Tanúsítási Jelentés

Hung-TJ-019-2004

a
DSign UI 1.6

elektronikus aláíró alkalmazásról

/MÁV INFORMATIKA Kft./

Készítette: HunGuard Kft.

1. A DSign UI 1.6 legfontosabb tulajdonságainak összefoglalása

A tanúsított termék a MÁV INFORMATIKA Kft. által fejlesztett és forgalmazott DSign UI 1.6 aláíró alkalmazás.

1.1. Architektúra

A DSign Ui 1.6 aláíró alkalmazás elektronikus dokumentumok elektronikus aláírással történő ellátását, és ezen aláírások kezdeti ellenőrzését támogatja. Az aláírt adat objektumot az ETSI TS 101 903 dokumentumában specifikált XAdES illetve XAdES-T (XML Advanced Electronic Signature) formátumban tárolja.

Az alkalmazás Microsoft Windows 2000/2003/XP operációs rendszeren és Microsoft . NET Framework környezetben működik. Az alkalmazás alapja a szintén a MÁV INFORMATIKA Kft. által fejlesztett DSign Library 1.6 programozói könyvtár. E könyvtárban lévő objektumokon keresztül éri el az operációs rendszer Crypto API-ját, amely az operációs rendszer részeként meg lévő, vagy más gyártó által írt CSP (Crypto Service Provider) segítségével tud kommunikálni aláíró eszközzel. Az aláírás folyamat során a megfelelő XML struktúrák legenerálódnak az aláírandó adatra az aláírás a CSP-n keresztül készül el.

1.2. Tulajdonságok

A DSIgn UI 1.6 aláíró alkalmazás elektronikus dossziék hatékony kezelésére alkalmazható. Ezekhez a dossziékhoz dokumentumok adhatóak, vagy törölhetőek ki akár csoportosan is. Ezekhez a dokumentumokhoz egyenként vagy összevontan elektronikus aláírás készíthető. Az aláírások ideje időpecséttel hitelessé tehető.

Az aláírandó adat kötelező tartalma:

- Az aláírt dokumentum(ok) tartalma és jellemzői (dokumentum neve, dokumentum fájlneve, dokumentum fájlmérete, dokumentum MIME típusa, dokumentum kódolása a csomagban, dokumentum létrehozásának és csomagba felvételének dátuma).
- Az aláíráshoz használt tanúsítvány egyes jellemzői (az aláírói tanúsítvány kiállítója, az aláírói tanúsítvány sorszáma, az aláírói tanúsítvány maga (pontosabban annak a hash értéke), illetve a tanúsítvány hash létrehozásához használt algoritmus)
- Az aláírás sorszáma (azonosítója), és elkészültének ideje

Az elektronikus aláírások a felhasználó igénye alapján az alábbi aláírt tulajdonságokkal bővíthetőek:

- A kiválasztott aláírási szabályzat (signature policy)
- A kiválasztott aláírási hely (signature production place)
- A kiválasztott aláírási szerepkörök (signer claimed role)
- Helytállás típusa (commitment type)

Az aláírások azonnal ellenőrizhetőek. Aláírás ellenőrzésekor az érvényes aláírási szabályzat betartása a felhasználó felelőssége. Az ellenőrzés kiegészíthető offline (a Windows tanúsítványában tárolt) vagy online (a tanúsítvány CRL elérési hely mezőjében leírt URL-ről közvetlenül letöltött) visszavonási lista vizsgálattal is. Az aláírás eredménye érvényes vagy érvénytelen lehet. Érvénytelen esetben kijelzésre kerül a hiba oka.

Aláírás ellenőrzéshez költségmentesen elérhető alkalmazás létezik DSign Viewer 1.6 néven.

A DSign UI 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 hatóköre

A jelen tanúsítás tárgya maga a DSign UI 1.6 aláíró alkalmazás.

