nem elégséges feltétele az információ hitelességének, hiányzik a küldő személye. Továbbá nem felel meg a hiteles információnak az sem, ha az információhoz csatolt digitális aláírás érvényes és minősített tanúsítvány van hozzá, mivel az aláírás érvényessége ugyan igen, de a minősítettség nem szükséges feltétele a hitelességnek.

1 CobiT: Control Objectives for Information and Related Technology, ©ISACA (http://www.isaca.org/cobit)

A sértetlenség az információknak az elvárások szerinti pontosságára, általános értelemben vett változatlanságára és teljességére, valamint az információk érvényességére és hitelességére vonatkozik. A bizalmasság vonatkozik arra, hogy megakadályozza, a bizalmas információk engedély nélküli megismerését, vagyis fontos információkhoz illetéktelenek ne férjenek hozzá. Két információkritériummal lehet a sértetlenséget még összetéveszteni, mégpedig a hatásosság információkritériummal, mely vonatkozik arra, hogy az információk a folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítják, illetve a megbízhatóság információkritériummal, mely vonatkozik arra, hogy a vezetés számára olyan időszerű és pontos információkat biztosítson, amelyek a folyamatok működtetéséhez, pénzügyi megbízhatóságához és irányításához szükségesek. Az óvatosság tehát nem árt a sértetlenség tárgyalásakor.

A hitelesség definíciója az, hogy valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti.

Nem keverendő a hitelesítés definíciójával, ami nem más, mint az állított azonosság megerősítése. Amikor a kibocsátónak állított forrás azonosságának ellenőrzése és a kibocsátott üzenet a tartalmának eredetisége megerősítetté vált, akkor a hitelesítési folyamat hitelességét részleteztük ki, és gyakorlati példa a hitelességre a felhasználói név és a hozzá tartozó jelszó megadása. A jelszó időnkénti biztonságos megváltoztatása a kompromittálódás elleni védelmi intézkedés.

Ezek szerint valami akkor tekinthető hitelesnek, ha a kibocsátónak állított forrás azonosságának ellenőrzése és a kibocsátott üzenet a tartalmának eredetisége megerősítetté vált. Lehetne azt is mondani, hogy akkor hiteles valami, ha az állított azonosság megerősítése megtörtént, de ebben az esetben minden állított azonosság megerősítéséről beszélnénk, ami több, mint a hitelesség. Ha a felhasználói nevet és a jelszót a felhasználó sikeresen megadta, akkor az azonosítás és hitelesítés kombinációját valósította meg.

Az üzenetek tartalmának hitelességét a digitális aláírás vagy az üzenethitelesítő kód műszaki eljárások biztosíthatják. Az elektronikus aláírás nem műszaki eljárás, így műszaki hitelességet nem biztosíthat.

A digitális aláírásnak a biztonsági intézkedések között az a feladata, hogy észlelhetővé tegye a tartalom megváltozását. A digitális aláírás nem tudja megakadályozni a módosítást, csak felfedi – a módosítás megakadályozására az írásvédelem szolgál. Továbbá nem tudja biztosítani a rendelkezésre állást sem, erre a redundáns infrastruktúra szolgálhat. Érdekesség, hogy önmagában nem a digitális aláírás biztosítja az aláíró személyének kilétét, hanem a tanúsítvány nyilvános kulcsa és a fizikai személy összekapcsolása. Az aláíró titkos kulcs csak a nyilvános kulcshoz kapcsolódik matematikailag, az aláíró személyére ez a kapcsolat nem tesz semmilyen megkötést, utalást.

Időben eltolva, ha egy tartalomhoz kapcsolt digitális aláírás ellenőrzése fél évvel ezelőtt sikeres volt, akkor most annyit tudunk pontosan megállapítani, hogy a tartalom a kibocsátás és a sikeres ellenőrzés között nem változott meg. Azt, hogy a tartalom ma is változatlan nem tudjuk, mert az utolsó ellenőrzés óta módosulhatott. Így azt sem tudhatjuk, hogy az aláíráshoz használt titkos kulcs most is érvényes-e, hiszen az aláíró kulcs azóta lejárhatott. A tartalom jelenlegi hitelessége a fél évvel ezelőtti aláírás sikeres ellenőrzésének természetesen nem következménye.

Egy számítógépes bejelentkezés folyamatában a hitelesítés megelőzi a feljogosítást, ugyanis először azonosítani kell azt, akit feljogosítanak, de a feljogosítás előtt még hitelesíteni is kell azt, akit feljogosítanak a bejelentkezés utáni munkavégzésre, erőforrás-használatra.

A letagadhatatlanság teljes körű biztosítása azt jelenti, hogy a tartalom kiállítója nem tudja a kiállítás tényét letagadni és a tartalom fogadója nem tudja a fogadás tényét letagadni. Az, hogy a tartalom kiállítója nem tudja a kiállítás tényét letagadni, a letagadhatatlanságnak szükséges, de nem elégséges feltétele. Továbbá letagadhatatlanság biztosítása esetén sem igaz az, hogy a tartalom hitelességét nem lehet megváltoztatni, mert a hitelesség ez esetben is megváltozhat menet közben.

A digitális aláírás egyik fő szerepe az, hogy biztosítsa az utólagos módosítások felderíthetőségét. Nem feladata az aláírás személyhez köthetőségének elvégzése, hiszen nem az aláírás, hanem az aláírás egyik adatához, a titkos kulcs nyilvános párjához kapcsolt személyes tanúsítvány biztosítja személyhez köthetőséget – mivel az aláíráshoz használt titkos kulcs és a tanúsítványban szereplő nyilvános kulcs kapcsolódik egymáshoz. Az aláírás nem biztosítja a tartalom megváltoztathatatlanságát, mert a tartalom változhat a digitális aláírás után is. A digitális aláírás továbbá nem biztosítja az eredeti tartalom visszaállíthatóságát sem, mert a digitális aláírás nem tartalmaz javító eljárásokat. Az aláírás biztosítja az utólagos módosítások felderíthetőségét.

Az üzenethitelesítő kód – a szimmetrikus kriptográfiát használó aláírás – is biztosítja az utólagos módosítások felderíthetőségét, de nem biztosítja a tartalom megváltoztathatatlanságát, sem pedig az eredeti tartalom visszaállíthatóságát, mivel az üzenethitelesítő kód aláírás szintén nem tartalmaz javító eljárásokat. Ez a kód sem biztosítja a kód személyhez köthetőségét, mert nem a kód, hanem a személyes tanúsítványban szereplő személyes adatok biztosítják személy megállapíthatóságát.

A hitelesség megállapítása az adat élettartama során folyamatosan szükséges lehet, ha nem lehet pontosan tudni, mikor kerül sor az adat felhasználására. Nem biztos, hogy az adat élettartamának kezdetén vagy az adat élettartamának végén szükséges ez, mert a felhasználás során is szükség van a hitelesség megállapítására. Lehet persze, hogy az adat élettartama során periodikusan szükséges a hitelesség megállapítása, de ebből nem tudható még, hogy a felhasználáshoz kapcsolódik-e a periodikus ellenőrzés, ami során meg lett állapítva a hitelesség, vagy a periodikus megállapítás öncélú lett, és nem történik felhasználás, csak ellenőrzés.

A sértetlenség megállapítása elegendő a hitelesség megállapításához. Nem fedi a valóságot az, hogy a sértetlenség megállapítása szükséges, de nem elégséges a hitelesség megállapításához, mert a sértetlenség tartalmazza a hitelességet részként. Ebből az is következik, hogy a sértetlenség megállapítása nem lényegtelen a hitelesség megállapításához, és nem ugyanazt jelenti, mint a hitelesség megállapítása – a sértetlenség bővebb, mint a hitelesség.

A letagadhatatlanság aszimmetrikus kriptográfiai eszközökkel valósítható meg. A szimmetrikus kriptográfiai eszközökkel (mint például üzenet-hitelesítő kóddal) azért nem lehet ezt megtenni, mert az aláíróknak és ellenőrzőknek ugyanarra a kulcsra van szükségük, így a kulcshasználat egyes birtokosok által önmagában letagadható. A letagadhatatlanság nem valósítható meg elektronikus aláírással, mert az elektronikus aláírások között szimmetrikus kulcsú aláírások is vannak, de figyelemmel kell lenni arra, hogy létezik olyan elektronikus aláírás, mellyel viszont megvalósítható.

Az adatsértetlenséget csak az adathoz csatolható további nyílt vagy rejtjelezett adatokkal lehet biztosítani. Ebbe beleérthető minden konkrét műszaki eljárás is. A helyes megfogalmazás az, hogy az adatsértetlenséget lehet biztosítani digitális aláírással vagy blokk-ellenőrző kóddal, de nem kizárólagosan. Említést érdemel, hogy titkosítással a bizalmasságot lehet biztosítani, nem pedig a sértetlenséget.

A nyílt infrastruktúrák biztonsági szolgáltatások alatt a hitelesítés, hozzáférés-ellenőrzés, adattitkosság, adatsértetlenség, letagadhatatlanság ötöst valósíthatják meg. A bizalmasság, sértetlenség – benne letagadhatatlanság és hitelesség, rendelkezésre állás biztonsági követelmények, valamint a minőség, megbízhatóság, biztonság üzleti követelmények, és a hatékonyság, illetőleg a hatásosság pedig információkritériumok, egyik sem nyílt infrastruktúrák biztonsági szolgáltatása.

A visszajátszás elleni védelmet nem a digitális aláírás, hanem az időpecsét valósítja meg. A digitális aláírás és az üzenet-hitelesítő kód a módosításokat teszi felfedhetővé, a hibajavító kód pedig az adatmegváltozási hibák javítását teszi lehetővé. A digitális aláírás nem tud ilyet alapesetben.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 37-45. oldal

2.2.2 Az elektronikus aláírás az Európai Információs Társadalomban

2.2.2.1 Az elektronikus aláírás fogalmai

A 93/1999 EU irányelv az elektronikus aláírást úgy definiálja, hogy az a hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat. Igaz, az is, hogy elektronikus aláírás minden olyan eljárás, amely hitelesítésre szolgál, de ez nem definíció, hanem egy általános megfogalmazás. Az elektronikus aláírás megvalósítási formái lehetnek a digitális aláírás és az üzenethitelesítő kód együttesen. Habár elektronikus aláírás az aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, de nem kizárólagosan, hiszen az üzenethitelesítő kód is része az elektronikus aláírás halmazának.

Az elektronikus aláírás fogalmát európai irányelvi szinten használták először jogi eredetű fogalomként, mert meg akarták különböztetni a szabályozási fogalmat minden más műszaki fogalomtól. Az elektronikus aláírást ebből következően műszaki szabványok nem említhetik legelőször az aszimmetrikus kriptográfiai eljárások kapcsán, és nem is korai matematikai definíciója alapján határozták meg, hiszen nem volt ilyen. A levelező rendszerek leírásaiban találkozhatunk elektronikus aláírással, de a levelező rendszerek aláírása nem is jogi értelemben vett használatra utal, hanem egy tetszőleges állandó karaktersorozat beillesztésére minden egyes kimenő levélbe.

Az elektronikus aláírás jogi szabályozására azért volt szükség, hogy meghatározzák az elektronikus dokumentumok tekintetében a saját kezű aláírások szerepét betölteni képes megoldások és gyakorlatok körét, mielőtt az nagyon elterjedne és sok különálló megoldás jönne létre, amit nem, vagy csak nagyon nehezen lehet egységesíteni. Ilyen előírás az EU jogalkotási rendjében nem volt, habár korábbi riportok már javasolták ezt az EU-nak. Szintén nem helyes az az elképzelés sem, mely szerint azért kellett az elektronikus aláírást jogilag szabályozni, hogy egyszerűsítsék a műszaki aláírás fogalmakat nem műszaki fogalom az elektronikus aláírás. És a szabályozás idején nem volt jellemző az, hogy az elektronikus dokumentumok aláírása tömeges méretekben kezdett elterjedni.

A beszkennelt kézi aláírás elektronikus dokumentum végére való beillesztése alkalmas hitelesítési funkció betöltésére, ezért alkalmas joghatás kiváltására is – habár igen korlátozott mértékben. Mivel elektronikus aláírásnak kell tekinteni, ezért nem tagadható meg bizonyítási eljárásban való felhasználása, miként egyetlen elektronikus aláírási formának sem. De nem lesz egyenértékű a kézírásos aláírással, hiszen arra a minősített aláírás alkalmas, a beszkennelt kézi aláírás pedig biztonsági tulajdonságai miatt nem funkcionálhat minősített aláírásként, csak normál aláírásként.

