Tanúsítási jelentés

Hung-TJ-020-2004

az
e-Sealer v1.0

elektronikus aláíró alkalmazásról

/Noreg Kft./

Tartalom

1. Az e-Sealer v1.0 legfontosabb tulajdonságainak összefoglalása

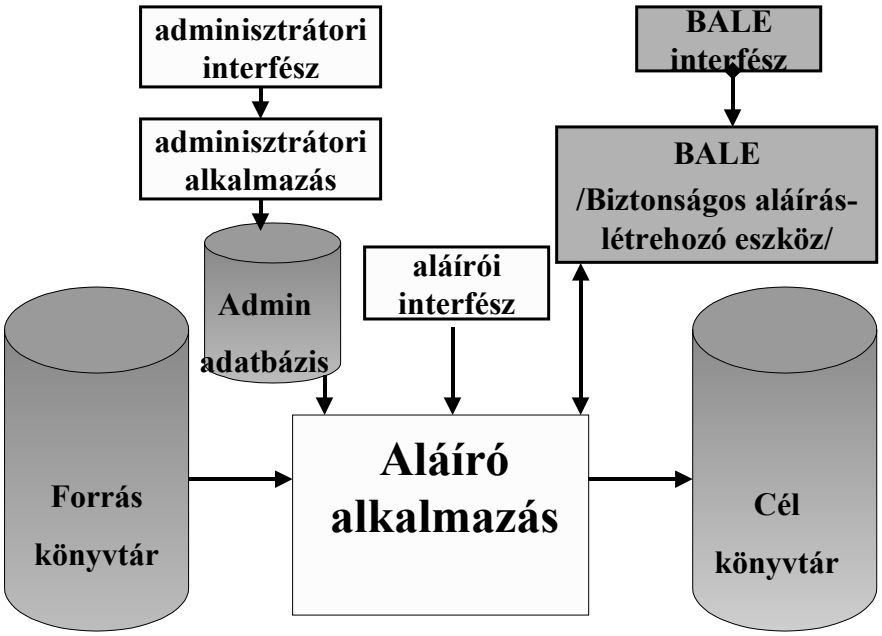
A tanúsított termék a Noreg Kft. által fejlesztett e-Sealer, verzió 1.0 elektronikus aláírás alkalmazás (a továbbiakban e-Sealer v1.0).

1.1 Architektúra, a tanúsítás hatóköre

Az e-Sealer v1.0 egy Windows (2000 vagy XP) operációs rendszer környezetbe épülő program-együttes az alábbi megosztásban:

- **adminisztrátori alkalmazás**
- **aláírói alkalmazás**, melynek része az automatikus aláírás ellenőrzési funkció

Az e-Sealer v1.0 szerkezeti felépítését, egyben az értékelés és tanúsítás hatókörét és határait az alábbi ábrák szemléltetik.



1. ábra: A tanúsítás határai (1)

Az 1. számú ábra alapján a tanúsítás tárgya egy olyan program, mely egy forráskönyvtár tartalmát (feldolgozandó, aláírandó fájlok) feldolgozva az eredményeket (feldolgozott, aláírt fájlok) egy célkönyvtárba helyezi el.

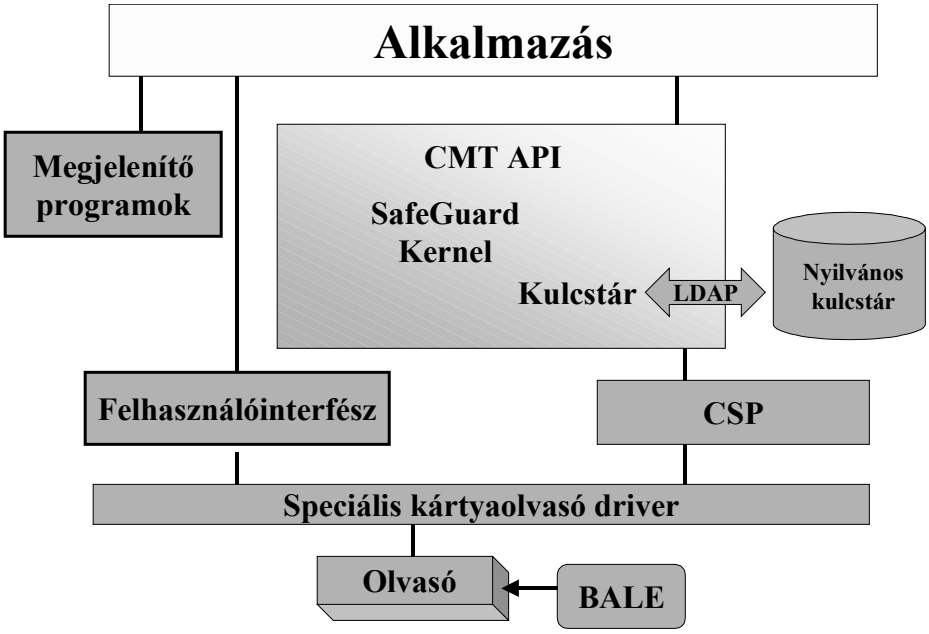
A tanúsítás hatókörének pontosítása:

- az az eljárás (és az ezt megvalósító informatikai alrendszer), mely a forráskönyvtár tartalmát előállítja, betölti és megvédi, nem tartozik a tanúsítás hatókörébe,
- az az eljárás (és az ezt megvalósító informatikai alrendszer), mely a célkönyvtár tartalmát tárolja, megvédi, átalakítja (titkosítja) és kommunikációs csatornán keresztül importálja (továbbítja a kliens oldalra) , nem tartozik a tanúsítás hatókörébe,
- a BALE által végzett ellenőrzések nem taroznak a tanúsítás hatókörébe, de az a felhasználói interfész igen, mely a kód bekérést és BALE felé továbbítását végzi,
- a PIN kód módosítás nem tartozik a tanúsítás hatókörébe.

Az e-Sealer v1.0 elsődleges célja egy biztonsági funkció, az aláírási szabályzatnak megfelelő feltételek szerint digitális aláírás létrehozása. Ez a fő funkció a digitálisan aláírt adatállományok hitelességét, sértetlenségét és letagadhatatlanságát hivatott biztosítani. A két alkalmazás további funkciói a digitális aláírással és annak ellenőrzésével kapcsolatos egyéb funkciók számára teremtenek keretet.
A tanúsítás tárgyát képezi a fentebb említett két program, valamint azon interfészek, melyek e két program és a környezet által megvalósítandó biztonsági célokat érvényre juttató operációs rendszerbeli elemek kapcsolatát teremtik meg a két alkalmazás oldaláról:

- az adminisztrátor számára biztosított alkalmazás (a megbízható pontok adatbázisának karbantartására)
- az aláíró számára biztosított alkalmazás (az aláírás környezetének beállítására és az aláírás végrehajtására)

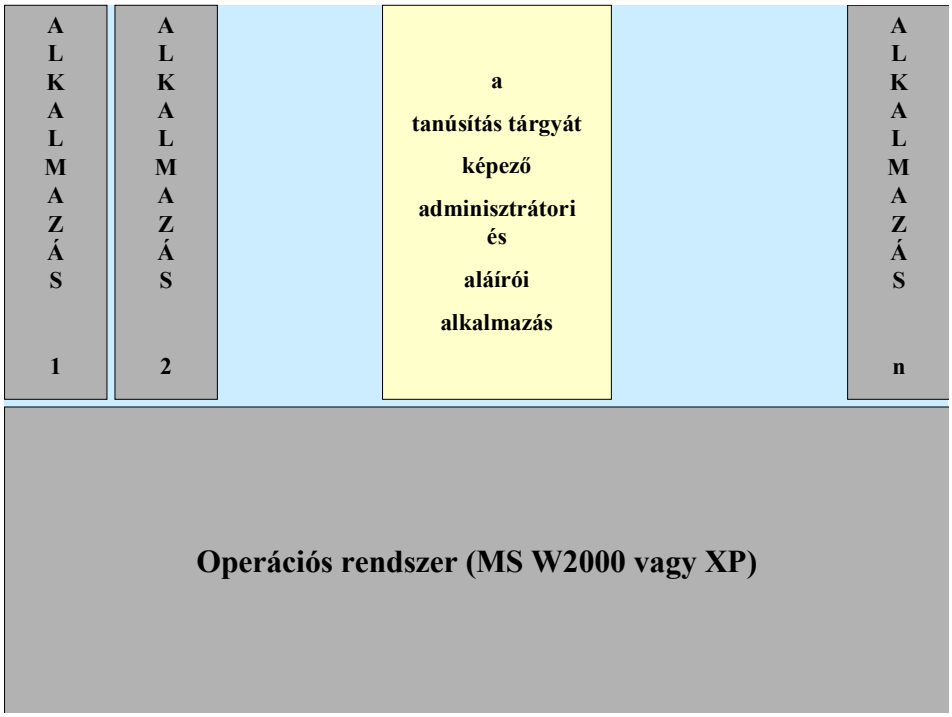
A biztonságos aláírás-létrehozó eszköz (intelligens kártya) is a tanúsítás hatókörén kívül áll.
A 2. sz. ábra a tanúsítás határait más megközelítésben pontosítja.



