ECDL Magyarország

ECDL VIZSGAPÉLDATÁR

Elektronikus hitelesség, elektronikus aláírás

Syllabus 1.0

www.ecdl.hu

ELEKTRONIKUS HITELESSÉG, ELEKTRONIKUS ALÁÍRÁS

AZ ELEKTRONIKUS HITELESSÉG, ELEKTRONIKUS ALÁÍRÁS MODUL TARTALMA

A modul 30 feladatot tartalmaz. Közülük egyet kell megoldani. A feladatok megoldása során előre elkészített fájlokat kell használni, amelyeket a vizsgaközpont tesz elérhetővé a vizsgázó számára.

ÁLTALÁNOS IRÁNYELVEK A MEGOLDÁSHOZ ÉS A JAVÍTÁSHOZ

A vizsgán csak akkreditált szoftvert lehet használni, egyéb programok használata nem megengedett.

Az elméleti kérdések megválaszolására a vizsgaközpont által megadott válasz-fájlt kell használni.

A vizsgaközpont a feladatokban szereplő meghajtó-, könyvtár- (mappa-), fájlnév hivatkozásokat és súgótémákat másra cserélheti, amennyiben ezt a feladat megoldhatósága indokolttá teszi. Hasonlóan kell eljárni az adott környezetben nem értelmezhető megnevezésekkel is.

Nyomtatáskor az alapértelmezés szerinti, vagy a vizsgaközpont által megjelölt nyomtatót kell használni.

A központ fájlba történő nyomtatást is kérhet, ilyenkor a megadott helyen és névvel kell létrehozni a fájlt.

A feladatlapok végén olvasható „Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.” utasítást a vizsgaközpont érvényben hagyhatja vagy törölheti saját igényének, illetve a feladatlap javíthatóságának megfelelően.

Az egyes részfeladatokra 1 pont adható. A pontszámok nem oszthatók.

Az elérhető maximális pontszám: **32**.

A sikeres vizsgához a vizsgázónak legalább **24** pontot kell megszereznie.

A vizsgázó által megoldott vizsgafeladatot a vizsgáztató a nemzetközileg meghatározott irányelveknek megfelelően értékeli.

A vizsgán semmilyen segédeszköz nem használható.

A vizsgafeladat megoldásához a rendelkezésre álló idő 45 perc.

(Az „Általános irányelvek a megoldáshoz és a javításhoz” című részt a vizsga megkezdése előtt a vizsgázónak meg kell kapnia.)

1 Elméleti kérdések az ECDL vizsgához

A kérdések egy része a fogalmak helyes értésére kérdez rá, míg más kérdések az összefüggésekre kíváncsiak. A kérdések csoportosítása megfelel az Elektronikus hitelesség, elektronikus aláírás című könyv felépítésének, így az egyes kérdéscsoportokhoz szükséges fejezetek könnyen és azonnal kikereshetők.

1.1 Információ és Információs Társadalom

1.1.1 Az információ fontossága

1. Mi az információ általános definíciója?
    a. nincs az információnak általánosan elfogadott definíciója
    b. minden információ, ami továbbítható
    c. az információ értelmezett adat
    d. az információ ismeretterjesztés, tudásbővítés
2. Az információ mérhetőségére vonatkozó állítások közül melyik igaz az alábbiak közül?
    a. az információ nem mérhető
    b. az információ mérhetősége annak valószínűségével függ össze
    c. az információ átalakítható energiává
    d. az információ mérhetősége a közlés hosszával függ össze
3. Mi az információ mértékének alapegysége?
    a. az információ mértékének alapegysége az események valószínűsége
    b. az információ mértékének alapegysége egy kétkimenetelű esemény valószínűségi értéke, a bit
    c. az információ mértékének alapegysége az 1, 0 számjegyek segítségével előállítható számok
    d. az információ mértékének alapegysége a kilobájt
4. Miért számít kiemelt alakzatnak a „világkép” az információtörténetben?
    a. Mert magában foglalja az összes többi alakzatot
    b. Mert másként transzformálódik, mint a többi
    c. Mert nem transzformálódik
    d. Mert kívül esik az ember-központú vizsgálódási területein
5. Az alábbiak közül melyik kommunikációs problémával foglalkozik a híradástechnika?
    a. hogyan lehet a közlés jelentését a lehető legpontosabban átvinni
    b. hogyan lehet nagy hatótávolságú kommunikációs berendezéseket építeni
    c. milyen pontosan vihetők át az adott hírközlési szimbólumok
    d. a fogadó milyen cselekvésre lesz képes az üzenet hatására

6. A híradástechnikai rendszerek feladata
    a. egy adott, maximális hosszúságú közlés átvitele
    b. minden közlés átvitele
    c. a lehetséges közlések összességéből véletlenül kiválasztott bármelyik közlésnek az átvitele
    d. kommunikációs rendszerek folyamatos működtetése az egész világon
7. Az információtartalomra az alábbi állítás igaz:
    a. az információtartalom a közlés hosszától függ
    b. az információtartalom nem mérhető
    c. az információtartalom függ az üzenet jelentésétől
    d. egy „képtelenség” és egy „nagy jelentéstartalmú üzenet” információtartalma lehet teljesen egyenértékű
8. A redundancia-mentes üzenet
    a. a legtömörebb érthető formában tartalmazza a közlést
    b. értelmezhetetlen, érdektelen a fogadó számára
    c. ismétléseket is tartalmazhat
    d. csupán katonai célokra alkalmazható
9. Az információfizika szerint az információ
    a. csak az emberi agyban létezik
    b. embertől független fizikai mennyiség
    c. a hőmennyiség közlésével függ össze
    d. kémiai úton előállítható anyag
10. Az információ archiválása azt jelenti, hogy
    a. információ-objektumokat hoznak létre, és azt legalább 100 évig őrzik
    b. információ-objektumokat őriz meg értelmezési adatokkal együtt, technológiaváltástól, adatformátumoktól és felhasználói közösségek változásától független módon
    c. archiváló rendszereket kell kiépíteni és működtetni
    d. össze kell gyűjteni az információ-objektum mindenkori értelmezéséhez szükséges adatokat
11. A nyílt archiválási rendszerek
    a. csak fizikai objektumok megőrzésére vonatkozó szabályokat rögzítenek
    b. leírják az információ 100 évre történő megőrzési formáját
    c. információ-objektumokat őriznek meg hosszú távon
    d. összegyűjtik az adat-objektum értelmezéséhez szükséges információkat és azt őrzik hosszú távon