A tanúsítás során feltételeztük, hogy az alkalmazás alapjául szolgáló Windows operációs rendszer, valamint az ennek részét képező CSP modul biztonságosan és helyesen működnek. A DSign UI 1.6 alapvetően az alábbi komponensekre épül:

- DSign Library 1.6
- Microsoft .NET Framework 1.1
- Microsoft Crypto API

2. A DSign UI 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 UI 1.6 aláíró alkalmazásra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy a DSign UI 1.6 aláíró alkalmazás megfelel-e az adott követelménynek.

Minthogy a DSign UI 1.6 aláíró alkalmazást fokozott aláíró alkalmazások fejlesztésére kívánják felhasználni, megfelelő tanúsítási vélemény akkor is adható, ha az UI 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 DSign UI 1.6 aláíró alkalmazás minden általa aláírt dokumentum esetén automatikus aláírás ellenőrzést végez.

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 DSign UI 1.6 aláíró alkalmazás minden általa aláírt dokumentum esetén a dokumentum nevét és MIME típusát attribútumként tárolja. A dokumentum fájlnevének kiterjesztése jelöli a tartalom-formátumot.

Konklúzió: **megfelel**

F_SDP_2: Amennyiben az aláírói dokumentum szemantikája nem függ annak megjelenítésétől, akkor vagy az aláírói dokumentumban vagy egy aláírás tulajdonságban meg kell adni a tartalom egyértelműséghez szükséges információkat.

Magyarázat: A DSign UI 1.6 aláíró alkalmazás minden általa aláírt dokumentum esetén a dokumentum nevét és MIME típusát attribútumként tárolja. A külső megjelenítő kiválasztása a dokumentum fájlnevének kiterjesztése alapján történik.

Konklúzió: **megfelel**

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: A DSign UI 1.6 aláíró alkalmazás minden általa aláírt dokumentum esetén a dokumentum nevét attribútumként tárolja. A külső megjelenítő kiválasztása a dokumentum fájlnevének kiterjesztése alapján történik.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás minden általa aláírt dokumentum esetén a dokumentum nevét attribútumként tárolja. A külső megjelenítő kiválasztása a dokumentum fájlnevének kiterjesztése alapján történik.

Konklúzió: **megfelel**

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

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás lehetőséget biztosít a következő aláírt aláírási tulajdonságok megjelenítését: Aláírás ideje; Aláírási szabályzat; Elfogadási Nyilatkozat; Aláírás helye; Állított szerepkör; Kötelezettség vállalás típusa.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a Windows tanúsítvány-megjelenítőjét használva ad lehetőséget az aláíró tanúsítvány megjelenítésére.

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: A DSign UI 1.6 aláíró alkalmazás az aláírás funkció kiváltása után, az aláírási tulajdonságok beállítása után még egyszer rákérdez a felhasználói akaratra.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás biztosítja az aláíró/ellenőrző számára a megfelelő funkciókat.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

Konklúzió: **megfelel**

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

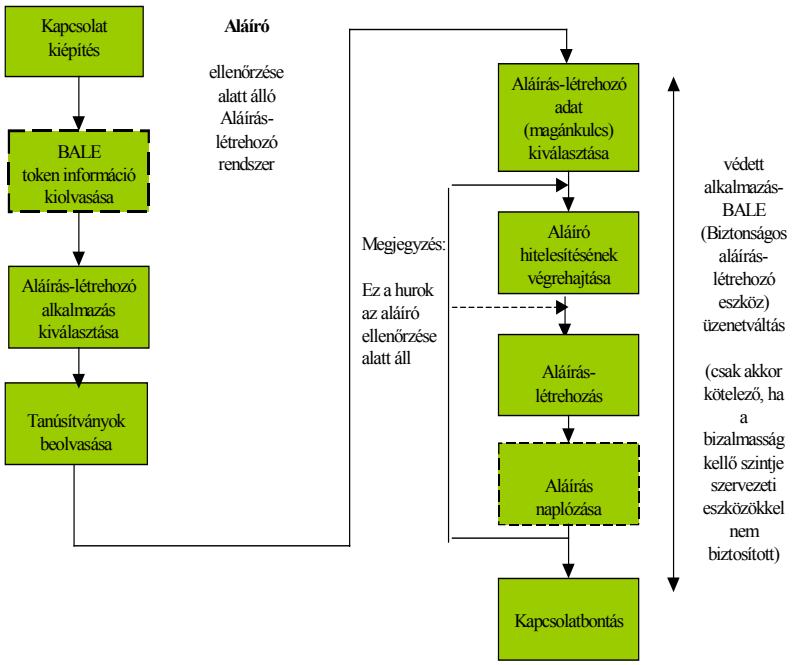
Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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: A DSign UI 1.6 aláíró alkalmazás minden szükséges kommunikációt végrehajt.