Az aláíráslétrehozó adat jogi értelemben kizárólag az aláíróhoz köthető és alkalmas az aláíró azonosítására – ez nem áll fenn az előbb említett beszkennelt kézi aláírásnál például. Az aláírás-létrehozó adat nem kizárólag PKI titkos kulcs lehet, legfeljebb a PKI-rendszerekben. Lehetséges, hogy az aláírás alapjául egy egyszer használatos kód szolgál, de ez szintén nem jogi fogalom. Arra sincs előírás, hogy az aláírás-létrehozó adat kizárólag kriptográfiai algoritmussal együtt használható lenne.

Érdekessége az elektronikus aláírásnak, hogy a szabályozás szerint elektronikus aláírás létrehozásához nem szükséges tanúsítvány, így az sem igaz, hogy csak minősített tanúsítvány lenne használható, hiszen aláíráshoz nem minősített tanúsítványhoz kapcsolódó aláírás-létrehozó adat is használható. Az aláírással szemben támasztott követelmények mindenhol mások lehetnek, nincs általános érvényű ajánlás erre, ezért nem lehet azt kimondani, hogy ajánlott legalább fokozott biztonságú tanúsítványt használni vagy csak saját kibocsátású tanúsítvány alkalmazható aláírásra, hiszen megbízható harmadik felektől származó tanúsítvány is használható aláírás létrehozásához.

Az ITU X.509 v3 tanúsítványokban szereplő adatok körében minden egyes esetben benne van a nyilvános kulcs, az általános név, a kiállító neve, de sosem szerepel benne a titkos kulcs.

Az aláíráshoz számos szabályozási és műszaki fogalom kapcsolódik. Legfontosabb szabályozási fogalom maga az elektronikus aláírás, és ebből adódóan a minősített elektronikus aláírás, a fokozott biztonságú elektronikus aláírás, és a teljes bizonyító erővel bíró aláírás.

A műszaki fogalmak körébe tartozik a digitális aláírás, a PKI titkos kulcs, és az X.509 v3 tanúsítvány is.

A PKI magánkulcs és a PKI nyilvános kulcs nem teljesen függetlenek egymástól, mivel függenek, de nem állíthatók egymásból elő, mert matematikai értelemben tartoznak csupán össze. Nem igaz továbbá az, hogy csak aláírásra használhatóak, hiszen aláírásra matematikai értelemben ugyanúgy használhatók a PKI-kulcsok, mint titkosításra.

A titkos kulcsok generálására alkalmas intelligens kártyák kriptográfiai funkciókat megvalósító eszközökkel bővített intelligens kártyák, ezért nem ugyanolyanok, mint a többi intelligens kártya (például SIM-kártya, bankkártya) lényeges eltérések vannak a kártyák között. Ezek az intelligens kártyák nemcsak akkreditált szervezet általi bevizsgálás után használhatók, mivel privát használatra bármilyen kártya megfelelő. Természetesen létezhetnek olyan előírások, melyek bizonyos körben csak akkreditált szervezet általi bevizsgálás utáni használhatóságot írnak elő, de ezeknek nincs általános érvényessége. Ebből az is következik, hogy az intelligens kártyák közül nem mindegyik biztonságos aláírás létrehozó eszköz, mert csak a megfelelő eszköztárral rendelkező tanúsított intelligens kártyák lehetnek biztonságos aláírás létrehozó eszközök.

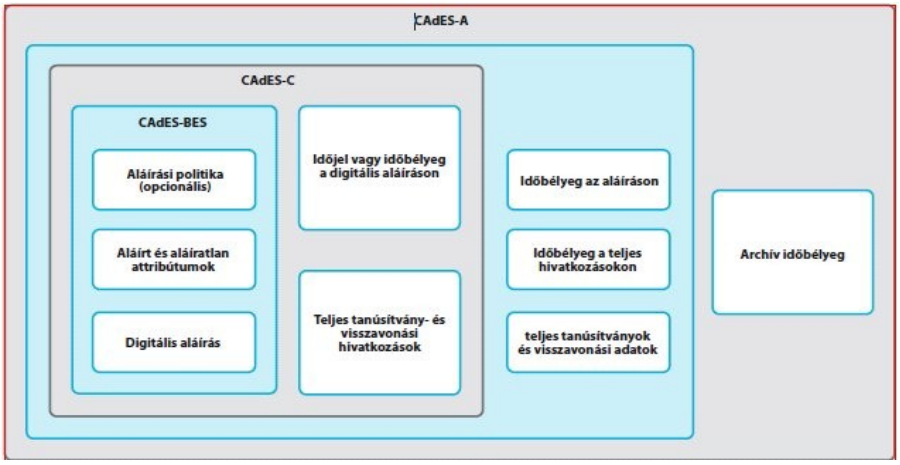
A titkos kulcsok generálására alkalmas USB-eszközökre (tokenek) ugyanezek igazak, nemcsak akkreditált szervezet általi bevizsgálás után használhatók, mert privát használatra bármilyen token megfelelő, nem ugyanolyanok, mint a többi kártya, mert lényeges eltérések vannak a kártyák és tokenek között és nemcsak a megfelelő eszköztárral rendelkező tanúsított tokenek lehetnek biztonságos aláírás létrehozó eszközök, hiszen nem mindegyik token biztonságos aláírás-létrehozó eszköz. De amelyik USB-eszköz titkos kulcsokat tud generálni, az biztos, hogy kriptográfiai funkciókat megvalósító eszközökkel bővített USB-eszköz lesz.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 47-60. oldal

2.2.2.2 Az EU céljai és az elektronikus aláírás jogi szabályozásának helyzete

Amikor az EU elektronikus aláírással kapcsolatos szabályozását kialakította, az volt a célja, hogy az elektronikus aláírás elterjedését nehezítő szabályozási akadályok létrejöttét megakadályozza. Nem akart az EU elektronikus aláírást terjeszteni szabályozással, és nem akarhatta az elektronikus aláírás elterjedését nehezítő szabályozási akadályok lebontását sem, mivel nem voltak még akadályok az elektronikus aláírás terjedését illetően. Az sem igaz, hogy egységes jogi fogalomrendszer elterjesztése volt a cél, hiszen a tagállamok eltérő rendelkezéseket is hozhatnak saját hatáskörükben az elektronikus aláírás egyes részterületeit illetően.

Az elektronikus aláírással kapcsolatos legfontosabb uniós szabályozások az elektronikus számla, közbeszerzés, elektronikus és digitalizált dokumentumok használata témakörökre vonatkoznak. A fő szabályozások lényegi tulajdonsága, hogy átfogó jellegűek és nem akarnak részletekbe menő előírásokat kidolgozni, mint például az elektronikus vámárunyilatkozat, e-adózás és minősített tanúsítványok napi használata, és nem akar szabványt sem szabályozásba beilleszteni a minősített hitelesítésszolgáltatók és aláírási politikákra vonatkozó szabványok tekintetében sem. Szintén nem szabályozási, hanem szabványügyi kérés, az alap, aláírási politikán alapuló, időbélyegzett, komplex és archív aláírások szabványosítása, melyet az EU szabványosítási kezdeményezése (EESSI) és a megfelelő szabványügyi intézet (ETSI) szabványosított.



Az elektronikus aláírásról szóló irányelv nem kötelezi az európai polgárokat az abban foglaltak ismeretére, nem kötelezi az európai magán- és jogi személyeket az abban foglaltak betartására és nem kötelezi a tagállamok kormányait az abban foglaltak ellenőrzésére, hiszen nem kötelező elektronikus aláírást implementálni a nemzeti gyakorlatokba. Az elektronikus aláírásról szóló irányelv ellenben kötelezi a tagállamokat az abban foglalt tartalmú szabályozás kialakítására, ha alkalmazni kívánják a technológiát.

A hitelesítésszolgáltatások szabad piacra lépésének követelménye azt jelenti, hogy az uniós tagállamok nem köthetik az üzleti hitelesítésszolgáltatási tevékenység megkezdését előzetes hatósági engedély megszerzéséhez. De ez nem jelenti azt, hogy az uniós tagállamok kötelesek ellenőrzés nélkül megengedni az üzleti hitelesítésszolgáltatási tevékenységek nyújtását, sem azt, hogy az uniós tagállamok nem írhatnak elő olyan szabályokat az üzleti hitelesítésszolgáltatási tevékenységek nyújtóinak, melyek a piaci tevékenységeiket korlátozzák, és azt sem, hogy az uniós tagállamok nem köthetik az üzleti hitelesítésszolgáltatási tevékenység megkezdését és folytatását

hatósági ellenőrzésekhez – létezik hatósági ellenőrzési tevékenység a tagállamokban.

Arra a kérdésre, hogy lehet-e kötelező az önkéntes akkreditáció egy hitelesítésszolgáltató számára, az a meglepő, de helyes válasz, hogy igen, minden további nélkül előírható kötelezően az önkéntes akkreditáció követelményrendszerének való megfelelés. Nem lehet ezt a kötelezettség-vállalást megtagadni arra való hivatkozással, hogy ez önkéntes, vagy csak kiemelt állami esetekben, vagy csak akkor lehetséges ez, ha a szolgáltató kéri, hogy akkreditálják – nincsenek ilyen megkülönböztetések kodifikálva.

Az irányelv kötelezi a tagállamokat arra, hogy a bírósági és hatósági eljárásokban az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként felhasználhatóak legyenek. Nem kötelez arra, hogy minden minősített aláírást el kell fogadniuk vagy arra, hogy írásbeliséget kielégítő elektronikus aláírást kell alkalmazni, de arra sem kötelesek a bírósági és hatósági eljárásokban, hogy teljes bizonyító erőt rendeljenek az aláírásokhoz, mivel a teljes bizonyító erőt csak az aláírások egy szűkebb köréhez kell rendelni, ahol minősített aláírás a követelmény.

A minősített tanúsítványt kibocsátó szolgáltatók a minősített tanúsítványban szereplő adatok valótlanságából eredő károkért felelnek. Nem tehetők felelősség az általuk kibocsátott minősített tanúsítványok segítségével készített aláírások valódiságáért, hiszen ezért a készítő felel, sem az általuk kibocsátott minősített tanúsítványok segítségével készített aláírások ellenőrzéséért, mert ezért az ellenőrző felel. A minősített tanúsítványok elvesztéséből adódó károkért pedig a tanúsítvány-birtokos felel.

Ha egy unión kívüli szolgáltató által nyújtott szolgáltatásokat unión belül is el szeretnének ismerni, akkor ezt az alábbi három módon tehetik meg az előírások szerint:

- a harmadik ország szolgáltatója teljesíti az irányelvben meghatározott követelményeket és egy uniós önkéntes akkreditációs folyamatban akkreditálják,
- egy uniós országban működő szolgáltató felelősséget vállal a harmadik országban működő szolgáltató által kiállított minősített tanúsítványért,
- az Unió és egy harmadik ország között létrejött kétoldalú vagy többoldalú nemzetközi szerződés úgy rendelkezik, hogy a harmadik ország szolgáltatóit el kell ismerni az Unión belül.

Nyilvánvalóan nem lehetséges ezt úgy megtenni, hogy a harmadik ország szolgáltatója felelősséget vállal az uniós országban működő szolgáltató által kiállított minősített tanúsítványért.

Az elektronikus aláírási uniós irányelv tagállami implementációja nem kötelező minden tagállam számára, de ha valamit tenni kíván ez ügyben, akkor az itt leírtakat kell alkalmaznia, ez a gyakorlatban meg is valósult Európa minden tagországában, kivétel nélkül minden tagállamban létezik nemzeti törvény az elektronikus aláírásról.

A magyar elektronikus aláírási fogalmi szabályozás jogszabály struktúrában elfoglalt helye törvényi és végrehajtási rendelet szintű. Van részszabályozás miniszteri rendeletek szintjén, kormányrendelet szintjén, de ezek nem általános érvényűek. Továbbá a legmagasabb szinten az elektronikus aláírás nem jelenik meg, azaz nincs benne az alkotmányról szóló törvényben.