12. A biztonságtechnikai szabványok szerint az adat

    a. tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás illetve távközlés céljára

    b. értelmezett információ

    c. az információk megszerzésével, tárolásával és feldolgozásával összefüggő ismeretek összessége

    d. olyan ismeretanyagot jelent, amelyet bármilyen formában továbbítani lehet

13. Egy adott társadalomban olyan bonyolultságú rendszereket lehet működtetni,

    a. amelyek működtetését jogszabályok előírják

    b. amelyeket önkéntesen működtetnek társadalmi szervezetek

    c. amennyire szabad információ-áramlást biztosítanak a társadalmi folyamatok

    d. amelyek működési költségeit a társadalom finanszírozza

14. Az információs társadalom alapértéke

    a. az időérték

    b. a számítógép

    c. az anyagi javak

    d. az információ

15. Időérték alatt az információs társadalom azt érti,

    a. ami az anyagi javakat tartalmazza

    b. amit valamely idő alatt az ember az erőforrások céltudatos felhasználása révén hoz létre

    c. ami egységnyi idő alatt jön létre

    d. ami az összjólétet magasabb szintre emeli

16. Az oktatásban az információs társadalom az alábbiak közül preferálja

    a. a személyes jellegű oktatás bevezetését

    b. az oktatás és nevelés teljes számítógépesítését

    c. a környezetszennyezés visszaszorítását

    d. a tanultak mielőbbi termelésben történő hasznosítását

17. Az információs társadalomban az ember társadalomban elfoglalt helyének megőrzéséhez szükséges

    a. pénzügyi információ

    b. jótékony megnyilvánulások

    c. hiteles, pontos, aktuális információ

    d. társadalmi munkavégzés

18. A digitális világban

a. minden információforrás egyenértékű

b. ugyanúgy vannak ismeretközlő és ezekről tájékoztató dokumentumok, mint a papír alapú világban

c. a hiteles digitális információ 3 ezreléke a teljes információnak

d. egyik információ sem számít hitelesnek

19. A digitális világban igaz az, hogy

a. a digitális források elérhetőségét és változatlanságát minden esetben garantálják

b. a digitális források elérhetőségét és változatlanságát sok esetben nem garantálják

c. a digitális források elérhetőségét és változatlanságát legtöbbször garantálják

d. a digitális források elérhetőségét és változatlanságát soha nem garantálják

20. Az internetes kereső programok

a. eltérő keresési kérdésre ugyanazt az eredményt adják

b. ugyanarra a keresési kérdésre ugyanazt az eredményt adják

c. különböző eredményeket adhatnak ugyanarra a keresési kérdésre

d. összehangoltan működnek és kiegészítik egymás hiányosságait

1.1.2 Hiteles és nem hiteles információ

21. Melyik biztonsági követelmény foglalkozik a hitelességgel?

a. bizalmasság

b. sértetlenség

c. letagadhatatlanság

d. megbízhatóság

22. Melyik üzleti követelmény foglalkozik a hitelességgel?

a. minőség

b. megbízhatóság

c. biztonság

d. megfelelőség

23. Mikor lesz egy információ hiteles?

a. ha ismert a küldője és digitálisan is alá van írva

b. ha az eredeti állapotának megfelel és teljes

c. ha az információhoz csatolt digitális aláírás érvényes

d. ha az információhoz csatolt digitális aláírás érvényes és minősített tanúsítvány van hozzá

24. Mire vonatkozik a sértetlenség?

a. arra vonatkozik, hogy megakadályozza, a bizalmas információk engedély nélküli megismerését, vagyis fontos információkhoz illetéktelenek ne férjenek hozzá

b. az információknak az elvárások szerinti pontosságára, általános értelemben vett változatlanságára és teljességére, valamint az információk érvényességére és hitelességére vonatkozik

c. arra, hogy az információk a folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítják

d. arra, hogy a vezetés számára olyan időszerű és pontos információkat biztosítson, amelyek a folyamatok működtetéséhez, pénzügyi megbízhatóságához és irányításához szükségesek

25. Mi a hitelesség definíciója?

a. az állított azonosság megerősítése

b. valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti

c. a kibocsátónak állított forrás azonosságának ellenőrzése és a kibocsátott üzenet a tartalmának eredetisége megerősítetté vált

d. a felhasználói név és a hozzá tartozó jelszó megadása

26. Mi a hitelesítés definíciója?

a. a kibocsátónak állított forrás azonosságának ellenőrzése és a kibocsátott üzenet a tartalmának eredetisége megerősítetté vált

b. az állított azonosság megerősítése

c. a jelszó időnkénti biztonságos megváltoztatása

d. valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti

27. Mikor tekinthető valami hitelesnek?

a. ha az állított azonosság megerősítése megtörtént

b. ha a kibocsátónak állított forrás azonosságának ellenőrzése és a kibocsátott üzenet a tartalmának eredetisége megerősítetté vált

c. ha a felhasználói nevet és a jelszót a felhasználó sikeresen megadta

d. ha valaminek a forrása az, amit megjelöltek, és a tartalma eredeti

28. Milyen műszaki eljárások biztosíthatják az üzenetek tartalmának hitelességét?
    a. digitális aláírás és elektronikus aláírás
    b. digitális aláírás vagy az üzenethitelesítő kód
    c. elektronikus aláírás és üzenethitelesítő kód
    d. csak az elektronikus aláírás
29. Mi a feladata a digitális aláírásnak a biztonsági intézkedések között?
    a. megakadályozza a tartalom módosítását
    b. biztosítja a tartalom rendelkezésre állását
    c. biztosítja az aláíró személyének kilétét
    d. észlelhetővé teszi a tartalom megváltozását
30. Ha egy tartalomhoz kapcsolt digitális aláírás ellenőrzése fél évvel ezelőtt sikeres volt, akkor
    a. a tartalom ma is változatlan
    b. az aláíráshoz használt titkos kulcs most is érvényes
    c. a tartalom hiteles
    d. a tartalom a kibocsátás és a sikeres ellenőrzés között nem változott meg
31. Egy számítógépes bejelentkezés folyamatában
    a. a hitelesítés megelőzi az azonosítást
    b. a hitelesítés megelőzi a feljogosítást
    c. a feljogosítás megelőzi a hitelesítést
    d. a feljogosítás megelőzi az azonosítást
32. A letagadhatatlanság teljes körű biztosítása azt jelenti, hogy
    a. a tartalom kiállítója nem tudja a kiállítás tényét letagadni
    b. a tartalom fogadója nem tudja a fogadás tényét letagadni
    c. a tartalom kiállítója nem tudja a kiállítás tényét letagadni és a tartalom fogadója nem tudja a fogadás tényét letagadni
    d. a tartalom hitelességét nem lehet megváltoztatni
33. A digitális aláírás
    a. biztosítja az aláírás személyhez köthetőségét
    b. biztosítja a tartalom megváltoztathatatlanságát
    c. biztosítja az utólagos módosítások felderíthetőségét
    d. biztosítja az eredeti tartalom visszaállíthatóságát