2. ábra: A tanúsítás határai (2)

A fájlok feldolgozását végző alkalmazás a SafeGuard Toolkit fejlesztő készlet (*2.50.02* verzió) különböző szolgáltatásaira épül. A fejlesztő készlet magas szintű alkalmazói program interfészén (a CMT API-n) keresztül a fejlesztő készlet számos elemét (különböző függvényeit, primitívjeit) használja fel. A meghívott funkciók (konkrétan felhívott, paraméterezett változatukban) részét képezik a tanúsításnak, míg a fejlesztő készlet többsége (a nem aktivizált részek) kívül esnek ezen.

A 3. sz. ábra a tanúsítás határait az operációs rendszer irányában pontosítja.



3. ábra: A tanúsítás határai (3)

Az értékelés tárgyát képező alkalmazás egy több felhasználós környezetben, a Windows 2000 vagy XP operációs rendszeren fut. Az operációs rendszer számos biztonsági funkcionalitást biztosít számára:

- hozzáférés ellenőrzés (a program elindításának jogosultsága, a program által használt védett fájlokhoz való hozzáférés, stb.),
- elkülönítés (az egyszerre futó programok által használt memória területek elkülönítésének a megvalósítása, átjárhatatlanságának a biztosítása.

Sem a megbízható alapot (absztrakt gépet) biztosító operációs rendszer, sem a többi alkalmazás nem képezi részét a tanúsítás tárgyának.

1.2 Tulajdonságok

Az aláírói alkalmazás egy megadott forráskönyvtárban (és annak alkönyvtáraiban) az aláírási funkció felhasználói interfésze elindításakor található valamennyi fájlt egyenként (az aláírási szabályzatban meghatározott szabályoknak megfelelően) digitálisan aláír, s az így előálló fájlokat egy megadott célkönyvtárba helyezi el (automatikusan ellenőrizve is az aláírásokat). Az alkalmazás szabványos formátumú (PKCS#7) minősített elektronikus aláírást hoz létre.
A célkönyvtár a forrás könyvtáréval hasonló fa szerkezetű lesz, ha valamelyik alkönyvtár hiányzik, akkor a program ezt automatikusan létrehozza.
A célkönyvtárban elhelyezett eredmény fájl neve (kiterjesztéssel együtt) ugyanaz lesz, mint az eredeti fájlé volt, csak a név második kiterjesztésként kiegészül a "sig" karakterhármassal, amennyiben a felhasználó „separate signature”-t nem kapcsolta be. Ez utóbbi esetben külön fájlként kerül a célkönyvtárba az aláírás.

A feldolgozás (elektronikus aláírás, a forráskönyvtárból a célkönyvtárba helyezéssel együtt) automatikusan történik, feldolgozás közben a feldolgozottság szintje folyamatosan követhető az aktuális feldolgozás alatt álló fájl nevének, valamint a feldolgozottság százalékos arányának a megjelenítésével.

A feldolgozás eredményéről riport készül, mely tartalmazza az alábbiakat:
- a feldolgozásra átadott fájlok száma,
- a sikeresen feldolgozott fájlok száma,
- a (valamilyen okból) nem feldolgozott fájlok száma,
- a forrás könyvtárban (s annak alkönyvtáraiban) található fájlok száma.

Az adminisztrátori alkalmazás segítségével az aláíró alkalmazás biztonsági tulajdonságainak kritikus részét (a megbízható pontokkal kapcsolatos adatokat) lehet felvinni, módosítani, illetve törölni, megfelelő (adminisztrátori) jogosultsággal.

Az e-Sealer v1.0 az alábbi biztonsági funkciókat valósítja meg:

- **Azonosítás és hitelesítés**
  Az e-Sealer v1.0 az aláírás létrehozási tevékenység előtt felhasználó hitelesítési kérelmet jelenít meg a felhasználói felületen (PIN kód bekérés), a hitelesítő adatot továbbítja a BALE felé.
- **Hozzáférés ellenőrzés**
  Az e-Sealer v1.0 csak az általa elért könyvtárban található állományokra végzi el az aláírás létrehozási és az automatikus aláírás ellenőrzési folyamatot.
- **Naplózás**
  Az alkalmazás szempontjából fontosnak ítélt napló események előállítását végző funkció.
  /A naplózási követelmények döntő részét az e-Sealer v1.0 környezete teljesíti: az operációs rendszer naplózza az alkalmazás jogos felhasználóinak bejelentkezésével kapcsolatos események bejegyzését, s a napló adatok megtekintését is (a környezethez tartozó) külön alkalmazás teszi lehetővé. A saját maga által generált naplóállományok védelmét annyiban vállalja fel az e-Sealer v1.0, hogy az elkészült napló-riport állományokat lezárás után „csak olvasható” attribútummal látja el, mely a véletlen törlés ellen véd./
- **Aláírás létrehozási funkció** (az egyik alapvető biztonsági funkció)
  Az aláíró magánkulcsot használja az aláírás generálására, és lehetővé teszi az aláírási információk generálását is. Az aláírás létrehozásával a sértetlenség, hitelesség és letagadhatatlanság biztonsági szolgáltatásokat valósítja meg az e-Sealer v1.0. Opcionálisan időbélyeg is kérhető.
- **Aláírás ellenőrzési funkció** (a másik alapvető biztonsági funkció)
  Ez dolgozza fel az aláírási információkat, például a PKCS#7 blob-ot, és a nyilvános kulcsot használja az aláírás ellenőrzéséhez. Ez a funkció-csomag függ a tanúsítási útvonal érvényességének ellenőrzése biztonsági funkciótól. Az aláírás ellenőrzési funkció a tanúsítási útvonal érvényesség ellenőrzés eredményét bemenetként használja fel.

- **Tanúsítási útvonal érvényesség ellenőrzése**
  Ez a funkció a tanúsítási útvonal érvényességét ellenőrzi. A megvalósítás az útvonal felépítéséből, majd a tanúsítási útvonal érvényességének ellenőrzéséből áll. A tanúsítási útvonal érvényességének ellenőrzése a tanúsítványok érvényességének ellenőrzéséből áll, oly módon, hogy ez az ellenőrzés egy megbízható pont által tanúsítottal kezdődik, és az aláírónak kibocsátottal fejeződik be.
  A tanúsítási útvonal érvényesség ellenőrzése az aktuális idő szerint történik (szemben például a vitás esetekben felmerülő régi aláírások ellenőrzésével).
- **CRL érvényesség ellenőrzése funkció**
  Ez a funkció a CRL érvényességének ellenőrzésére szolgál. Olyan teljes CRL feldolgozására használható, amelyre egy CRL szétosztó pont kiterjesztés mutat egy tanúsítványban.
- **Aláírandó fájlok listájának megjelenítése**
  Az aláírás létrehozási funkció aktivizálásakor megjelenő hitelesítő ablakban látható gomb (Show files) megnyomása után az aláírásra összeállított fájlok listáját mutatja be a felhasználónak. A könyvtár időközbeni módosítását figyelmen kívül hagyja ezen aláírás létrehozási szakaszban.

2. Az e-Sealer v1.0 megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 követelményrendszereiből fakadó) funkcionális és biztonsági követelményeket, melyek minősített aláírások létrehozására és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy az e-Sealer v1.0 megfelel-e az adott követelménynek.

Minthogy az e-Sealer v1.0 aláíró alkalmazást minősített aláírásra kívánják felhasználni, megfelelő tanúsítási végeredmény csak akkor adható, ha az alkalmazás valamennyi rá vonatkozó követelményeknek megfelel.

2.1 A funkcionális követelményeknek való megfelelés

F_SCA_1: Minden aláírás-létrehozó rendszer tartalmazzon egy (teljes) aláírás-ellenőrző rendszert is.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	❍

Magyarázat: Az e-Sealer v1.0 az aláírás létrehozása során ellenőrzi a tanúsítványláncot, a CRL-t, és az időbélyeget. Aláírás után pedig automatikusan ellenőrzi az elkészült PKCS#7 csomag szintaktikáját és az aláírást.
Konklúzió: **megfelel**

F_SDP_1: Minden aláírói dokumentumnak közvetett módon tartalmaznia kell egy tartalom-formátumot, amely meghatározza azokat a részleteket, ahogyan a dokumentumot az ellenőrző számára meg kell jeleníteni, vagy ahogyan fel kell használni.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: A PKCS#7-es aláírt adatobjektum tárolja az aláírt adatok közt a tartalom formátumot. (Separate signarure esetén ez ugyan nincs így, de az aláírási szabályzat alapján csak két teljesen eltérő formátum van engedélyezve, ami közvetett módon tartalmazza a tartalom formátumot.) A PKCS#7 csomag fájlnevében tartalmazza az eredeti fájl nevét.
Konklúzió: **megfelel**

F_SDP_2: Amennyiben az aláírói dokumentum szemantikája nem függ annak megjelenítésétől, akkor vagy az aláírói dokumentumban vagy egy aláírás tulajdonságban meg kell adni a tartalom egyértelműséghez szükséges információkat.
Magyarázat: A szemantika függ a megjelenítéstől.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SDP_3: Amennyiben az aláírói dokumentum szemantikája függ annak megjelenítésétől, akkor az aláírónak elegendő információval kell ellátnia az aláírás ellenőrzőjét a dokumentum pontos megjelenítéséhez.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	❍

Magyarázat: Az e-Sealer v1.0 programmal PDF vagy XML fájlok írhatók alá. A PKCS#7-es aláírt adatobjektum tárolja az aláírt adatok közt a tartalom formátumot. (Separate signarure esetén nem.) A PKCS#7 csomag fájlnevében tartalmazza az eredeti fájl nevét.

