Tanúsítási Jelentés

Hung-TJ-018-2004

a
DSignLibrary 1.6

elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói könyvtárról

/MÁV Informatika Kft./

1 A DSign Library 1.6 legfontosabb tulajdonságainak összefoglalása

A tanúsított termék a MÁV Informatika Kft. által fejlesztett és forgalmazott DSign Library 1.6 elektronikus aláíró és ellenőrző alkalmazás kifejlesztésére alkalmas függvény csomag.

1.1 Architektúra

A DSign Library 1.6 egy programozói könyvtár, amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.
Mindezt szabványos formában (XAdES XML Advanced Electronic Signatures ETSI TS 101 903) teszi.
A DSign Library teljes mértékben a Windows operációs rendszer erőforrásaira, eszközeire támaszkodik. A Crypto API-n keresztül a Microsoft vagy más gyártók CSP-jét használja. Ezen keresztül szólítja meg akár az aláírás-létrehozó eszközt. Az aláírás során legenerálható vele a megfelelő XML struktúra, majd az aláírandó XML elemre a Microsoft Crypto API-ján keresztül elkészíthető az aláírás.

1.2 Tulajdonságok

A DSign Library 1.6 fejlesztő készlet elektronikus aláírással és az aláírás ellenőrzésével kapcsolatos funkcionalitást valósít meg a Microsoft Crypto API-jára és azon keresztül különböző CSP-kre épülve. A Library képes különböző aláírási szabályzatoknak megfelelni, de azokat szabványos elektronikus aláírási szabályzatként automatikusan nem képes kezelni. A tág keretek közti variálhatósága miatt azonban számos aláírási szabályzat megvalósítható a Library segítségével.

A DSign Library 1.6 jellemző tulajdonságai:

- XAdES és XAdES-T szabvány szerinti hiteles dokumentum formátum
- Szabványos X.509 tanúsítványok kezelése (Windows tanúsítványtárban)
- Az RFC 3161 szabvány szerinti időbélyeg szolgáltatás támogatása
- Felhasználó azonosítás támogatása időbélyeg szolgáltatás használatához
- Tanúsítvány érvényességi állapot teljes körű ellenőrzése.
- Aláíró eszköz kezelése (CSP-n keresztül)

1.3 A tanúsítás tárgya és hatóköre

Jelen tanúsítás tárgya a DSign Library 1.6 fejlesztő készlet.

A tanúsítás során feltételezzük, hogy a DSign Library 1.6 fejlesztő készlet alapját képező Windows operációs rendszer, és annak részét képező CSP modul biztonságosan és helyesen működnek. A DSign Library 1.6 alapvetően a következő operációs rendszer komponensre épül:

- Microsoft .NET Framework 1.1
- Microsoft Crypto API

2 A DSign Library 1.6 megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 követelményrendszerekből fakadó) funkcionális és biztonsági követelményeket, melyek minősített elektronikus aláírások létrehozására és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.
Megnevezzük azokat a követelményeket, amelyek a DSign Library 1.6 programozói könyvtárra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy a DSign Library 1.6 programozói könyvtár megfelel-e az adott követelménynek.

Minthogy a DSign Library 1.6 programozói könyvtárt fokozott aláíró alkalmazások fejlesztésére kívánják felhasználni, megfelelő tanúsítási végeredmény akkor is adható, ha a Library nem felel meg minden rá vonatkozó követelménynek.

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet tartalmaz ellenőrzési funkciókat is, tehát vele készíthető olyan aláíró alkalmazás, amely ellenőrzi 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.

Magyarázat: *A DSignLibrary v 1.6 kezeli a tartalom-formátumot, de mint paramétert kapja meg az őt hívó alkalmazástól. A tartalom-formátum helyes használata a felhívó alkalmazás feladata.*

Konklúzió: **nem vonatkozik rá a követelmény**

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: Nincs meghatározva, hogy a DSignLibrary v 1.6 milyen típusú anyagokat kezelhet. Az aláírói dokumentumban a tartalom-formátumot viszont kezeli.

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.

