Tanúsítási jelentés

Hung-TJ-010-2003

a MultiSigno Developer Professional

aláíró alkalmazás fejlesztő készletről

/Kopint-Datorg Rt./

/verzió: Pack.dll 2.0/

Tartalom

1. A MultiSigno Developer Professional legfontosabb tulajdonságainak összefoglalása

A **MultiSigno Developer Professional** egy olyan fejlesztői készlet, mely Windows 32-bites operációs rendszerhez biztosít DLL felületet (a későbbiekben a termékre **Pack.dll 2.0** néven is hivatkozni fogunk). Önmagában működésképtelen, megbízható aláíró alkalmazások fejlesztésére használható fel.
A MultiSigno Developer Professional által nyújtott felület lehetőséget nyújt XML csomagok nyitására, digitális aláírására, az aláírások ellenőrzésére, valamint objektumok és aláírások kezelésére.
A MultiSigno Developer Professional segítségével olyan aláíró (aláírás-létrehozó és aláírás-ellenőrző) alkalmazások fejleszthetők, melyek alkalmasak minősített elektronikus aláírások létrehozására és ellenőrzésére.

A MultiSigno Developer Professional az alábbi szabványos formátumokat és protokollokat támogatja:

„XML Advanced Digital Signature" (XAdES) szabványos csomagok kezelése, közte:

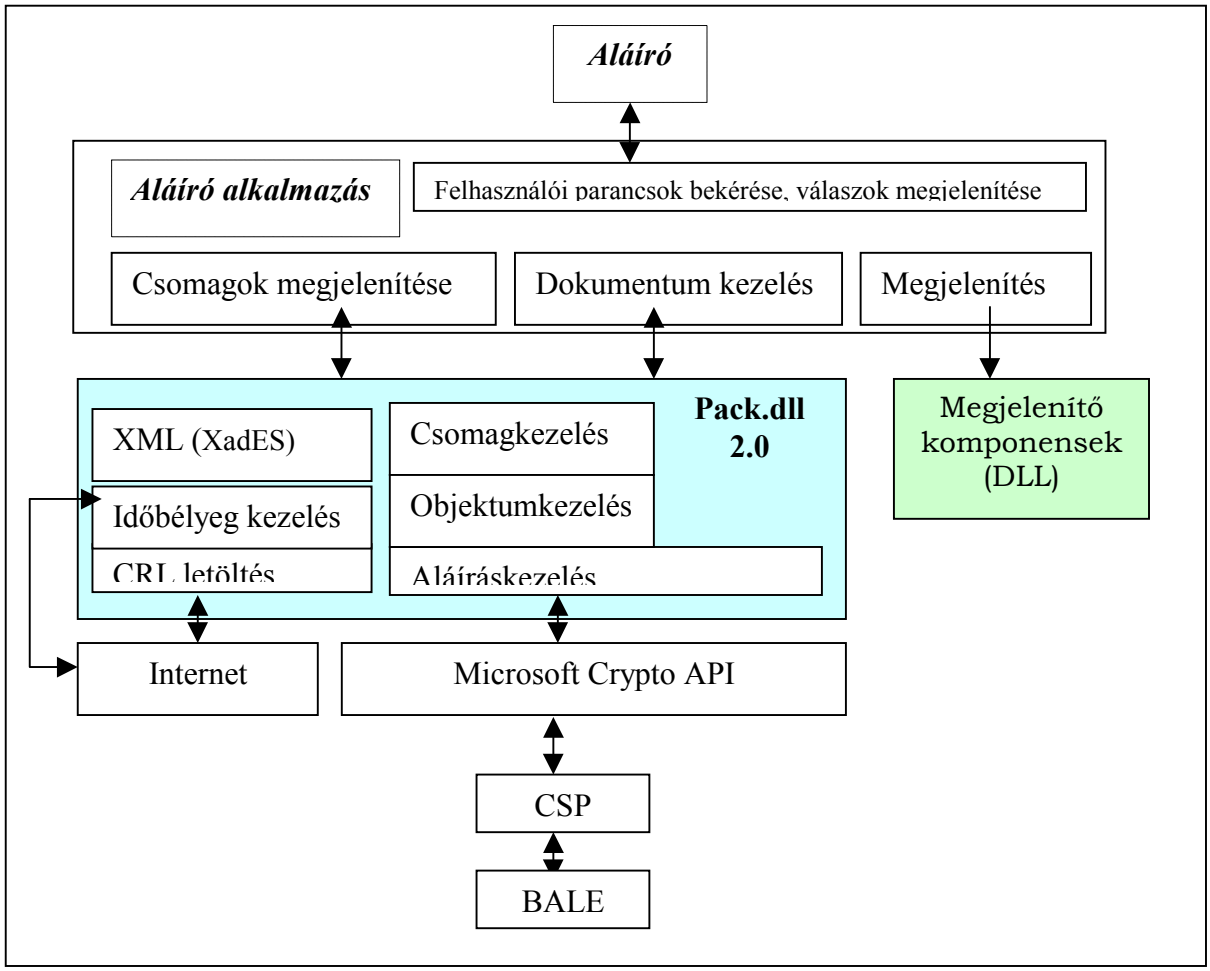
- együttes aláírások kezelése (több dokumentumot összefogó csomag aláírása),
- többszörös aláírások kezelése (több személy aláírása ugyanazon a csomagon),
- X.509 v3 tanúsítványok kezelése,
- tanúsítvány visszavonási listák lekérdezése a hitelesítés-szolgáltatóktól (HTTP, HTTPS, LDAP protokollokkal, a tanúsítványból kiolvasott elérési helyről),
- az aláírás időpontjának aláírt biztonsági tulajdonságként való kezelése,
- időbélyegzés készíttetés és ellenőrzés (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve),
- aláírás ellenőrzés (ahol az ellenőrzés alapja az időbélyegzésben szereplő időpont).

A fenti aláírás létrehozó és ellenőrző funkciókon kívül a MultiSigno Developer Professional támogatja a csomagok titkosítását és dekódolását is, de ez a funkcionalitás kívül esik jelen tanúsítvány hatókörén.
Ugyancsak kívül esnek jelen tanúsítvány hatókörén a MultiSigno Developer Professional bázisán fejlesztett aláíró alkalmazások (bár a fejlesztő eszköz funkcionalitása, biztonságos és korrekt megvalósítása nyilván átöröklődik az ebből – szakszerűen és gondosan – fejlesztett alkalmazásokba).

A MultiSigno Developer Professional (Pack.dll 2.0) fejlesztő készlet a Windows operációs rendszerek erőforrásaira, eszközeire támaszkodik. A DLL egyes elemei a Microsoft Crypto API függvényeit hívják meg, s ezen keresztül (tetszőleges szabványos CSP-t használva, valamint a CSP-vel kommunikáló driver-eken keresztül) magát az aláírás-létrehozó eszközt (intelligens kártyát) szólítják meg, mely szintén igen sokféle lehet. Az aláírandó/ellenőrizendő XML struktúrára az MS Crypto API-n

valamint egyéb saját fejlesztésű komponenseken keresztül történik az aláírás létrehozásának/ ellenőrzésének aktivizálása.

Az alábbi ábra a MultiSigno Developer Professional (Pack.dll) strukturális felépítését, valamint egy aláíró rendszeren belül elfoglalt helyét szemlélteti. A kék háttérszínnel jelzett rész egyben jelen tanúsítvány hatókörét is jelzi.



A MultiSigno Developer Professional az alábbi algoritmusokat valósítja meg, illetve aktivizálja:

- a MultiSigno Developer Professional által megvalósított (egy csomagon belül kezelt dokumentumok integritásának ellenőrzésére használt) lenyomatoló függvény: **SHA-1**
- a MultiSigno Developer Professional által a CSP-n aktivizált (az XML struktúra digitális aláírására használt) lenyomatoló függvény: **SHA-1**
- a MultiSigno Developer Professional által a CSP-n aktivizált, az intelligens kártyával végrehajtott (XML struktúra aláírására használt) digitális aláíró algoritmus: **RSA (1024 bit)**

A MultiSigno Developer Professional képes együttműködni minden szabványos PC/SC kompatibilis kártyaolvasóval és minden SHA-1-t, 1024 bites RSA algoritmust és szabványos MS Crypto API-t támogató kártyatípussal.
A MultiSigno Developer Professional fejlesztő készlet (pack.dll 2.0) elemei lehetőséget nyújtanak szabványos XML csomagok nyitására, különböző objektumok kezelésére, valamint aláírásra és az aláírások ellenőrzésére.
Az alábbiakban áttekintjük a fejlesztő készlet által kínált lehetőségeket, logikus felhasználásuk sorrendjében.