Konklúzió: **megfelel**

F_SDP_4: Az ellenőrzési folyamatok helyesen értelmezzék a F_SDP_1, F_SDP_2 és F_SDP_3 által megkövetelt információkat, illetve ezek alapján egyértelműen és helyesen jelenítsék azt meg az ellenőrző számára.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

*Magyarázat: Megjelenítés esetén az e-Sealer v1.0 program ráhívja a fájlokra az operációs rendszerben beállított, fájltípustól függő alapértelmezett megjelenítőt. A program nem ellenőrzi a megjelenítők integritását. Ennek védelmét az informatika biztonsági környezetnek kell megoldania. Csak olyan külső megjelenítőt szabad telepíteni, amelyik az aláírandó dokumentumon változtatni nem képes.*Konklúzió: **megfelel**

F_SAV_1: Mind az aláíró, mind az ellenőrző számára meg kell jeleníteni az aláírási tulajdonságokat, különös tekintettel a következőkre:

- az aláíró tanúsítványa,
- az aláíró dokumentumának tartalom-formátuma (ha szerepel),
- az aláírási szabályzat (ha szerepel),
- a kötelezettségvállalás típusa (ha szerepel).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az aláíró tanúsítványa megnézhető, akárcsak az aláírásra felkínált anyagok.(A könyvtár struktúrában látszanak a fájlnevek, külön ikonnal a megfelelő formátumúak.)

Konklúzió: **megfelel**

F_SAV_2: Lehetőséget kell biztosítani az aláíró/ellenőrző számára ahhoz, hogy az aláíráshoz csatolandó/csatolt tanúsítványt átvizsgálja.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az aláíró tanúsítványa megtekinthető.

Konklúzió: **megfelel**

F_SIC_1: Egy aláírás létrehozása előtt meg kell győződni arról, hogy az aláíró valóban létre kíván hozni egy minősített elektronikus aláírást.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
		●	●	●

Magyarázat: Az aláírás folyamata a Start gombbal indítható, és a PIN kód bekérő ablaknál a folyamat még az aláírások előtt megszakítható. A folyamat egyébként az egyes fájlok aláírása közben is megszakítható.

Konklúzió: **megfelel**

F_SIC_2: Az aláíró/ellenőrző számára vezérlő funkciók szükségesek, melyen keresztül irányíthatja az aláírási/ellenőrzési folyamatot és az aláírás-alkalmazás tevékenységét.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az aláírás folyamata a Start gombbal indítható, és a PIN kód bekérő ablaknál a folyamat még az aláírások előtt megszakítható. A folyamat egyébként az egyes fájlok aláírása közben is megszakítható.

Konklúzió: **megfelel**

F_SIC_3: Egy elektronikus aláírás létrehozása előtt a biztonságos aláírás-létrehozó eszköznek és az aláírás-létrehozó alkalmazásnak is meg kell győződnie arról, hogy az aláíró a biztonságos aláírás-létrehozó eszköz tulajdonosa (vagy jogosult használója).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az e-Sealer v1.0 program PIN kódot kér az aláírási folyamat indítása előtt.

Konklúzió: **megfelel**

F_DTBSF_1: Ki kell alakítani a szabványos formattált aláírandó adatot az aláíró dokumentumából, az aláírási tulajdonságok felhasználásával.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: A PKCS#7-es csomagot az Utimaco SafeGuard Toolkit 2.50.02 állítja már össze a program által begyűjtött adatok alapján.

Konklúzió: **megfelel**

F_DTBSF_2: Ha az aláírandó adatnak tartalmaznia kell az aláírói dokumentum lenyomatát, és ha ez még nem létezik, akkor a DTBSF összetevőnek kezdeményezni kell a lenyomatolási eljárást a formattált aláírandó adat kialakítása előtt.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 végzi a lenyomatolást.

Konklúzió: **megfelel**

F_DHC_1: Az aláírás-létrehozó folyamat kiváltása utáni első lépésként végre kell hajtani a lenyomatolást.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 végzi a lenyomatolást.

Konklúzió: **megfelel**

F_DHC_2: Második lépéseként végre kell hajtani a lenyomat formattálását (feltöltését).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 végzi a PKCS#7 csomag elkészítését.

Konklúzió: **megfelel**

F_SSC_1: Egy aláíró ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani az 1. ábrán jelölt minden szükséges kommunikációt.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az e-Sealer v1.0 végrehajtja az aláírás folyamatát.

Konklúzió: **megfelel**

F_SSC_2: Egy szolgáltató ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 2. ábrán jelölt minden szükséges kommunikációt.

Magyarázat: A rendszer aláíró ellenőrzése alattinak tekinthető.

Konklúzió: **nem vonatkozik rá a követelmény**

F_SSC_3: Az aláírás-létrehozó alkalmazásnak legalább egy fizikai interfésszel kell rendelkeznie, amely alkalmas a biztonságos aláírás-létrehozó eszközzel való kommunikációra.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	●	●

Magyarázat: Az e-Sealer v1.0-t futtató számítógép megfelelő kártyaolvasóval rendelkezik.

Konklúzió: **megfelel**

F_SSC_4: A biztonságos aláírás-létrehozó eszköz funkcionalitása megvalósítható egy olyan platformon (pl. intelligens kártya), amely egy vagy több biztonságos aláírás-létrehozó eszköz funkciót (amelyeket gyakran biztonságos aláírás-létrehozó eszköz alkalmazásnak is neveznek) hordoz és, ezen felül esetleg más alkalmazásokat is. Ilyen több-alkalmazásos platform esetén az aláírás-létrehozó alkalmazásnak ki kell választania az egyiket.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az e-Sealer v1.0 programmal manuálisan lehet váltani az alkalmazások között, ahol már csak az aláírási szabályzatban meghatározott tanúsítvánnyal rendelkező kulcsok választhatóak ki.

Konklúzió: **megfelel**

F_SSC_5: Egy biztonságos aláírás-létrehozó eszköz hordozhat több tanúsítványt is. Ebben az esetben ki kell tudni választani az egyiket.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az e-Sealer v1.0 csak az aláírási szabályzatban meghatározott tanúsítványokat engedi kiválasztani. Több megfelelő tanúsítványból is ki lehet választani az aláírót.

Konklúzió: **megfelel**

F_SSC_6: Ha egy biztonságos aláírás-létrehozó eszköz egynél több aláírás-létrehozó adatot (magánkulcsot) tartalmaz, akkor a megfelelőt ki kell tudni választani az aláíró szándéka szerint.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	❍

Magyarázat: Az e-Sealer v1.0 a kulcsokat a tanúsítványokon keresztül kezeli.

Konklúzió: **megfelel**

F_SSC_7: A biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikátor (SSC) összetevőnek át kell vennie az aláírót hitelesítő adatot az aláírót hitelesítő összetevőtől egy megbízható útvonalon keresztül, és el kell küldenie egy megfelelő parancs (utasítás) kíséretében a biztonságos aláírás-létrehozó eszköznek összehasonlításra.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	❍

Magyarázat: Az e-Sealer v1.0 kéri be a PIN kódot, és adja át az Utimaco SafeGuard Toolkit 2.50.02-nek. A Toolkit adja tovább a BALE-nek.

Konklúzió: **megfelel**

F_SSC_8: Az aláírás létrehozó folyamat utolsó lépéseként ki kell számíttatni (a biztonságos aláírás-létrehozó eszköz által megvalósítva) magát az aláírást.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az e-Sealer v1.0 az Utimaco SafeGuard Toolkit 2.50.02-enkeresztül végezteti el az aláírást a BALE eszközzel.

Konklúzió: **megfelel**

F_SSC_9: A befejezett aláírásokat naplózni kell.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	●	●

Magyarázat: Az egyes aláírások naplózásra kerülnek.

Konklúzió: **megfelel**

F_SSA_1: Ha az aláírás-létrehozás egy - szolgáltató ellenőrzése alatt álló – aláírás-létrehozó rendszeren történik meg, akkor az aláírónak képesnek kell lennie annak megállapítására, hogy feltételezhet-e ugyanolyan szintű bizalmasságot, mint amit a saját ellenőrzése alatt álló aláírás-létrehozó rendszer esetén elérhet.

Magyarázat: Az e-Sealer v1.0 az *aláíró ellenőrzése alatt áll.*

Konklúzió: **nem vonatkozik rá a követelmény**

F_SDC_1: Lehetővé kell tenni az aláíró számára az aláírói dokumentum létrehozását vagy kiválasztását.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	●	❍

Magyarázat: Az aláírói dokumentumok automatikusan, más rendszer által kerülnek be a forrás könyvtárba. Az aláíró a tényleges aláírás előtt ellenőrizheti az aláírásra váró dokumentumokat. Az e-Sealer v1.0 ellenőrzi a fájlokhoz való kizárólagos hozzáférést is.

Konklúzió: **megfelel**

F_SDOC_1: Össze kell kapcsolni a biztonságos aláírás-létrehozó eszköz kimeneti adatát (az elektronikus aláírást) a formattált aláírt adattal, a szabvány formátumnak megfelelően.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az aláírást az Utimaco SafeGuard Toolkit 2.50.02 teszi a PKCS#7 formátumú csomagba.

Konklúzió: **megfelel**

F_SLC_1: Minden létrehozott/ellenőrzött aláírásra egy napló bejegyzés tárolandó.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	●	●

Magyarázat: A napló tartalmazza az aláírás sikerességét.