Az elektronikus aláírások jogi elismerésével kapcsolatos fontosabb előírásokat tehát az elektronikus aláírási törvény (Eat.) tartalmazza, nem pedig kormányrendelet, vagy az alkotmány, esetleg miniszteri rendeletek fogalmazták meg a jogi elismerésekkel kapcsolatos általános szabályokat.

Elektronikus aláírásokkal kapcsolatos szolgáltatások az elektronikus aláírás törvény szerint pontosan a hitelesítésszolgáltatás, az időbélyegzés, az aláíráslétrehozó adat elhelyezése, és az archiválásszolgáltatás összessége. Nem helyes, hiányos tehát az a megközelítésmód, mely ezeket nem tartalmazza, mint például időbélyegzés, aláíráslétrehozó adat elhelyezése, archiválásszolgáltatás vagy hitelesítésszolgáltatás, időbélyegzés, archiválásszolgáltatás hármasok, de szintén helytelen a hitelesítésszolgáltatási funkciókat – regisztráció, tanúsítvány kibocsátás, nyilvántartás, módosítás, közzététel, állapotinformáció szolgáltatás – aláírásokkal kapcsolatos szolgáltatásoknak tekinteni.

A hitelesítésszolgáltatás keretében az elektronikus aláírás törvény szerint a hitelesítésszolgáltató a regisztráció, tanúsítványkibocsátás, nyilvántartás, módosítás, közzététel, állapotinformáció szolgáltatások nyújtását végzi. Nem keverendő össze az Eat. szerinti szolgáltatásokkal (hitelesítésszolgáltatás, időbélyegzés, aláírás-létrehozó adat elhelyezés, archiválásszolgáltatás) vagy ezek bármely részhalmazával.

Az elektronikus aláírással kapcsolatos szolgáltatásokat végző szolgáltatókra az igaz, hogy a minősített szolgáltatókra erősebb követelmények vonatkoznak, mint a nem minősített szolgáltatókra. Nem igaz tehát az a megállapítás, hogy a minősített és nem minősített szolgáltatókra ugyanazok a követelmények vonatkoznak mert a követelmények jelentősen eltérnek, sokkal szigorúbbak a minősített szolgáltatókra, ebből adódik, hogy az is hamis állítás, hogy a minősített szolgáltatókra gyengébb követelmények vonatkoznak, mint a nem minősített szolgáltatókra. Továbbá az sem felel meg a valóságnak, hogy a minősített és nem minősített szolgáltatókra nincsenek előírt követelmények, mivel a legfontosabb követelmények az Eat.-ben és a 3/2005. IHM Rendeletben vannak megfogalmazva.

Egy hitelesítésszolgáltató működése során azonosítja az igénylő személyét, majd a saját

elektronikus aláírásával aláírt tanúsítvánnyal hitelesíti az igénylő elektronikus aláírását, azaz a tanúsítványkibocsátás folyamán az azonosítás után – jó pár lépést követően – a hitelesítésszolgáltató aláírja az igénylő tanúsítványát, a benne szereplő nyilvános kulccsal, mely egyben hitelesíti a titkos kulcsot az összetartozásuk kinyilvánításával, továbbá fogadja és feldolgozza a tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról, valamint a tanúsítványokkal kapcsolatos elektronikus információkat – beleértve az azok előállításával összefüggőket is – megőrzi a megőrzési idő végéig. Nem a hitelesítésszolgáltató, hanem az időbélyegzés-szolgáltató fogadja a beérkező időbélyegkéréseket és előállítja az időbélyeget, amit aláírásával lát el.

Az időbélyegző jogi értelemben egy a szolgáltató által kiállított, harmadik feleknek szóló olyan igazolás, amely egy elektronikus dokumentumnak az időbélyegzőn szereplő időpontban történő létezését igazolja. Az időbélyeg lehet minősített és nem minősített, a szolgáltató besorolásától függően. Az időbélyegző általában nem teljes bizonyító erejű magánokirat és nem teljes bizonyító erejű közokirat, hiszen az önmagában egy kivonat és egy időpont gép által digitálisan aláírva – ezért ez a gépi aláírás nem lehet minősített, és az sem fedi a valóságot, hogy az időbélyegző egy a kérelmező által kiállított harmadik feleknek szóló olyan igazolás, amely egy elektronikus dokumentumnak az időbélyegzőn szereplő időpontban történő létezését igazolja, mivel az igazolást nem a kérelmező állítja ki, csak a kérelmet.

Az aláírás-létrehozó adat aláírás-létrehozó eszközön való elhelyezése során a szolgáltató a szolgáltatás nyújtását követően biztosítja, hogy az igénybe vevő aláíráslétrehozó adatáról semmilyen másolatot ne tároljanak. Nem lehetséges tehát az aláíró kérésére kulcsletéti szolgáltatás keretében letétbe helyezni az aláíró kulcsot, mert az elhelyezés a generáló eszközből az aláírás-létrehozó eszközbe történik és nem képződik másolat a kulcsról alapesetben. Nem lehet továbbá biztonsági okokból sem minden aláírás-létrehozó adatot a szolgáltatónak tárolnia és archiválnia, mert a minősített aláírás-létrehozó adat tárolása tilos és műszakilag is kivitelezhetetlen. Így ebből következően az sem megoldható, hogy a szolgáltató átadhassa az aláíráslétrehozó adat másodpéldányát az erre kijelölt, hatósági jogkörrel felruházott nyomozati szervezetnek.

Az algoritmusok változhatnak, elévülhetnek. A kriptográfiai algoritmusok fejlődésének figyelemmel kísérése a szolgáltató jogszabályi kötelessége. Nem köteles az algoritmusok figyelésére az aláíró és az ellenőrző – de azért megteheti ezt saját belátása alapján.

Azokhoz az elektronikus aláírástermékekhez szükséges a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolás megléte, amelyekkel tanúsítvány és időbélyegző előállítást, valamint minősített elektronikus aláírás létrehozását végzik.

Nem kötelező igazolás létezése azokhoz az eszközökhöz, melyekkel fokozott biztonságú elektronikus aláírás és időbélyegző előállítását végzik, amelyekkel nem minősített elektronikus aláírás létrehozását végzik, vagy amelyekkel általában tanúsítvány, időbélyegző és elektronikus aláírás előállítását végzik, ha nincs ott a minősített megkötés.

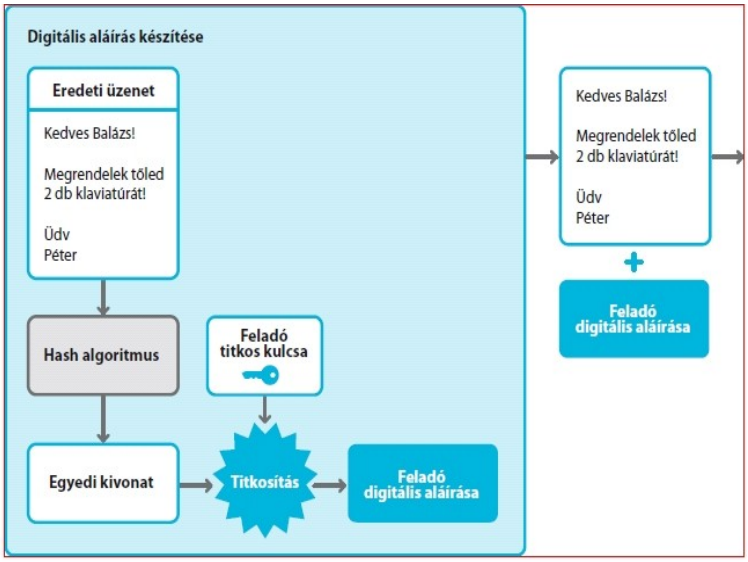
Az elektronikus aláírási termékekre vonatkozó terméktanúsítványokat tehát nem a hitelesítésszolgáltatók, nem a Nemzeti Hírközlési Hatóság, és nem is a szoftverfejlesztők, hanem az erre akkreditált tanúsításra jogosult szervezetek állítják ki, más szereplőnek erre nincs felhatalmazása.

Az időbélyegben nem kizárólag a pontos idő szerepel, mert az idő pontossága szükséges, de nem elégséges tulajdonság az időbélyegzéshez. Nem is a helyi idő szerepel itt, hiszen a helyi idők időzónánként különbözők. Itt fogalmilag meg kell különböztetni a pontos időt és hiteles időt, hiszen attól, hogy egy idő pontos, még nem lesz hiteles – fordítva viszont igaz, tehát az időbélyegben szereplő idő csak a hiteles idő lehet.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 60-72. oldal

2.2.2.1 Az elektronikus aláírás működése

Az elektronikus aláírás működésére az igaz, hogy minden digitális aláírás egyben elektronikus aláírás is. Ebből adódóan nem igaz az, hogy minden elektronikus aláírás egyben digitális aláírás is, mivel van olyan elektronikus aláírás, mely nem digitális, sőt az sem helyes, hogy minden digitális aláírás egyben nyilvános kulccsal történő titkosítás is, mivel az aláírás a titkos kulccsal történik. Ennek a fordítottja is téves állítás, hogy minden nyilvános kulccsal történő titkosítás egyben digitális aláírás is, ugyanezen ok miatt.



A digitális aláírás elkészítéséhez több lépés tartozik, mégpedig az aláírandó adatokból elkészül egy fix kivonat, a kivonat rejtjelzése a titkos kulcs segítségével megtörténik, és a digitális aláírás az üzenethez kapcsolódik, hiszen a digitális aláírás fizikai vagy logikai kapcsolása része az aláírás készítésének. Nem része a digitális aláírás készítési lépéseinek ellenben az, amikor a digitális aláírásból a nyilvános kulcs segítségével előáll az eredeti kivonat.

A digitális aláírás ellenőrzéséhez szintén több lépés tartozik, mégpedig az aláírt adatokból elkészül egy fix kivonat, a digitális aláírásból a nyilvános kulcs segítségével előáll az eredeti kivonat, valamint az eredeti kivonat és az új kivonat összehasonlítása megtörténik. Nem része viszont az ellenőrzés lépéseinek a kivonat rejtjelezése a titkos kulcs segítségével.

A digitális aláírás sikeres ellenőrzéséből következik, hogy az aláírt adatok ugyanazok, amit a küldő elküldött, az adatok aláírását a nyilvános kulcshoz tartozó titkos kulccsal végezték, valamint amennyiben a nyilvános kulcshoz létezik tanúsítvány, és tanúsítványban szereplő névhez tartozó személyt megbízható módon kapcsolták, akkor az a fizikai személy is ismert, aki aláírta az adatokat. Nem következik viszont az aláírás sikeres ellenőrzéséből, hogy az aláírást biztonságos aláírás-

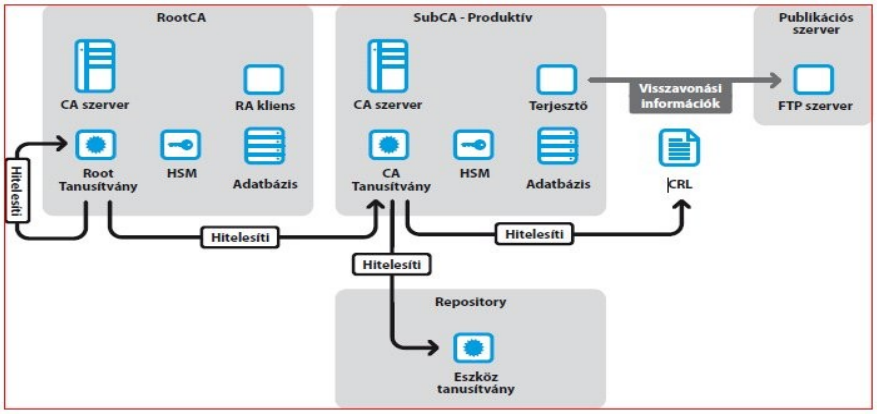
létrehozó eszközzel végezték el vagy sem.

A digitális aláírás ellenőrzése nem lehet attól sikertelen, ha az adatok a küldés során nem változtak meg, vagy ha az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták, és akkor sem, ha a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette a saját rendszerében, mert ezek szükséges feltételei egy sikeres ellenőrzésnek. Az ellenőrzés sikertelenségét viszont egyértelműen okozhatja az, ha a tanúsítvány lejárt.