A munka kezdete (csomag létrehozása vagy megnyitása)
Egy új XML csomag létrehozása mellett négyféleképp lehet csomagot megnyitni:

- létező file-ból /a pack.dll 2.0 által korábban létrehozott XML csomag megnyitása/,
- a memóriában /egy üres csomag létrehozása a megadott paraméterekkel/,
- létező, titkosított file-ból /a pack.dll 2.0 által titkosítva mentett file-ból a dekódolás után a csomag megnyitása/,
- titkosított, memóriában tárolt forrásból.

A létrehozott vagy megnyitott csomagra ezután beállítható vagy kiolvasható a csomag tulajdonosának neve, a csomag létrehozási ideje, valamint a csomag azonosítója.

Csomag feltöltése adatokkal
A csomagba kétféle adat vihető be közvetlenül: dokumentum és megjegyzés. E kétféle objektum bevitele történhet file-ból vagy közvetlenül memóriából.

Csomag tartalmának visszanyerése (lekérés)
Egy csomag tartalma kétféleképp kérhető le:

- a csomagban lévő objektumok azonosítója alapján közvetlenül (amennyiben ismert ez az érték),kérdezése/,
- közvetve, a csomag elemszámának lekérdezése után egyesével, a lekérdezett objektumokról egyúttal listát is készítve.

aláírás, aláírás ellenőrzése
Ez a pack.dll fő funkciója, számos függvény szolgál erre:

- egyszerű digitális aláírás (egy objektum egy aláíró általi aláírása),
- többszörös digitális aláírás (egy objektum több aláíró általi független aláírása),
- együttes digitális aláírás (több objektum egy aláíró általi aláírása),
- többszörös együttes digitális aláírás (a többszörös és együttes aláírás tetszőleges kombinációja),
- digitális aláírás ellenőrzése,
- egy aláírás által hitelesített objektumok visszaadása (együttes aláírás esetén hasznos),
- aláírásból az aláíró tanúsítványát visszanyerése.

csomag mentése, lezárása
A megnyitáshoz hasonlóan egy XML csomagot négyféleképp lehet menteni:

- file-ba, kódolatlanul,
- file-ba titkosítva /egy titkosító nyilvános kulcs alkalmazásával/,
- memóriába, kódolatlanul,
- memóriába titkosítva /egy titkosító nyilvános kulcs alkalmazásával/.

Funkcionalitásuk szerint az alábbi függvénytípusok vannak:

- csomagkezelő függvények,
- objektum (dokumentum és megjegyzés) kezelő függvények,
- aláíráskezelő függvények,
- tanúsítványkezelő függvények,
- utility függvények.

Összehasonlítás a pack 1.2 verzióval

A 2.0 verzió funkcionalitásában lefedi az 1.2 verziót (lásd HUNG-TJ-003/2003 számú tanúsítási jelentést az előző – 1.2-es - verzióról).

- magasabb biztonsági szintet biztosít (csak magas szintű biztonságot garantáló algoritmusokat hív fel, forrásszintű független ellenőrzésre került sor, stb.),
- közvetlenül támogatja a minősített aláírások kezelését (egy szigorú aláírási szabályzat támogatásával, mely például nem enged meg aktív kódot vagy makrót tartalmazható adatformátum aláírását, mely az aláírás időpontját mindig aláírt biztonsági tulajdonságként kezeli, stb.)
- egyszerűbb, áttekinthetőbb feladatmegosztást valósít meg az egyes függvények között,
- hibatűrő paraméterkezelés megvalósítása (a specifikációnak megfelelő, de hibás paraméterek lekezelése),
- egyszerűbb objektumkezelés (a dokumentumok és a megjegyzések egységes kezelése).

A 2.0 verzió interfésze megváltozott, nem kompatibilis a régebbi verzióval.

megkötések a támogatott aláírási szabályzatokra:

A MultiSigno Developer Professional által támogatott (megvalósított, illetve érvényre juttatott) aláírási szabályzat leglényegesebb (még nem említett) elemei az alábbiak:

- az XML struktúra mindig tartalmazza az aláíró teljes tanúsítványláncát, és az aláírás időpontjában beszerezhető CRL-t (következésképpen a kezdeti ellenőrzéshez az aláírást fogadónak nem kell semmilyen érvényesítő adatot beszereznie), s ez a CRL később az utólagos ellenőrzés során frissebb változatra le is cserélhető,
- az aláírandó adatban mindig szerepel a tartalom formátuma, az engedélyezett formátumok a következők: XML. PDF, RTF, TXT.
- több kötelezettségvállalás típust is kezel a rendszer.

2. A MultiSigno Developer értékelési követelményei a CEN/ISSS: 14170 és 14171 munkacsoport egyezményei szerint

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. A fent említett nemzetközi (és nyilvánosan elérhető) dokumentumok által felállított funkcionális modellben szereplő összetevőket és egyéb fogalmakat ismertnek tételezzük fel. Ezek rövid összefoglalóját az „Aláíró alkalmazások funkcionális modellezése” című anyag is tartalmazza (készítette a HunGuard Kft.).

2.1 Funkcionális követelmények minősített elektronikus aláírásokat létrehozó/ellenőrző alkalmazások számára

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

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.

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.

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.

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.

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).

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

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

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

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).

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

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.

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

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

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.

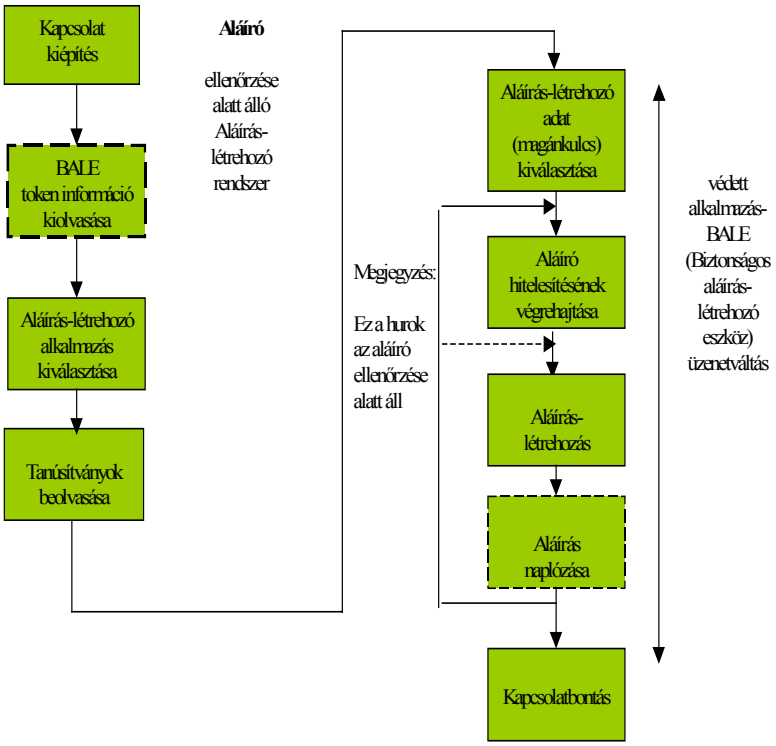
F_SSC_2: Egy szolgáltató ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 2. ábrán jelölt minden szükséges kommunikációt.