Konklúzió: **megfelel**

F_SCPC_1: A hitelesítés-szolgáltatóval való kapcsolat felvételén keresztül képesnek kell lennie az alábbiakra:

- az aláírói tanúsítványok megszerzése,
- az aláírói tanúsítványok állapotának lekérése.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	❍	❍

Magyarázat: Az e-Sealer v1.0 az adminisztrátor által adatbázisba töltött tanúsítványokkal képes dolgozni. A CRL listákat ugyancsak az adminisztrátor tölti le és helyezi el a megfelelő könyvtárba. Illetve az Utimaco SafeGuard Toolkit 2.50.02 képes LDAP-on keresztül megszerezni a megfelelő CRL-eket. (HTTP felületen keresztül az e-Sealer v1.0 nem képes megszerezni a CRL-t.)

Konklúzió: **megfelel**

F_I/O-1: Ha aláírás-létrehozásnál a biztonságos aláírás-létrehozó eszköz nem tartalmaz minden szükséges tanúsítványt az aláírási folyamathoz (mert csak a tanúsítvány azonosítókat tartalmazza), vagy ha aláírás-ellenőrzésnél az aláírótól nem érkezett meg a szükséges tanúsítvány (csak annak azonosítója), akkor az aláírás-alkalmazásnak képesnek kell lennie arra, hogy ezeket a tanúsítványokat megszerezze (lekérdezze a hitelesítés-szolgáltatótól).

Magyarázat: Az e-Sealer v1.0 teljes tanúsítványokkal dolgozik, amelyeket az adminisztrátor tölt be az adatbázisába.

Konklúzió: **nem vonatkozik rá a követelmény**

F_I/O-2: Az aláírás-alkalmazásnak képesnek kell lennie arra, hogy a megszerzett tanúsítványok hitelességét ellenőrizze.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	●	●

Magyarázat: A tanúsítványlánc összeállítását és ellenőrzését, valamint a CRL-ek ellenőrzését az Utimaco SafeGuard Toolkit 2.50.02 végzi.

Konklúzió: **megfelel**

F_I/O-3: Ha az aláírói dokumentumot, vagy annak egy részét, vagy az aláírási tulajdonságokat egy input/output interfészen keresztül adják meg, az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy egyetlen rejtett rész se játszhasson szerepet, és hogy egyetlen aláírandó adat összetevőt se cserélhessenek ki.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az aláíró kulcs tanúsítványának kiválasztása, és az időbélyeg kérése I/O-n keresztül történik. Ezek helyesen kerülnek be a PKCS#7-es csomagba.

Konklúzió: **megfelel**

F_ISV-1: Az érvényesítő adatokat az ellenőrzőnek be kell gyűjtenie, és az aláírási szabályzat minden követelményét teljesítenie kell.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	❍	❍

Magyarázat: Ez a követelmény csak a fogadó oldali (kliens) alkalmazásra vonatkozik

Konklúzió: **nem vonatkozik rá a követelmény**

F_ISV-2: Ha szükség lehet utólagos ellenőrzésre, az érvényesítő adatoknak tartalmazniuk kell annak bizonyítékát, hogy a felhasznált tanúsítvány lánc érvényes volt az aláírás létrehozásának időpontjában.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	❍	❍

Magyarázat: Az utólagos ellenőrzés megegyezik az elsődleges ellenőrzéssel. Problémát csak az aláírás idejének hitelessége jelenthet. Ezt biztosítja az időbélyeg, vagy ha nem használják, akkor a rendszeridő védelmét az informatika biztonsági környezetnek kell biztosítania.

Konklúzió: **megfelel**

F_USV-1: A kezdeti ellenőrzés során begyűjtött érvényesítő adatok ellenőrzésénél az aláírási szabályzat minden követelményét teljesíteni kell.

Magyarázat: Az utólagos ellenőrzés megegyezik az elsődleges ellenőrzéssel.

Konklúzió: **nem vonatkozik rá a követelmény**

F_human_1: Az aláírás-ellenőrző rendszernek eszközt kell biztosítania a felhasználó számára, amelyen keresztül az kommunikálni tud a rendszerrel. Ha az aláírt adatokhoz egynél több aláírás van hozzárendelve, akkor ennek a kommunikációnak azzal kell kezdődnie, hogy kijelzésre kerül az aláírások száma, amelyek feltehetően léteznek, és fel kell kínálni, hogy melyik legyen az ellenőrizendő.

Magyarázat: Az e-Sealer v1.0 csak aláírás létrehozást támogat, illetve az ehhez szükséges automatikus aláírás ellenőrzést valósítja meg.

Konklúzió: **nem vonatkozik rá a követelmény**

F_human_2: Az aláírás-ellenőrző rendszernek interaktív eszközt kell biztosítania a felhasználó számára, hogy megnézhesse az aláírási szabályzat teljes egészét, vagy legalább az alkalmazási területre és feltételekre vonatkozó részeket.
Magyarázat: Az e-Sealer v1.0 csak aláírás létrehozást támogat, illetve az ehhez szükséges automatikus aláírás ellenőrzést valósítja meg.
Konklúzió: **nem vonatkozik rá a követelmény**

F_human_3: A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az "Ami megjelenik, azt írták alá." követelményt. Ha valamilyen okból az aláírói dokumentum nem jeleníthető meg pontosan a megfelelő módon, akkor ezt a felhasználói interfésznek világosan jeleznie kell.
Magyarázat: Az e-Sealer v1.0 csak aláírás létrehozást támogat, illetve az ehhez szükséges automatikus aláírás ellenőrzést valósítja meg.
Konklúzió: **nem vonatkozik rá a követelmény**

F_human_4: Az aláíró azonosítójának, vagyis az állítólagos aláíró nevének vagy felvett nevének megjeleníthetőnek kell lenni. Az adott nevet az aláíró tanúsítványában szereplő, "megkülönböztető név" információjából kell venni. Ha az aláíró nem bocsátotta rendelkezésre a tanúsítványt, a hitelesítés-szolgáltató nevét kell megjeleníteni ehelyett, és ha ez a név elfogadható, akkor az adott tanúsítványt a hálózati interfész felhasználásával be kell szerezni. Az említett névnek csak a tanúsítványt kibocsátó hitelesítés-szolgáltató számára van jelentése, ezért a hitelesítés-szolgáltató nevét az aláíró nevével együtt ki kell jelezni.
A kezdeti aláírás-ellenőrzési folyamat kimenő állapota az alábbiak egyike legyen:

- "érvényes" állapot (sikeres ellenőrzés),
- "érvénytelen" állapot (sikertelen ellenőrzés),
- "befejezetlen ellenőrzés" állapot (befejezetlen ellenőrzés)

Magyarázat: Az e-Sealer v1.0 csak aláírás létrehozást támogat, illetve az ehhez szükséges automatikus aláírás ellenőrzést valósítja meg.
Konklúzió: **nem vonatkozik rá a követelmény**

F_human_5: "Befejezetlen ellenőrzés" állapot esetén az aláírás-ellenőrző alkalmazásnak javasolnia kell a felhasználó számára, hogy szerezze be azt az információt, ami az aláírást érvényessé teszi hosszú távra.
Magyarázat: Az e-Sealer v1.0 csak aláírás létrehozást támogat, illetve az ehhez szükséges automatikus aláírás ellenőrzést valósítja meg.
Konklúzió: **nem vonatkozik rá a követelmény**

F_human_6: A felhasználói interfészekre teljesüljenek az F_principles egyszerűségre és hibamentességre vonatkozó speciális elvárásai.
Magyarázat: Az e-Sealer v1.0 csak aláírás létrehozást támogat, illetve az ehhez szükséges automatikus aláírás ellenőrzést valósítja meg.
Konklúzió: **nem vonatkozik rá a követelmény**

Az automatizált feldolgozás esetében alkalmazói program interfészek (API-k) használhatók. Bár az ilyen interfészek kialakításának többféle módja van, ezeket két csoportba lehet sorolni:

- Az 1-es típusú API-k arra szolgálnak, hogy az elektronikus aláírásban tárolt adatokat kigyűjtsék.
- A 2-es típusú API-k az elektronikus aláírás ellenőrzésére és az érvényesítő adatok beszerzésére szolgálnak.