Konklúzió: **megfelel**



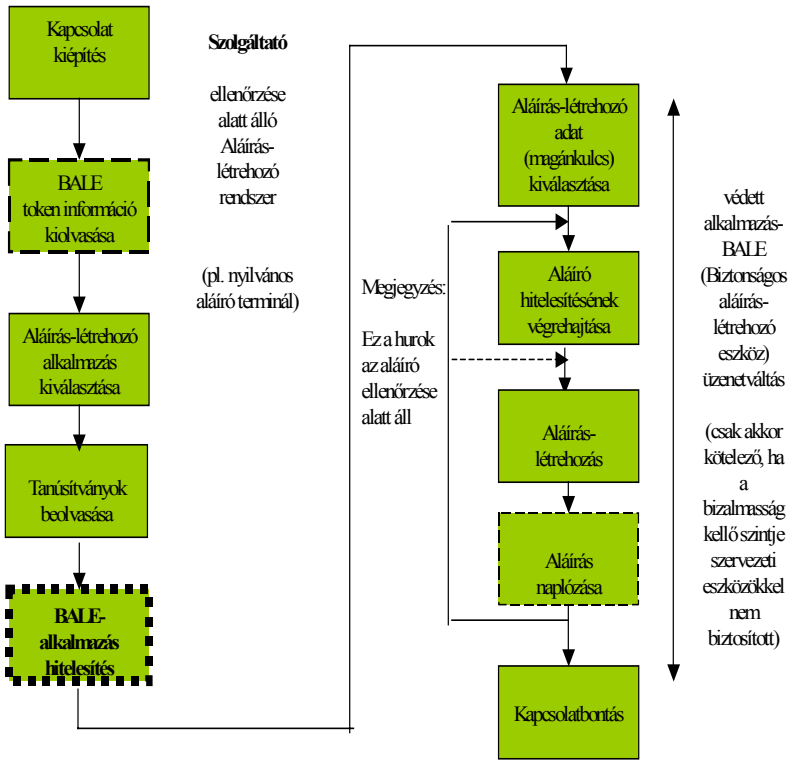
1. ábra

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: A DSign UI 1.6 aláíró alkalmazást nem külső szolgáltató ellenőrzése alá tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**



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 DSign UI 1.6 aláíró alkalmazás az operációs rendszer erőforrásainak igénybevételével képes fizikai interfészen keresztül aláíró eszközzel kommunikálni.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó alkalmazásnak a 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 DSign UI 1.6 aláíró alkalmazás támogatja a több tanúsítványból történő választást. A tanúsítványok tárolására az operációs rendszer tanúsítványtárát használja.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

Konklúzió: **megfelel**

F_SSC_9: A befejezett aláírásokat naplózni kell.

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető. 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 DSign UI 1.6 aláíró alkalmazást nem külső szolgáltató ellenőrzése alá tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazást lehetővé teszi az aláírói dokumentum(ok) kiválasztását.

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető. 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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető. A rendszer csak az aláírói tanúsítványok állapotának lekérésére képes. Tanúsítványok megszerzésére nincs szükség, mivel az aláíró tanúsítványa aláírási tulajdonságként 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás az aláíró tanúsítványának érvényességének és hitelességének ellenőrzéséhez képes a megfelelő adatok (hitelesítő szolgáltató tanúsítványa, visszavonási lista, aláírás ideje) begyűjtésére.