34. Az üzenethitelesítő kód
    a. biztosítja az utólagos módosítások felderíthetőségét
    b. biztosítja a tartalom megváltoztathatatlanságát
    c. biztosítja az eredeti tartalom visszaállíthatóságát
    d. biztosítja a kód személyhez köthetőségét
35. A hitelesség megállapítása
    a. az adat élettartamának kezdetén szükséges
    b. az adat élettartamának végén szükséges
    c. az adat élettartama során folyamatosan szükséges
    d. az adat élettartama során periodikusan szükséges
36. A sértetlenség megállapítása
    a. elegendő a hitelesség megállapításához
    b. szükséges, de nem elégséges a hitelesség megállapításához
    c. lényegtelen a hitelesség megállapításához
    d. ugyanazt jelenti, mint a hitelesség megállapítása
37. A letagadhatatlanság megvalósítható
    a. szimmetrikus kriptográfiai eszközökkel
    b. aszimmetrikus kriptográfiai eszközökkel
    c. elektronikus aláírással
    d. üzenet-hitelesítő kóddal
38. Az adatsértetlenséget
    a. kizárólag digitális aláírással lehet biztosítani
    b. csak az adathoz csatolható további nyílt vagy rejtjelezett adatokkal lehet biztosítani
    c. csak blokk-ellenőrző kóddal lehet biztosítani
    d. kizárólag titkosítással lehet biztosítani
39. Az X.800 ajánlás a biztonsági szolgáltatások alatt a következőket definiálja:
    a. bizalmasság, sértetlenség, rendelkezésre állás, minőség, megbízhatóság
    b. biztonság, megbízhatóság, minőség, hatékonyság, hatásosság
    c. hitelesítés, hozzáférés-ellenőrzés, adattitkosság, adatsértetlenség, letagadhatatlanság
    d. bizalmasság, sértetlenség, letagadhatatlanság, hitelesség, rendelkezésre állás

40. A visszajátszás elleni védelmet az alábbi intézkedés valósítja meg:

a. digitális aláírás
b. üzenet-hitelesítő kód
c. időpecsét
d. hibajavító kód

1.2 Az elektronikus aláírás az Európai Információs Társadalomban

1.2.1 Az elektronikus aláírás fogalmai

41. Mi az elektronikus aláírás definíciója a 93/1999 irányelv szerint?

a. elektronikus aláírás minden olyan eljárás, amely hitelesítésre szolgál
b. elektronikus aláírás a hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
c. elektronikus aláírás a digitális aláírás és az üzenethitelesítő kód együttesen
d. elektronikus aláírás az aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás

42. Az elektronikus aláírás fogalmát

a. műszaki szabványok említik legelőször az aszimmetrikus kriptográfiai eljárások kapcsán
b. korai matematikai definíciója alapján határozták meg
c. a levelező rendszerek használták először jogi értelemben
d. európai irányelvi szinten használták először jogi eredetű fogalomként

43. Az elektronikus aláírás jogi szabályozására azért volt szükség,

a. mert az EU jogalkotási rendje előírta
b. hogy meghatározzák az elektronikus dokumentumok tekintetében a saját kezű aláírások szerepét betölteni képes megoldások és gyakorlatok körét
c. hogy egyszerűsítsék a műszaki aláírás fogalmakat
d. mert az elektronikus dokumentumok aláírása tömeges méretekben kezdett elterjedni

44. A beszkennelt kézi aláírás elektronikus dokumentum végére való beillesztése

a. egyáltalán nem alkalmas joghatás kiváltására
b. egyenértékű a kézírásos aláírással
c. minősített aláírásként funkcionál
d. alkalmas hitelesítési funkció betöltésére

45. Az aláírás létrehozó adat jogi értelemben

a. kizárólag PKI titkos kulcs lehet
b. egyszer használatos kód is lehet
c. kizárólag kriptográfiai algoritmussal együtt használható lehet
d. kizárólag az aláíróhoz köthető és alkalmas az aláíró azonosítására

46. Elektronikus aláírás létrehozásához
    a. nem szükséges tanúsítvány
    b. csak minősített tanúsítvány használható
    c. ajánlott legalább fokozott biztonságú tanúsítványt használni
    d. csak saját kibocsátású tanúsítvány alkalmazható
47. Melyik adat nem szerepel az ITU X.509 v3 tanúsítványokban?
    a. nyilvános kulcs
    b. titkos kulcs
    c. általános név
    d. kiállító neve
48. Az alábbiak közül melyik nem műszaki fogalom?
    a. digitális aláírás
    b. PKI titkos kulcs
    c. X.509 v3 tanúsítvány
    d. elektronikus aláírás
49. Az alábbiak közül melyik műszaki fogalom?
    a. fokozott biztonságú elektronikus aláírás
    b. minősített elektronikus aláírás
    c. teljes bizonyító erővel bíró aláírás
    d. digitális aláírás
50. A PKI magánkulcs és a PKI nyilvános kulcs
    a. teljesen függetlenek egymástól
    b. egyik a másikból előállítható
    c. matematikai értelemben tartoznak csupán össze
    d. csak aláírásra használhatóak
51. A titkos kulcsok generálására alkalmas intelligens kártyák
    a. ugyanolyanok, mint a többi kártya
    b. csak akkreditált szervezet általi bevizsgálás után használhatók
    c. kriptográfiai funkciókat megvalósító eszközökkel bővítettek
    d. mindegyike biztonságos aláírás létrehozó eszköz

52. A titkos kulcsok generálására alkalmas USB-eszközök (tokenek)

a. csak akkreditált szervezet általi bevizsgálás után használhatók

b. ugyanolyanok, mint a többi kártya

c. mindegyike biztonságos aláírás létrehozó eszköz

d. kriptográfiai funkciókat megvalósító eszközökkel bővítettek

1.2.2 Az EU céljai és az elektronikus aláírás jogi szabályozásának helyzete

53. Mi volt a célja az EU elektronikus aláírással kapcsolatos szabályozásának?

a. az elektronikus aláírás elterjesztése

b. az elektronikus aláírás elterjedését nehezítő szabályozási akadályok létrejöttének megakadályozása

c. az elektronikus aláírás elterjedését nehezítő szabályozási akadályok lebontása

d. egységes jogi fogalomrendszer elterjesztése

54. Mely témakörökre vonatkoznak a legfontosabb uniós szabályozások?

a. elektronikus számla, közbeszerzés, elektronikus és digitalizált dokumentumok használata

b. elektronikus vámárunyilatkozat, e-adózás és minősített tanúsítványok

c. minősített hitelesítésszolgáltatók és aláírási politikákra vonatkozó szabványok

d. alap, aláírási politikán alapuló, időbélyegzett, komplex és archív aláírások szabványosítása