F_machine_1: Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére és az elektronikus aláírás formátumának meghatározására.
Amennyiben az aláírási szabályzat explicit, akkor a szabályzat azonosítóját magából az elektronikus aláírásból kell kinyerni az 1-es típusú API-jainak felhasználásával.
Magyarázat: Az aláírási szabályzat implicit.
Konklúzió: **nem vonatkozik rá a követelmény**

F_machine_2: A 2-es típusú API-k az elektronikus aláírások hitelesítését és/vagy ellenőrzését kell lehetővé tenniük, illetve be kell szerezniük az aláírói információkat, az output állapotot és az érvényesítő adatokat.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	❍	●

Magyarázat: Az API az Utimaco SafeGuard Toolkit 2.50.02 része.
Konklúzió: **megfelel**

F_general_1: A rendszer által megvalósított aláírás-ellenőrzési folyamatnak meg kell felelnie egy ember számára olvasható formájú leírásnak, feltételezve, hogy az aláírási szabályzat minden feldolgozási szabálya világosan meghatározott.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	❍	●	●

Magyarázat: Az aláírás folyamán keletkezett napló, (melynek a tartalma a képernyőn is megjelenik) olvasható formátumú.
Konklúzió: **megfelel**

F_protocol: Mind az aláírás-létrehozó, mind az aláírás-ellenőrzési alkalmazásnak szabványos protokollt kell használnia a megbízható szolgáltatóval (szolgáltatókkal) történő kommunikáció során. Ez a következőket foglalja magában:

- tanúsítvány visszavonási állapot megszerzésekor;
- időbélyeg kérelem és válasz esetén;
- egyéb esetekben (pl. központi archiválási, időjelzési, naplózási szolgáltatások igénybe vétele esetén).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	❍	●	●

Magyarázat: Az e-Sealer v1.0 szabványos formátumokkal dolgozik és szabványos protokollokat használ az Utimaco SafeGuard Toolkit 2.50.02-en keresztül. HTTP FTP felületen keresztül nem tud CRL-t lekérni a program. Csak olyan szolgáltatót lehet választani, amely a program által elfogadott formátumban szolgáltatja a CRL-t.
Konklúzió: **megfelel**

F_format: Mind az aláírás-létrehozó, mind az aláírás-ellenőrzési alkalmazásnak képesnek kell lennie szabványos formátumok kezelésére az alábbi területeken:

- szabványos aláírási formátumok;
- szabványos tanúsítvány formátumok.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	❍	●	❍

Magyarázat: Az e-Sealer v1.0 szabványos formátumokkal dolgozik az Utimaco SafeGuard Toolkit 2.50.02-en keresztül. A program nem kezeli a BASE64 formátumú tanúsítvány és CRL állományokat.

Konklúzió: **megfelel**

F_principles: A felhasználói (aláírói, aláírás-ellenőrzői) felületek tervezésekor a következő elveket kell figyelembe venni:

- alkalmasnak kell lennie a feladatra;
- konzisztensnek kell lennie;
- felhasználóbarátnak (könnyen érthető, egyszerűen használható) kell lennie;
- ellenőrizhetőnek kell lennie;
- hibatűrőnek kell lennie;
- lehetővé kell tennie az egyedi beállításokat;
- egyenlőségen alapuló hozzáférést kell biztosítania;
- megfelelő állapotjelzéseket és hibaüzeneteket kell küldenie a felhasználó számára.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az e-Sealer v1.0 átlátható, egyszerűen kezelhető.

Konklúzió: **megfelel**

2.2 A biztonsági követelményeknek való megfelelés

Bizt_köv1: Az aláírás-létrehozó alkalmazásnak meg kell őriznie a következők sértetlenségét:

- aláírandó adat (DTBS), formattált aláírandó adat (DTBSF), aláírandó adat reprezentáns (DTBSR) és minden egyéb, az aláíró által szolgáltatott információ,
- Az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között áramló valamennyi protokoll adat.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Részben az e-Sealer v1.0, részben az Utimaco SafeGuard Toolkit 2.50.02 feladata.

Konklúzió*:* **megfelel**

Bizt_köv2: Az aláírás-létrehozó alkalmazásnak meg kell őriznie az aláírandó adat komponensek, a formattált aláírandó adat és az aláírót hitelesítő adatok bizalmasságát.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	❍	❍	❍

Magyarázat: Részben az e-Sealer v1.0, részben az Utimaco SafeGuard Toolkit 2.50.02 feladata. Az e-Sealer v1.0 hosszú ideig tárolja az aláírót hitelesítő adatot, amit meg kell védeni.

Konklúzió*:* **megfelel**

A következő négy követelmény csak a nyilvános aláírás-létrehozó alkalmazásokra vonatkozik.

Bizt_köv3: … Bizt_köv6:

Magyarázat: A 3.-6. követelmények csak a nyilvános aláíró alkalmazásokra vonatkoznak (melyek egy szolgáltató ellenőrzése alatt állnak). e-Sealer v1.0 aláíró alkalmazás nem ilyen.

Konklúzió: **nem vonatkoznak rá a követelmények**

Bizt_köv7: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy az aláírónak bemutatott aláírandó adat ugyanaz, mint amit az aláíró kiválasztott.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	❍

Magyarázat: A adatok védelme részben az e-Sealer v1.0, részben az Utimaco SafeGuard Toolkit 2.50.02 feladata. A megjelenítőket pedig védeni kell.

Konklúzió: **megfelel**

Bizt_köv8: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy a formattált aláírandó adat és aláírandó adat reprezentáns előállításához felhasznált aláírandó adat komponensek ugyanazok, mint amelyeket az aláírónak bemutattak a bemutatási eljárás során, és amelyeket a felhasználó kiválasztott.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	❍

Magyarázat: Részben az e-Sealer v1.0, részben az Utimaco SafeGuard Toolkit 2.50.02 feladata.

Konklúzió: **megfelel**

A következő két követelmény csak osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozik.

Bizt_köv9: … Bizt_köv10:
Magyarázat: Az az e-Sealer v1.0 nem osztott architektúrájú aláíró alkalmazás.
Konklúzió: **nem vonatkoznak rájuk a követelmények**

Bizt_köv11: Meg kell gátolni, hogy az aláírási folyamatba beavatkozhassanak olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	❍	❍

Magyarázat: Mivel az e-Sealer v1.0 egy alkalmazás, ezért a futtató környezetnek kell biztosítania, hogy az e-Sealer v1.0 alkalmazás által megvalósított folyamatba ne avatkozhassanak be nem megbízható folyamatok.
Konklúzió: **feltétellel megfelel** (lásd 2. számú feltétel)

Bizt_köv12: Az aláírandó adatnak tartalmaznia kell egy aláírói dokumentumot. (Egy 0 hosszú "üres" dokumentumhoz ne lehessen aláírást előállítani).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	❍	❍

Magyarázat: A probléma az aláírási szabályzat által engedélyezett .pdf és .xml fájlokra nem következhet be.
Konklúzió: **megfelel**

Bizt_köv13: Az aláírandó adatnak tartalmaznia kell az aláírónak azt a tanúsítvány-azonosítóját, amely az elektronikus aláírás létrehozásánál a biztonságos aláírás-létrehozó eszköz által felhasznált aláírás-létrehozó adathoz kapcsolódik, s amely az aláíró szándékának megfelel.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	❍	●

Magyarázat: Nem csak az aláíró kulcs tanúsítványát tartalmazza a PKCS#7-es csomag, hanem a teljes tanúsítvány láncot, és a hozzá tartozó CRL-eket is.
Konklúzió: **megfelel**

Bizt_köv14: Az aláírandó adatnak tartalmaznia kell egy hivatkozást az aláírási szabályzatra.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	●	●	❍

Magyarázat: Az aláírási szabályzatot implicit módon valósítja meg az e-Sealer v1.0.
Konklúzió: **megfelel**

Bizt_köv15: Az aláírandó adatnak tartalmaznia kell a kötelezettségvállalás típus tulajdonságot, ha az aláírási szabályzat egynél több kötelezettségvállalás típust határoz meg.
Magyarázat: Az aláírási szabályzat egy kötelezettségvállalási típust definiál.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv16: Ha az alkalmazás vagy az érvényben lévő biztonsági szabályzat egynél több aláírói dokumentum tartalom formátumot enged meg, az aláírandó adatnak tartalmaznia kell az aláírói dokumentum tartalom formátumot.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	❍

Magyarázat: A tartalom formátum tárolódik az aláírandó adatok között. Ezen kívül a PKCS#7 csomag neve is tartalmazza nevében az eredeti fájl kiterjesztését. /Separate signature esetén az aláírandó adatok közt nem kerül tárolásra a tartalom formátum. Ebben az esetben védeni kell a fájlokat az átnevezéstől./

Konklúzió: **megfelel**

Bizt_köv17: Az aláíró dokumentumát megjelenítő összetevőnek lehetővé kell tennie az aláírói dokumentum tartalom-formátumának csatolását vagy közvetett módon az aláírási szabályzat részeként, vagy pedig egy közvetlen aláírás tulajdonságként.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	❍

Magyarázat: A tartalom formátum tárolódik az aláírandó adatok között. Ezen kívül a PKCS#7 csomag neve is tartalmazza nevében az eredeti fájl kiterjesztését. /Separate signature esetén az aláírandó adatok közt nem kerül tárolásra a tartalom formátum. Ebben az esetben védeni kell a fájlokat az átnevezéstől./

Konklúzió: **megfelel**

Bizt_köv18: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha a dokumentum nem felel meg a tartalom formátummal meghatározott szintaxisnak, és lehetővé kell tennie az aláíró számára, hogy félbeszakítsa az aláírási folyamatot.

Magyarázat: Megjelenítőt nem tartalmaz a program.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv19: A használati útmutatóban jelezni kell, hogy milyen tartalom formátum helyes kezelésére alkalmas az aláíró dokumentumát megjelenítő összetevő.

Magyarázat: Megjelenítőt nem tartalmaz a program.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv20: A használati útmutatóban jelezni kell, hogy milyen lehetséges következménnyel jár, ha az aláíró tévesen választja ki a tartalom formátumot.

Magyarázat: Megjelenítőt nem tartalmaz a program.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv21: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha olyan aláírói dokumentumot kíván aláírni, amelynek tartalom formátumát nem támogatja.