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

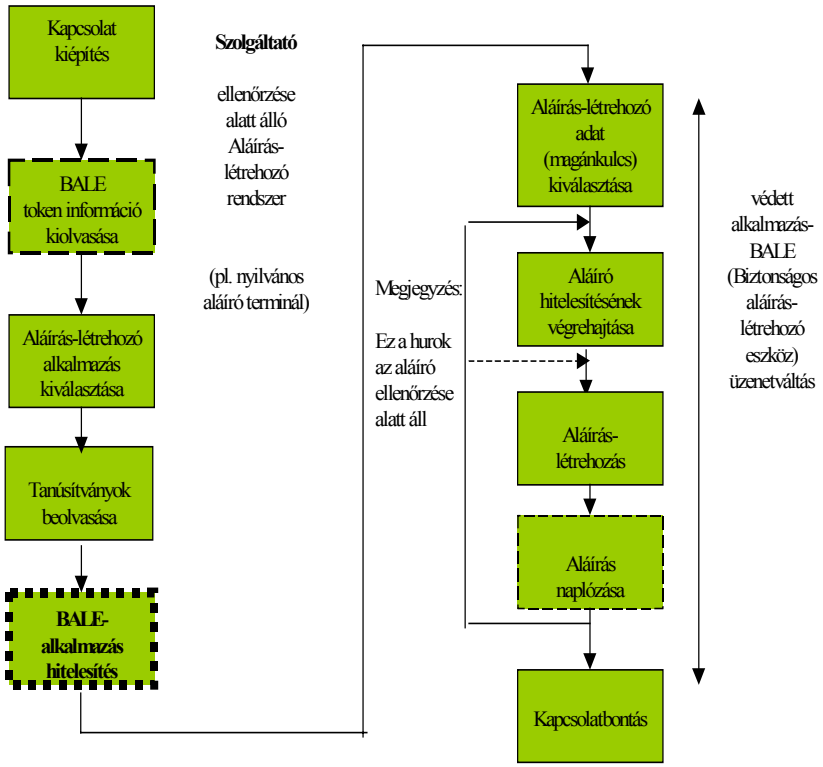
F_SSC_4: A biztonságos aláírás-létrehozó eszköz funkcionalitása megvalósítható egy olyan platformon (pl. intelligens kártya), amely egy vagy több biztonságos aláírás-létrehozó eszköz funkciót (amelyeket gyakran biztonságos aláírás-létrehozó eszköz alkalmazásnak is neveznek) hordoz és, ezen felül esetleg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

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

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.



1. ábra
Az aláíró ellenőrzése alatt álló aláírás-létrehozó rendszer esetén megvalósítandó együttműködési sorozat az aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között



2. ábra
Egy szolgáltató ellenőrzése alatt álló aláírás-létrehozó rendszer esetén megvalósítandó együttműködési sorozat az aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között

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.

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

F_SSC_9: A befejezett aláírásokat naplózni kell.

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.

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

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

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

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

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

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).

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

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.

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

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.

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

Ember által történő ellenőrzés esetén:

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.

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.

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.

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)

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.

F_human_6: A felhasználói interfészekre teljesüljenek az F_principles egyszerűségre és hibamentességre vonatkozó speciális elvárásai.

Gépi (automatikus) ellenőrzés esetén:

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.

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.

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.

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).

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.

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.

A felhasználókkal (aláírók, ellenőrzők) párbeszédet folytató rendszer teljesítse az alábbiakat:

- félreérthetetlen felhasználói útmutatót kell szolgáltatnia arra nézve, hogy hogyan kell a rendszert installálni, konfigurálni és használni;
- ön-leírónak kell lennie abban az értelemben, hogy minden párbeszéd-lépésnek azonnal érthetőnek kell lennie vagy a rendszertől kapott visszajelzéseken keresztül, vagy úgy, hogy az ellenőrző kérésére a rendszer magyarázatot ad;
- meg kell felelnie a felhasználók szokásos elvárásainak, azaz tudásuknak, képzettségüknek, tapasztalatuknak és az általánosan elfogadott konvencióknak;
- adaptálhatónak kell lennie, azaz támogatnia kell a felhasználók egyéni igényeit és preferenciáit;
- hibatűrőnek kell lennie úgy, hogy a nyilvánvaló input hibák ellenére az eredményt el lehessen érni minimális javításokkal.
- tájékoztató hiba üzeneteket kell küldenie, a felhasználó továbbhaladása érdekében;
- visszajelzéseket kell szolgáltatnia, mely megerősíti a felhasználó által végrehajtott tevékenység helyességét (vagy helytelenségét);
- a hibaüzenetek legyenek kellően informatívak, adjanak eligazítást a hiba okáról, a szükséges teendőkről (pl. a “Hibakód: 213” hibaüzenet nem igazán segítőkész);
- szabatos és minden részletre kiterjedő terminológia helyett hétköznapi kifejezéseket kell használni (a technikai kifejezéseket ugyanis a legtöbb felhasználó nem érti, és nem is kell értenie);
- alkalmaznia kell a színek használatára vonatkozó konvenciókat (pl. piros = hiba, zöld = továbbhaladás/siker);
- minden időpontban képesnek kell lennie arra, hogy az éppen végrehajtás alatt álló műveletet félbeszakítsa és vagy visszatérjen a főmenübe, vagy teljesen kilépjen a rendszerből;
- a felhasználói egyének számára biztosítania kell a magántitok jelleget (pl. azáltal, hogy az információkat nem teszi mások számára hozzáférhetővé a felhasználói interfészen keresztül).

A műveletek helyes időzítésével elegendő időt kell biztosítani minden felhasználónak a folyamatok befejezéséhez (figyelembe véve azt a tényt is, hogy az emberek olvasási és reagálási és reagálási képességei különbözők).

2.2 Biztonsági követelmények minősített elektronikus aláírásokat létrehozó/ellenőrző alkalmazások számára

2.2.1 Követelmények az aláírás-létrehozó alkalmazás (SCA) egészére

Az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz közötti megbízható útvonalra vonatkozó követelmények:

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.

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

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

Bizt_köv3: Az aláírás-létrehozó alkalmazásnak biztonságosan törölnie kell az aláíráshoz kapcsolódó összes adatot az aláírási folyamat befejeződése után.

Bizt_köv4: Egy nyilvános aláíró alkalmazás nem őrizheti meg, illetve nem másolhatja le az aláíráshoz kapcsolódó érzékeny elemeket (aláírót hitelesítő adatok, DTBS, DTBSF) egyetlen olyan partner számára sem, akit az aláíró nem jogosított fel erre.

Bizt_köv5: Zárt láncú televíziók nem helyezhetők el úgy, hogy azok venni tudják az aláírót hitelesítő adatokat.

Bizt_köv6: Az aláírás-létrehozó rendszert úgy kell elhelyezni és tervezni, hogy az ne tegye lehetővé mások számára, hogy megfigyeljék/rögzítsék az aláírót hitelesítő adatokat.

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

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.

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

Bizt_köv9: Minden aláírót hitelesítő adatot, amely átvitelre kerül az aláírás-létrehozás alkalmazás osztott összetevői között, egy olyan megbízható útvonalon keresztül kell továbbítani, amely sértetlenséget és bizalmasságot biztosít.

Bizt_köv10: Minden aláírandó adatot, amely átvitelre kerül az aláírás-létrehozás alkalmazás osztott összetevői között, egy olyan megbízható útvonalon keresztül kell továbbítani, amely sértetlenséget és bizalmasságot biztosít.

A nem megbízható folyamatokból/kommunikációs portokból adódó követelmény

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.

Az aláírandó adatra vonatkozó követelmények

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

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

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

Bizt_köv15: Az aláírandó adatnak tartalmaznia kell a kötelezettségvállalás típus tulajdonságot, ha az aláírási szabályzat egynél több kötelezettségvállalás típust határoz meg.

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.

2.2.2 Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP)

A tartalom formátumra vonatkozó követelmények:

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.

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.

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

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

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

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.

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).

Bizt_köv24: Az aláíró dokumentumát megjelenítő összetevőnek nem szabad lehetővé tennie az aláíró számára, hogy az aláírói dokumentum bármely részét megváltoztassa.

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.

Az aláíró dokumentumára vonatkozó egyértelműségi 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.

A nem megjelenítés-érzékeny aláírói dokumentumokra vonatkozó követelmény:

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.

A rejtett szövegre és aktív kódra vonatkozó követelmény:

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.

2.2.3 Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV)

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

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.

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

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.

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.

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

2.2.4 Követelmények az aláíróval kölcsönható összetevőre (SIC)

Az aláírás kiváltására vonatkozó követelmények

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.

Az inaktivitási időkorlátra vonatkozó biztonsági követelmények

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

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.

2.2.5. Követelmények az aláírót hitelesítő összetevőre (SAC)

A tudáson alapuló aláírót hitelesítő adatokra vonatkozó követelmények

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.

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

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.

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.

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.

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).

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).

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.

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

Bizt_köv46: Megbízható útvonalat kell biztosítani a biometrikus adatok továbbítására a biometrikus érzékelő egység és a biztonságos aláírás-létrehozó eszköz közé.