Konklúzió: **feltétellel megfelel**

***1 számú feltétel**: Ha az aláírási szabályzat kiköti a CRL ellenőrzést, valamint az adott hitelesítés-szolgáltató a már lejárt tanúsítványokat törli a visszavonási listából, akkor - mivel a CRL érvényességét az ellenőrzés időpontjához viszonyítja a DSign UI 1.6 aláíró alkalmazás - CRL ellenőrzést csak akkor szabad kérni, ha az ellenőrzés időpontja korábbi, mint a tanúsítvány érvényesség lejárati dátuma. Ellenkező esetben a CRL ellenőrzés nem valós eredményt adhat.*

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 DSign UI 1.6 aláíró alkalmazás a kezdeti ellenőrzés folyamán minden érvényesítő adatot begyűjt. 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 CWA14171 5. fejezet 5.1. pontja alapján az utólagos ellenőrzés fogalma jóval későbbi (évek eltelte utáni), a kezdetben letöltött érvényesítő adatokon kívüli új adatok lekérése nélküli ellenőrzést jelent. A DSign UI 1.6 aláíró alkalmazás utólagos ellenőrzés során nem tud korábbi visszavonási listákat a szolgáltatótól lekérni, sem letárolt, lejárt visszavonási listákat kezelni.

Konklúzió: **nem felel meg**

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 DSign UI 1.6 aláíró alkalmazás támogatja a fenti elvárást.

Konklúzió: **megfelel**

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 DSign UI 1.6 aláíró alkalmazás támogatja a fenti elvárást.

Konklúzió: **megfelel**

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 DSign UI 1.6 aláíró alkalmazás a dokumentum nevének kiterjesztése alapján kiválasztott külső megjelenítőt alkalmaz. A külső megjelenítők helyes telepítése, működése a felhasználó felelőssége.

Konklúzió: **feltétellel megfelel**

2. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírni kívánt dokumentumokhoz szükséges megjelenítő alkalmazások megfelelő módon telepítve és konfigurálva legyenek.*

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 DSign UI 1.6 aláíró alkalmazás érvényes vagy érvénytelen állapotot ismer. Az érvénytelen állapot kijelzése az érvénytelenség okával történik

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: A DSign UI 1.6 aláíró alkalmazás csak érvényes vagy érvénytelen állapotot ismer.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás teljesíti a fenti elvárást.

Konklúzió: **megfelel**

Gépi (automatikus) ellenőrzés esetén:

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 DSign UI 1.6 aláíró alkalmazást nem automatikus ellenőrzésre tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

F_machine_2: A 2-es típusú API-k az elektronikus aláírások hitelesítését és/vagy ellenőrzését kell lehetővé tenniük, illetve be kell szerezniük az aláírói információkat, az output állapotot és az érvényesítő adatokat.
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 DSign UI 1.6 aláíró alkalmazást nem automatikus ellenőrzésre tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

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: A DSign UI 1.6 aláíró alkalmazást teljesíti a fenti elvárást.

Konklúzió: **megfelel**

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

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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: A DSign UI 1.6 aláíró alkalmazást teljesíti a fenti elvárást.

Konklúzió: **megfelel**

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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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 DSign UI 1.6 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

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: A DSign UI 1.6 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

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 DSign UI 1.6 aláíró alkalmazás a külső alkalmazásnak bemutatásra közvetlenül az XAdES csomagból adja át a dokumentumot.

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 DSign UI 1.6 aláíró alkalmazás az aláírás folyamán a XAdES csomag DOCS szekciójában lévő a dokumentumot írja alá.

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 DSign UI 1.6 aláíró alkalmazás nem osztott arhitektúrájú aláíró alkalmazás.

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 DSign UI 1.6 aláíró alkalmazás nem osztott arhitektúrájú aláíró alkalmazás.