Egy tanúsítvány megbízhatónak tekinthető akkor, ha ha a kibocsátó aláírása sértetlen. Nem attól függ a tanúsítvány megbízhatósága, ha azt igazolja, hogy az aláíró kulcs az adott személy birtokában van, mert a tanúsítvány direkt módon csak az ellenőrző kulcs aláíróhoz tartozását igazolja, és ezen keresztül – indirekt módon – igazolható az aláíró kulcs aláíróhoz való tartozása. Az sem jelent megbízhatóságot, ha a tanúsítványt egy működőképes vállalkozás állította ki, hiszen megbízható lehet nonprofit szervezet által kiállított tanúsítvány is. Továbbá nem attól megbízható egy tanúsítvány, ha az aláíró a titkos kulcs felett kizárólagosan rendelkezik – ez a fokozott biztonságú aláírás egyik követelménye.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 73-80. oldal

2.2.3 Publikus Kulcsú Infrastruktúra, PKI



2.2.3.1 *Kriptográfiai háttérismeretek*

A kétkulcsos titkosítást az is jellemzi, hogy a második kulcsból nem hozható létre az első kulcs. Nem igaz kétkulcsos titkosításra, hogy mind a két kulcs azonos, hiszen ha a két kulcs azonos, akkor egykulcsos a titkosítás. Az sem állja meg a helyét, hogy a második kulcsból létrehozható az első kulcs, mivel a két kulcs összefügg, de egymásból nem állíthatók elő és így az első kulcsból sem hozható létre a második kulcs.

A digitális aláírás során az aláíró a titkos kulcs birtokosa, a fogadó pedig a nyilvános kulcsot használja. Téves megfogalmazás az, hogy a fogadó a titkos kulcs birtokosa, az aláíró pedig a nyilvános kulcsot használja, mert ez titkosításnál van így. A digitális aláírás szűkített esetében a fogadó titkosít a titkos kulccsal, az aláíró pedig megoldja azt a nyilvános kulccsal, ez csak 50%-ban fedi le azt, hogy mi történik digitális aláírás során, ha van fogadó és aláíró, ráadásul ez a fogadó oldali aláírás metódusa, hiányzik az aláíró aláírásának metódusa. Digitális aláírás vonatkozásában

hibás az az állítás is mely szerint a titkos üzenetet csak az adott felhasználó képes elolvasni, mert az aláírás nem titkosítja az üzenetet.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 81-85. oldal

2.2.3.2 A PKI elemei

A PKI elemei közé soroljuk a hitelesítésszolgáltatót, a döntőbírót, az aláírás-létrehozó alkalmazást, de nem PKI elem a kötelezettségvállalás típusa. Ezt a felek szabadon állapítják meg maguk között.

A tanúsítványt igénylő személy azonosítását a regisztrációs felelős PKI elem végzi. Nem azonosít a tanúsítványkibocsátó, mivel a tanúsítványkibocsátó a tanúsítványok kibocsátását végzi, szintén nem azonosít az időbélyeg-szolgáltató, hiszen az időbélyegzés-szolgáltató az időbélyegek kibocsátását végzi és nem azonosít az archiválásszolgáltató sem, mert az archiválásszolgáltató a dokumentumok hosszú távú megőrzését végzi.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 85-94. oldal

2.2.4 Digitális tanúsítványok

2.2.4.1 A tanúsítványok fogalmi rendszerei

A gyökér tanúsítvány-kibocsátó feladata az alsóbb szintű tanúsítvány-kibocsátók hitelesítése. A gyökér tanúsítvány-kibocsátó általában nem ad ki felhasználói tanúsítványokat, a gyökér tanúsítvány-kibocsátó általában nem von vissza felhasználói tanúsítványokat, és a gyökér tanúsítvány-kibocsátó általában nem ad ki weboldal-hitelesítő tanúsítványokat sem.

A digitális tanúsítvány egy nyilvános kulcs és a hozzá tartozó titkos kulcs birtokosa adatainak összetartozását igazoló digitális objektum, melyet lehet digitális személyi igazolványnak is nevezni, azonban a digitális személyi igazolvány nem definíció, hanem allegória, hasonlóan a digitális útlevél fogalomhoz. Az persze igaz, hogy a hitelesítésszolgáltató a nyilvános kulcson elhelyezett aláírásával igazolja a nyilvános kulcshoz csatolt ellenőrző fizikai adatainak hitelességét, egy digitális tanúsítványban, de ez a működésének leírása, nem pedig a megnevezése.

Egy tanúsítvány a lejárati időpontjáig érvényes. Nem igaz az, hogy addig érvényes, amíg vissza nem vonják, mivel a visszavont tanúsítvány is lehet érvényes, de ekkor természetesen nem lesz aktív. Az sem helyes megfogalmazás, hogy addig érvényes, amíg fel nem függesztik, ugyanezen okok miatt. És persze a kezdeti időpontig sem lehet érvényes, hiszen a kezdeti időpont előtt nincs még tanúsítvány.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 95-105. oldal

2.2.4.2 A tanúsítványok használata

A tanúsítványigénylés során megadott adatokból nem szerepel a tanúsítványban a webcím, de szerepel a név vagy álnév, a lakcím – valamely formában, és az e-mail cím is általában része a tanúsítványban foglalt adatoknak.

A legbiztonságosabb regisztrációnak az számít, amikor a tanúsítvány igénylője személyes

megjelenéssel teszi ezt az azonosító okmányai bemutatásával együtt. Nem számít ennyire biztonságosnak, de esetenként megfelelő eljárás a faxon elküldött adatok és okmánymásolatokkal történő regisztráció, vagy a webes felületen kitöltött adatokkal való regisztrálás és a postán elküldött adatok és okmánymásolatok is lehetnek egy regisztrációs folyamat részei, de nem akkora biztonsági szinttel, mint a személyes megjelenés.

A tanúsítványigénylés során a telefonszám megadására nincs szükség, ezt pusztán kényelmi okok miatt szokták kérni, mivel az e-mail cím is tökéletesen megfelelő kommunikációs csatorna lehet. A tanúsítványra vonatkozó szabvány előírja a személyes adatok tanúsítványba foglalását, a jogszabályi előírások tartalmaznak azonosító okmányokra vonatkozó bemutatási kötelezettséget az igénylés során, valamint a privát és a nyilvános kulcspár közül a nyilvános kulcs az X 509 v3 tanúsítványoknak szintén kötelező eleme.

A tanúsítvány előállítás első lépése egy kulcspár generálása. Ezt követően lehetséges a kiállított tanúsítványt aláírni, a kész tanúsítványt közzétenni, és már létező tanúsítványt megújítani.

A nyilvános hitelesítésszolgáltatótól a közzétett tanúsítványokat bárki letöltheti. Nincs ilyen korlátozás, hogy csak a tulajdonosuk, vagy a tulajdonos munkáltatója – nem is biztos, hogy van ilyen, vagy az s hamis, hogy csak állami hatóságok érhetnék el a tanúsítványtárat.

Az aláíró magánkulcs szerepe a tanúsítvány igénylésekor az, hogy a nyilvános kulcs birtoklását igazolja. A tanúsítványkérelem kitöltésekor a nyilvános kulcs párja igazolja azt, hogy a kérelmező birtokában van a titkos kulcsnak, tehát jogos számára a tanúsítvány kiadása. A magánkulcsot a hitelesítésszolgáltató nem helyezheti be a tanúsítványba, hiszen a tanúsítványban sosem lehet magánkulcs. A magánkulcsot a hitelesítésszolgáltató nem teheti közzé a tanúsítványtárban, mivel a hitelesítésszolgáltató nem ismerheti meg és nem is tárolhatja a magánkulcsot, és hamis az is, hogy a hitelesítésszolgáltató biztonsági másolatot készít az aláíró magánkulcsról, mert a hitelesítésszolgáltató nem igényléskor készít másolatot a magánkulcsról, hanem maximum letéti szolgáltatás igénybe vételekor, amennyiben ez nem minősített aláírás-létrehozó adat.

Az aláírás-aktivizáló adattal a tulajdonos az aláírás megtételét engedélyezi, hagyja jóvá, aktivizálja a titkos kulcsot ezzel. Nem az aláírás aktivizáló adat szolgál a tanúsítványok megújítására, vagy a tanúsítványok visszavonására – a tanúsítványok visszavonásához a visszavonási jelszót használják. Továbbá nem helyes megállapítás az sem, hogy az aláírás-aktivizáló adat az aláírás ellenőrzésére használatos, mert az aláírás ellenőrzésére a nyilvános kulcs szolgál.

Elektronikusan általában nem szokták aláírni a vírusokat, rosszindulatú kódokat. Az elektronikus leveleket ezzel szemben aláírhatják, a szoftvereket általában ma már a fejlesztők aláírják, a statikus weboldalakat is egyre többször aláírják a sértetlenség védelmében (deface elleni feltáró védelem).

Tanúsítási láncnak nevezzük a tanúsítványkibocsátók felülről lefelé építkező aláírásait. Nem összetévesztendő ez a fogalom a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítésével – ilyen nincs is, az NHH nyilvántartásba vesz és ellenőriz. Nem lehetnek tanúsítási láncok a szoftvereken szereplő aláírások sem, mert a szoftver-aláírások a kód sértetlenségét igazoló digitális aláírások. Továbbá a tanúsítványtárban szereplő gyökér tanúsítványok sem tanúsítási láncok, mivel a gyökér tanúsítvány egy tanúsítási láncnak csak a legfelső eleme lehet.

A tanúsítási lánc tetején nem a felhasználó saját aláírása áll, a felhasználó saját aláírása a dokumentumokon szerepel. A tanúsítási lánc tetején nem is a tanúsítványtárat értjük, a tanúsítványtár nem része a tanúsítási láncnak. Nem is a felhasználói tanúsítványt kiadó hitelesítésszolgáltató aláírása lesz a lánc tetején, mivel a felhasználói tanúsítványt kiadó hitelesítésszolgáltatók általában a lánc középső részén helyezkednek el, a gyökér tanúsítvány és a felhasználói tanúsítvány között. A tanúsítási lánc tetején tehát általában – fa-struktúrában – a gyökér hitelesítésszolgáltató önaláírása szerepel.

Ha megváltozik a tanúsítványban szereplő e-mail cím, akkor a tanúsítványt vissza kell vonni, és újat kell igényelni. Nem lehetséges a tanúsítványt frissíteni e-mail cím megváltozásakor. A tanúsítványban nem lehet módosítani az e-mail címet sem, mivel ekkor annak digitális aláírása érvényét vesztené, és az sem fedi a valóságot, hogy az összes korábbi aláírást vissza kell vonni, mivel aláírást nem lehet visszavonni.

Emiatt nem meglepő, hogy nem szerepelnek a tanúsítványtárban a felhasználó aláírásai, csak a felhasználó saját tanúsítványai, mások tanúsítványai, és hitelesítésszolgáltatók tanúsítványai.

Az aláírás során használat adatok közül nem számít titkosnak maga a tanúsítvány. Ezzel szemben javasolt titokban tartani az aktivizáló adatot, mivel ez aktivizálja a titkos kulcsot, természetesen titokban kell tartani a magánkulcsot, és a visszavonási jelszót sem javasolt szétkürtölnie a tanúsítványbirtokosnak, hogy csak ő tudjon visszavonást kezdeményezni.

Hamis továbbá az alkalmazások tanúsítványtárával kapcsolatban az az állítás, hogy a tanúsítvány a rendszerek tanúsítványtáraiban felfüggeszthető. Ezzel kapcsolatos megengedett műveletek közé tartozik az, hogy a tanúsítvány a tanúsítványtárba bemásolható, a tanúsítvány a tanúsítványtárból törölhető, a tanúsítvány a tanúsítványtárból kimásolható (exportálható).

A felhasználói tanúsítványok aláírását nem a felhasználó a saját titkos kulcsával végzi, mivel a felhasználó a titkos kulcsával dokumentumokat ír alá, nem tanúsítványokat. A felhasználói tanúsítványok aláírását a hitelesítésszolgáltató a saját titkos kulcsával teszi meg, nem pedig a nyilvános kulcsával – a hitelesítésszolgáltató a nyilvános kulcsával nem ír alá semmit. Lehetnek a tanúsítványok önaláírtak, de nem hitelesítésszolgáltató által kibocsátott felhasználói tanúsítványok, legfeljebb a gyökértanúsítványok önaláírtak, a felhasználói tanúsítványokat az azt kibocsátó hitelesítésszolgáltató írja alá digitálisan.