Bizt_köv47: Biztosítani kell az aláírót hitelesítő adatok kriptográfiai védelmét (ha egy nyilvános biometrikus tulajdonságot használnak) a hitelesség garantálására és a visszajátszásos támadások elkerülésére.

2.2.6 Követelmények az aláírandó adat formattáló összetevőre (DTBSF)

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

2.2.7 Követelmények az adat lenyomat készítő összetevőre (DHC)

Bizt_köv49: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy „elfogadott” (szabványos és elterjedt) lenyomatoló algoritmus használatát lenyomatolásra.

Bizt_köv50: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy „elfogadott” (szabványos és elterjedt) elektronikus aláírás input formátum (feltöltési módszer) használatát.

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

2.2.8 Követelmények a biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikáció összetevőre (SSC)

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.

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

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.

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

2.2.9 Követelmények az SSCD/SCA hitelesítő összetevőre (SSA)

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.

2.2.10 Követelmények az Input/Output interfészre (I/O)

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.

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

Bizt_köv59: Intézkedéseket kell tenni az aláírás-létrehozó alkalmazásban arra, hogy importált aláírás-létrehozó alkalmazás komponenseket csak egy biztonságos letöltés felhasználásával lehessen telepíteni.

Bizt_köv60: Az aláírás-rendszer összes, az aláírás-létrehozás vagy aláírás-ellenőrzés folyamattal kölcsönhatásba lépő összetevőjét egy biztonságos területen[1] kell megvalósítani.

[1] A **biztonságos területet** egy olyan területet, melyen belül speciális ellenintézkedésekkel védekeznek a feldolgozott és tárolt adatok, illetve a folyamatok sikeres manipulálása ellen. Technikai módszerekkel (tehát nem adminisztratív úton) az alábbi három különböző módon lehet megvalósítani:

- Egy **szoftver modul**ban, melyben a biztonsági ellenintézkedések szoftverben vannak megvalósítva. Az így elérhető biztonság a működtető környezet biztonságától függ.
- Egy **módosítást-jelző modul**ban, ahol a biztonsági ellenintézkedéseket olyan módon valósítják meg, hogy a manipuláció ugyan nem akadályozható meg, de a felhasználó észlelheti azt. Ez azt jelenti, hogy a felhasználó védve van a biztonságos területen manipulált komponensek véletlen használatától.
- Egy **módosításnak ellenálló modul**ban, ahol a biztonsági ellenintézkedéseket olyan módon valósítják meg, hogy a manipuláció reális erőfeszítésekkel nem megvalósítható.

A MultiSigno Developer Professional biztonságos területe szoftver modul. Az ezzel elérhető biztonság korlátozottságáról, illetve az ebből fakadó, a működtető környezetre vonatkozó feltételeket a 4. fejezet 3. és 5. feltételei tartalmazzák.

3. A MultiSigno Developer Professional követelményeknek való megfelelése

Az alábbiakban összefoglaljuk az „Értékelési jelentés a MultiSigno Developer Professional aláíró alkalmazás fejlesztő készletről” című dokumentum eredményeit.

3.1 A MultiSigno Developer Professional megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés (**I**gen/**N**em/ **N**em **V**onatkozik rá)	**Magyarázat**
F_SCA_1	**I**	A MultiSigno Developer Professional tartalmaz aláíró és ellenőrző rutint is. Az ellenőrzés mindhárom alábbi funkcióját támogatja: 1. aláírás ellenőrzése (az aláírt adat lenyomata megegyezik-e a digitális aláírás dekódolása után visszakapott értékkel) 2. aláíró tanúsítványának az ellenőrzése (jól van-e aláírva, érvényes-e, stb.) 3. a tanúsítvány érvényességének ellenőrzése (nincs-e visszavonva) (letárolt aktuális visszavonási listában való kereséssel, illetve ennek hiányában az aktuális CRL letöltésével a hitelesítés-szolgáltatóval kiépített szabványos – HTTP, HTTPS, LDAP - protokollal)
F_SDP_1	**I**	A MultiSigno Developer Professional kezeli a tartalom-formátumot, és csak az alábbi négy (aktív kódot és makrót garantáltan nem tartalmazó) formátumot támogat: XML. PDF, RTF, TXT.
F_SDP_2	**I**	A MultiSigno Developer Professional az általa megengedett négyféle formátumra (XML, PDF, RTF, TXT) a tartalom-formátumot a dokumentummal együtt tárolja.
F_SDP_3	**N**	A MultiSigno Developer Professional nem támogatja.
F_SDP_4	**I**	A feladat nagy részét a DLL feletti alkalmazás végzi. A DLL viszont támogatást nyújt, amit meg kell valósítania azt korrekt módon teszi.
F_SAV_1	**I**	A MultiSigno Developer Professional támogatja az aláírói tanúsítvány, az időbélyegző, a tartalom-formátum, valamint a kötelezettségvállalás típus megjelenítését.
F_SAV_2	**I**	A MultiSigno Developer Professional támogatja az aláíráshoz csatolt tanúsítvány átvizsgálását (kiolvasható, megjeleníthető).
F_SIC_1	**N**	A MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak kell megvalósítania.
F_SIC_2	**N**	A MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak kell megvalósítania.
F_SIC_3	**NV**	A PIN kód bekérést a CSP végzi.
F_DTBSF_1	**I**	A MultiSigno Developer Professional támogatja. /A szabványos XML Advanced Digital Signature (ETSI TS 101 903) aláírási struktúra megvalósítása a MultiSigno Developer Professional nagy erénye/.
F_DTBSF_2	**I**	A MultiSigno Developer Professional támogatja, illetve jól felhívja a CSP megfelelő függvényét (SHA1 hash képezés).
F_DHC_1	**I**	A MultiSigno Developer Professional támogatja. A felhívás sorrendjét (közvetlenül az aláírás-létrehozás folyamat kiváltása után) a MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak kell megvalósítania.

F_DHC_2	**I**	A MultiSigno Developer Professional támogatja (a lenyomat értékét beteszi az XML struktúra megfelelő helyére). A felhívás sorrendjét (közvetlenül a lenyomatolás végrehajtása után) a MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak kell megvalósítania. .
F_SSC_1	**I**	A MultiSigno Developer Professional támogatja. Bizonyos részeket nem ő kezel le, hanem a Crypto API (pl. a magánkulcs kiválasztása), vagy a fölé írt alkalmazás (pl. a naplózás). A felhívások sorrendjét is az alkalmazásnak kell megvalósítania.
F_SSC_2	**NV**	Ez a funkcionális követelmény csak egy szolgáltató ellenőrzése alatt (is) működő aláíró rendszerre vonatkozik. A MultiSigno Developer Professional fejlesztő készletet munkahelyi és otthoni felhasználásra szolgáló aláíró alkalmazásokhoz tervezték, ezért ez a követelmény nem vonatozik rá.
F_SSC_3	**I**	A MultiSigno Developer Professional támogatja a szabványos PC/SC kompatibilis olvasókat, melyek rendelkeznek ilyen fizikai interfésszel.
F_SSC_4	**NV**	A megfelelő funkcionalitással rendelkező CSP ezt megvalósítja.
F_SSC_5	**NV**	A Crypto API támogatja, a megfelelő funkcionalitással rendelkező CSP ezt megvalósítja. A MultiSigno Developer Professional paraméterként kapja azt az egyetlen tanúsítványt, amivel dolgozik.
F_SSC_6	**NV**	A Crypto API támogatja, a megfelelő funkcionalitással rendelkező CSP ezt megvalósítja. Az aláíró kulcsot a Crypto API a paraméterként megadott tanúsítvány alapján kezeli.
F_SSC_7	**NV**	Ez a funkcionalitás a CSP része.
F_SSC_8	**I**	A MultiSigno Developer Professional támogatja (kiszámíttatja az aláírást). A felhívás az alkalmazásnak kell megvalósítania.
F_SSC_9	**N**	A MultiSigno Developer Professional nem támogatja. Az alkalmazásnak kell megoldania.
F_SSA_1	**NV**	Ez a funkcionális követelmény csak egy szolgáltató ellenőrzése alatt (is) működő aláíró rendszerre vonatkozik. A MultiSigno Developer Professional fejlesztő készletet munkahelyi és otthoni felhasználásra szolgáló aláíró alkalmazásokhoz tervezték, ezért ez a követelmény nem vonatozik rá.
F_SDC_1	**N**	A MultiSigno Developer Professional nem támogatja. Az alkalmazásnak kell megoldania.
F_SDOC_1	**I**	A MultiSigno Developer Professional támogatja (az XML struktúrában megvan a helyük).
F_SLC_1	**N**	A MultiSigno Developer Professional nem támogatja. Az alkalmazásnak kell megoldania.
F_SCPC_1	**I**	A MultiSigno Developer Professional képes CRL letöltésére. (Az OCSP-t nem támogatja.) Tanúsítványt nem képes letölteni, de erre nincs is szükség, mert a támogatott aláírási szabályzat szerint az XML struktúra mindig tartalmazza az aláíró teljes tanúsítványláncát .
F_I/O-1	**NV**	A MultiSigno Developer Professional nem képes tanúsítványt letölteni, de erre nincs is szükség, mert a támogatott aláírási szabályzat szerint az XML struktúra és a BALE mindig tartalmazza az aláíró teljes tanúsítványláncát.
F_I/O-2	**I**	A MultiSigno Developer Professional támogatja. Nem szerez meg tanúsítványt, hanem megkapja, de képes a tanúsítványokat ellenőrizni.
F_I/O-3	**N**	A MultiSigno Developer Professional nem támogatja. Osztott aláíró rendszer felvállalása esetén a követelményt az alkalmazásnak kell kielégítenie.