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: Lévén a DSign UI 1.6 egy szoftveralkalmazás, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek (operációs rendszer) kell biztosítani

Konklúzió: **feltétellel megfelel**

3. számú feltétel *A DSign UI 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).

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás, amennyiben az aláíró az aláírás előtt megadja, a XAdES csomagban tárolja a hivatkozást az aláírási szabályzatra, 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 DSign UI 1.6 aláíró alkalmazás, amennyiben az aláíró az aláírás előtt megadja, a XAdES csomagban tárolja a hivatkozást az aláírási szabályzatra, 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 DSign UI 1.6 aláíró alkalmazás, a dokumentum kiterjesztése alapján határozza meg az aláírói dokumentum tartalom formátumát. Ezt a XAdES csomagban tárolja, mint aláírt aláírási tulajdonság.

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 DSign UI 1.6 aláíró alkalmazás, a dokumentum nevének kiterjesztése alapján határozza meg az aláírói dokumentum tartalom formátumát. Ezt a XAdES csomagban tárolja, mint aláírt aláírási tulajdonság.

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: A DSign UI 1.6 aláíró alkalmazás, a rendszerre telepített, adat formátumonként akár különböző, külső megjelenítőket használ.

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: A DSign UI 1.6 aláíró alkalmazás külső megjelenítőket használ, ezért elvileg bármely tartalom formátumot támogat. A korlátozást nem a felhasználói dokumentációban, hanem az adott helyen érvényes aláírási szabályzatban kell meghatározni.

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: A DSign UI 1.6 aláíró alkalmazás külső megjelenítőket használ, ezért elvileg bármely tartalom formátumot támogat. A korlátozást nem a felhasználói dokumentációban, hanem az adott helyen érvényes aláírási szabályzatban kell meghatározni.

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: A DSign UI 1.6 aláíró alkalmazásban nincs megkötés a tartalom formátumban.

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 DSign UI 1.6 aláíró alkalmazás a külső alkalmazásnak bemutatásra közvetlenül az XAdES csomagból adja át a dokumentumot.

Konklúzió: **feltétellel megfelel**

2. számú feltétel *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírni kívánt dokumentumokhoz szükséges megjelenítő alkalmazások megfelelő módon telepítve és konfigurálva legyenek.*

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: A DSign UI 1.6 aláíró alkalmazás külső megjelenítőket használ, ezért elvileg bármely tartalom formátumot támogat. Amennyiben ez egy aláírt adat objektum akkor megjelenítőként a megfelelő ellenőrző rendszert hívja meg.

Konklúzió: **feltétellel megfelel**

2. számú feltétel *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírni kívánt dokumentumokhoz szükséges megjelenítő alkalmazások megfelelő módon telepítve és konfigurálva legyenek.*

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

Megjegyzés: A DSign UI 1.6 aláíró alkalmazás külső megjelenítőket használ, a megjelenítendő file-t a XAdES csomagból temporális file-ba másolja. E file módosítása nem hat a csomag tartalmára.

Konklúzió: **megfelel**

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: A DSign UI 1.6 aláíró alkalmazás, a rendszerre telepített, adat formátumonként akár különböző, külső megjelenítőket használ. Ezek működése túlmutat az alkalmazás hatókörén.

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 DSign UI 1.6 aláíró alkalmazás, a dokumentum kiterjesztése alapján határozza meg az aláírói dokumentum tartalom formátumát. Ezt a XAdES csomagban tárolja, mint aláírt aláírási tulajdonság.

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 DSign UI 1.6 aláíró alkalmazás, a dokumentum kiterjesztése alapján határozza meg az aláírói dokumentum tartalom formátumát. Ezt a XAdES csomagban tárolja, mint aláírt aláírási tulajdonság.

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: A DSign UI 1.6 aláíró alkalmazás az aláírási szabályzatban foglalt korlátozások automatikus ellenőrzését nem támogatja. Az aláírói dokumentum belső tartalmára érzéketlen.

Konklúzió: **nem felel meg**

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 DSign UI 1.6 aláíró alkalmazás lehetőséget ad az aláírási tulajdonságok megtekintésére.