Magyarázat: Megjelenítőt nem tartalmaz a program.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv22: Az aláíró dokumentumát megjelenítő összetevőnek biztosítania kell, hogy az aláírónak megmutatott aláírói dokumentum ugyanaz, mint amit az aláírási folyamat fog használni, és ugyanaz, mint amit az aláíró választott ki aláírásra.

Magyarázat: Megjelenítőt nem tartalmaz a program.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv23: A megjelenítő folyamatnak tájékoztatnia kell az aláírót, hogy egyéb aláírt adatok vannak beágyazva az aláírói dokumentumba (az aláíró dokumentumát megjelenítő összetevőnek kapcsolódnia kell egy aláírás ellenőrző rendszerrel az ilyen aláírások ellenőrzésére).
Magyarázat: Megjelenítőt nem tartalmaz a program.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv24: Az aláíró dokumentumát megjelenítő összetevőnek nem szabad lehetővé tennie az aláíró számára, hogy az aláírói dokumentum bármely részét megváltoztassa.
Magyarázat: Az aláírási szabályzat által engedélyezett .pdf és .xml fájlok megjelenítéséhez csak olyan megjelenítő összetevőt szabad használni, amely nem engedi megváltoztatni az aláírandó dokumentumot (tehát csak nézegetőt szabad telepíteni a gazdagépre, szerkesztőt nem).
Konklúzió: **feltétellel megfelel** (lásd 3. számú feltétel)

Bizt_köv25: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha nem képes az aláírói dokumentum minden részének a helyes, tartalom formátumnak megfelelő megjelenítésére.
Magyarázat: Az e-Sealer v1.0 az operációs rendszerben beállított alapértelmezett megjelenítőt használja.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv26: Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy tartalom formátum tulajdonság csatolását az aláírandó adatokhoz annak biztosítására, hogy az aláíró dokumentumának megjelenítése egyértelmű legyen. Vagyis pontosan úgy lehessen azt a későbbiekben megjeleníteni, mint ahogyan az aláírónak a megjelenítési folyamat során.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	❍

Magyarázat: A tartalom formátum tárolódik az aláírandó adatok között. Ezen kívül a PKCS#7 csomag neve is tartalmazza nevében az eredeti fájl kiterjesztését. Separate signature esetén az aláírandó adatok közt nem kerül tárolásra a tartalom formátum.
Konklúzió: **megfelel**

Bizt_köv27: Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy tartalom formátum tulajdonság csatolását az aláírandó adatokhoz annak biztosítására, hogy az aláíró dokumentum szemantikáját csak egyféleképpen lehessen értelmezni.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	❍

Magyarázat: A tartalom formátum tárolódik az aláírandó adatok között. Ezen kívül a PKCS#7 csomag neve is tartalmazza nevében az eredeti fájl kiterjesztését. Separate signature esetén az aláírandó adatok közt nem kerül tárolásra a tartalom formátum.
Konklúzió: **megfelel**

Bizt_köv28: Az aláírás-létrehozó alkalmazásnak figyelmeztetnie kell az aláírót a rejtett szövegek, makrók vagy aktív kódok jelenlétére. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.

Magyarázat: Az aláírás szabályzat által megengedett, s az e-Sealer v1.0 által elfogadott tartalom formátumok között nincs olyan, amely aktív kódrészt tartalmazhat.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv29: Az aláírás tulajdonság megjelenítési folyamatának lehetővé kell tennie az aláíró számára az aláírás tulajdonságok megtekintését.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az aláíró számára biztosítva van a tartalom formátum és a tanúsítvány megnézésének lehetősége.

Konklúzió: **megfelel**

Bizt_köv30: Az aláírás tulajdonságokat megjelenítő folyamatnak biztosítania kell, hogy az aláírónak megjelenített aláírás tulajdonság ugyanaz, mint ami az aláírás folyamatában aláírásra kerül majd, és amit az aláíró kiválasztott az aláíráshoz.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	❍	●	●

Magyarázat: Részben az e-Sealer v1.0, részben az Utimaco SafeGuard Toolkit 2.50.02 feladata. /A tanúsítványláncot a Windows tanúsítványtárába is telepíteni kell./

Konklúzió: **megfelel**

Bizt_köv31: Az aláírás tulajdonságok sértetlenségét és hitelességét meg kell védeni.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Részben az e-Sealer v1.0, részben az Utimaco SafeGuard Toolkit 2.50.02 feladata.

Konklúzió: **megfelel**

Bizt_köv32: Az aláírót figyelmeztetni kell az aláírás tulajdonságokban jelenlévő bármilyen rejtett szövegről, makróról vagy aktív kódról. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.

Magyarázat: Az aláírási tulajdonságok nem tartalmaznak aktív kódrészt.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv33: Az aláírás tulajdonság megjelenítő folyamatnak figyelmeztetnie kell az aláírót bármely, az aláírás tulajdonságokba beágyazott rejtett vagy aktív komponens (pl. word processzor makró) jelenlétére. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.

Magyarázat: Az aláírási tulajdonságok nem tartalmaznak aktív kódrészt.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv34: Az aláírás tulajdonság megjelenítő összetevőnek lehetővé kell tennie az aláíró számára, hogy átvizsgálja a kiválasztott, aláírandó adatokhoz csatolandó tanúsítvány fő összetevőit.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az aláíró az aláírás előtt megnézheti aláíró kulcs tanúsítványát.
Konklúzió: **megfelel**

Bizt_köv35: Az aláírási folyamat megkezdése előtt az aláíróval kölcsönható összetevőnek egy olyan nem nyilvánvaló, az aláírás-létrehozó alkalmazással folytatott, aláírás kiváltási cselekvést kell elvárnia az aláírótól, amely véletlenül valószínűleg nem következne be.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az aláírás tényleges megkezdése előtt az e-Sealer v1.0 PIN kódot kér be.
Konklúzió: **megfelel**

Bizt_köv36: Az aláírás-létrehozó alkalmazásnak egy korlátot kell megadnia arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet.

Magyarázat: A PIN kód megadása után azonnal elkezdődik az aláírási folyamat, melynek során az Utimaco SafeGuard Toolkit 2.50.02 a BALE-val együttműködve állítja elő a PKCS#7 csomagot. /Az e-Seale v1.0 sorozat aláírást készíttet, vagyis az aláírás kiváltása után a forráskönyvtár teljes tartalma aláírásra kerül./

Konklúzió: **megfelel**

Bizt_köv37: Ha az időkorlát letelik, az egész aláírási folyamatot félbe kell szakítani, az aláírótól az aláírási folyamat újraindítását követelve meg, hitelesítő adatainak újra megadását is beleértve. Az újraindítás szükségességéről tájékoztatni kell az aláírót.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az időkorlát a forráskönyvtár teljes tartalmának aláírásához szükséges idő. Ha ez idő alatt a BALE-t kiveszik az olvasóból, akkor az aláírás folyamata megszakad. /A PIN kód megadása után azonnal elkezdődik az aláírási folyamat, melynek során az Utimaco SafeGuard Toolkit 2.50.02 a BALE-val együttműködve állítja elő a PKCS#7 csomagot./

Konklúzió: **megfelel**

Bizt_köv38: Az aláírás-létrehozó alkalmazásnak eszközt kell biztosítania a felhasználó számára ahhoz, hogy az megadhassa az aláírót hitelesítő adatot ezen keresztül a biztonságos aláírás-létrehozó eszköz számára.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: A PIN kód bekérése biztosított.
Konklúzió: **megfelel**

Bizt_köv39: Az aláírás-létrehozó alkalmazásnak meg kell őriznie az aláírót hitelesítő adatok bizalmasságát, és biztonságosan törölnie kell azokat, amint azokra nincs már szükség.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	●	❍	●	❍

Magyarázat: Az e-Sealer v1.0 törli a PIN kódot, mikor már erre nincs szüksége. Ezt a törlést az értékelők forráskód szinten is ellenőrizték.
Konklúzió: **megfelel**

Bizt_köv40: Ha az aláírni szándékozó egy korlátot meghaladó számban helytelen hitelesítő adatot ad meg, akkor az újrapróbálkozást le kell tiltani, egyúttal hibajelzést kell adni az aláíró részére, ha az aláíró hitelesítési módszert már nem blokkolta korábban a biztonságos aláírás-létrehozó eszköz. Az aláírni szándékozó részére egy megfelelő üzenetet kell küldeni.
Magyarázat: Ez a BALE feladata
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv41: Ha az aláírni szándékozó ismételten helytelen hitelesítő adatot ad meg (pl. három egymást követő alkalommal), a biztonságos aláírás-létrehozó eszköznek félbe kell szakítania az aláíró hitelesítését, és erről informálnia kell az aláírás-létrehozó alkalmazást, amelynek az aláíró részére egy megfelelő üzenetet kell küldeni.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	❍	●

Magyarázat: Hibás PIN kód megadásakor az e-Sealer v1.0 tájékoztatást ad.
Konklúzió: **megfelel**

Bizt_köv42: Egy megbízható útvonalat kell biztosítani a PIN/jelszó továbbítására a PIN pad (vagy billentyűzet) és a biztonságos aláírás-létrehozó eszköz között az aláírás-létrehozó alkalmazáson keresztül.
Magyarázat: Ez a BALE és a PKCS#11-es middleware feladata.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv43: Biztosítani kell egy olyan funkciót, amellyel a tudáson alapuló hitelesítő adatok lecserélhetőek (hacsak ez nincs tiltva egy aláírás-létrehozó alkalmazás típus esetében az alkalmazás szolgáltatójának biztonsági szabályzatában).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	❍	❍

Magyarázat: A PIN kód cserére a BALE megfelelő szoftvere használható.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv44: A megadott PIN kódot (vagy jelszót) nem szabad kijelezni, bár egy számjegy vagy karakter begépelését vissza kell jelezni egy megfelelő jellel (pl. egy csillag karakterrel), amely nem fedi fel magát a PIN-t (vagy a jelszót).