F_ISV-1	**I**	A MultiSigno Developer Professional támogatja. /Majdnem minden adat benne van az XML csomagban, kivéve az utólagos ellenőrzést is támogató CRL, de ez is betehető./.
F_ISV-2	**I**	A MultiSigno Developer Professional támogatja. /Minden adat benne van az XML csomagban./
F_USV-1	**I**	A MultiSigno Developer Professional támogatja. /A tervezett aláírási szabályzat minden követelményét teljesíteni lehet./
F_human_1	**I**	A MultiSigno Developer Professional támogatja (a függvénykészlet segítségével az aláírások száma lekérdezhető, majd egy kiválasztott aláírás leellenőrizhető). Az aláíró felé az interfészt a fejlesztő készletre épülő alkalmazásnak kell megvalósítania.
F_human_2	**N**	A MultiSigno Developer Professional nem támogatja. Az alkalmazásnak kell megoldania.
F_human_3	**I**	A MultiSigno Developer Professional támogatja (a megfelelő függvény valóban a neki megadott paraméterekkel meghatározott dokumentumot írja alá). Az „ami megjelenik, azt írják alá” követelményt az aláíró alkalmazásnak és annak környezetének is támogatnia kell.
F_human_4	**I**	A MultiSigno Developer Professional támogatja (egy megfelelő függvény hívással kiolvasható a Tanúsítvány subject mezője). Az aláíró felé az interfészt az alkalmazásnak kell megvalósítania.
F_human_5	**I**	A MultiSigno Developer Professional támogatja. (Befejezetlen ellenőrzés csak utólagos ellenőrzésnél lehetséges, itt viszont a megfelelő függvény figyelmeztet, ha az aláírás nem állja ki az utólagos ellenőrzést. Ekkor le kell tölteni a CRL-t.) Az aláíró felé az interfészt az alkalmazásnak kell megvalósítania.
F_human_6	**N**	A MultiSigno Developer Professional nem támogatja. Az alkalmazásnak kell megoldania.
F_machine_1	**I**	A MultiSigno Developer Professional támogatja (a megfelelő függvényekkel az aláírásban tárolt adatok kigyűjthetők).
F_machine_2	**I**	A MultiSigno Developer Professional támogatja (az ellenőrző és az ellenőrzéshez szükséges adatokat begyűjtő függvényekkel).
F_general_1	**N**	A fejlesztő készlet segítségével fejlesztett alkalmazásnak kell biztosítania, hogy a MultiSigno Developer Professional által támogatott funkciók segítségével megvalósítható ellenőrzés világos feldolgozási szabályt kövessen.
F_general_2	**N**	A MultiSigno Developer Professional nem támogatja. A követelmény felvállalása esetén, ezt az alkalmazásnak kell megoldania.
F_protocol	**I**	A MultiSigno Developer Professional támogatja az alábbi szabványos protokollok használatát a megbízható szolgáltatóval (szolgáltatókkal) történő kommunikáció során: ▪ tanúsítvány visszavonási állapot megszerzésekor (HTTP, HTTPS, LDAP); ▪ időbélyeg kérelem és válasz esetén (RFC 3161);
F_format	**I**	A MultiSigno Developer Professional az alábbi szabványos formátumokat kezeli: ▪ aláírási formátum: /XML Advanced Digital Signature/, ▪ tanúsítvány formátum /X509.v3, RFC 2459/, ▪ visszavonási lista /CRL, RFC 2459/.
F_principles	**N**	A felhasználói felületeket (s így felhasználó barátságát) az aláíró alkalmazásnak kell megvalósítania.

3.2 A MultiSigno Developer megfelelése a biztonsági követelményeknek

Az alábbiakban áttekintjük, hogy a minősített aláírásra vonatkozó biztonsági követelmények teljesítéséből melyeket támogat a MultiSigno Developer, vagy egy általa felhívott egyéb komponens (a CSP vagy a PC/SC szabványos kártyaolvasó).
A nem teljesített biztonsági követelményeket a MultiSigno Developer fejlesztő készlet segítségével fejlesztett alkalmazásnak, illetve ezen alkalmazás működtetési környezetének kell megoldania, vagy biztonsági maradványkockázatként kell elfogadni.

Biztonsági követelmény	Teljesülés (**I**gen/**N**em/**N**em **V**onatkozik rá)	**Magyarázat**
Bizt_köv1	**I**	A MultiSigno Developer Professional támogatja (egyetlen függvénye sem írja felül azokat az adatokat, melyek sértetlenségét meg kell őrizni). A sértetlenség megőrzését az aláíró alkalmazásnak és annak környezetének is támogatnia kell.
Bizt_köv2	**I**	A MultiSigno Developer Professional támogatja (egyetlen függvénye sem tartalmaz rosszindulató, a bizalmasság megsértését okazó részt). A bizalmasság megőrzését az aláíró alkalmazásnak és annak környezetének is támogatnia kell.
Bizt_köv3	**I**	A követelmény csak nyilvános[2] aláíró alkalmazásokra vonatkozik. Bár a MultiSigno Developer Professional-nak nem célja a nyilvános alkalmazások támogatása, ezt a követelményt biztonsági megfontolásokból mégis támogatja.
Bizt_köv4	**I**	A követelmény csak nyilvános aláíró alkalmazásokra vonatkozik. Bár a MultiSigno Developer Professional-nak nem célja a nyilvános alkalmazások támogatása, ezt a követelményt biztonsági megfontolásokból mégis támogatja.
Bizt_köv5	**N**	A követelmény csak nyilvános aláíró alkalmazásokra vonatkozik. /A MultiSigno Developer Professional nem nyilvános aláíró alkalmazások fejlesztésére készült./
Bizt_köv6	**N**	A követelmény csak nyilvános aláíró alkalmazásokra vonatkozik. /A MultiSigno Developer Professional nem nyilvános aláíró alkalmazások fejlesztésére készült./
Bizt_köv7	**I**	Alapvetően ezt a követelményt a MultiSigno Developer Professional segítségével fejlesztett alkalmazásnak kell megvalósítania. /A MultiSigno Developer Professional ezt annyiban támogatja, (pontosabban csak annyit tud garantálni), hogy meghívott függvényei valóban az átadott paraméterekben meghatározott fájlt küldik aláírásra./
Bizt_köv8	**I**	Alapvetően ezt a követelményt a MultiSigno Developer Professional segítségével fejlesztett alkalmazásnak kell megvalósítania. /A MultiSigno Developer Professional ezt annyiban támogatja, (pontosabban csak annyit tud garantálni), hogy meghívott függvényei valóban az átadott paraméterekben meghatározott aláírandó adat komponenseket küldik aláírásra./

[2] A nyilvános aláíró alkalmazás egy szolgáltató ellenőrzése alatt áll (pl. postahivatal, Internet-kávézó, stb.), ahová a felhasználó betérhet, hogy aláírást létrehozzon, illetve ellenőrizzen.