A tanúsítványban általában nem szerepel a telefonszám, a születési idő, mivel ezek nem kötelező elemei az X 509 v3 tanúsítványnak, és nem szerepel a visszavonás ideje sem, mert a visszavonás ideje nem a tanúsítványban jelenik meg, hanem a visszavonási listában. Ha már mindenképpen kötelező adatok keresünk, akkor a munkahely neve kötelező eleme egy szervezeti szerepkör tanúsítványnak, a személyes kötelező adatokon kívül.

A tanúsítványt akkor lehet szabályosan megújítani, amikor a tanúsítvány érvényes. Nem célszerű megújítani felfüggesztett tanúsítványt, mert ezt vagy vissza lehet vonni, vagy újra érvénybe lehet helyezni és az érvénybe helyezés után lehet majd esetleg megújítani. Nem lehetséges továbbá visszavont tanúsítványt sem megújítani, mert visszavont tanúsítvánnyal semmit sem lehet csinálni annak lejártáig, és utána lejárt tanúsítványt sem lehetséges megújítani.

Nem megengedett a tanúsítvánnyal kapcsolatban az a művelet, amelyik a tanúsítványt módosítani akarja. Megengedett viszont az, hogy a tanúsítványt levélben elküldjék, a tanúsítványt visszavonják, és az is, hogy a tanúsítványt megújítsák – amennyiben ezt az egyéb feltételek lehetővé teszik.

Személyes megjelenés re van szükség a tanúsítvány-birtokos részéről minden esetben a minősített tanúsítvány igénylésekor. Nincs személyes megjelenéshez kötve a minősített tanúsítvány megújítása, mert minősített aláírással a minősített tanúsítvány megújítási kérelme beadható. Nem szükséges személyesen visszavonni a minősített tanúsítványt, hiszen a minősített tanúsítvány visszavonása írásban is kérelmezhető, illetve a minősített tanúsítvány felfüggesztésekor sem kötelező személyes megjelenés, mivel a minősített tanúsítvány felfüggesztése telefonon is kérhető.

A tanúsítvány elkészítésének nem része tanúsítvány tesztelése. A kulcsgenerálás, a tanúsítvány aláírása, a tanúsítvány közzététele, publikálása a tanúsítvány készítési folyamatnak a része lehet.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 105-119. oldal

2.2.4.3 Digitális tanúsítványok a mai rendszerekben

A telepített rendszerek tanúsítványtárolói vegyesen, minden megkülönböztetés nélkül tartalmazhatnak teljesen eltérő erősségű szolgáltatásokhoz kapcsolódó szolgáltatói tanúsítványokat. Nem helyes az, hogy kizárólag megbízható tanúsítványok lehetnek itt, mivel a megbízhatóság megítélése a felhasználótól is függ. Az sem igaz, hogy kizárólag a gyártó tanúsítványait tartalmazná, mert a tanúsítványtárolókban a gyártók mellett harmadik felek, személyek tanúsítványai is lehetnek. Továbbá az is hamis, hogy a telepített rendszerek tanúsítványtárolói vegyesen, minden megkülönböztetés nélkül tartalmazhatnak saját kibocsátású és használatú szolgáltatói tanúsítványokat, mert saját kibocsátású szolgáltatói tanúsítványokat a telepített rendszerek nem tartalmazhatnak.

A tanúsítványok a tanúsítványtárban szegmentálódnak, részekre tagolódnak mégpedig úgy, hogy valamennyi felhasználónak, szerviznek és magának a gépnek is van egy szegmense.

Nem fedi a valóságot az, hogy sehogy nem tagozódnak és minden tanúsítványt mindenki használhat, az sem, hogy felhasználók szerint vannak a tanúsítványok szegmentálva, mivel a felhasználóknak lehetnek saját tanúsítványtárolóik, de nem kizárólagosan és az is hamis, hogy az alkalmazások szerint vannak a tanúsítványok szegmentálva, habár az alkalmazásoknak lehetnek saját tanúsítványtárolóik, de itt sem kizárólagosan.

A felhasználói profilra azért kell ezek alapján vigyázni, mert a magánkulcsok és a tanúsítványok részei a felhasználói profilnak. Nem azért fenyegeti a biztonságot a profil nem megfelelő kezelése, mert a profil tartalmazza a bejelentkezési jelszavakat – a bejelentkezési jelszavakat nem tárolja a rendszer, vagy mert minden dokumentum a profilban van letárolva – a dokumentumok nemcsak a profilban lehetnek letárolva, valamint mert más gépek felhasználói is hozzáférhetnek a profilokhoz – az egyes felhasználói profilokhoz más felhasználók nem feltétlenül férhetnek hozzá.

Most már az is érthető, hogy a vándorló profil alkalmazása a tanúsítványok használata szempontjából miért jelent nagyobb kockázatot a helyi profil alkalmazásánál. Azért, mert a mobil felhasználók magánkulcsukat számos gépen otthagyhatják. Nem indoka a vándorló profil kockázatainak, hogy a vándorló profil nem biztonságos, mert önmagában a vándorló profil nem minősíthető nem biztonságosnak indoklás nélkül, vagy hogy a vándorló profil adatai mások számára is megismerhetők, mivel alapértelmezésben a vándorló profilok csak a tulajdonosaik számára ismerhetők meg, továbbá hogy a mobil felhasználók a tanúsítványaikat számos gépen otthagyhatják, hiszen a tanúsítványok nyugodtan otthagyhatók bárhol, az a cél, hogy terjedjenek.

Több különböző célú tanúsítvánnyal rendelkező felhasználónak aláírás előtt ki kell választania az adott aláíráshoz megfelelő tanúsítványt. Az alkalmazások nem képesek automatikusan kiválasztani a megfelelő tanúsítványt, mivel az alkalmazás alapértelmezés vagy beállítás szerint választhat csak tanúsítványt, ez nem feltétlenül egyezik meg az aláíráshoz megfelelő tanúsítvánnyal. Nem biztos, hogy mindig a legerősebb tanúsítvány a megfelelő, és az sem 100%, hogy az operációs rendszer automatikusan használni fogja a megfelelő tanúsítványt, hiszen az operációs rendszer alapértelmezés szerint választhat csak tanúsítványt, ez nem feltétlenül egyezik meg itt sem az aláíráshoz megfelelő tanúsítvánnyal.

Azt a tanúsítványt tekintjük hibásnak, amelyik más című webszerverre van kiállítva, mint amelyen található. Az nem hiba, ha egy tanúsítvány nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet, mivel álneves tanúsítványok létezése megengedett. Az sem hiba, ha egy tanúsítványt nem minősített hitelesítésszolgáltató adott ki, hiszen nem minősített hitelesítésszolgáltató tanúsítványa is elfogadott és az a tanúsítvány sem hibás, amelyikkel nem lehet aláírni, csak titkosítani, mert egy titkosító tanúsítvány használata rendeltetésszerű működésre utal.

A szoftvertanúsítványoknak az a célja, hogy garantálják az aláírt program származását és sértetlenségét. Nem tekinthető a szoftvertanúsítvány céljának az, hogy garantálják az aláírt szoftver sértetlenségét – a szoftver sértetlenségének garantálása szükséges, de nem elégséges célja a szoftvertanúsítványok alkalmazásának, és hogy igazolják az aláírt program helyességét – a programhelyesség bizonyítása nem hitelességi probléma, továbbá az sem cél, hogy igazolják a gyártó megbízhatóságát – a gyártók megbízhatósága nem a tanúsítványukból derül ki alapértelmezésben.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 119-131. oldal

2.2.4.4 Visszavonási listák, a visszavonási állapot ellenőrzése

Egy tanúsítvány visszavonásakor az tehetik még – a tanúsítvány visszavonási listában való szerepeltetésén túl, hogy a titkos kulcsot hordozó eszközt leselejtezik, amennyiben azt a felhasználó bevitte a szolgáltatóhoz. Nem jelenti a tanúsítvány visszavonását a titkos kulcs megsemmisítése, hiszen ha a titkos kulcs vagy az eszközök a birtokosnál vannak, nem mindig lehetséges azt megsemmisíteni. Ugyanígy nem lehetséges a tanúsítványt megsemmisíteni, hiszen nem lehet tudni, hogy éppen most hány helyen van a világban, a tanúsítvány sok helyen lehet, általában nem lehetséges mindegyiket – egyszerre vagy egymás után módszeresen – megsemmisíteni. Nem jelent visszavonást – de annál nagyobb butaságot – az, ha a titkos kulcsot vagy az ezt tartalmazó tanúsítványt felteszik egy nyilvános listára, ráadásul a titkos kulcs nincs a szolgáltató birtokában, nincs benne a tanúsítványban és nem is lehet egy biztonságos eszközről kinyerni.

Ha a kibocsátó hitelesítésszolgáltatónál katasztrófaesemény történik, attól ez a tény nem okozza egy tanúsítvány érvénytelenségét. Ellenben a tanúsítványlánc bármely eleméhez tartozó aláíró adat bizalmasságának sérülése esetében az összes ez alá tartozó tanúsítványt visszavonják, érvénytelenítik, valamint a tanúsítvány előállítása során alkalmazott aláírási algoritmus vagy kulcshossz gyengesége kiderülése esetében a tanúsítványt visszavonják, érvénytelenítik, továbbá szervezeti változás esetén is – mint például megváltozott hovatartozású vagy lejárt tanúsítvány – érvénytelenítik a tanúsítványt, míg a lejárt tanúsítvány automatikusan érvényét nem veszti.

A tanúsítvány visszavonási lista feltalálási helye nem a minősített aláírásban van, mivel a minősített aláírásnak nem kötelező tartalmaznia a tanúsítvány visszavonási lista helyét, nem is az

időbélyegben van, mert az időbélyegnek sem kötelező tartalmaznia a tanúsítvány visszavonási lista helyét, de nem is a fokozott biztonságú aláírásban van, hiszen a fokozott biztonságú aláírásnak szintén nem kötelező tartalmaznia a tanúsítvány visszavonási lista helyét. A tanúsítvány visszavonási lista feltalálási helye a tanúsítványban van rögzítve.

A kivárási idő alatt az aláírás és a következő visszavonási lista kibocsátása között eltelt időt kell érteni. Nem lehet kivárási idő az aláírás és a megelőző visszavonási lista kibocsátása között eltelt idő, mert a megelőző visszavonási lista semmilyen információt nem tartalmaz kivárási idővel kapcsolatban, továbbá nem lehet kivárási idő az aláírás és az ellenőrzés között eltelt idő sem, mivel ez nem a kivárási idő, hanem a felhasználási idő fogalma, de nem kivárási idő a két megismételt ellenőrzés között eltelt idő sem, hiszen a két megismételt ellenőrzés között eltelt időnek nincs köze a kivárási időhöz.

A tanúsítvány visszavonási lista meghatározott adatokat tartalmaz, ezek a sorszám, visszavonás ideje, visszavonás oka. A tulajdonos nincs benne a tanúsítvány visszavonási listában, hasonlóan a kibocsátó sincs benne a tanúsítvány visszavonási listában, hiszen minden hitelesítésszolgáltató a saját maga által kibocsátott tanúsítványokat vonhatja vissza.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 131-138. oldal

2.2.5 Az elektronikus aláírások osztályozása és készítése

2.2.5.1 Az elektronikus aláírások osztályozása

Az elektronikus aláírásokat típusaik szerint több osztályba lehet sorolni beágyazódás és készítési sorrend szerint. A „beágyazott aláírás” fogalma az, amikor az aláírás beágyazódik egy magasabb szintű aláírt egységbe. A beágyazott aláírás szűkített esete az, amikor az aláírás beágyazódik egy dokumentumba, mivel nemcsak dokumentumba lehetséges az aláírásnak beágyazódnia.

A „különálló aláírás” azt jelenti, amikor az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele.

A „beágyazódó aláírás” definícióját az írja le, amikor az aláírásba ágyazódnak bele az aláírandó információk.

A „párhuzamos aláírás” fogalmát az írja le, ahol a párhuzamos aláírás a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól.

Ha az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni, akkor „szekvenciális aláírás” definíciójáról beszélünk.

Az „ellenjegyző aláírás” létrehozásakor a párhuzamos aláírás a meglévők felett álló, azoktól függő módon arra rárakódó aláírás jön létre.