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: A megadott PIN kód a képernyőn nem látható.
Konklúzió: **megfelel**

Bizt_köv45: Az aláírás-létrehozó alkalmazásnak meg kell követelnie az új PIN kód (jelszó) kétszeri megadását, és ellenőriznie kell ezek azonosságát, mielőtt az új PIN kódot (jelszót) továbbítaná a biztonságos aláírás-létrehozó eszköznek.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	❍	❍

Magyarázat: A PIN kód cserére a BALE megfelelő szoftvere használható.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv46: Megbízható útvonalat kell biztosítani a biometrikus adatok továbbítására a biometrikus érzékelő egység és a biztonságos aláírás-létrehozó eszköz közé
Magyarázat: Nincsenek biometrikus adatok a rendszerben.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv47: Biztosítani kell az aláírót hitelesítő adatok kriptográfiai védelmét (ha egy nyilvános biometrikus tulajdonságot használnak) a hitelesség garantálására és a visszajátszásos támadások elkerülésére.
Magyarázat: Nincsenek biometrikus adatok a rendszerben.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv48: Az aláírás-létrehozó alkalmazásnak azt a helyes aláírandó adat formátumot kell előállítania, amelyet az aláíró által kiválasztott aláírási szabályzat határoz meg.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 állítja elő a PKCS#7 formátumú csomagot, ahogyan azt az aláírási szabályzat meghatározza.
Konklúzió: **megfelel**

Bizt_köv49: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy “elfogadott” lenyomatoló algoritmus használatát lenyomatolásra.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az e-Sealer v1.0 az SHA1 lenyomatoló algoritmus használatának beállításával hívja meg az Utimaco SafeGuard Toolkit 2.50.02 megfelelő függvényét a PKCS#7 elkészítéséhez.
Konklúzió: **megfelel**

Bizt_köv50: Az aláírás-létrehozó alkalmazásnak biztosítania kell az “emsa-pkcs1-v1_5” elektronikus aláírás input formátum (feltöltési módszer) kizárólagos használatát.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 készíti el az aláírást, s ehhez a szabványos /emsa-pkcs1-v1.5/ feltöltést használja.
Konklúzió: **megfelel**

Bizt_köv51: Az aláírás-létrehozó alkalmazásnak biztosítania kell a helyes aláírandó adatreprezentáns előállítását az elektronikus aláíráshoz.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 állítja elő a PKCS#7 formátumú csomagot.

Konklúzió: **megfelel**

Bizt_köv52: Az aláírás-létrehozó rendszernek támogatnia kell a fizikai interfész minden fontos részletét egy meghatározott tartományon belül, vagy egy meghatározott jellegzetességgel, az általa támogatott biztonságos aláírás-létrehozó eszköz típusok megfelelő működésének biztosítása érdekében.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az Utimaco SafeGuard Toolkit 2.50.02 támogat minden PKCS#11 felülettel rendelkező BALE eszközt.

Konklúzió: **megfelel**

Bizt_köv53: Amennyiben vezeték nélküli összeköttetést használnak az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között, az SSC összetevőnek megfelelő eszközöket kell biztosítania a lehallgatás és a zavarás megakadályozása érdekében.

Magyarázat: Nem használhat az alkalmazást futtató számítógép vezeték nélküli eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv54: Az SSC összetevőnek biztosítania kell a biztonságos aláírás-létrehozó eszköz helyes funkcionalitásának kiválasztását, amennyiben a biztonságos aláírás-létrehozó eszköz ilyen kiválasztást tesz szükségessé (mert pl. több alkalmazást támogat párhuzamosan). Biztosítania kell az aláíró választása szerinti, az aláírás tulajdonságoknak megfelelő aláírás-létrehozó adat (magánkulcs) használatát, amennyiben több magánkulcs van a biztonságos aláírás-létrehozó eszközön tárolva.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	●	●

Magyarázat: Az e-Sealer v1.0 lehetővé teszi a kulcsok kiválasztását, de csak az olyanokét, amelyek megfelelő tartalmú tanúsítvánnyal rendelkeznek.

Konklúzió: **megfelel**

Bizt_köv55: Az SSC-t védeni kell a jogosulatlan módosításokkal szemben.

Magyarázat: A biztonságos kommunikációnak az Utimaco SafeGuard Toolkit 2.50.02 és a BALE közt kell fennállnia.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv56: Az SSA-nak támogatnia kell az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között az entitások hitelesítését, hogy megbízható jelzést adhasson az aláírónak egy sikeres hitelesítésről, és védenie kell az ezt követő kommunikációt egy biztonságos üzenetközvetítéssel.

Magyarázat: A biztonságos kommunikációnak az Utimaco SafeGuard Toolkit 2.50.02 és a BALE közt kell fennállnia.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv57: Intézkedéseket kell tenni annak biztosítására, hogy vírusok ne ronthassák el az SCA összetevőket, és hogy az esetlegesen vírussal fertőzött SCA összetevők megfelelően helyre legyenek állítva.
Magyarázat: Ez az operációs rendszer feladata.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv58: Az SCA-nak védenie kell funkcionális összetevőinek sértetlenségét, és meg kell akadályozni, hogy behatolók elrontsák ezeket.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	❍	●	❍

Magyarázat: Mivel az e-Sealer v1.0 egy alkalmazás, ezért a futtató környezetnek és az operációs rendszernek kell biztosítania az e-Sealer v1.0 alkalmazás funkcionális összetevőinek sértetlenségét.
Konklúzió: **védett környezetben megfelel** (lásd 2. számú feltétel)

Bizt_köv59: Intézkedéseket kell tenni az aláírás-létrehozó alkalmazásban arra, hogy importált aláírás-létrehozó alkalmazás komponenseket csak egy biztonságos letöltés felhasználásával lehessen installálni.
Magyarázat: Nincsenek importált aláírás létrehozó komponensek..
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv60: Az aláírás-rendszer összes, az aláírás-létrehozás vagy aláírás-ellenőrzés folyamattal kölcsönhatásba lépő összetevőjét egy **biztonságos területen** kell megvalósítani.

Értékelés módja:	Interjú	Dokumentáció	Tapasztalat	Teszt
	❍	●	❍	❍

Magyarázat: Mivel az e-Sealer v1.0 egy alkalmazás, ezért a futtató környezetnek és az operációs rendszernek kell biztosítania a biztonságos területet.
Konklúzió: **védett környezetben megfelel** (lásd 2. számú feltétel)

3. Az e-Sealer v1.0 megfelelése a követelményeknek

3.1 Az e-Sealer v1.0 megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	**megfelel**
F_SDP_2	nem vonatkozik rá a követelmény
F_SDP_3	**megfelel**
F_SDP_4	**megfelel**
F_SAV_1	**megfelel**
F_SAV_2	**megfelel**
F_SIC_1	**megfelel**
F_SIC_2	**megfelel**
F_SIC_3	**megfelel**
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**megfelel**
F_SSC_1	**megfelel**
F_SSC_2	nem vonatkozik rá a követelmény
F_SSC_3	**megfelel**
F_SSC_4	**megfelel**
F_SSC_5	**megfelel**
F_SSC_6	**megfelel**
F_SSC_7	**megfelel**
F_SSC_8	**megfelel**
F_SSC_9	**megfelel**
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	**megfelel**
F_SDOC_1	**megfelel**
F_SLC_1	**megfelel**
F_SCPC_1	**megfelel**
F_I/O_1	nem vonatkozik rá a követelmény
F_I/O_2	**megfelel**
F_I/O_3	**megfelel**
F_ISV_1	nem vonatkozik rá a követelmény
F_ISV_2	**megfelel**
F_USV_1	nem vonatkozik rá a követelmény
F_human_1	nem vonatkozik rá a követelmény
F_human_2	nem vonatkozik rá a követelmény
F_human_3	nem vonatkozik rá a követelmény
F_human_4	nem vonatkozik rá a követelmény
F_human_5	nem vonatkozik rá a követelmény
F_human_6	nem vonatkozik rá a követelmény
F_machine_1	nem vonatkozik rá a követelmény
F_machine_2	**megfelel**
F_general_1	**megfelel**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	**megfelel**