55. Az elektronikus aláírásról szóló irányelv

a. kötelezi az európai polgárokat az abban foglaltak ismeretére

b. kötelezi az európai magán és jogi személyeket az abban foglaltak betartására

c. kötelezi a tagállamok kormányait az abban foglaltak ellenőrzésére

d. kötelezi a tagállamokat az abban foglalt tartalmú szabályozás kialakítására

56. A hitelesítésszolgáltatások szabad piacra lépésének követelménye azt jelenti, hogy

a. az uniós tagállamok kötelesek ellenőrzés nélkül megengedni az üzleti hitelesítésszolgáltatási tevékenységek nyújtását

b. az uniós tagállamok nem köthetik az üzleti hitelesítésszolgáltatási tevékenység megkezdését előzetes hatósági engedély megszerzéséhez

c. az uniós tagállamok nem írhatnak elő olyan szabályokat az üzleti hitelesítésszolgáltatási tevékenységek nyújtóinak, melyek a piaci tevékenységeiket korlátozzák

d. az uniós tagállamok nem köthetik az üzleti hitelesítésszolgáltatási tevékenység megkezdését és folytatását hatósági ellenőrzésekhez

57. Lehet-e kötelező az önkéntes akkreditáció egy hitelesítésszolgáltató számára?

a. nem, mivel ez önkéntes

b. igen, de csak kiemelt állami esetekben

c. igen, minden további nélkül

d. igen, de csak ha a szolgáltató kéri

58. Mire kötelezi az irányelv a tagállamokat a bírósági és hatósági eljárásokban?
    a. arra, hogy minden minősített aláírást el kell fogadniuk
    b. arra, hogy írásbeliséget kielégítő elektronikus aláírást kell alkalmazni
    c. arra, hogy az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként felhasználhatóak legyenek
    d. arra, hogy teljes bizonyító erőt rendeljenek az aláírásokhoz
59. Miért felelnek a minősített tanúsítványt kibocsátó szolgáltatók?
    a. az általuk kibocsátott minősített tanúsítványok segítségével készített aláírások valódiságáért
    b. az általuk kibocsátott minősített tanúsítványok segítségével készített aláírások ellenőrzéséért
    c. a minősített tanúsítványban szereplő adatok valótlanságából eredő károkért
    d. a minősített tanúsítványok elvesztéséből adódó károkért
60. Melyik eset nem vonatkozik egy unión kívüli szolgáltató által nyújtott szolgáltatások unión belüli elismerésére?
    a. a harmadik ország szolgáltatója teljesíti az irányelvben meghatározott követelményeket és egy uniós önkéntes akkreditációs folyamatban akkreditálják
    b. egy uniós országban működő szolgáltató felelősséget vállal a harmadik országban működő szolgáltató által kiállított minősített tanúsítványért
    c. 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
    d. a harmadik ország szolgáltatója felelősséget vállal az uniós országban működő szolgáltató által kiállított minősített tanúsítványért
61. Az elektronikus aláírási uniós irányelv tagállami implementációja
    a. kötelező minden tagállam számára, és meg is valósult
    b. nem kötelező minden tagállam számára, de megvalósult
    c. kötelező minden tagállam számára, de nem valósult meg
    d. nem kötelező minden tagállam számára, és nem is valósult meg
62. A magyar elektronikus aláírási fogalmi szabályozás jogszabály struktúrában elfoglalt helye
    a. miniszteri rendeletek szintjén van
    b. Kormányrendelet szintű
    c. törvényi és végrehajtási rendelet szintű
    d. Alkotmányban foglalt
63. Az elektronikus aláírások jogi elismerésével kapcsolatos fontosabb előírásokat
    a. Kormányrendelet tartalmazza
    b. az elektronikus aláírási törvény tartalmazza
    c. az Alkotmány rögzíti
    d. miniszteri rendeletek írják le

64. Elektronikus aláírásokkal kapcsolatos szolgáltatások az elektronikus aláírás törvény szerint
    a. időbélyegzés, aláíráslétrehozó adat elhelyezése, archiválásszolgáltatás
    b. hitelesítésszolgáltatás, időbélyegzés, archiválás szolgáltatás
    c. hitelesítésszolgáltatás, időbélyegzés, aláíráslétrehozó adat elhelyezése, archiválásszolgáltatás
    d. regisztráció, tanúsítvány kibocsátás, nyilvántartás, módosítás, közzététel, állapotinformáció szolgáltatás
65. A hitelesítésszolgáltatás keretében az elektronikus aláírás törvény szerint a hitelesítésszolgáltató az alábbiakat végzi:
    a. regisztráció, tanúsítványkibocsátás, nyilvántartás, módosítás, közzététel, állapotinformáció szolgáltatás
    b. hitelesítésszolgáltatás, időbélyegzés, aláírás-létrehozó adat elhelyezés, archiválásszolgáltatás
    c. időbélyegzés, aláírás-létrehozó adat elhelyezés, archiválásszolgáltatás
    d. hitelesítésszolgáltatás, időbélyegzés, archiválásszolgáltatás
66. Az elektronikus aláírással kapcsolatos szolgáltatásokat végző szolgáltatókra az alábbi állítások közül melyik igaz:
    a. a minősített és nem minősített szolgáltatókra ugyanazok a követelmények vonatkoznak
    b. a minősített szolgáltatókra gyengébb követelmények vonatkoznak, mint a nem minősített szolgáltatókra
    c. a minősített szolgáltatókra erősebb követelmények vonatkoznak, mint a nem minősített szolgáltatókra
    d. a minősített és nem minősített szolgáltatókra nincsenek előírt követelmények
67. Az alábbiak közül melyiket nem végzi egy hitelesítésszolgáltató:
    a. azonosítja az igénylő személyét, majd a saját elektronikus aláírásával aláírt tanúsítvánnyal hitelesíti az igénylő elektronikus aláírását
    b. fogadja és feldolgozza a tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról
    c. fogadja a beérkező időbélyeg-kéréseket és előállítja az időbélyeget, amit aláírásával lát el
    d. a tanúsítványokkal kapcsolatos elektronikus információkat - beleértve az azok előállításával összefüggőket is - megőrzi
68. Az időbélyegző jogi értelemben
    a. teljes bizonyító erejű magánokirat
    b. egy a szolgáltató által kiállított, harmadik feleknek szóló olyan igazolás, amely egy elektronikus dokumentumnak az időbélyegzőn szereplő időpontban történő létezését igazolja
    c. teljes bizonyító erejű közokirat
    d. egy a kérelmező által kiállított harmadik feleknek szóló olyan igazolás, amely egy elektronikus dokumentumnak az időbélyegzőn szereplő időpontban történő létezését igazolja