Magyarázat: Nincs meghatározva, hogy a DSignLibrary v 1.6 milyen típusú anyagokat kezelhet. Az aláírói dokumentumban a tartalom-formátumot viszont kezeli.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A megjelenítés nem a DSignLibrary v 1.6 feladata. A megjelenítéshez szükséges aláírási tulajdonságokat képes visszaadni a hívó alkalmazás számára.

Konklúzió: **nem vonatkozik rá a követelmény**

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).

Magyarázat: Mind a négy aláírási tulajdonságot kezeli a DSignLibrary v 1.6, és képes ezeket a tulajdonságokat visszaadni a hívó alkalmazásnak Ezen kívül képes még tárolni és visszaadni az aláírás helyét és idejét, időbélyeget, és állított szerepköröket.

Konklúzió: **megfelel**

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

Magyarázat: Interaktív felületet követel, a DSignLibrary v 1.6 fölé írt alkalmazás feladata. A Library metódusai segítségével képes a XAdES csomagból kiolvasni a tanúsítványt.

Konklúzió: **megfelel**

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

Magyarázat: Interaktív felületet követel, a DSignLibrary v 1.6 fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Interaktív felületet követel, a DSignLibrary v 1.6 fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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).

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A XAdES-es csomagot a DSignLibrary v 1.6 megfelelően összeállítja.

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.

Magyarázat: A DSignLibrary v 1.6 elvégzi a lenyomatolást.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 elvégzi a lenyomatolást.

Konklúzió: **megfelel**

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

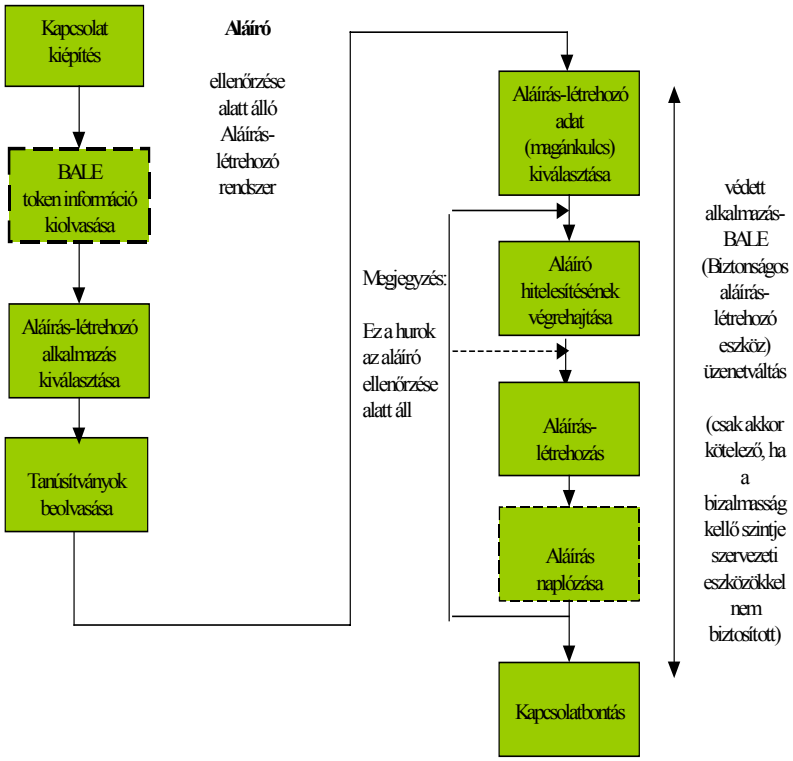
Magyarázat: A DSignLibrary v 1.6 elvégzi a XAdES csomag helyes feltöltését.

Konklúzió: **megfelel**

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

Magyarázat: DSignLibrary v 1.6 fejlesztő készlet segítségével felépíthető a feltételt kielégítő aláíró alkalmazás.