Az elektronikus aláírási irányelv előírásai közé tartozik az, hogy biztosítani kell, hogy az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként felhasználhatók legyenek bírósági eljárásokban, és hogy a minősített elektronikus aláírással aláírt elektronikus dokumentumoknak ugyanolyan joghatást kell biztosítani, mint a saját kezű aláírással ellátott papírdokumentumoknak, továbbá az is, hogy ha a minősített aláírás ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott. Nem tartozik az irányelv előírásai közé az, hogy biztosítani kell, hogy az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként felhasználhatók legyenek hatósági eljárásokban.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 138-153. oldal

2.2.5.2 Az elektronikus aláírások készítése

Az aláíró alkalmazások együttműködésére vonatkozóan az igaz, hogy az aláíró alkalmazások együttműködési teszteken bizonyítják együttműködési képességeiket. Ezeknek a teszteknek az alapján lehetséges együttműködő alkalmazásokra osztani a programokat. Nem lehetséges olyan általános megállapításokat tenni, hogy az aláíró alkalmazások nem működnek együtt egymással, hiszen van rá példa, hogy együttműködnek (ETSI PlugTest, MELASZ Ready 2.0), vagy hogy az aláíró alkalmazások mindegyike együttműködik a másikkal, mert a teljes kompatibilitást nem sikerült idáig megvalósítani és nem is biztos, hogy ez célkitűzés lenne.

Az sem igaz, hogy az aláíró alkalmazások együttműködési képességét a fejlesztőjük igazolja, mert a fejlesztő legfeljebb nyilatkozatot tud kiadni a termékének tulajdonságáról, igazolást általában független harmadik fél adhat.

Nem igaz továbbá az sem, hogy az aláíróprogramok mindegyike el tudja az összes XAdES szabványos aláírást készíteni, mivel nem kötelező minden szabványos aláírást támogatni, és a fejlesztők élnek is ezzel a lehetőséggel. Hamis az is, hogy az aláíróprogramok különböző, de szabványos aláírásokat tudnak készíteni, mivel az aláíróprogramok képesek lehetnek nem szabványos aláírásokat is létrehozni, ha éppen ez a készítő szándéka. Továbbá téves az az állítás is, hogy az aláíróprogramok mindegyike különböző aláírást készít, hiszen az egymással kompatibilis aláíróprogramok képesek ugyanolyan aláírást készíteni, ettől lesznek kompatibilisek egymással. Az természetesen igaz megállapítás minden programra, hogy az aláíróprogramok a fejlesztő szándéka szerinti aláírásokat tudnak készíteni, mely képességüket független szervezet tanúsíthatja.

Vannak olyan programok, melyekkel lehetséges és amelyekkel nem lehetséges digitális aláírásokat készíteni. Elsőre példa az MS Office, az OpenOffice és a legtöbb levelezőprogram, ezek a programok fel vannak készítve a digitális aláírások készítésére, a másodikra példa a böngészőprogramok, amelyek alapértelmezésben nincsenek digitális aláírás készítésére felkészítve.

Aláírási politikának nevezzük azt a szabályrendszert, mely biztosítja az egyes aláírások érvényességének technikai konzisztenciáját bármely környezetben. Az aláírás készítéséhez használt szabályrendszer része az aláírási politikának, de általában nem egyezik meg vele, hasonlóan az aláírás ellenőrzéséhez használt szabályrendszer is része az aláírási politikának, de általában szintén nem egyezik meg vele. Az aláírási politikában benne lehet az a szabályrendszer is, mely biztosítja az aláírás hosszú távú érvényességét, de általában ez sem egyezik meg vele teljes mértékben.

Az aláírási politika szabályrendszere biztosítja, hogy az aláírást követően nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége. Nem helyes az, hogy az aláírást megelőzően nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége, mert az aláírást megelőzően nem lehet az aláírásról semmit sem állítani, továbbá az sem, hogy az aláírás ellenőrzését követően nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége, hiszen az aláírási politika nem az aláírás ellenőrzése utáni időpontra vonatkozik, hanem kiterjed már az aláírás készítésére is. Az sem állja meg a helyét, mely szerint az aláírást követő CRL kibocsátása után nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége, mert az aláírást követő CRL-nek a kivárási idő meghatározásában van szerepe, ami pedig része az aláírási politikának.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 153-165. oldal

2.2.6 Kormányzati és hivatali ügyintézés elektronikusan

2.2.6.1 Az elektronikus aláírás és a kormányzás kapcsolata

Az Alapvető közszolgáltatások egységes listája szerint a legfejlettebb ügyintézési szint a személyes megjelenés nélküli teljes elektronikus ügyintézés. Az online információk letöltése a közigazgatási szolgáltatokról a legalapvetőbb szolgáltatás, az űrlapok letölthetősége az alapszintre ráépülő, de nem a legfejlettebb szolgáltatás, és a nyomtatványok online kitöltése, hitelesítése már fejlett, de szintén nem a legfejlettebbnek számító szolgáltatás.

A közigazgatási ügyekben az elektronikus ügyintézés nem kötelező, az ügyfél és az eljárásban részt vevő más személy nem kötelezhető arra, hogy eljárási cselekményeit elektronikus úton végezze, amennyiben törvény eltérően nem rendelkezik. A Ket. csak a lehetőséget teremti meg az elektronikus ügyintézésre, nem teszi azt kötelezővé, az sem fedi a valóságot, hogy általában kötelező, de az ügyfelet mindig megilleti a választás joga az elektronikus és a hagyományos ügyintézési forma között, de az igaz, hogy az ügyfelet általában megilleti a választás joga az elektronikus és a hagyományos ügyintézési forma között, de nem mindig – léteznek kizárások is. Nem helyes az sem, hogy nem kötelező a közigazgatási ügyekben az elektronikus ügyintézés, és nem is kötelezhető erre az ügyfél, hiszen jogszabály kötelezheti elektronikus ügyintézésre az ügyfeleket, ahogyan ez például az eBev szolgáltatások esetében történik.

Az elektronikus aláírás használatára Magyarországon számos működő példa van, ilyen például az elektronikus adóigazolások kiadása is. Nem igaz az, hogy még nem használják, hiszen már több helyen kötelezően használják, például a cégeljárásban is Magyarországon, valamint külföldön is több helyen működik már, például az Európai Bizottság dokumentumkezelésében, és hamis az, hogy nem nyilvános, mert nyilvános használatra példa a Magyar Közlöny elektronikusan közzétett példányainak aláírása is.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 167-189. oldal

2.2.6.2 Elektronikus aláírás és internetbanking

Ha jogszabály a szerződés érvényességéhez írásbeli alakot rendel, nem alkalmazható a legalább fokozott biztonságú elektronikus aláírással nem ellátott e-mail, vagy más szóval normál e-mail.

Alkalmazható továbbá a levélváltás, mert a levélváltás szerepel az írásbeliség alaki felsorolásában, a táviratváltás, mivel a táviratváltás is szerepel az írásbeliség alaki felsorolásában, és a távgépírón és telefax útján történt üzenetváltás is alkalmazható, hiszen a távgépírón és telefax útján történt üzenetváltás szintén szerepel az írásbeliség alaki felsorolásában.

Az elektronikus pénz készpénz átvétele vagy számlapénz átutalása ellenében kibocsátott elektronikus pénzeszközön tárolt pénzérték. Nem elektronikus pénz az elektronikusan aláírt pénzérték, a bankkártya segítségével felhasználható pénzérték – a bankkártya elektronikus fizetőeszköznek számít, és a hitelkártya által felhasználható pénzérték sem, mivel a hitelkártya is elektronikus fizetőeszköznek számít.

A pénzintézet a bankszámla feletti rendelkezési jog elektronikus gyakorlása esetén a hitelességet általában véve úgy biztosítja, hogy ellenőrzi a megbízáson feltüntetett aláírást (ideértve az elektronikus kódot is), hogy megegyezik-e a rendelkezésre jogosult hitelintézetnél bejelentett aláírásával (elektronikus kódjával). Nem lehet a hitelességet biztosítani általánosságban véve azzal hogy ellenőrzi a megbízáson lévő mobil aláírást, vagy ellenőrzi a megbízáson lévő digitális aláírást, avagy ellenőrzi, hogy a megbízást saját internetbanki szoftverrel készítették-e, mivel ezek egy lehetséges ellenőrzési módok, de nem kizárólagosak.

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 189-195. oldal

2.2.6.3 Az e-adózás és e-számla

Az elektronikus adóbevallás és adatszolgáltatás azt jelenti, hogy azt, hogy az adózó kötelező jelleggel elektronikus úton adja be adóbevallásait, adatszolgáltatásait. Lehetőség van ugyanakkor arra, hogy az adózó a saját elektronikus aláírásával aláírva küldje el az adóhatóságnak az összes szükséges bevallást, adatot, de az elektronikus aláírás ma még csak lehetőség a nyomtatványkitöltő programban, és nem kötelező. Az sem igaz, hogy az adózó választhatja az elektronikus adóbevallást az adózási folyamataiban, mert vannak olyan adózók, akiknek kötelező az eBev használata (pl. egyéni vállalkozók). Hamis az is, hogy az adózó e-mailben közli az adóhatósággal a bevallásait, adatait, mivel általában az adóhatóság e-mailben nem fogad bevallásokat és adatokat, csak a központi nyomtatványkitöltő programon és az Ügyfélkapun keresztül.

E-számlának nevezik azt az elektronikus adatot, mely vagy elektronikus adatcsererendszerben elektronikus adatként jön létre és továbbítódik, vagy olyan elektronikus dokumentumként áll elő, amely legalább fokozott biztonságú aláírással és időbélyeggel van ellátva. Nem tekinthető e-számlának a papír alapú számla beszkennelt változata, mert a papír alapú számla beszkennelt változatát digitalizált számlának nevezik. Nem e-számla az olyan elektronikus dokumentum sem, amely fokozott biztonságú aláírással és időbélyeggel van ellátva, mert ez a követelmény csak egy része az e-számlákkal szemben támasztottaknak, nem egyezik meg vele. És ugyanígy nem e-számla az e-mailben küldött számla, hiszen az e-mailben küldött számla csupán elektronikusan küldött számlának tekinthető, de még nem biztos, hogy megfelel az e-számla követelményeinek

ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 195-207. oldal

2.3 Gyakorlati feladatok megoldásai

Megjegyzés: az ECDL modultankönyvben a gyakorlatok úgy vannak megadva, hogy a felhasználó számára megfelelő szabadságot biztosítson az operációs rendszer, az irodai alkalmazás és az aláíró program megválasztásában, ezért emiatt a választási szabadság miatt több kérdésre egyértelmű válasz nem adható. Ebben a jegyzetben a feladatok szövegezése és egy-egy képernyőkép segíti a gyakorlat végrehajtását. A feladatok megegyeznek az ECDL modultankönyvben leírt gyakorlati feladatokkal.

2.3.1 Tanúsítványok adatainak elérése

A legfelső szintű tanúsítványtárból válassza ki az egyik szolgáltatói tanúsítványt az alábbiak közül, és gyűjtse ki a megadott mezőit!

a) Excentrikust Secure Server Certification Authority

b) Thawte Personal Freemail CA

c) Belgacom E-Trust Primary CA

Megoldás:

Adatok	Entrust.net Secure Server Certification Authority	Thawte Personal Freemail CA	Belgacom E-Trust Primary CA
I. Kibocsátó adatai	Entrust.net Secure Server Certification Authority Entrust.net www.entrust.net/CPS incorp. by ref. (limits liab.), (c) 1999 Entrust.net Limited US	Thawte Personal Freemail CA Thawte Consulting Certification Services Division Cape Town Western Cape ZA emailAddress: personal-freemail@thawte.com	0.9.2342.19200300.100.1.3 = info@e-trust.be CN = Belgacom E-Trust Primary CA OU = MTM O = Belgacom C = be
II. Tulajdonos adatai	Entrust.net Secure Server Certification Authority Entrust.net www.entrust.net/CPS incorp. by ref. (limits liab.), (c) 1999 Entrust.net Limited	Thawte Personal Freemail CA Thawte Consulting Certification Services Division Cape Town	0.9.2342.19200300.100.1.3 = info@e-trust.be CN = Belgacom E-Trust Primary CA OU = MTM O = Belgacom

Adatok	Entrust.net Secure Server Certification Authority	Thawte Personal Freemail CA	Belgacom E-Trust Primary CA
	US	Western Cape ZA emailAddress: personal-freemail@thawte.com	C = be
III. Érvényesség kezdete és	1999-05-25 16.09.40 GMT	1996-01-01 00.00.00 GMT	1998. november 4. 15:04:39
IV. Érvényesség vége, továbbá	2019-05-25 16.39.40 GMT	2020-12-31 23.59.59 GMT	2010. január 21. 15:04:39
V. Tanúsítvány aláíró algoritmus	sha1WithRSAEncryption	md5WithRSAEncryption	sha1RSA

2.3.2 Tanúsítványok igénylése, tanúsítványlánc

Igényeljen egy teszt aláíró-tanúsítványt valamelyik alábbi szolgáltatónál a saját e-mail címét hitelesítve, a saját webfelületen keresztül elérhető postaládája segítségével! Az igényelt teszt tanúsítvány hitelesítési láncát (issuer mezők tartalmával) írja le a gyökér tanúsítványtól kezdve a teszt tanúsítványig a Tanúsítványlánc vagy Tanúsítvány hierarchia ablakban megjelenő kibocsátói nevekkel!