69. Az aláírás-létrehozó adat aláírás-létrehozó eszközön való elhelyezése során a szolgáltató
    a. az aláíró kérésére kulcsletéti szolgáltatás keretében letétbe helyezheti az aláíró kulcsot
    b. biztonsági okokból minden aláírás-létrehozó adatot köteles tárolni és archiválni
    c. a szolgáltatás nyújtását követően biztosítania kell, hogy az igénybe vevő aláírás-létrehozó adatáról semmilyen másolatot ne tároljanak
    d. köteles azonnal átadni annak másodpéldányát az erre kijelölt, hatósági jogkörrel felruházott nyomozati szervezetnek
70. Kinek jogszabályi kötelessége figyelemmel kísérnie a kriptográfiai algoritmusok fejlődését?
    a. a szolgáltatónak
    b. az aláírónak
    c. az ellenőrzőnek
    d. az aláírónak és ellenőrzőnek
71. Mely elektronikus aláírástermékekhez szükséges a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolás?
    a. amelyekkel fokozott biztonságú elektronikus aláírás és időbélyegző előállítását végzik
    b. amelyekkel tanúsítvány és időbélyegző előállítást, valamint minősített elektronikus aláírás létrehozását végzik
    c. amelyekkel minősített és nem minősített elektronikus aláírás létrehozását végzik
    d. amelyekkel tanúsítvány, időbélyegző és elektronikus aláírás előállítását végzik
72. Mely elektronikus aláírási termékekhez nem szükséges a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolás?
    a. amelyekkel tanúsítvány előállítását végzik
    b. amelyekkel időbélyegző előállítását végzik
    c. amelyekkel fokozott biztonságú elektronikus aláírás létrehozását végzik
    d. amelyekkel minősített elektronikus aláírás létrehozását végzik
73. Az elektronikus aláírási termékekre vonatkozó terméktanúsítványokat
    a. a hitelesítésszolgáltatók állítják ki
    b. a Nemzeti Hírközlési Hatóság állítja ki
    c. tanúsításra jogosult szervezetek állítják ki
    d. a szoftverfejlesztők állítják ki
74. Az időbélyegben a következő idő szerepel:
    a. pontos idő
    b. hiteles idő
    c. helyi idő
    d. pontos és hiteles idő

1.2.3 Az elektronikus aláírás működése

75. Melyik állítás az igaz az alábbiak közül?

a. minden elektronikus aláírás egyben digitális aláírás is

b. minden digitális aláírás egyben elektronikus aláírás is

c. minden digitális aláírás egyben nyilvános kulccsal történő titkosítás is

d. minden nyilvános kulccsal történő titkosítás egyben digitális aláírás is

76. Melyik lépés nem tartozik a digitális aláírás elkészítéséhez?

a. az aláírandó adatokból elkészül egy fix kivonat

b. a kivonat rejtjelzése a titkos kulcs segítségével

c. a digitális aláírásból a nyilvános kulcs segítségével előáll az eredeti kivonat

d. a digitális aláírás az üzenethez kapcsolódik

77. Melyik lépés nem tartozik a digitális aláírás ellenőrzéséhez?

a. az aláírt adatokból elkészül egy fix kivonat

b. a digitális aláírásból a nyilvános kulcs segítségével előáll az eredeti kivonat

c. az eredeti kivonat és az új kivonat összehasonlítása

d. a kivonat rejtjelezése a titkos kulcs segítségével

78. A digitális aláírás sikeres ellenőrzéséből mely állítás nem következik?

a. az aláírt adatok ugyanazok, amit a küldő elküldött

b. az aláírást biztonságos aláírás-létrehozó eszközzel végezték

c. az adatok aláírását a nyilvános kulcshoz tartozó titkos kulccsal végezték

d. 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

79. A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

a. az adatok a küldés során nem változtak meg

b. a tanúsítvány lejárt

c. az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták

d. a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette a saját rendszerében

80. Mikor tekinthető egy tanúsítvány megbízhatónak?

a. ha a kibocsátó aláírása sértetlen

b. ha azt igazolja, hogy az aláíró kulcs az adott személy birtokában van

c. ha azt egy működőképes vállalkozás állította ki

d. ha az aláíró a titkos kulcs felett kizárólagosan rendelkezik

1.3 Publikus Kulcsú Infrastruktúra, PKI

1.3.1 Kriptográfiai háttérismeretek

81. Mi jellemzi a kétkulcsos titkosítást?

a. mind a két kulcs azonos
b. a második kulcsból létrehozató az első kulcs
c. az első kulcsból létrehozható a második kulcs
d. a második kulcsból nem hozható létre az első kulcs

82. A digitális aláírás során

a. az aláíró a titkos kulcs birtokosa, a fogadó pedig a nyilvános kulcsot használja
b. a fogadó a titkos kulcs birtokosa, az aláíró pedig a nyilvános kulcsot használja
c. a fogadó titkosít a titkos kulccsal, az aláíró pedig megoldja azt a nyilvános kulccsal
d. a titkos üzenetet csak az adott felhasználó képes elolvasni

1.3.2 A PKI elemei

83. Melyik elem nem a PKI eleme?

a. hitelesítésszolgáltató
b. döntőbíró
c. aláírás-létrehozó alkalmazás
d. kötelezettség-vállalás típus

84. Melyik PKI elem szolgál a tanúsítvány igénylő azonosítására?

a. tanúsítvány-kibocsátó
b. időbélyeg-szolgáltató
c. regisztrációs felelős
d. archiválás szolgáltató

1.4 Digitális tanúsítványok

1.4.1 A tanúsítványok fogalmi rendszerei

85. Mi a gyökér tanúsítvány-kibocsátó feladata?

a. a végfelhasználói tanúsítványok kiadása
b. a végfelhasználói tanúsítványok visszavonása
c. az alsóbb szintű tanúsítvány-kibocsátók hitelesítése
d. weboldalak hitelesítése

86. Mi a digitális tanúsítvány?

a. digitális személyi igazolvány

b. digitális útlevél

c. egy nyilvános kulcs és a hozzá tartozó titkos kulcs birtokosa adatainak összetartozását igazoló digitális objektum

d. a hitelesítésszolgáltató a nyilvános kulcson elhelyezett aláírásával igazolja a nyilvános kulcshoz csatolt ellenőrző fizikai adatainak hitelességét, egy digitális tanúsítványban

87. Meddig érvényes egy tanúsítvány?

a. amíg vissza nem vonják

b. amíg fel nem függesztik

c. a lejárati időpontig

d. a kezdeti időpontig

1.4.2 A tanúsítványok használata

88. A tanúsítványigénylés során megadott alábbi adatokból mi nem szerepel a tanúsítványban?

a. név

b. lakcím

c. webcím

d. email cím

89. Melyik a legbiztonságosabb regisztráció az alábbiak közül?

a. faxon elküldött adatok és okmánymásolatok

b. webes felületen kitöltött adatok

c. személyes megjelenés azonosító okmányokkal

d. postán elküldött adatok és okmánymásolatok

90. A tanúsítványigénylés során az alábbiak közül mire nincs szükség?

a. személyes adatok

b. telefonszám

c. azonosító okmányok

d. privát és nyilvános kulcspár

91. Mi a tanúsítvány előállítás első lépése az alábbiak közül?

a. tanúsítvány megújítása

b. tanúsítvány aláírása

c. kulcspár generálása

d. tanúsítvány közzététele

92. Ki töltheti le a tanúsítványokat a hitelesítésszolgáltatótól?

a. csak a tulajdonosuk
b. a tulajdonos munkáltatója
c. bárki
d. csak állami hatóságok