Konklúzió: **megfelel**



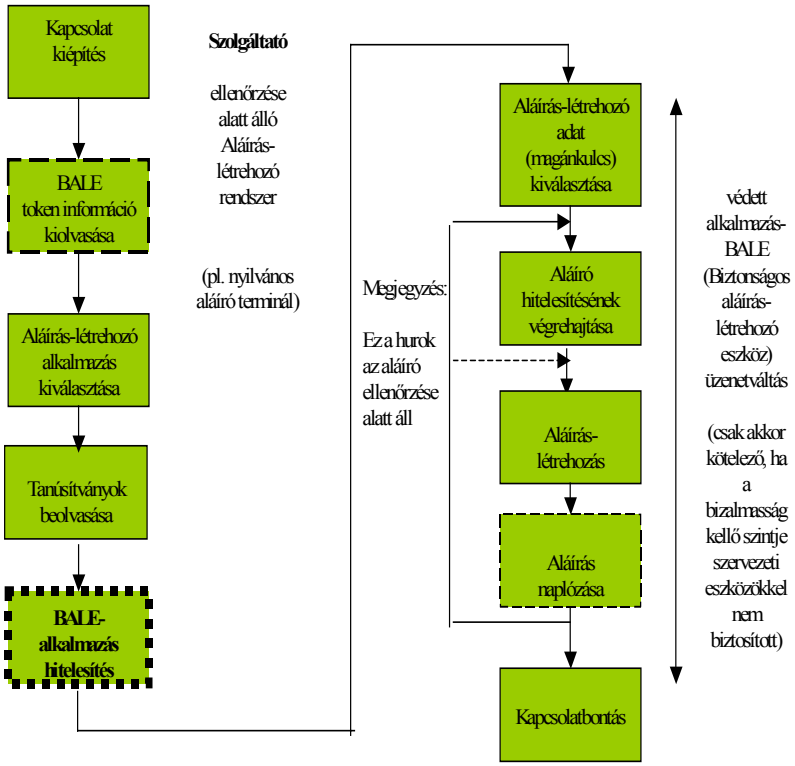
1. ábra

Az aláíró ellenőrzése alatt álló aláírás-létrehozó rendszer esetén megvalósítandó együtt-működési sorozat az aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között

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: DSignLibrary v 1.6 fejlesztő készlet segítségével felépíthető a feltételt kielégítő aláíró alkalmazás.

Konklúzió: **megfelel**



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_3: Az aláírás-létrehozó alkalmazásnak legalább egy fizikai interfésszel kell rendelkeznie, amely alkalmas a biztonságos aláírás-létrehozó eszközzel való kommunikációra.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszköz funkció kiválasztása a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a tanúsítványt paraméterként kapja.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. A magán kulcs kiválasztása a tanúsítvány alapján a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-ján keresztül kiszámítatja az aláírást.

Konklúzió: **megfelel**

F_SSC_9: A befejezett aláírásokat naplózni kell.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet képes a XAdES csomagból egy logot készíteni. Itt a napló inkább egyfajta kivonata a csomagnak és nem a tényleges eseményekkel egy időben keletkeznek a naplóbejegyzések. Fokozott biztonságú aláíró alkalmazásnál ez elegendő.

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: A DSignLibrary v 1.6 fejlesztő készlet nem ellenőrzi a környezetét. Ez nem is feladata. A környezet biztonságát az operációs rendszerrel kel megteremteni.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet paraméterkén kapja meg, hogy mely dokumentumot tárolja el a XAdES csomagban, és a csomag mely dokumentumát írja alá.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A biztonságos aláírás-létrehozó eszköz kimeneti adatát a DSignLibrary v 1.6 fejlesztő készlet XAdES csomagba teszi.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet képes a XAdES csomagból egy logot készíteni. Itt a napló inkább egyfajta kivonata a csomagnak és nem a tényleges eseményekkel egy időben keletkeznek a naplóbejegyzések. Fokozott biztonságú aláíró alkalmazásnál ez elegendő.

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet képes az aláírói tanúsítványok állapotának lekérésére. Tanúsítványok megszerzésére nincs szükség, mivel az szerepel a XAdES csomagban.

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: A DSignLibrary v 1.6 fejlesztő készlet a Windows tanúsítványtárát használja a tanúsítványok eléréséhez. Itt a teljes tanúsítvány megtalálható.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet képes egy tanúsítvány hitelességének megállapítására. Képes ellenőrizni a teljes tanúsítványláncot illetve tanúsítvány visszavonási listában való szereplését. offline vagy online módon. Offline mód esetén a CRL-t a Microsoft tanúsítványtárából veszi. Használata nem kötelező. Sem a CRL, sem az elvárt ellenőrzés módja nem kerül letárolásra a XAdES csomagban.