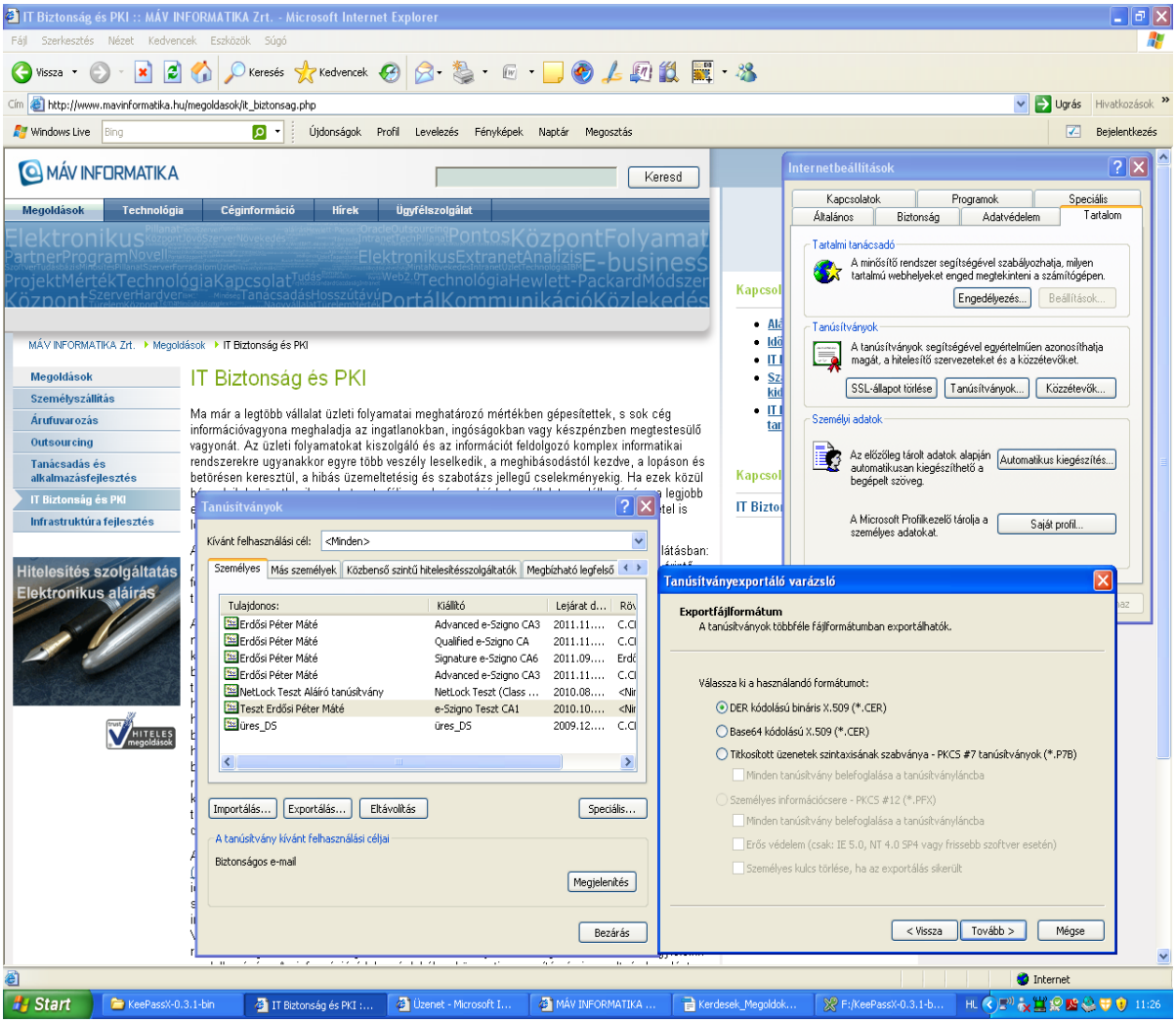
Megoldás: A következő táblázat a Szerző saját példáin keresztül mutatja be a megoldásokat.

Szolgáltató	Teszt Tanúsítvány	Közbülső CA tanúsítvány	Legfelső CA tanúsítvány
a) http://srv.e-szigno.hu/menu/index.php?lap=teszt_igenyles	Sorozatszám = 1.3.6.1.4.1.21528.2.2.99.3598 E = perdosi@chello.hu CN = Teszt Erdősi Péter Máté L = Budaörs C = HU	CN = e-Szigno Teszt CA1 OU = e-Szigno CA O = Microsec Ltd. L = Budapest C = HU	CN = Microsec e-Szigno Teszt Root CA OU = e-Szigno CA O = Microsec Ltd. L = Budapest C = HU
b) https://www.netlock.hu/index.cgi?lang=HU&tem=ANONYMOUS/online/online_indul.tem	E = perdosi@chello.hu CN = NetLock Teszt Aláíró tanúsítvány OU = -- O = -- L = -- S = -- C = --	nincs	E = info@netlock.hu CN = NetLock Teszt (Class T3) CA OU = Tanúsítványkiadók O = NetLock Kft. L = Budapest C = HU

2.3.3 Más szervezetek tanúsítványainak az exportálása

Válassza ki a személyes tanúsítványok közül a Teszt CA által Teszt névre kiállított tanúsítványt! A kiválasztott tanúsítványt mentse el (exportálja) X.509 DER formátumban \Desktop\Alairo1.xxx néven. (Vigyázat, Internet Explorerben .der, Firefoxban .cer kiterjesztéssel jön létre a DER formátum!)

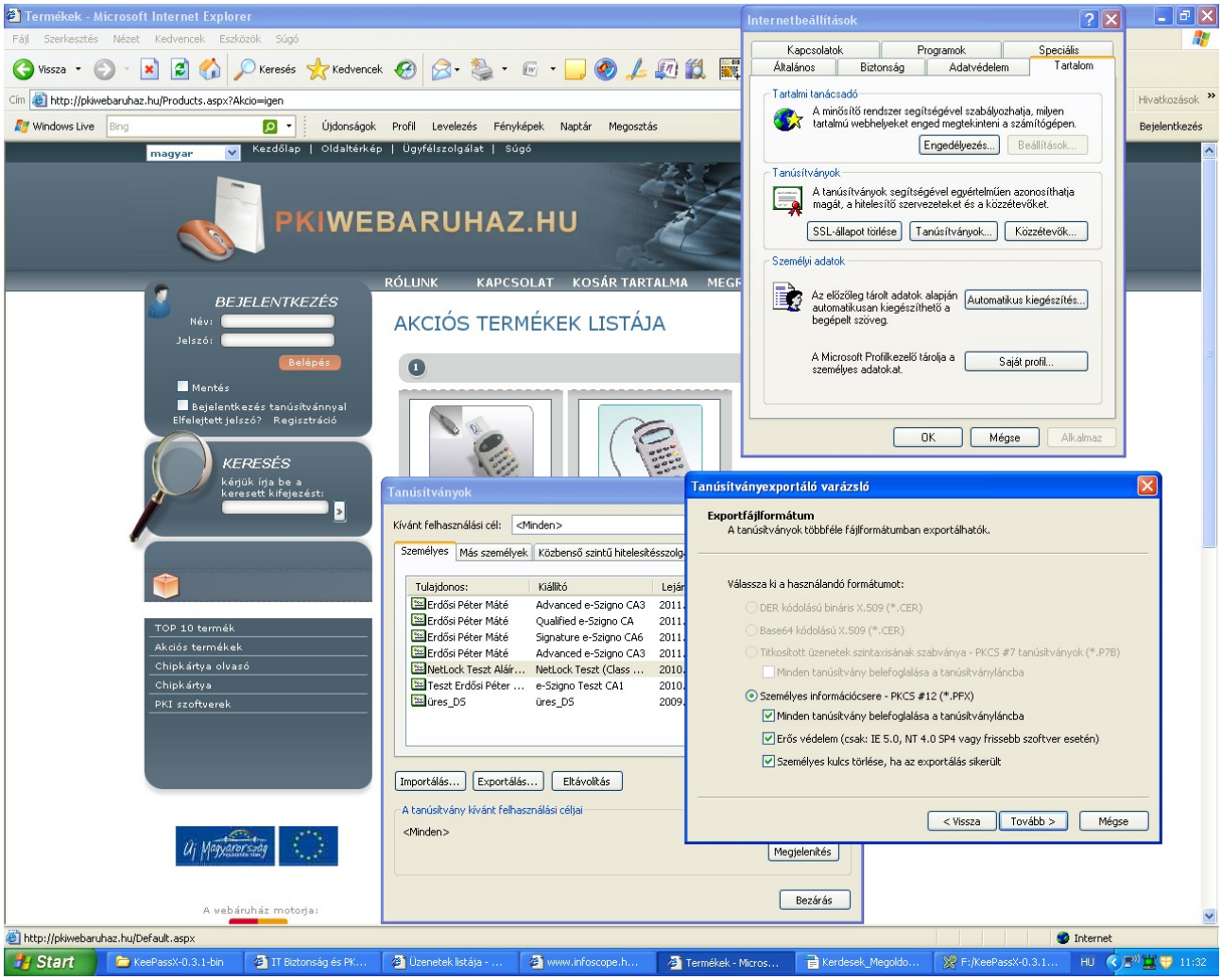
Megoldás:



2.3.4 Saját, személyes tanúsítvány exportálása titkos kulccsal

Válasszon ki a tanúsítványtárban egy személyes teszt vagy éles aláírói tanúsítványt! Exportálja a titkos kulccsal együtt (PKCS#12 kódolással), erős védelemmel és jelszóval a \Desktop könyvtárba Alairo2.pfx néven, 123456 jelszóval!

Megoldás:



2.3.5 Szolgáltatói tanúsítványok adatainak ellenőrzése

A közbülső szintű tanúsítványtárból válassza ki az egyik szolgáltatói tanúsítványt az alábbiak közül és ellenőrizze, hogy a tanúsítványban szereplő ujjlenyomat értéke megegyezik-e a szolgáltató honlapján közzétett tanúsítványban szereplő értékkel! (ha nem lennének a tanúsítványtárban, itt[2] elérheti ezeket.)

Megoldás:

Tanúsítvány	Ujjlenyomat-érték
a) Qualified e-Szigno CA (sorozatszám: 00 f2 67 09 3a 96 d0 be 9a 93 a4 cf ac f3 86 55 d8)	78 a6 88 93 d9 6a 7f 1e 20 5f b6 c6 09 70 99 a3 6e 02 17 9a
b) Advanced Class 3 e-Szigno CA 2009 (sorozatszám: 0e)	7c 28 e2 a0 be 01 53 c3 2a f0 4a 2d 8c 0d 1f c5 fe 80 12 24
c) Advanced e-Szigno CA2 (sorozatszám: 6a 8a 26 76 97 a5 7b f6 39 3b da 91 de 7b 6d 02)	93 f3 fb e3 d1 25 fe c5 61 df 93 6b b3 c1 fb 8c 5c 6f 2b 50

2 http://srv.e-szigno.hu/menu/index.php?lap=szolgaltatoi_tanusitvanyok

2.3.6 SSL-tanúsítványok adatainak ismerete

Válasszon ki egy SSL védelemmel rendelkező oldalt az alábbi listából! Ellenőrizze, hogy a webszerver tanúsítványát mely oldal védelmére állították ki! Állapítsa meg a tanúsítvány általános nevét (tulajdonosát, azaz a weboldal tanúsítványban szereplő címét) és a tanúsítvány kiállítóját, valamint sorozatszámát!