Bizt_köv9	**N**	A követelmény csak osztott architektúrájú aláíró alkalmazásokra vonatkozik. /A MultiSigno Developer Professional ezt nem így épül fel./
Bizt_köv10	**N**	A követelmény csak osztott architektúrájú aláíró alkalmazásokra vonatkozik. /A MultiSigno Developer Professional ezt nem így épül fel./
Bizt_köv11	**N**	A MultiSigno Developer Professional nem támogatja. Az alkalmazásnak, illetve ezen alkalmazás működtetési környezetének kell majd kielégítenie.
Bizt_köv12	**I**	A MultiSigno Developer Professional támogatja (pontosabban kikényszeríti, mert megfelelő függvényei üres objektumot nem is továbbítanak aláírásra).
Bizt_köv13	**I**	A MultiSigno Developer Professional támogatja. /A támogatott aláírási szabályzat szerint az aláírás XML struktúrájába letárolásra kerül a tanúsítvány, az egész tanúsítványlánc és a CRL is./
Bizt_köv14	**I**	A MSigno Developer Professional tartalmaz OID alapú szabályzat azonosítást. (Ugyanakkor az aláírási szabályzatok azonosítóval (OID-vel) történő ellátása még nem megoldott Magyarországon.)
Bizt_köv15	**I**	A MultiSigno Developer Professional által támogatott (implicit) aláírási szabályzat több kötelezettségvállalás típust is meghatároz. Ezeket a kötelezettségvállalás típusokat a megfelelő függvények helyesen kezelik, s bekerülnek az aláírandó adat XML struktúrájába.
Bizt_köv16	**I**	A MultiSigno Developer Professional támogatja.
Bizt_köv17	**I**	A MultiSigno Developer Professional támogatja. /A tartalom formátum bekerül az aláírandó adat XML struktúrájába. / A függvények ugyanakkor nem ellenőrzik a megadott tartalom formátum megfelelését a tényleges tartalom formátumával. Ezt az ellenőrzést MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak, vagy a működtetési környezet egyéb elemének kell majd elvégeznie.
Bizt_köv18	**I**	A MultiSigno Developer Professional támogatja. /Nem engedélyezett tartalom formátum megadása esetén a megfelelő függvények hibajelzéssel térnek vissza. / A tényleges szintaxis ellenőrzést, valamint az aláíróval való kommunikációt a MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak kell majd elvégeznie, s ehhez esetleg a működtetési környezet egyéb elemére is szükség lesz.
Bizt_köv19	**I**	A MultiSigno Developer Professional támogatja. /A fejlesztőknek készült leírás tartalmazza a MultiSigno Developer Professional által támogatott négy formátumot./ A felhasználók megfelelő tájékoztatása az alkalmazás fejlesztők későbbi feladata marad.
Bizt_köv20	**N**	A MultiSigno Developer Professional nem támogatja. A felhasználók figyelmeztetése, megfelelő tájékoztatása az alkalmazás fejlesztők későbbi feladata marad.
Bizt_köv21	**I**	A MultiSigno Developer Professional biztosítja a szükséges támogatást. /Nem engedélyezett tartalom formátum megadása esetén a megfelelő függvények hibajelzéssel térnek vissza. / A tényleges szintaxis ellenőrzést, valamint az aláíróval való kommunikációt a MultiSigno Developer Professional fejlesztő készlet segítségével fejlesztett alkalmazásnak kell majd elvégeznie, s ehhez esetleg a működtetési környezet egyéb elemére is szükség lesz.

Bizt_köv22	**I**	A MultiSigno Developer Professional támogatja. /A megfelelő függvények valóban a paraméterként meghatározott fájlt dolgozzák fel, azt teszik be az XML dokumentumba, azt küldik aláírásra./ A követelmény kielégítéséhez szükséges az aláíró alkalmazás és annak működtetési környezetének későbbi támogatása is.
Bizt_köv23	**N**	A MultiSigno Developer Professional nem támogatja. A követelményt az alkalmazásnak kell kielégítenie.
Bizt_köv24	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró tájékoztatását az alkalmazásnak kell megvalósítania.
Bizt_köv25	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró figyelmeztetését az alkalmazásnak kell megvalósítania.
Bizt_köv26	**I**	A MultiSigno Developer Professional támogatja /A megfelelő függvények mindig beépítik a tartalom formátumot az aláírandó adat XML struktúrájába./
Bizt_köv27	**I**	A MultiSigno Developer Professional támogatja /A tartalom formátum megadható az aláírandó adatokhoz./
Bizt_köv28	**N**	A MultiSigno Developer Professional nem támogatja A MultiSigno Developer fejlesztő készlet segítségével fejlesztett alkalmazásnak kell megvalósítania.
Bizt_köv29	**I**	A MultiSigno Developer Professional támogatja a legtöbb aláírási tulajdonság aláírás előtti megtekintését. Az automatikusan kitölthető és kitöltendő aláírási tulajdonságokat az aláírással egy időben hozza létre (pl. az aláírás időpontját), így ezek előzetes megmutatása nem lehetséges, de erre nincs is szükség.
Bizt_köv30	**I**	A MultiSigno Developer Professional támogatja /A megfelelő függvények a kapott paramétereknek megfelelően építik be az aláírási tulajdonságokat az aláírandó adat XML struktúrájába./ A MultiSigno Developer fejlesztő készlet segítségével fejlesztett alkalmazásnak, illetve ezen alkalmazás működtetési környezetének is támogatást kell biztosítania.
Bizt_köv31	**I**	A MultiSigno Developer Professional támogatja. /Az aláírás tulajdonságokat a megfelelő függvények vagy az aláírandó részbe helyezik, vagy már eleve önállóan alá lettek írva (pl. tanúsítványok, CRL), ahogy az XML Advanced Digital Signature szabvány ezt előírja. Így minden aláírási tulajdonság sértetlensége és hitelessége védve van./
Bizt_köv32	**I**	A MultiSigno Developer Professional által támogatott aláírási tulajdonságok (tanúsítvány, CRL, időbélyegző, stb.) mindegyike szabványos formátumú, és nem tartalmazhat rejtett szöveget, makrót, vagy aktív kódot (erről a hitelesítés-szolgáltatónak kell gondoskodnia). Következésképpen a MultiSigno Developer Professional által elvégzett ellenőrzések (pl. érvényes és szabályos-e a tanúsítvány, a CRL, az időbélyeg, stb.) indirekt módon biztosítják azt is, hogy ilyen rejtett információ ne kerülhessen az aláírás tulajdonságok közé.

Bizt_köv33	**I**	A MultiSigno Developer Professional által támogatott aláírás tulajdonságok egyike sem tartalmazhat beágyazott rejtett szöveget, makrót, vagy aktív kódot. Így ezek ellenőrzése formálisan a követelményt is kielégíti.
Bizt_köv34	**I**	A MultiSigno Developer Professional támogatja. /Megjeleníthető a teljes tanúsítvány./
Bizt_köv35	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazásnak kell majd megvalósítania.
Bizt_köv36	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazásnak kell majd megvalósítania.
Bizt_köv37	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazásnak kell majd megvalósítania.
Bizt_köv38	**N**	A MultiSigno Developer Professional funkcionálisan nem vállalja fel a hitelesítő adat BALE-hoz való továbbítását. /Erre nincs is szükség, mert az aláíró alkalmazás a CSP segítségével képes a megkövetelt funkcionalitás közvetlen biztosítására/.
Bizt_köv39	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak a CSP segítségével kell majd megvalósítania.
Bizt_köv40	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak a CSP segítségével kell majd megvalósítania.
Bizt_köv41	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak a CSP segítségével, és a BALE aktív támogatásával kell majd megvalósítania.
Bizt_köv42	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak a CSP segítségével, és a BALE aktív támogatásával kell majd megvalósítania.
Bizt_köv43	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak a CSP segítségével, és a BALE aktív támogatásával kell majd megvalósítania.
Bizt_köv44	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak kell majd megvalósítania.
Bizt_köv45	**NV**	Minthogy a MultiSigno Developer Professional nem működik közre a hitelesítő adat BALE-hoz való továbbításában, ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak kell majd megvalósítania.
Bizt_köv46	**N**	A követelmény csak a biometrikus aláírót hitelesítő adatokat használó aláíró alkalmazásokra vonatkozik. /A MultiSigno Developer Professional ezt nem támogatja./
Bizt_köv47	**N**	A követelmény csak a biometrikus aláírót hitelesítő adatokat használó aláíró alkalmazásokra vonatkozik. /A MultiSigno Developer Professional ezt nem támogatja./
Bizt_köv48	**I**	A MultiSigno Developer Professional támogatja. /Az aláírandó adat formátum egyértelmű: a szabványos XML