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet biztosítja a fenti elvárást.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet nem egy konkrét aláírási szabályzatra készült. A fejlesztő készlettel különböző aláírási szabályzatok kielégíthetők. A készlet a XAdES és a XAdES-T formátumot támogatja.

Konklúzió: **megfelel**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet deklaráltan a XAdES és a XAdES-T formátumot támogatja. A CRL megőrzéséről az ellenőrzőnek kell gondoskodnia.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet nem egy konkrét aláírási szabályzatra készült. A fejlesztő készlettel különböző aláírási szabályzatok kielégíthetők. A készlet a XAdES és a XAdES-T formátumot támogatja.

Konklúzió: **megfelel**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet közvetlenül nem tud kommunikálni a felhasználóval, de eszközt biztosít az aláírások ellenőrzésére.

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: A DSignLibrary v 1.6 fejlesztő készlet közvetlenül nem tud kommunikálni a felhasználóval, de eszközt biztosít az aláírási szabályzat tárolására és visszakérésére.

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: A DSignLibrary v 1.6 fejlesztő készlet nem jeleníti meg az aláírói dokumentumot.

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: A DSignLibrary v 1.6 fejlesztő készlet hiba vagy hiányosság esetén többféle hibaüzenetet ad vissza. Ezekből a hibaüzenetekből a fejlesztő készletet használó aláíró alkalmazás képes kikeverni a felsorolt állapotokat.

Konklúzió: **megfelel**

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: Ez a DSignLibrary v 1.6 fejlesztő készletet használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Ez a DSignLibrary v 1.6 fejlesztő készletet használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

<u>Gépi (automatikus) ellenőrzés esetén:</u>

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: A DSignLibrary v 1.6 fejlesztő készlete önmagában nem képes automatikusan ellenőrizni a XAdES csomagot, de a csomagban tárolt adatokat képes visszaadni a fejlesztő készletet használó aláíró alkalmazás számára.

Konklúzió: **megfelel**

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.
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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlete önmagában nem képes automatikusan ellenőrizni a XAdES csomagot, meg vannak benne valósítva az aláírás ellenőrző függvények és az érvényesítő adatlekérő függvények.

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.

Magyarázat: Ez a DSignLibrary v 1.6 fejlesztő készletet használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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).

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlete szabványos protokollokat használ.

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlete szabványos formátumokat használ. Aláírási formátumként XAdES és XAdES-T, tanúsítvány formátumként X509v3.

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.

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).

Magyarázat: Ez a DSignLibrary v 1.6 fejlesztő készletet használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet teljesíti a követelményt.

Konklúzió: **megfelelt**

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

Magyarázat: A jelen tanúsítási jelentéshez figyelembe vett a fejlesztőktől független ellenőrző vizsgálat EAL-2-es garancia szintjén ez nem lett ellenőrizve. Az ellenőrzéshez forráskód mélységű elemzés szükséges.

Konklúzió: **nincs ellenőrizve**

/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.

Magyarázat: A jelen tanúsítási jelentéshez figyelembe vett a fejlesztőktől független ellenőrző vizsgálat EAL-2-es garancia szintjén ez nem lett ellenőrizve. Az ellenőrzéshez forráskód mélységű elemzés szükséges. Ez egyébként a DSignLibrary v 1.6 fejlesztő készletet használó alkalmazás feladata is.

Konklúzió: **nincs ellenőrizve**

Bizt_köv4: Egy nyilvános aláírás-létrehozó rendszer nem őrizheti meg, illetve nem másolhatja le az aláíráshoz kapcsolódó érzékeny elemeket (aláírót hitelesítő adatok, aláírandó adat, formattált aláírandó adat) egyetlen olyan partner számára sem, akit az aláíró nem jogosított fel erre.