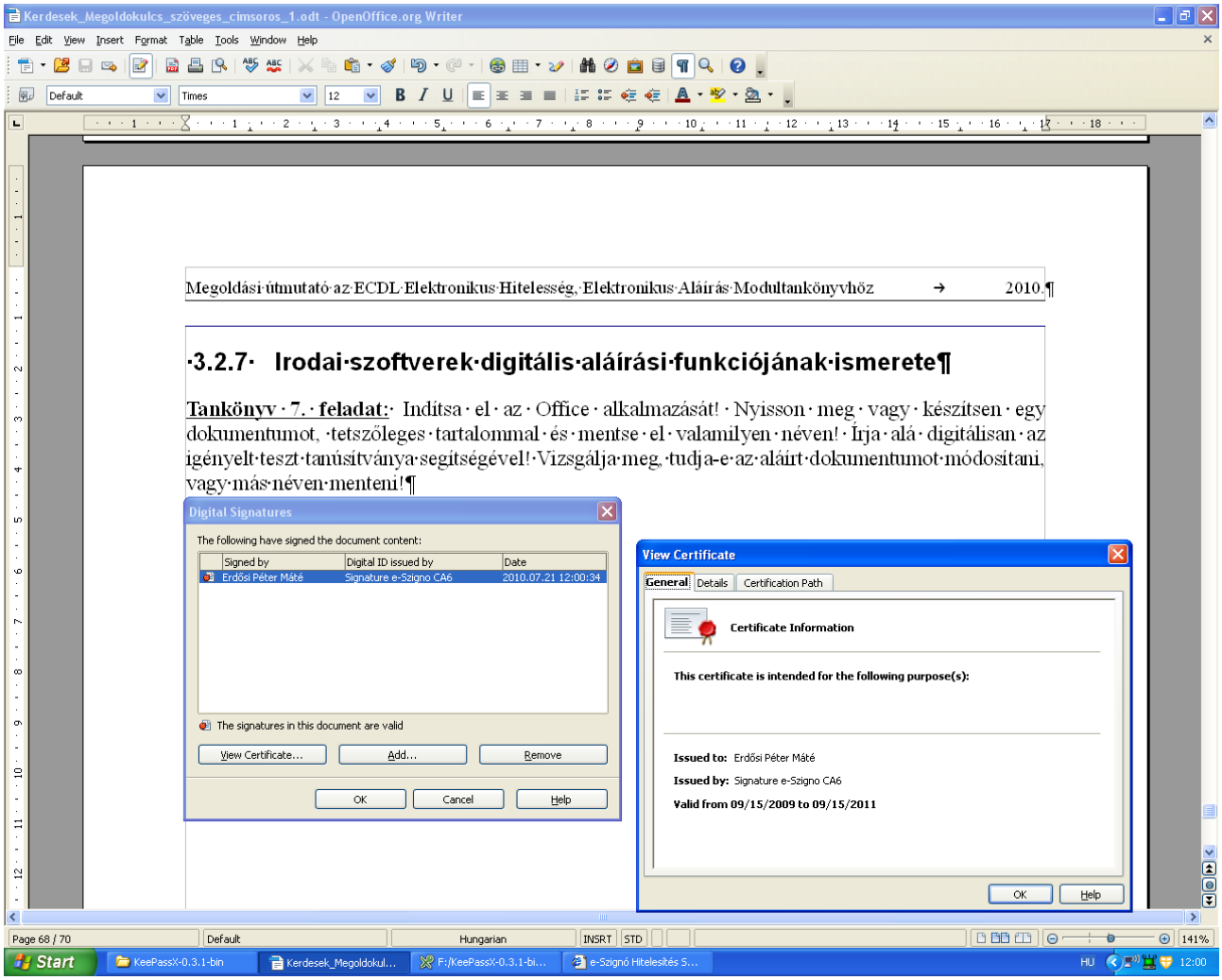
Megoldás:

Cím	Weboldal	Általános név	Kiállító	Sorozatszám
a) https://www.otpbank.hu/	www.otpbank.hu	www.otpbank.hu OTP Bank Nyrt. ITUIG Budapest Budapest HU Ismeretlen mezőnév1.3.6.1.4.1.311.60.2.1.3: HU Ismeretlen mezőnév2.5.4.15: V1.0, Clause 5.(b) serialNumber: CG 01-10-041585 postalCode: 1051 streetAddress: Nador utca 16.	VeriSign Class 3 Extended Validation SSL SGC CA VeriSign, Inc. VeriSign Trust Network, Terms of use at https://www.verisign.com/rpa (c)06 US	0x1C A1 23 2D 46 C1 48 CA CE 9D 67 EA 4A A4 D5 8D
b) http://www.magyarorszag.hu/	nincs SSL tanúsítvány!	nincs SSL tanúsítvány!	nincs SSL tanúsítvány!	nincs SSL tanúsítvány!
c) https://www.melasz.hu/	www.melasz.hu	www.melasz.hu Magyar Elektronikus Aláírás Szövetség Budapest HU	NetLock Uzleti (Class B) Tanusitvanykiado NetLock Halozatbiztonsagi Kft. Tanusitvanykiadok Budapest HU	0x15eb
d) https://www.magyarorszag.hu/	www.magyarorszag.hu	www.magyarorszag.hu Budapest, KOPINT-DATORG zRt. HU emailAddress: fabos.zsolt@kopdat.hu serialNumber: 1.3.6.1.4.1.21528.2.3.2.641	Advanced e-Szigno CA3 Microsec Ltd. e-Szigno CA Budapest HU	0x54b6

2.3.7 Irodai szoftverek digitális aláírási funkciójának ismerete

Indítsa el az Office alkalmazását! Nyisson meg vagy készítsen egy dokumentumot, tetszőleges tartalommal és mentse el valamilyen néven! Írja alá digitálisan az igényelt teszt tanúsítványa segítségével! Vizsgálja meg, tudja-e az aláírt dokumentumot módosítani, vagy más néven menteni!

Megoldás:



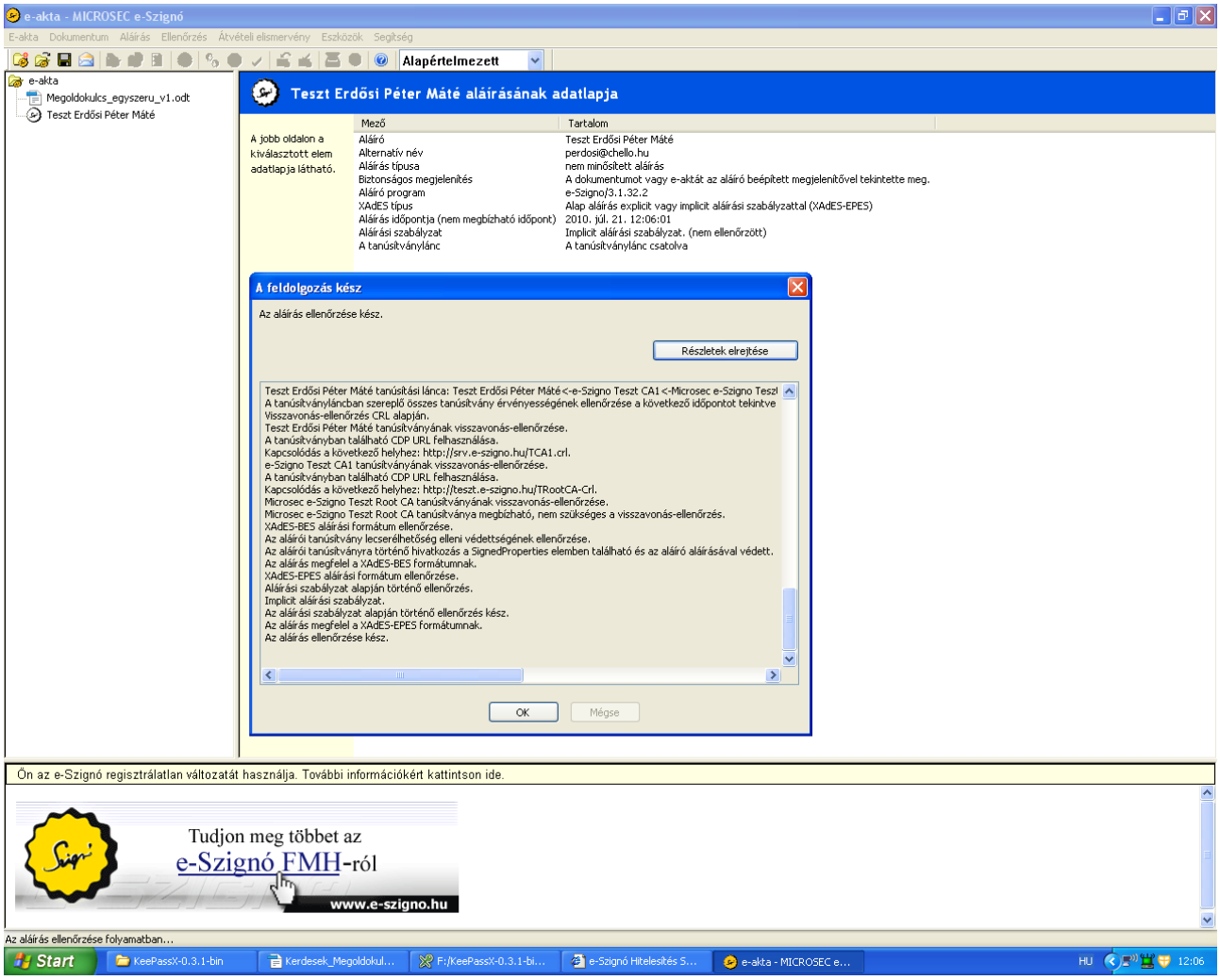
Megjegyzés: a különböző Office programok különböző módon reagálnak a digitálisan aláírt dokumentumok módosítási kísérleteire:

- tiltás, nem enged az aláírt dokumentumban módosítani az irodai programcsomag,
- megengedés, de ekkor figyelmeztet a digitális aláírás érvényességének elvesztésére.

2.3.8 Aláíró célszoftver használata

Indítsa el az aláírás-létrehozó alkalmazását! Az aláíró program tulajdonságától függően hozza létre az aláírandó dokumentumot (PDF, es3 vagy más formában)! Állítsa be az aláíró alkalmazást úgy, hogy XAdES-EPES aláírást készítsen el! Készítsen aláírást a teszt tanúsítványa segítségével az aláírandó dokumentumra! Mentést követően ellenőrizze le az aláírás érvényességét az alkalmazás megfelelő funkciója segítségével!

Megoldás: Az igazság az, hogy több lehetséges megoldás is lehet helyes erre a kérdésre, egy lehetséges megoldási utat mutat be az alábbi ábra.



ECDL Elektronikus Hitelesség, Elektronikus Aláírás Modultankönyv 231-232. oldal

3 Irodalomjegyzék

[1] Almási János – Balázs László – Erdősi Péter Máté – Kovács Árpád – Rátai Balázs – Schvéger Judit: ECDL Elektronikus Hitelesség, Elektronikus Aláírás modultankönyv; OTY StarTel Kft, 2010, ISBN: 978 963 06 8727 0
http://www.elektronikusalairaskonyv.hu

[2] W. Chan Kim – Renée Mauborgne: Kék óceán stratégia – a verseny nélküli piaci tér; Park könyvkiadó, 2008, ISBN: 978 963 530 800 2
http://www.blueoceanstrategy.com

[3] A következő 50 év – A tudomány a huszonegyedik század első felében (Szerkesztő: John Brockman); Vince kiadó, 2003, ISBN: 963 9323 95 0

[4] Radó István: Jólét növekedés nélkül?; Controlling Portál, M&C Hírlevelek 37. szám, 2010
http://www.controllingportal.hu/?doc=mc&mc=37

[5] ECDL – az informatikai írástudás nemzetközi bizonyítványa,
http://www.ecdl.hu/index.php?cim=nyitolap

[6] Magyar Elektronikus Aláírás Szövetség, MELASZ
http://www.melasz.hu

[7] MELASZ E-aláírás tudástár, 2010.
http://www.melasz.hu/lang-hu/e-alairas-tudastar