93. Mi az aláíró magánkulcs szerepe a tanúsítvány igénylésekor?

a. a hitelesítésszolgáltató behelyezi a tanúsítványba
b. a nyilvános kulcs birtoklását igazolja
c. a hitelesítésszolgáltató közzéteszi a tanúsítványtárban
d. a hitelesítésszolgáltató biztonsági másolatot készít róla

94. Mire való az aláírás aktivizáló adat?

a. a tanúsítványok megújítására
b. a tanúsítványok visszavonására
c. az aláírás megtételére
d. az aláírás ellenőrzésére

95. Mit nem írnak alá általában elektronikusan az alábbiak közül?

a. elektronikus levelek
b. szoftverek
c. vírusok
d. weboldalak

96. Mi az a tanúsítási lánc?

a. a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
b. a szoftvereken szereplő aláírások
c. a tanúsítványtárban szereplő gyökér tanúsítványok
d. a tanúsítvány-kibocsátók felülről lefelé építkező aláírásai

97. Mi áll a tanúsítási lánc tetején?

a. a felhasználó saját aláírása
b. a gyökér hitelesítésszolgáltató önaláírása
c. a felhasználói tanúsítványt kiadó hitelesítésszolgáltató aláírása
d. a tanúsítványtár

98. Mi a teendő, ha megváltozik a tanúsítványban szereplő email cím?

a. a tanúsítványt vissza kell vonni, és újat kell igényelni
b. a tanúsítványt frissíteni kell
c. módosítani kell a tanúsítványban az email címet
d. az összes korábbi aláírást vissza kell vonni

99. Mi nem szerepel a tanúsítványtárban az alábbiak közül?

a. a felhasználó saját tanúsítványai
b. mások tanúsítványai
c. a felhasználó aláírásai
d. hitelesítésszolgáltatók tanúsítványai

100. Melyik adat nem titkos az alábbiak közül?

a. az aktivizáló adat
b. a magánkulcs
c. a tanúsítvány
d. a visszavonási jelszó

101. Melyik állítás hamis az alkalmazások tanúsítványtárával kapcsolatban?

a. a tanúsítvány a tanúsítványtárba bemásolható
b. a tanúsítvány a tanúsítványtárban felfüggeszthető
c. a tanúsítvány a tanúsítványtárból törölhető
d. a tanúsítvány a tanúsítványtárból kimásolható

102. Ki írja alá a felhasználói tanúsítványt?

a. a felhasználó a saját titkos kulcsával
b. a hitelesítésszolgáltató a saját titkos kulcsával
c. a hitelesítésszolgáltató a nyilvános kulcsával
d. a tanúsítványok önaláírtak

103. Melyik adat szerepel a tanúsítványban az alábbiak közül?

a. munkahely neve
b. telefonszám
c. születési idő
d. visszavonás ideje

104. Melyik esetben lehet a tanúsítványt megújítani?
   a. amikor a tanúsítvány fel van függesztve
   b. amikor a tanúsítvány vissza van vonva
   c. amikor a tanúsítvány érvényes
   d. amikor a tanúsítvány lejárt

105. Melyik művelet nem megengedett a tanúsítvánnyal kapcsolatban?
   a. a tanúsítvány levélben elküldhető
   b. a tanúsítvány visszavonható
   c. a tanúsítvány módosítható
   d. a tanúsítvány megújítható

106. Mikor szükséges a személyes megjelenés?
   a. a minősített tanúsítvány megújításakor
   b. a minősített tanúsítvány igénylésekor
   c. a minősített tanúsítvány visszavonásakor
   d. a minősített tanúsítvány felfüggesztésekor

107. Melyik lépés nem része a tanúsítvány elkészítésének?
   a. kulcsgenerálás
   b. tanúsítvány közzététele
   c. tanúsítvány aláírása
   d. tanúsítvány tesztelése

1.4.3 Digitális tanúsítványok a mai rendszerekben

108. Milyen tanúsítványokat tartalmazhatnak a telepített rendszerek tanúsítvány-tárolói?
   a. kizárólag megbízható tanúsítványokat
   b. kizárólag a gyártó tanúsítványait
   c. vegyesen, minden megkülönböztetés nélkül tartalmazhatnak teljesen eltérő erősségű szolgáltatásokhoz kapcsolódó szolgáltatói tanúsítványokat
   d. vegyesen, minden megkülönböztetés nélkül tartalmazhatnak saját kibocsátású és használatú szolgáltatói tanúsítványokat

109. Hogyan szegmentálódnak a tanúsítványok a tanúsítványtárban?
   a. sehogy, minden tanúsítványt mindenki használhat
   b. felhasználók szerint vannak a tanúsítványok szegmentálva
   c. alkalmazások szerint vannak a tanúsítványok szegmentálva
   d. valamennyi felhasználónak, szerviznek és magának a gépnek is van egy szegmense

110. Miért kell vigyázni a felhasználói profilra?

a. mert a magánkulcsok és a tanúsítványok részei a felhasználói profilnak

b. mert a profil tartalmazza a bejelentkezési jelszavakat

c. mert minden dokumentum a profilban van letárolva

d. mert más gépek felhasználói is hozzáférhetnek a profilokhoz

111. Miért jelent nagyobb kockázatot a vándoró profil alkalmazása a tanúsítványok használata szempontjából a helyi profil alkalmazásánál?

a. mert a vándorló profil nem biztonságos

b. mert a vándorló profil adatai mások számára is megismerhetők

c. mert a mobil felhasználók magánkulcsukat számos gépen otthagyhatják

d. mert a mobil felhasználók a tanúsítványaikat számos gépen otthagyhatják

112. Mit kell tennie több különböző célú tanúsítvánnyal rendelkező felhasználónak aláírás előtt?

a. semmit, az alkalmazás automatikusan kiválasztja a megfelelő tanúsítványt

b. ki kell választania az adott aláíráshoz megfelelő tanúsítványt

c. ki kell választania a legerősebb aláíró tanúsítványt

d. semmit, az operációs rendszer automatikusan használni fogja a megfelelő tanúsítványt