Magyarázat: A jelen tanúsítási jelentéshez figyelembe vett a fejlesztőktől független ellenőrző vizsgálat EAL-2-es garancia szintjén ez nem lett ellenőrizve. Az ellenőrzéshez forráskód mélységű elemzés szükséges. Ez egyébként a DSignLibrary v 1.6 fejlesztő készletet használó alkalmazás feladata is.

Konklúzió: **nincs ellenőrizve**

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

Magyarázat: Nem a DSignLibrary v 1.6 fejlesztő készlet hatásköre. Más módon kell biztosítani.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: Nem a DSignLibrary v 1.6 fejlesztő készlet hatásköre. Más módon kell biztosítani.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet önmagában nem képes megoldani, de a benne eltárolt dokumentumot helyesen adja vissza.

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a XAdES csomagban eltárolt dokumentumot tudja feldolgozni.

Konklúzió: **megfelel**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet nem osztott architektúrájú aláíró alkalmazások fejlesztésére készült.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet nem osztott architektúrájú aláíró alkalmazások fejlesztésére készült.

Konklúzió: **nem vonatkozik rá a követelmény**

A nem megbízható folyamatokból és 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.

Magyarázat: A DSignLibrary v 1.6 egy fejlesztő készlet, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek kell biztosítani

Konklúzió: **feltétellel megfelel**

1. számú feltétel *A DSign Library 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be 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).

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlettel 0 hosszú fájlt nem lehet alá írni.

Konklúzió: **megfelel**

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet a XAdES csomagban tárolja az aláíró tanúsítványát, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet képes a XAdES csomagban aláírási szabályzatot tárolni, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet képes a XAdES csomagban kötelezettségvállalás típust tárolni, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet képes tárolni a XAdES csomagban aláírói dokumentum tartalom formátumát, aláírt aláírási tulajdonságkén, így nem módosítható.

Konklúzió: **megfelel**

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet képes tárolni és visszaadni a XAdES csomagban az aláírói dokumentum tartalom formátumát

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata.

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata. A fejlesztő készlet képes több tartalom formátumot kezelni. A vele kifejlesztett alkalmazás leírásának feladata.

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata.

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata. A fejlesztő készlet képes több tartalom formátumot kezelni.

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: A DSignLibrary v 1.6 fejlesztő készlet csak az XAdES csomagban eltárolt dokumentumot tudja aláírni.

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).

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata.

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: A DSignLibrary v 1.6 fejlesztő készlet csak az XAdES csomagban eltárolt dokumentumot tudja aláírni..

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet képes tárolni a XAdES csomagban aláírói dokumentum tartalom formátumát, aláírt aláírási tulajdonságkén, így nem módosítható.

Konklúzió: **megfelel**

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet képes tárolni a XAdES csomagban aláírói dokumentum tartalom formátumát, aláírt aláírási tulajdonságkén, így nem módosítható.

Konklúzió: **megfelel**

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet nem jelenít meg aláírási tulajdonságokat, de képes azokat visszaadni az aláíró alkalmazásnak.

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.

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet biztosítja a neki paraméterként átadott aláírt aláírási tulajdonságok hitelességét és sértetlenségét.

Konklúzió: **megfelel**

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

Megjegyzés: A DSignLibrary v 1.6 fejlesztő készlet alkalmazásakor az aláírási tulajdonságokat maga az aláírás védi.

Konklúzió: **feltétellel megfelel**

2. számú feltétel: *A DSign Library 1.6 programozói könyvtárban a dokumentumhoz illetve magához a dossziéhoz kapcsolt megjegyzések nem minősülnek aláírási tulajdonságnak. Az alkalmazandó Aláírási Szabályzatnak tiltania kell jogi következménnyel járó adatok írását a megjegyzésekbe.*

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: A DSignLibrary v 1.6 fejlesztő készlet aláírási tulajdonságai nem tartalmaznak rejtett szöveget vagy aktív kódot.

Konklúzió: **megfelel**

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: A DSignLibrary v 1.6 fejlesztő készlet aláírási tulajdonságai nem tartalmaznak rejtett szöveget vagy aktív kódot.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet paraméterként kapja meg az aláíró adatokhoz csatolandó tanúsítványt. A megjelenítés az őt hívó alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Megjegyzés: Nem a DSignLibrary v 1.6 fejlesztő készlet feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat bekérése a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP 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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP 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).