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 DSign UI 1.6 aláíró alkalmazás biztosítja az aláírt aláírási tulajdonságok hitelességét és sértetlenségét.

Konklúzió: **megfelel**

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

Megjegyzés: A DSign UI 1.6 aláíró alkalmazásban az aláírási tulajdonságokat maga az aláírás védi.

Konklúzió: **feltétellel megfelel**

4. számú feltétel *A DSign UI 1.6 aláíró alkalmazásban 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás a Windows tanúsítvány-megjelenítőjét használva ad lehetőséget az aláíró tanúsítvány megjelenítésére.

Konklúzió: **megfelel**

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.

Magyarázat: A DSign UI 1.6 aláíró alkalmazás az aláírás funkció kiváltása után, az aláírási tulajdonságok beállítása után még egyszer rákérdez a felhasználói akartra.

Konklúzió: **megfelel**

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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

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 DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

Konklúzió: **megfelel**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás a DSign Library 1.6 fejlesztő készletre épül. A HUNG-TJ-018-2004 számú tanúsítási jelentés alapján a fejlesztő készlet megfelel a követelménynek. A követelmény ezért automatikusan teljesítettnek vehető

Konklúzió: **megfelel**

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 DSign UI 1.6 aláíró alkalmazás képes fizikai interfészen keresztül aláíró eszközzel kommunikálni.

Konklúzió: **megfelel**

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 DSign UI 1.6 aláíró alkalmazás a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat védelme a CSP feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 egy 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 biztosítania.

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

5. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazás a Microsoft Crypto API-jára támaszkodik.

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 DSign UI 1.6 egy szoftver alkalmazás, önállóan nem képes megvédenie saját integritását. Nem lehet feladata a vírusok elleni védelem és a helyreállítás sem. Mindezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítania.

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

6. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 egy szoftver alkalmazás, önállóan nem képes megvédenie saját integritását. Nem lehet feladata a behatolók elleni védekezés sem. Mindezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítania.

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

7. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A DSign UI 1.6 aláíró alkalmazás 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 DSign UI 1.6 aláíró alkalmazásban 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. Biztonságos területen a szoftver modult a működtetési környezetnek kell megvalósítania.

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

8. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a DSign UI 1.6 aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

3. A DSign UI 1.6 aláíró alkalmazás megfelelése a követelményeknek

3.1. A DSign UI 1.6 aláíró alkalmazás megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	megfelel
F_SDP_1	megfelel
F_SDP_2	megfelel
F_SDP_3	megfelel
F_SDP_4	megfelel
F_SAV_1	megfelel
F_SAV_2	megfelel
F_SIC_1	megfelel
F_SIC_2	megfelel
F_SIC_3	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	nem vonatkozik rá a követelmény
F_SSC_3	megfelel
F_SSC_4	nem vonatkozik rá a követelmény
F_SSC_5	megfelel
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	megfelel
F_SDOC_1	megfelel
F_SLC_1	megfelel
F_SCPC_1	megfelel
F_I/O-1	nem vonatkozik rá a követelmény
F_I/O-2	megfelel
F_I/O-3	megfelel
F_ISV-1	feltétellel megfelel
F_ISV-2	megfelel
F_USV-1	nem felel meg
F_human_1	megfelel
F_human_2	megfelel
F_human_3	feltétellel megfelel
F_human_4	megfelel
F_human_5	nem vonatkozik rá a követelmény
F_human_6	megfelel
F_machine_1	nem vonatkozik rá a követelmény
F_machine_2	nem vonatkozik rá a követelmény
F_general_1	megfelel
F_protocol	megfelel
F_format	megfelel
F_principles	megfelel