1. Melyik tanúsítvány hibás?

a. amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet

b. amelyiket nem minősített hitelesítésszolgáltató adta ki

c. amelyik más című webszerverre van kiállítva, mint amelyen található

d. amelyikkel nem lehet aláírni, csak titkosítani

2. Mi a célja a szoftvertanúsítványoknak?

a. hogy garantálják az aláírt szoftver sértetlenségét

b. hogy garantálják az aláírt program származását és sértetlenségét

c. hogy igazolják az aláírt program helyességét

d. hogy igazolják a gyártó megbízhatóságát

1.4.4 Visszavonási listák, a visszavonási állapot ellenőrzése

3. Mit tesznek egy tanúsítvány visszavonásakor?

a. a titkos kulcsot megsemmisítik

b. a tanúsítványt megsemmisítik

c. a titkos kulcsot vagy az ezt tartalmazó tanúsítványt felteszik egy nyilvános listára

d. a titkos kulcsot hordozó eszközt leselejtezik

4. Melyik tény nem okozza egy tanúsítvány érvénytelenségét?
    a. a tanúsítványlánc bármely eleméhez tartozó aláíró adat bizalmasságának sérülése
    b. az alkalmazott aláírási algoritmus vagy kulcshossz gyengesége
    c. ha a kibocsátó hitelesítésszolgáltatónál katasztrófaesemény történik
    d. szervezeti okok, mint például megváltozott hovatartozású vagy lejárt tanúsítvány
5. Hol van a tanúsítvány visszavonási lista feltalálási helye?
    a. a minősített aláírásban
    b. az időbélyegben
    c. a fokozott biztonságú aláírásban
    d. a tanúsítványban
6. Mi a kivárási idő?
    a. az aláírás és a következő visszavonási lista kibocsátása között eltelt idő
    b. az aláírás és a megelőző visszavonási lista kibocsátása között eltelt idő
    c. az aláírás és az ellenőrzés között eltelt idő
    d. a két megismételt ellenőrzés között eltelt idő
7. A tanúsítvány visszavonási lista mely adatokat tartalmazza?
    a. tulajdonos, sorszám, kibocsátó
    b. sorszám, kibocsátó, visszavonás ideje
    c. sorszám, visszavonás ideje, visszavonás oka
    d. sorszám, kibocsátó, visszavonás oka

1.5 Az elektronikus aláírások osztályozása és készítése

1.5.1 Az elektronikus aláírások osztályozása

8. Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?
    a. az aláírás beágyazódik egy magasabb szintű aláírt egységbe
    b. az aláírásba ágyazódnak bele az aláírandó információk
    c. az aláírás beágyazódik egy dokumentumba
    d. az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele
9. Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?
    a. az aláírás beágyazódik egy magasabb szintű aláírt egységbe
    b. az aláírásba ágyazódnak bele az aláírandó információk
    c. az aláírás beágyazódik egy dokumentumba
    d. az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

10. Az alábbiak közül melyik írja le a „beágyazódó aláírás” fogalmát?

    a. az aláírás beágyazódik egy magasabb szintű aláírt egységbe

    b. az aláírásba ágyazódnak bele az aláírandó információk

    c. az aláírás beágyazódik egy dokumentumba

    d. az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

11. Az alábbiak közül melyik írja le a „párhuzamos aláírás” fogalmát?

    a. az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni

    b. a párhuzamos aláírás a meglévők felett álló, azoktól függő módon arra rárakódó aláírás

    c. a párhuzamos aláírás a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól

    d. az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

12. Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

    a. a szekvenciális aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni

    b. a szekvenciális aláírás a meglévők felett álló, azoktól függő módon arra rárakódó aláírás

    c. a szekvenciális aláírás a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól

    d. a szekvenciális aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

13. Az alábbiak közül melyik írja le az „ellenjegyző aláírás” fogalmát?

    a. az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni

    b. az ellenjegyző aláírás a meglévők felett álló, azoktól függő módon arra rárakódó aláírás

    c. az ellenjegyző aláírás a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól

    d. az ellenjegyző aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

14. Melyik nem tartozik az elektronikus aláírási irányelv előírásai közé?

    a. biztosítani kell, hogy az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként felhasználhatók legyenek bírósági eljárásokban

    b. biztosítani kell, hogy az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként felhasználhatók legyenek hatósági eljárásokban

    c. a minősített elektronikus aláírással aláírt elektronikus dokumentumoknak ugyanolyan joghatást kell biztosítani, mint a saját kezű aláírással ellátott papírdokumentumoknak

d. ha a minősített aláírás ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott

1.5.2 Az elektronikus aláírások készítése

15. Melyik állítás igaz az aláíró alkalmazások együttműködésére vonatkozóan?

a. az aláíró alkalmazások nem működnek együtt egymással

b. az aláíró alkalmazások mindegyike együttműködik a másikkal

c. az aláíró alkalmazások együttműködési teszteken bizonyítják együttműködési képességeiket

d. az aláíró alkalmazások együttműködési képességét a fejlesztőjük igazolja

16. Melyik igaz az aláíró programokra?

a. az aláíró programok mindegyike el tudja az összes XAdES szabványos aláírást készíteni

b. az aláíró programok különböző, de szabványos aláírásokat tudnak készíteni

c. az aláíró programok a fejlesztő szándéka szerinti aláírásokat tudnak készíteni, mely képességüket független szervezet tanúsíthatja

d. az aláíró programok mindegyike különböző aláírást készít

17. Mely programokkal nem lehet digitális aláírásokat készíteni?

a. MS Office

b. Open Office

c. levelező programok

d. böngészők

18. Mi az aláírási politika?

a. az a szabályrendszer, mely biztosítja az egyes aláírások érvényességének technikai konzisztenciáját bármely környezetben

b. az a szabályrendszer, melyet az aláírás készítéséhez használnak

c. az a szabályrendszer, melyet az aláírás ellenőrzéséhez használnak

d. az a szabályrendszer, mely biztosítja az aláírás hosszú távú érvényességét

19. Az aláírási politika szabályrendszere biztosítja, hogy

a. az aláírást követően nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége

b. az aláírást megelőzően nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége

c. az aláírás ellenőrzését követően nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége

d. az aláírást követő CRL kibocsátása után nem lehetséges az időben olyan pillanat, melyben nem dönthető el az aláírás érvényessége vagy érvénytelensége