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP feladata.

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).

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a CSP feladata.

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: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet az ETSI TS 101 903 dokumentumában leírt XAdES és XAdES-T formátumot használja.

Konklúzió: **megfelel**

2.2.7 Követelmények az adat lenyomat készítő összetevőre (DHC)

Bizt_köv49: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy „elfogadott” lenyomatoló algoritmus használatát lenyomatolásra. (Lásd „A biztonságos digitális aláírás algoritmusai és paraméterei” fejezet 2. táblázatának elfogadott lenyomatoló algoritmusait.)

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet az SHA1 lenyomatoló algoritmust használja.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet az aláírt adatra megkövetelt feltöltési módszert alkalmazza.

Konklúzió: **megfelel**

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet megfelel a feltételnek.

Konklúzió: **megfelel**

3. számú feltétel[1]: *A DSign Library 1.6 programozói könyvtárat olyan Elektronikus Aláírási Szabályzattal együtt kell használni, amely az elektronikus aláírás során használt algoritmusokra és input formátumokra az alábbi, megfelelő követelményeket fogalmazza meg:*

- *aláíró algoritmus: RSA*
- *lenyomatoló algoritmus: SHA-1*
- *aláírás formátum: emsa-pkcs1-v1_5*

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat védelme a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

[1] A feltétel mindhárom DHC-vel kapcsolatos biztonsági követelményre vonatkozik.

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Lévén a DSignLibrary v 1.6 fejlesztő készlet szoftver alkalmazás, önállóan nem képes megvédenie sem saját, sem egyes moduljainak integritását. Ezért nem lehet feladata a kommunikációs összetevő módosítással szembeni védelme. Ezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítani.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**

4. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírás-létrehozó eszközzel kommunikáló összetevőt (CSP) ne lehessen jogosulatlanul módosítani.*

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.

Magyarázat: A DSignLibrary v 1.6 fejlesztő készlet a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: Lévén a DSignLibrary v 1.6 fejlesztő készlet szoftver alkalmazás, önállóan nem képes megvédenie sem saját, sem egyes moduljainak integritását. Ezért nem lehet feladata a kommunikációs összetevő módosítással szembeni védelme. Ezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítani.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**

5. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:*

- *vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint*
- *az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.*

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

Magyarázat: Lévén a DSignLibrary v 1.6 fejlesztő készlet szoftver alkalmazás, önállóan nem képes megvédenie sem saját, sem egyes moduljainak integritását. Ezért nem lehet feladata a kommunikációs összetevő módosítással szembeni védelme. Ezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítani.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**

6. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A DSign Library 1.6 programozói könyvtár funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

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

Magyarázat: A DSignLibrary v 1.6 fejlesztő készletben nincs importált komponens.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.11 Követelmények az aláírás-rendszer védelmére (biztonságos terület)

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

Magyarázat: A rendszer jellegéből adódóan csak egy szoftver modul jöhet számításba. A biztonságos szoftver modult a működtetési környezetnek kell megvalósítania.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**.

7. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a DSign Library 1.6 programozói könyvtárat, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

3 A DSign Library 1.6 programozói könyvtár megfelelése a követelményeknek.

3.1 A DSign Library 1.6 programozói könyvtár megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	megfelel
F_SDP_1	nem vonatkozik rá a követelmény
F_SDP_2	nem vonatkozik rá a követelmény
F_SDP_3	nem vonatkozik rá a követelmény
F_SDP_4	nem vonatkozik rá a követelmény
F_SAV_1	megfelel
F_SAV_2	megfelel
F_SIC_1	nem vonatkozik rá a követelmény
F_SIC_2	nem vonatkozik rá a követelmény
F_SIC_3	nem vonatkozik rá a követelmény
F_DTBSF_1	megfelel
F_DTBSF_2	megfelel
F_DHC_1	megfelel
F_DHC_2	megfelel
F_SSC_1	megfelel
F_SSC_2	megfelel
F_SSC_3	nem vonatkozik rá a követelmény
F_SSC_4	nem vonatkozik rá a követelmény
F_SSC_5	nem vonatkozik rá a követelmény
F_SSC_6	nem vonatkozik rá a követelmény
F_SSC_7	nem vonatkozik rá a követelmény
F_SSC_8	megfelel
F_SSC_9	megfelel
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	nem vonatkozik rá a követelmény
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	megfelel
F_ISV-2	megfelel
F_USV-1	megfelel
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	megfelel
F_human_5	nem vonatkozik rá a követelmény
F_human_6	nem vonatkozik rá a követelmény
F_machine_1	megfelel
F_machine_2	megfelel
F_general_1	nem vonatkozik rá a követelmény
F_protocol	megfelel
F_format	megfelel
F_principles	nem vonatkozik rá a követelmény