		Advanced Digital Signature struktúrájának BASE 64 kódolt képe./
Bizt_köv49	**I**	A MultiSigno Developer Professional támogatja. /Az aláírandó adatra SHA-1 lenyomatot számoltat (a CSP-vel)./
Bizt_köv50	**I**	A MultiSigno Developer Professional támogatja. /Az aláírandó adatra a megkövetelt feltöltési módszert alkalmazza (a CSP segítségével)./
Bizt_köv51	**I**	A MultiSigno Developer Professional támogatja. /Elkészít egy XML node-ot, amit aztán aláír./
Bizt_köv52	**NV**	A MultiSigno Developer Professional nem működik közre az adatok BALE-hoz való továbbításában, ezért ez a követelmény nem vonatkozik rá. A CSP-k támogatják, a PC/SC-nek megfelelő kártyaolvasók és az ISO 7816 1-4 –t támogató BALE-k automatikusan biztosítják, az alkalmazásoknak sem lesz ezzel feladatuk.
Bizt_köv53	**NV**	A követelmény csak a vezeték nélküli összeköttetést használó aláíró alkalmazásokra vonatkozik. A MultiSigno Developer Professional nem működik közre az adatok BALE-hoz való továbbításában, ezért ez a követelmény nem is vonatkozik rá.
Bizt_köv54	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazásnak kell majd megvalósítania a CSP-k támogatásának aktivizálásával.
Bizt_köv55	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazásnak, illetve ezen alkalmazás működtetési környezetének kell majd kielégítenie.
Bizt_köv56	**NV**	A MultiSigno Developer Professional nem működik közre az adatok BALE-hoz való továbbításában, ezért ez a követelmény nem vonatkozik rá. Az aláíró alkalmazásnak a CSP segítségével, és a BALE aktív támogatásával kell majd megvalósítania.
Bizt_köv57	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazás működtetési környezetének kell majd kielégítenie.
Bizt_köv58	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazás működtetési környezetének kell majd kielégítenie.
Bizt_köv59	**N**	A MultiSigno Developer Professional nem támogatja. Amennyiben importált aláíró alkalmazás komponensekre szükség lesz, a követelményt az aláíró alkalmazásnak és működtetési környezetének kell kielégítenie.
Bizt_köv60	**N**	A MultiSigno Developer Professional nem támogatja. Az aláíró alkalmazás működtetési környezetének kell majd kielégítenie, melyhez az aláíró alkalmazás is támogatást nyújthat.

4. A Tanúsítási jelentés eredménye, érvényességi feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek betartása hozzájárul a MultiSigno Developer Professional segítségével fejlesztett aláíró alkalmazások biztonságához.
Ezek a feltételek a fejlesztésekkel szembeni általános minőségbiztonsági (tervezési, tesztelési, dokumentálási stb.) követelményeken túlmutatóan az aláírás-specifikus elemek ellenőrzött védelmi szintjét szándékoznak garantálni.

A feltételek arra vonatkoznak, hogy a MultiSigno Developer Professional felhasználásával aláíró alkalmazásokat fejlesztők, hogyan használják ezt a terméket, saját fejlesztésükhöz. Így tulajdonképpen nem is a MultiSigno Developer Professional termékre, hanem az ebből fejlesztett (esetelegesen későbbi tanúsítási eljárás hatókörébe tartozó) aláíró alkalmazásra vonatkoznak.

4.1 Kötelezően betartandó feltételek

1. A MultiSigno Developer Professional-t felhasználóihoz (akik aláíró alkalmazásokat fejlesztenek felhasználásukkal) CD-n szállítják. Használatba vétel előtt kötelező másolatot készíteni róla, hogy az eredetit mesterpéldányként lehessen felhasználni a későbbiekben végrehajtandó sértetlenség ellenőrzések során.

2. A MultiSigno Developer Professional-lal fejlesztett aláíró alkalmazások elkészülésekor a fejlesztők felelőssége a felhasznált és a mesterpéldányként elmentett MultiSigno Developer Professional függvényeinek sértetlenségének ellenőrzése /valóban a tanúsított fejlesztő készlet elemeit építették-e be/.

4.2 Ajánlások minősített aláírásokat kezelő alkalmazások fejlesztőinek

A MultiSigno Developer Professional /”aláíró alkalmazást fejlesztő munkaállomásokon”/ alapvetően elszigetelt működtetési környezetben használandó, de kiegészítő feltételek garantálása esetén védett működtetési környezetben is lehet fejleszteni vele (sőt a teljes funkcionalitás végső tesztelése csak ilyen körülmények között valósítható meg).

Elszigetelt működtetési környezet (kisebb fejlesztéseknél ez a tipikus eset) esetén a fejlesztői készletet (és egyúttal a fejlesztés alatt álló aláíró alkalmazást) az védi, hogy nincs (sohasem) kapcsolódás kommunikációs hálózatokra (Internet, Intranet), és a működtetési környezetben olyan védelmi intézkedéseket valósítanak meg, melyek kivédik a jogosulatlan manuális hozzáférésen és adathordozóról történő adatbevitelen alapuló támadásokat is/. A Pack.dll 2-0 felhasználásával alapvetően ilyen környezetben ajánlott fejleszteni, tesztelni. Ugyanakkor az ebből fejlesztett, teljes funkcionalitást biztosító végterméket nem lehet teljeskörűen ebben a működtetési környezetben tesztelni, mivel a MultiSigno Developer Professional bázisán kifejlesztett aláíró alkalmazás:

- aláírás létrehozásánál nem képes tesztelni az időbélyegzés részét (hiszen nem kerülhet hálózati kapcsolatba egyetlen időbélyeg-szolgáltatóval sem),
- aláírás ellenőrzéséhez nem képes tesztelni azt a funkcióját, hogy amennyiben az adott munkaállomás nem rendelkezik érvényes visszavonási listával (amit elszigetelt környezetben adminisztratív úton, egy más munkaállomáson letöltött CRL adathordozóról történő betöltésével lehet biztosítani).

Védett működtetési környezet (kisebb fejlesztések esetén nem ez a tipikus eset) esetén a fejlesztői készletet (és egyúttal a fejlesztés alatt álló aláíró alkalmazást) a működtetési környezet nagy bizonyossággal megvédi a kommunikációs hálózatok (Internet, Intranet) irányából érkező, valamint a jogosulatlan manuális hozzáférésen és az adathordozóról történő adatbevitelen alapuló támadásoktól.

4.2.1 Általános működtetési feltételek

3. Eljárásrendi/szervezeti védelmi intézkedésekkel kell támogatni az aláíró alkalmazás fejlesztést megvalósító számítógép(ek)re irányuló olyan támadások kivédését, melyek manuális hozzáférésen, illetve adathordozóról történő adatbevitelen alapulnak. Garantálni kell, hogy a fejlesztés technikai környezete, valamint a fejlesztett programok és az ehhez felhasznált fejlesztő készlet funkcióit ne lehessen manipulálni, melyet különösen vírus és Trójai faló bejuttatása okozhat. Minden újonnan telepített szoftvernek manipulációtól mentesnek kell lennie.
   /A fenti intézkedések döntően ahhoz kellenek, hogy a fejlesztendő aláíró alkalmazás és az ennek bázisát képező fejlesztő készlet ne manipulálódjon./

4. A fejlesztő környezetben konfiguráció menedzselési eljárások kidolgozásával és betartásával kell garantálni a fejlesztett termék sértetlenségét azzal, hogy fegyelmet és ellenőrzést követelnek meg a fejlesztendő termék és más ezzel összefüggő információ pontosításában és módosításában.
   /A konfiguráció menedzselése akadályozza a fejlesztés alatt álló alkalmazások egyes verzióinak jogosulatlan módosítását, bővítését vagy törlését, illetve hozzájárul a mégis bekövetkező felhatalmazás nélküli változtatások észleléséhez (a verziónként elkülönítetten is letárolt példányok időszakos összehasonlításával)./

4.2.2 A védett működtetési környezetben történő felhasználás járulékos feltételei

5. Amennyiben a fejlesztő környezetnek hálózati kapcsolatai is vannak a 4. feltételben elvárt konfiguráció menedzselési eljárásokon kívül rendszeres időnként ellenőrizni kell a fejlesztő készlet és a fejlesztett aláíró alkalmazás verziók sértetlenségét (az elkülönítetten is letárolt (mester) példányok időszakos összehasonlításával).