1.6 Kormányzati és hivatali ügyintézés elektronikusan

1.6.1 Az elektronikus aláírás és a kormányzás kapcsolata

20. Melyik a legfejlettebb ügyintézési szint az Alapvető közszolgáltatások egységes listája szerint?

    a. nyomtatványok on-line kitöltése, hitelesítése

    b. on-line információk a közigazgatási szolgáltatokról

    c. űrlapok letölthetősége

    d. személyes megjelenés nélküli teljes elektronikus ügyintézés

21. Kötelező-e a közigazgatási ügyekben az elektronikus ügyintézés?

    a. nem, az ügyfél és az eljárásban részt vevő más személy nem kötelezhető arra, hogy eljárási cselekményeit elektronikus úton végezze, amennyiben törvény eltérően nem rendelkezik

    b. igen, a Ket. pontosan ezt írja le

    c. általában igen, de az ügyfelet mindig megilleti a választás joga az elektronikus és a hagyományos ügyintézési forma között

    d. nem, és nem is kötelezhető erre az ügyfél

22. Van-e működő példa az elektronikus aláírás használatára Magyarországon?

    a. nincs, még nem használják

    b. nincs, külföldön sem használják

    c. van, de nem nyilvános

    d. van, ilyen például az elektronikus cégeljárás is

1.6.2 Elektronikus aláírás és internet banking

23. Ha jogszabály a szerződés érvényességéhez írásbeli alakot rendel, melyik forma nem alkalmazható az alábbiak közül?

    a. levélváltás

    b. legalább fokozott biztonságú elektronikus aláírással nem ellátott e-mail

    c. táviratváltás

    d. távgépírón és telefax útján történt üzenetváltás

24. Mi az elektronikus pénz?

    a. elektronikusan aláírt pénzérték

    b. bankkártya segítségével felhasználható pénzérték

    c. hitelkártya által felhasználható pénzérték

    d. készpénz átvétele, vagy számlapénz átutalása ellenében kibocsátott elektronikus pénzeszközön tárolt pénzérték

25. Hogyan biztosítja a pénzintézet a bankszámla feletti rendelkezési jog elektronikus gyakorlása esetén a hitelességet?

    a. ellenőrzi a megbízáson lévő mobil aláírást

    b. ellenőrzi a megbízáson feltüntetett aláírást (ideértve az elektronikus kódot is), hogy megegyezik-e a rendelkezésre jogosult hitelintézetnél bejelentett aláírásával (elektronikus kódjával)

    c. ellenőrzi a megbízáson lévő digitális aláírást

    d. ellenőrzi, hogy a megbízást saját internetbanki szoftverrel készítették-e

1.6.3 Az e-adózás és e-számla

26. Mit jelent az elektronikus adóbevallás és adatszolgáltatás?

    a. azt, hogy az adózó a saját elektronikus aláírásával aláírva küldi el az adóhatóságnak az összes szükséges bevallást, adatot

    b. azt, hogy az adózó választhatja az elektronikus adóbevallást az adózási folyamataiban

    c. azt, hogy az adózó kötelező jelleggel elektronikus úton adja be adóbevallásait, adatszolgáltatásait

    d. azt, hogy az adózó e-mailben közli az adóhatósággal a bevallásait, adatait

27. Mit neveznek e-számlának?

    a. az e-számla a papírlapú számla beszkennelt változata

    b. az e-számla vagy elektronikus adatcsererendszerben elektronikus adatként jön létre és továbbítódik, vagy olyan elektronikus dokumentumként áll elő, amely legalább fokozott biztonságú aláírással és időbélyeggel van ellátva

    c. az e-számla az olyan elektronikus dokumentumk, amely fokozott biztonságú aláírással és időbélyeggel van ellátva

    d. az e-számla az e-mailben küldött számla

2 Gyakorlati feladatok

A gyakorlati feladatok azt a célt szolgálják, hogy bemutassák az ECDL Elektronikus Hitelesség, Elektronikus Aláírás vizsgán teljesítendő gyakorlati feladatok típusait. A feladatokhoz néhány instrukció figyelembe vétele is ajánlott, a vizsga megkönnyítése érdekében. A gyakorlati feladatok nem strukturáltak, céljuk az eredményes aláírási tevékenységek mérése.

2.1 Instrukciók

A gyakorlatok elvégzése közben több előre elkészített fájllal kell dolgozni. Ezek a fájlok egy adott könyvtár-struktúrába szerveződnek. A gyakorláshoz használt legfelső szintű könyvtárban két alkönyvtárt célszerű létrehozni:

a. ELOZETES: mely az előre elkészített, vagy a feladatok megoldásához szükséges kész fájlokat (munkafájlok, szolgáltatói tanúsítványok, teszt-tanúsítványok) tartalmazza, az alábbi bontásban:

   DOC: előre elkészített dokumentumok, előre meghatározott formátumban

   CERT: előre letöltött szolgáltatói és aláírói tanúsítványok

   PROGS: az előre letöltött aláíró és ellenőrző programok könyvtára

b. EREDMENY: mely a gyakorlatok során elkészített eredmény-fájlokat foglalja magában. Ebben a könyvtárban az alábbi alkönyvtárakat célszerű még létrehozni:

   CERT: a gyakorlatok során letöltött, vagy az egyes feladatok során kiválasztott tanúsítványok számára, továbbá

   RESULT: a gyakorlatok során elkészített (aláírt) fájlok, eredmény-dokumentumok könyvtára

Az eredmények kiértékelésével elektronikus aláírási szakértőt is meg lehet keresni, aki segít a válaszok esetleges hibáinak kijavításában. Sok sikert a gyakorló feladatokhoz!

2.2 Gyakorlati feladatok

1. A legfelső szintű tanúsítványtárból válassza ki az egyik szolgáltatói tanúsítványt az alábbiak közül és gyűjtse ki a megadott mezőit!
   a. Entrust.net Secure Server Certification Authority
   b. Thawte Personal Freemail CA
   c. Belgacom E-Trust Primary CA
      i. Kibocsátó adatai (pl. Általános név és ország mező)
      ii. Tulajdonos adatai
      iii. Érvényesség kezdete és
      iv. Érvényesség vége, továbbá
      v. Tanúsítvány aláíró algoritmus

2. Igényeljen egy teszt aláíró tanúsítványt valamelyik alábbi szolgáltatónál a saját e-mail címét hitelesítve, a saját web-felületen 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!
    a. http://srv.e-szigno.hu/menu/index.php?lap=teszt_igenyles
    b. https://www.netlock.hu/index.cgi?lang=HU&tem=ANONYMOUS/online/online_indul.tem
    c. https://tesztca.mavinformatika.hu/
3. 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)!
4. Válasszon ki a tanúsítvány-tárban 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!
5. 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!
    a. Qualified e-Szigno CA (sorozatszám: 00 f2 67 09 3a 96 d0 be 9a 93 a4 cf ac f3 86 55 d8)
    b. Advanced Class 3 e-Szigno CA 2009 (sorozatszám: 0e)
    c. Advanced e-Szigno CA2 (sorozatszám: 6a 8a 26 76 97 a5 7b f6 39 3b da 91 de 7b 6d 02)
6. 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 web-oldal tanúsítványban szereplő címét) és a tanúsítvány kiállítóját valamint sorozatszámát!
    a. https://www.otpbank.hu/
    b. http://www.magyarorszag.hu/
    c. https://www.melasz.hu/
    d. https://www.magyarorszag.hu
7. 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!
8. 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! Írja alá a teszt-tanúsítványa segítségével az aláírandó dokumentumot! Mentést követően ellenőrizze le az aláírás érvényességét az alkalmazás megfelelő funkciója segítségével!