3.2 A DSign Library 1.6 programozói könyvtár megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	megfelel
Bizt_köv2	nincs ellenőrizve
Bizt_köv3	nincs ellenőrizve
Bizt_köv4	nincs ellenőrizve
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
Bizt_köv12	megfelel
Bizt_köv13	megfelel
Bizt_köv14	megfelel
Bizt_köv15	megfelel
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	nem vonatkozik rá a követelmény
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	feltétellel megfelel
Bizt_köv32	megfelel
Bizt_köv33	megfelel
Bizt_köv34	nem vonatkozik rá a követelmény
Bizt_köv35	nem vonatkozik rá a követelmény
Bizt_köv36	nem vonatkozik rá a követelmény
Bizt_köv37	nem vonatkozik rá a követelmény
Bizt_köv38	nem vonatkozik rá a követelmény
Bizt_köv39	nem vonatkozik rá a követelmény
Bizt_köv40	nem vonatkozik rá a követelmény
Bizt_köv41	nem vonatkozik rá a követelmény
Bizt_köv42	nem vonatkozik rá a követelmény
Bizt_köv43	nem vonatkozik rá a követelmény
Bizt_köv44	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
Bizt_köv53	nem vonatkozik rá a követelmény
Bizt_köv54	nem vonatkozik rá a követelmény
Bizt_köv55	feltétellel megfelel
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	feltétellel megfelel
Bizt_köv58	feltétellel megfelel
Bizt_köv59	nem vonatkozik rá a követelmény
Bizt_köv60	feltétellel megfelel

4 A Tanúsítási jelentés eredménye, érvényességi feltételei.

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltételek teljesülése esetén a DSign Library 1.6 programozói könyvtár alkalmas fokozott elektronikus aláíró és ellenőrző alkalmazások fejlesztésére. A feltételek nem a megvalósított programozói könyvtárra vonatkoznak, hanem annak telepítésére, környezetére, illetve az alkalmazható Elektronikus Aláírási Szabályzatra vonatkoznak.

4.2 Érvényességi feltételek

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a DSign Library 1.6 programozói könyvtárral kifejlesztett elektronikus aláíró alkalmazások által kezelt aláírások biztonságához.

1. számú feltétel *A DSign Library 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.*

Érintett biztonsági követelmény: Bizt_köv11

2. számú feltétel: *A DSign Library 1.6 programozói könyvtárban a dokumentumhoz illetve magához a dossziéhoz kapcsolt megjegyzések nem minősülnek aláírási tulajdonságnak. Az alkalmazandó Aláírási Szabályzatnak tiltania kell jogi következménnyel járó adatok írását a megjegyzésekbe.*

Érintett biztonsági követelmény: Bizt_köv31

3. számú feltétel: *A DSign Library 1.6 programozói könyvtárat olyan Elektronikus Aláírási Szabályzattal együtt kell használni, amely az elektronikus aláírás során használt algoritmusokra és input formátumokra az alábbi, megfelelő követelményeket fogalmazza meg:*

- *aláíró algoritmus: RSA*
- *lenyomatoló algoritmus: SHA-1*
- *aláírás formátum: emsa-pkcs1-v1_5*

Érintett biztonsági követelmények: Bizt_köv49
Bizt_köv50
Bizt_köv51

4. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírás-létrehozó eszközzel kommunikáló összetevőt (CSP) ne lehessen jogosulatlanul módosítani.*