4.2.3 Az elszigetelt működtetési környezetben történő felhasználás feltételei

Az elszigetelés számos fenyegetést eleve kizár (hálózati támadások), a fenyegetések más részét pedig az általános működtetési feltételek lefedik. (Nincs járulékos feltétel).

5. A követelményeknek való megfelelést ellenőrző független vizsgálat módszere és hangsúlyai

A jelen Tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálatok meghatározásakor figyelembe vettük az alábbi speciális szempontokat:

- a MultiSigno Developer Professional fejlesztő készlet segítségével különböző aláíró alkalmazások fejlesztése várható a jövőben, melyek biztonsága függ ezen fejlesztő készlet biztonságos működésétől,
- a MultiSigno Developer Professional fejlesztő készlet nagysága (száz körüli külső és belső függvény) még lehetővé tette a forráskódok általános független ellenőrzését.

Mindkét fenti szempontot mérlegelve a független vizsgálatok a forráskódok ellenőrzésre és a tesztelésre helyezte a hangsúlyt, az egyéb (a biztonságos tervezésre, megvalósításra és működésre indirekt úton bizalmat erősítő) értékelési megközelítések kisebb szerephez jutottak.

Az ellenőrző vizsgálat a MultiSigno Developer Professional biztonsági viselkedésének megértése érdekében elemezte a biztonsági funkciókat, ehhez felhasználta az alábbi fejlesztői dokumentációkat:

- MultiSigno koncepcionális terv /funkcionális felépítés, általános vállalások és nem vállalások/
- Pack._dll 2.0 áttekintés /magas szintű fejlesztői leírás a DLL könyvtárról/
- Pack.h, xmlHandleWrapper.h, MyByteArray.h, KDLDAP.h /a függvények részletes leírása, paraméterezése és a paraméterek leírása/

Az ellenőrző vizsgálat kitért a következők elemzésére:

- a minősített aláírásokra is alkalmazható aláíró alkalmazások mely funkcionális és biztonsági követelményeit kell, illetve célszerű kielégítenie a DLL-nek, s mely maradhat az aláíró alkalmazás feladata,
- a DLL felvállalja-e a szükséges követelmények kielégítését,
- a DLL teljesíti-e a felvállalt követelményeket.

A fentieken kívül:

- a MultiSigno Developer Professional forráskódjainak elemzésével hangsúlyosan vizsgálta az alábbiakat:
  - nincs-e hiba a programban,
  - hibás paramétereket lekezeli-e a program,
  - a kritikus részek tényleg azt végzik-e, amit kell,
  - a belső függvények meghívása, visszaadott hibaüzenetek lekezelése megfelelő-e.
- funkcionális teszteket végzett (a DLL egyes függvényeire, külön erre a célra kifejlesztett speciális tesztprogram felhasználásával),
- áttekintette a fejlesztők által végzett tesztelést, elemezte ennek teljeskörűségét,
- a fejlesztőktől független minta tesztelést végzett /minta felhívó programokkal/,
- értékelte a biztonsági funkciók erősségét, a termék sebezhetőségét.

6. A MultiSigno Developer biztonsági funkciók értékelt erőssége

Még ha az értékelés tárgyának (jelen esetben a MultiSigno Developer aláíró alkalmazás fejlesztő készletnek) a biztonsági funkcióit nem is lehet megkerülni, kiiktatni vagy tönkretenni, akkor is lehet lehetőség kijátszani azokat, ha a mögöttes biztonsági mechanizmusok sebezhetőek. E funkciók biztonsági viselkedése minősíthető a mechanizmusok biztonsági viselkedésének mennyiségi vagy statisztikai alapú elemzési eredményeinek felhasználásával és az ilyen mechanizmusok legyőzésére vonatkozó erőfeszítések segítségével.

A biztonsági funkciókat a biztonsági mechanizmusok valósítják meg. Például egy jelszókezelő mechanizmus az azonosítás és hitelesítés biztonsági funkciók megvalósításában használható fel.

A biztonsági funkciók erősségének elemzése a biztonsági mechanizmusok szintjén zajlott (döntően az SHA-1 lenyomatoló függvényt érintve).
Eredménye a vizsgált biztonsági funkcióknak az azonosított veszélyek elleni fellépés képességére vonatkozó információt tartalmazza.

A biztonsági funkciók erőssége: **magas szintű**

7. A tanúsításhoz figyelembe vett dokumentumok

7.1 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: Signature Creation Application and Procedures for Electronic Signature Verification

ETSI TS 101 733 Electronic Signature Formats

ETSI TS 101 903 XML Advanced Electronic Signatures (XadES)

7.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

7.2.1 A tanúsításhoz figyelembe vett egyéb fejlesztői dokumentumok

Kérelem a tanúsítás elvégzésére

Kérdőív a tanúsítás kérelmezéséhez

MultiSigno koncepcionális terv /funkcionális felépítés, általános vállalások és nem vállalások/

Pack._dll 2.0 áttekintés /magas szintű fejlesztői leírás a DLL könyvtárról/

Pack.h, xmlHandleWrapper.h, MyByteArray.h, KDLDAP.h /a függvények részletes leírása, paraméterezése és a paraméterek leírása/

Pack.dll /a függvény könyvtár/

Pack.cpp, xmlHandleWrapper.cpp, MyByteArray.cpp, KDLDAP.cpp /forráskódok/

7.2.2 A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés a MultiSigno Developer (1.2) aláíró alkalmazás fejlesztő készletről /Bizalmas dokumentum, készítette a HunGuard Kft./

Aláíró alkalmazások funkcionális modellezése
/Nyilvános dokumentum, készítette a HunGuard Kft./

CAPI	Microsoft Cryptographic Application Programming Interface
PKCS #1	RSA Cryptography Standard /RFC 2313/
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/

8. Rövidítések

API	Application Programming Interface
CEN	European Comittee for Standardization
CSP	Cryptograpic Service Provider /kriptográfiai szolgáltató/
CRL	Certification Revocation List /tanúsítvány visszavonási lista/
DHC	Data hashing component /adatlenyomat-készítő összetevő/
DTBS	Data to be Signed /aláírandó adat/
DTBSF	DTBS formatter /aláírandó adat formattáló/
DTBSR	Data to be Signed Representation /aláírandó adat reprezentáns/
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol sECURE
I/O	Input/Output
ISO	International Organization for Standardization
ISSS	Information Society Standardization System
ISV	Initial Signature Verification /kezdeti aláírás ellenőrzés/
LDAP	Lightweight Directory Access Protocol
PC/SC	Personal Computer Smart Card
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #1	RSA Cryptography Standard
RFC	Request for Comment
RSA	Rivest-Shamir-Adleman (public key cryptosystem)
SAC	(Signer's authentication component) aláírót hitelesítő összetevő
SAV	Signature attribute viewer /aláírási tulajdonság megjelenítő/
SCA	Signature creation application /aláírás-létrehozó alkalmazás/
SDC	Signer's document composer /aláírói dokumentum szerkesztő/
SDOC	Signed data object composer /aláírt adat objektum szerkesztő/
SDP	Signer's document presenter /aláírói dokumentumot megjelenítő/
SHA-1	Secure Hash Algorithm
SHI	SSCD holder indicator /Az SSCD tulajdonos jelző/
SIC	Signer's interaction component /aláíróval kölcsönható összetevő/
SLC	Signature logging component /aláírás-naplózási összetevő/
SP	Signature Policy /aláírási szabályzat/
SSA	SSCD/SCA Communicator authenticator /az SSCD/SCA közötti kommunikációt hitelesítő összetevő /
SSC	SSCD/SCA Communicator /az SSCD és SCA közötti kommunikáció összetevője/
SSCD	Secure signature creation device /biztonságos aláírás-létrehozó eszköz, BALE/
USV	(Usual Signature Verification /utólagos aláírás ellenőrzés/
XML	eXtensible Markup Language