3.2 Az e-Sealer v1.0 megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	**megfelel**
Bizt_köv2	**megfelel**
Bizt_köv3	nem vonatkozik rá a követelmény
Bizt_köv4	nem vonatkozik rá a követelmény
Bizt_köv5	nem vonatkozik rá a követelmény
Bizt_köv6	nem vonatkozik rá a követelmény
Bizt_köv7	**megfelel**
Bizt_köv8	**megfelel**
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	**feltétellel megfelel** (lásd 2. számú feltétel)
Bizt_köv12	**megfelel**
Bizt_köv13	**megfelel**
Bizt_köv14	**megfelel**
Bizt_köv15	nem vonatkozik rá a követelmény
Bizt_köv16	**megfelel**
Bizt_köv17	**megfelel**
Bizt_köv18	nem vonatkozik rá a követelmény
Bizt_köv19	nem vonatkozik rá a követelmény
Bizt_köv20	nem vonatkozik rá a követelmény
Bizt_köv21	nem vonatkozik rá a követelmény
Bizt_köv22	nem vonatkozik rá a követelmény
Bizt_köv23	nem vonatkozik rá a követelmény
Bizt_köv24	**feltétellel megfelel** (lásd 3. számú feltétel)
Bizt_köv25	nem vonatkozik rá a követelmény
Bizt_köv26	**megfelel**
Bizt_köv27	**megfelel**
Bizt_köv28	nem vonatkozik rá a követelmény
Bizt_köv29	**megfelel**
Bizt_köv30	**megfelel**
Bizt_köv31	**megfelel**
Bizt_köv32	nem vonatkozik rá a követelmény
Bizt_köv33	nem vonatkozik rá a követelmény
Bizt_köv34	**megfelel**
Bizt_köv35	**megfelel**
Bizt_köv36	**megfelel**
Bizt_köv37	**megfelel**
Bizt_köv38	**megfelel**
Bizt_köv39	**megfelel**
Bizt_köv40	nem vonatkozik rá a követelmény
Bizt_köv41	**megfelel**
Bizt_köv42	nem vonatkozik rá a követelmény
Bizt_köv43	nem vonatkozik rá a követelmény
Bizt_köv44	**megfelel**
Bizt_köv45	nem vonatkozik rá a követelmény
Bizt_köv46	nem vonatkozik rá a követelmény
Bizt_köv47	nem vonatkozik rá a követelmény
Bizt_köv48	**megfelel**
Bizt_köv49	**megfelel**
Bizt_köv50	**megfelel**
Bizt_köv51	**megfelel**
Bizt_köv52	**megfelel**
Bizt_köv53	nem vonatkozik rá a követelmény
Bizt_köv54	**megfelel**

Bizt_köv55	nem vonatkozik rá a követelmény
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	nem vonatkozik rá a követelmény
Bizt_köv58	**feltétellel megfelel** (lásd 2. számú feltétel)
Bizt_köv59	nem vonatkozik rá a követelmény
Bizt_köv60	**feltétellel megfelel** (lásd 2. számú feltétel)

4. A Tanúsítási jelentés eredménye, érvényességi feltételei

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltétel teljesülése esetén az e-Sealer v1.0 aláíró alkalmazás alkalmas minősített elektronikus aláírások létrehozására.

4.2 Érvényességi feltételek

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az e-Sealer v1.0 aláíró alkalmazás által kezelt aláírások biztonságához.
A feltételek nem a megvalósított e-Sealer v1.0 aláíró alkalmazásra, hanem annak telepítésére, környezetére és működtetésére vonatkoznak.

1. számú feltétel
Az e-Sealer v1.0 aláíró alkalmazást olyan biztonságos aláírás-létrehozó eszköz felhasználása mellett alkalmazzák, mely szerepel a Nemzeti Hírközlési Hatóság BALE nyilvántartásában.
Érintett biztonsági követelmények: Bizt_köv38,
Bizt_köv52,
Bizt_köv54.

2. számú feltétel
Az e-Sealer v1.0 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy **biztonságos területen** valósítsák meg.
/Mivel az e-Sealer v1.0 alkalmazás egy szoftver, ezért a futtató környezetnek biztosítania kell, hogy magát az e-Sealer v1.0 alkalmazást ne lehessen lecserélni./
Érintett biztonsági követelmény: Bizt_köv11,
Bizt_köv58,
Bizt_köv60.

3. számú feltétel
Az aláírási szabályzat által engedélyezett .pdf és .xml fájlok megjelenítéséhez olyan megjelenítő összetevőt kell telepíteni, amely nem engedi megváltoztatni az aláírandó dokumentumot (tehát csak nézegetőt szabad telepíteni a gazdagépre, szerkesztőt nem).
Érintett biztonsági követelmények: Bizt_köv24

5. A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A jelen tanúsításhoz figyelembe vett, a fejlesztőktől független értékelés az informatikai termékek technológia szempontú értékelésére szolgáló, kialakítás alatt álló nemzeti séma, a **Magyar Informatikai Biztonsági és Értékelési Séma** /MIBÉTS/ módszertanát követte.
Ennek a fejlesztőktől független értékelés garancia szintje az ISO 14508 /Common Criteria/ **EAL 3**-as szintjéhez hasonló volt. /megfelelt a MIBÉT Séma **fokozott értékelési garanciaszint**jének, mely a fejlesztőktől függetlenül garantált biztonság közepes szintjét biztosítja./

A fejlesztőktől független értékelés összefoglalásaként egy értékelési jelentés készült.

Az értékelési jelentésnek a fő megállapításai az alábbiak voltak:

Az értékelés tárgya, az e-Sealer v1.0 elektronikus aláíró program, megfelel biztonsági előirányzatának (kielégíti az "e-Sealer v1.0 elektronikus aláíró program biztonsági előirányzata, verzió 1.2, 2004-04-05" dokumentumban megfogalmazott funkcionális és garanciális biztonsági követelményeket).

Az értékelés tárgya, az e-Sealer v1.0 elektronikus aláíró program, megfelel aláírási szabályzatának (kielégíti az "Erste Bank Hungary Rt. - Elektronikus egyenleg aláíró program - Elektronikus aláírási szabályzata - verzió 1.0, 2004-04-30" dokumentumban megfogalmazott szabályokat és elvárásokat).

Az értékelés tárgya, az e-Sealer v1.0 elektronikus aláíró program, megfelel a minősített aláírások létrehozását és ellenőrzését végző alkalmazásokra vonatkozó (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 dokumentumokban meghatározott) **mértékadó funkcionális és biztonsági követelményeknek.**

Az e-Sealer v1.0 biztonsági funkciónak megvalósításában jelentős szerepet játszó **beépített függvények** /Utimaco SafeGuard Toolkit, vizsgált API verziószám: UMB/CW/V02.50.02/W (Feb 9 2004 / 15:56:42)/ **helyesen, a leírásuknak megfelelően működnek**.

A jelen tanúsítási jelentés az értékelési jelentésben megfogalmazott és dokumentált eredményekre épül.

Az értékelés az alábbi garanciaosztályokra terjedt ki:
- konfiguráció menedzselés,
- kiszállítás és működtetés,
- fejlesztés,
- útmutató dokumentumok,
- életciklus támogatás,
- tesztek,
- sebezhetőség felmérése.

6. A tanúsításhoz figyelembe vett dokumentumok

6.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign; Area G1, 14170 munkacsoport egyezmény: Security Requirements for Signature Creation Systems

CEN/ISSS/E-Sign; Area G2, 14171 munkacsoport egyezmény: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign; Area V, 14172-4 munkacsoport egyezmény: EESSI Conformity Assessment Guidance - Part 4: Signature Creation Application and Procedures for Electronic Signature Verification

6.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1 A tanúsításhoz figyelembe vett fejlesztői dokumentumok

Kérelem a tanúsítás elvégzésére
Kérdőív a tanúsítás kérelmezéséhez
Az e-Sealer v1.0 elektronikus aláíró program biztonsági előirányzata v1.2
Erste Bank Hungary Rt. - Elektronikus egyenleg aláíró program - Elektronikus aláírási szabályzata v1.0
Konfigurációmenedzselési terv, e-Sealer 1.0
Összefoglaló az 1. helyszíni szemlén végzett interjúról
e-Sealer v1.0 Adminisztrátori kézikönyv
e-Sealer v1.0 Használati útmutató
Technikai specifikáció az Erste Bank Rt. részére fejlesztendő elektronikus egyenleg aláíró program server-oldali moduljára (Funkcionális specifikáció) v1.0
Az e-Sealer V1.0 aláíró alkalmazás alrendszerei, biztonsági funkciói és mechanizmusai (magas szintű terv) v1.3
Erste Bank, Elektronikus egyenleg aláíró program, Fejlesztői teszt terv v1.0
Erste Bank, Elektronikus egyenleg aláíró program, Fejlesztői tesztelés eredménye v1.01

6.2.2 A tanúsításhoz figyelembe vett fejlesztőktől független dokumentumok

Értékelési jelentés az e-Sealer v1.0 elektronikus aláíró programról
e-Sealer V1.0, A fejlesztői tesztelés lefedettségi elemzése v1.1
e-Sealer V1.0, A fejlesztői tesztelés mélységi elemzése v1.0
ERSTE Bank, Elektronikus egyenleg aláíró program, e-Sealer V1.0, Sebezhetőségi elemzés v1.0
Telephely látogatás Jegyzőkönyve
Független Tesztelés Jegyzőkönyve
2. számú Független Tesztelés Jegyzőkönyve
e-Sealer V1.0, Az áthatolás tesztelés eredménye

7. Rövidítések

API	Application Programming Interface
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DHC	Data Hashing Component
DTBS	Data To Be Signed
DTBSF	DTBS Formatter
EAL	Evaluation Assurance Level
PIN	Personal Identification Number
SAC	Signer's Authentication Component
SAV	Signature Attribute Viewer
SCA	Signature Creation Application
SDC	Signer's Document Composer
SDOC	Signed Data Object Composer
SDP	Signer's Document Presenter
SIC	Signer's Interaction Component
SLC	Signature Logging Component
SSA	SSCD/SCA Communicator Authenticator
SSC	SSCD/SCA Communicator
SSCD	Secure Signature Creation Device
TJ	Tanúsítási jelentés