Érintett biztonsági követelmény: Bizt_köv55

5. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:*

- *vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint*
- *az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.*

Érintett biztonsági követelmény: Bizt_köv57

6. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A DSign Library 1.6 programozói könyvtár funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

Érintett biztonsági követelmény: Bizt_köv58

7. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a DSign Library 1.6 programozói könyvtárat, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

Érintett biztonsági követelmény: Bizt_köv60

4.3 Automatikus érvényesség

Bizonyos Funkcionális és Biztonsági követelmények automatikusan teljesülnek a DSign Library 1.6 programozói könyvtárral fejlesztett elektronikus aláíró alkalmazásokra. Feltéve, hogy a Library-t helyesen használják. Az alkalmazásra automatikusan teljesülő követelmények a következők:

F_DTBSF_1
F_DTBSF_2
F_DHC_1
F_DHC_2
F_SSC_8
F_SSC_9
F_SDOC_1
F_SLC_1
F_SCPC_1
F_I/O-2
F_protocol
F_format
Bizt_köv12
Bizt_köv48
Bizt_köv49
Bizt_köv50
Bizt_köv51

5 A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

Jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ **EAL 2**-es szintjéhez hasonló volt. / Az EAL 2 a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét biztosítja, mely elegendő a fokozott biztonságú elektronikus aláíráshoz használható aláírási termékekre. /

A fejlesztőktől függetlenül ellenőrző vizsgálatról összefoglalásként egy értékelési jelenté készült.
Jelen tanúsítási jelentés alapvetően a fejlesztői bizonyítékokra, valamint az értékelési jelentésben megfogalmazott és dokumentált eredményekre épül.

Az értékelés az alábbi garancia osztályokra terjedt ki:

- Konfiguráció menedzselés
- kiszállítás és működtetés
- fejlesztés
- útmutató dokumentumok
- tesztek

Az értékelés során a fejlesztőktől független minta tesztelésre is sor került.

6 A tanúsításhoz figyelembe vett egyéb 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 fro Signature Creation System

CEN/ISSS/E-Sign; Area G2 14171 munkacsoport egyezmény: Procedures for Elecronic 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)

6.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1 A tanúsításhoz figyelembe vett fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- DSign Library 1.6 Telepítési útmutató – 2004.02.17
- Funkció specifikáció - A DSign Library programozói könyvtárhoz 1.6 verzió – 2004.02.20
- Magas szintű terv - - A DSign Library programozói könyvtárhoz 1.6 verzió – 2004.02.27
- DSign Library 1.6 Adminisztrátori útmutató – 2004.02.17
- DSign Library 1.6 Felhasználói útmutató – 2004.02.17
- DSign Library 1.6 Teszt jegyzőkönyvek – 2004.02.17
- DSign Library 1.6 Tesztlefedettség elemzés – 2004.02.25

6.2.2 A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés a DSignLibrary 1.6 elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói könyvtárról (Készítette HunGuard Kft.)

7 Rövidítések

API (application programing interface)

CRL (certification revocation list) tanúsítvány visszavonási lista

CSP (cryptograpic service provider) kriptográfiai szolgáltató

DHC (Data hashing component) adatlenyomat-készítő összetevő az aláírandó adat reprezentáns

DTBS (Data To Be Signed) aláírandó adat

DTBSF (DTBS formatter) aláírandó adat formattáló

EAL (Evaluation Assurance Level)

ÉJ értékelési jelentés

OCSP (on-line certfication status protocol) valósidejű tanúsítvány állapot protokoll

PKI (Public Key Infrastructure)

PIN (Personal Identification Number)

SAC (Signer's authentication component) aláírót hitelesítő összetevő

SAV (Signature attribute viewer) aláírási tulajdonság megjelenítő

SCA (Signature creation application) aláírás-létrehozó alkalmazás

SCS (Signature creation system) aláírás-létrehozó rendszer

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

SDX (Signed Document eXpert)

SIC (Signer's interaction component) aláíróval kölcsönható összetevő

SLC (Signature logging component) aláírás-naplózási összetevő

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