3.2. A DSign UI 1.6 aláíró alkalmazás megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	megfelel
Bizt_köv2	nincs ellenőrizve
Bizt_köv3	nem vonatkozik rá a követelmény
Bizt_köv4	nem vonatkozik rá a követelmény
Bizt_köv5	nem vonatkozik rá a követelmény
Bizt_köv6	nem vonatkozik rá a követelmény
Bizt_köv7	megfelel
Bizt_köv8	megfelel
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	feltétellel megfelel
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	feltétellel megfelel
Bizt_köv23	feltétellel megfelel
Bizt_köv24	megfelel
Bizt_köv25	nem vonatkozik rá a követelmény
Bizt_köv26	megfelel
Bizt_köv27	megfelel
Bizt_köv28	nem felel meg
Bizt_köv29	megfelel
Bizt_köv30	megfelel
Bizt_köv31	feltétellel megfelel
Bizt_köv32	megfelel
Bizt_köv33	megfelel
Bizt_köv34	megfelel
Bizt_köv35	megfelel
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	megfelel
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 UI 1.6 aláíró alkalmazás alkalmas fokozott biztonságú elektronikus aláírások létrehozására és ellenőrzésére.
A feltételek nem a megvalósított aláíró alkalmazásra 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 UI 1.6 aláíró alkalmazás által kezelt aláírások biztonságához.

***1 számú feltétel**: Ha az aláírási szabályzat kiköti a CRL ellenőrzést, valamint az adott hitelesítés-szolgáltató a már lejárt tanúsítványokat törli a visszavonási listából, akkor - mivel a CRL érvényességét az ellenőrzés időpontjához viszonyítja a DSign UI 1.6 aláíró alkalmazás - CRL ellenőrzést csak akkor szabad kérni, ha az ellenőrzés időpontja korábbi, mint a tanúsítvány érvényesség lejárati dátuma. Ellenkező esetben a CRL ellenőrzés nem valós eredményt adhat.*

Érintett funkcionális követelmény: F_ISV-1

***2. számú feltétel:** A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírni kívánt dokumentumokhoz szükséges megjelenítő alkalmazások megfelelő módon telepítve és konfigurálva legyenek.*

Érintett funkcionális követelmény: F_human-3

Érintett biztonsági követelmények: Bizt_köv-22
Bizt_köv-23

***3. számú feltétel** A DSign UI 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

4. számú feltétel *A DSign UI 1.6 aláíró alkalmazásban 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

5. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás 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

6. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás 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

7. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A DSign UI 1.6 aláíró alkalmazás funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

Érintett biztonsági követelmény: Bizt_köv58

8. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a DSign UI 1.6 aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

Érintett biztonsági követelmény: Bizt_köv60

5. A követelményeknek való megfelelést ellenőrző vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ EAL 2-es szintjéhez hasonló volt. /Az EAL2 a fejlesztőktől független garantált biztonság mérsékelt szintjét biztosítja./

A fejlesztőktől független ellenőrző vizsgálat összefoglalásaként egy értékelési jelentés készült.
Jelen tanúsítási jelentés alapvetően a fejlesztői bizonyítékokra, valamint az értékelési jelentésben megfogalmazott és dokumentált eredményekre épül.

Az érékelés az alábbi garanciaosztályokra terjedt ki:

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

Az értékelés során, a fentieken kívül a fejlesztőktől független minta, tesztelésre, illetve áthatolás tesztelésre is sor került.

6. Az 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 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)

6.2. A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1. A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- Kérdőív a tanúsítás kérelmezéséhez
- DSign UI 1.6 telepítési útmutató 2004. február 17.
- Funkció specifikáció DSign UI 1.6 2004. február 20.
- Magas szintű terv DSign UI 1.6 2004. február 25.
- DSign UI 1.6 használati útmutató 2004. február 17.
- Fejlesztői tesztjegyzőkönyv 1-24 2004. február 17.
- Fejlesztői teszt lefedettség elemzés 2004. február 25.

6.2.2. A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Hung-TJ-0xx-2004 számú Tanúsítási jelentés a DSignLibrary 1.6 elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói könyvtárról (készítette: HunGuard Kft)
- Értékelési jelentés a DSign UI 1.6 elektronikus aláíró alkalmazásról (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