



TANÚSÍTÁSI JELENTÉS

HUNG-TJ-024-2004

**Az
IngridSigno Feldolgozó Modul 2.1.31**

**minősített elektronikus aláírás ellenőrző
alkalmazásról**

/Pénzügyi Szervezetek Állami Felügyelete/

**Készítette: HunGuard Kft.
2004. december 14.**

1.	Az IngridSigno Feldolgozó Modul 2.1.31 legfontosabb tulajdonságainak összefoglalása	4
1.1.	<i>Architektúra</i>	4
1.2.	<i>Tulajdonságok.....</i>	4
1.3.	<i>A tanúsítás tárgya hatóköre</i>	5
2.	Az IngridSigno Feldolgozó Modul 2.1.31 megfelelése a funkcionális és biztonsági követelményeknek	6
2.1.	<i>Funkcionális követelmények minősített elektronikus aláírásokat létrehozó/ellenőrző alkalmazások számára</i>	6
2.2.	<i>Biztonsági követelmények minősített elektronikus aláírásokat létrehozó/ellenőrző alkalmazások számára</i>	19
2.2.1.	Követelmények az aláírás-létrehozó alkalmazás (SCA) egészére	19
2.2.2.	Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP).....	22
2.2.3.	Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV).....	24
2.2.4.	Követelmények az aláíróval kölcsönható összetevőre (SIC).....	26
2.2.5.	Követelmények az aláíró hitelesítő összetevőre (SAC)	26
2.2.6.	Követelmények az aláírandó adat formattáló összetevőre (DTBSF).....	28
2.2.7.	Követelmények az adat lenyomat készítő összetevőre (DHC).....	28
2.2.8.	Követelmények a biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikáció összetevőre (SSC).....	29
2.2.9.	Követelmények az SSCD/SCA hitelesítő összetevőre (SSA)	30
2.2.10.	Követelmények az Input/Output interfészre (I/O)	30
2.2.11.	Követelmények az aláírás-rendszer védelmére (biztonságos terület)	31
3.	Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelelése a követelményeknek.....	32
3.1.	<i>Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelelése a funkcionális követelményeknek</i>	32
3.2.	<i>Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelelése a biztonsági követelményeknek</i>	33
4.	A tanúsítási jelentés eredménye, érvényességi feltételei	35
4.1.	<i>Eredmények.....</i>	35
4.2.	<i>Érvényességi feltételek:.....</i>	35
5.	A követelményeknek való megfelelést ellenőrző vizsgálat garancia szintje.....	36
6.	A tanúsításhoz figyelembe vett egyéb dokumentumok.....	37
6.1.	<i>Termékmegfelelőségi követelményeket tartalmazó dokumentumok</i>	37
6.2.	<i>A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok.....</i>	37
6.2.1.	A tanúsításhoz figyelembe vett, fejlesztői dokumentumok	37
6.2.2.	A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentum.....	37
7.	Rövidítések	38

1. Az IngridSigno Feldolgozó Modul 2.1.31 legfontosabb tulajdonságainak összefoglalása

A tanúsított termék a Pénzügyi Szervezetek Állami Felügyelete által fejlesztetett Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás

1.1. Architektúra

Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás elektronikus dokumentumok elektronikus aláírásának kezdeti és utólagos ellenőrzését támogatja.

Az ellenőrzés a Pénzügyi Szervezetek Állami Felügyelete által készített Elektronikus Aláírási Szabályzat OID: 1.3.6.1.4.1.16261.3.2.1.2.3 alapján valósul meg.

Az IngridSigno Feldolgozó Modul 2.1.31 az alábbi komponenseket valósította meg:

- Aláírói dokumentum megjelenítő
- Aláírási tulajdonság megjelenítő
- Aláírandó adat formattáló
- Ellenőrzővel kölcsönható
- Adatlenyomat készítő
- Aláírás naplózó
- Hitelesítés szolgáltatóval való kölcsönhatás összetevője

Az alkalmazás Microsoft Windows 98SE/2000/2003/XP operációs rendszeren működik. Az alkalmazás alapja a Kopint-Datorg RT által fejlesztett MultiSigno 2.2.b7 programozói könyvtár. E könyvtárban lévő objektumokon keresztül éri el az operációs rendszer Crypto API-ját.

1.2. Tulajdonságok

Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás feladata, foglalkoztatók és egyéni vállalkozók magánnyugdíj tagdíjbevallásának valamint a pénztár nyugtaüzeneteinek kezdeti és utólagos ellenőrzése. Képes a PSZÁF által közzétett adatszerkezeti leírásban meghatározott szerkezetű adatszolgáltatás fájlok és könyvtárak reprodukálására. A bevallók számára ajánlott telepítőkészlet ezt a funkciót a paraméterek között letiltja.

Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megbízható időpontként az aláírt adat objektumban található időbélyeget fogadja el. Az ellenőrzéshez megfelelő visszavonási listát szerez és csatol az aláírt adat objektumhoz. Érvénytelen esetben kijelzésre kerül a hiba oka. Amennyiben az érvényes aláírási szabályzatban meghatározott késleltetésű visszavonási lista az aláírás időpontjában nem áll rendelkezésre ezért a kezdeti ellenőrzést az alkalmazás megismételteti.

Az IngridSigno Feldolgozó Modul 2.1.31 jellemző tulajdonságai:

- RFC3275 szabvány szerinti dokumentum formátum
- Szabványos X.509 tanúsítványok kezelése (Windows tanúsítványtárban)
- Az RFC 3161 szabvány szerinti időbélyeg szolgáltatás támogatása
- Tanúsítvány érvényességi állapot teljes körű ellenőrzése.

1.3. A tanúsítás tárgya hatóköre

A tanúsítás tárgy maga az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás.

A tanúsítás során feltételeztük, hogy az alkalmazás alapjául szolgáló Windows operációs rendszer, valamint az ennek részét képező CSP modul biztonságosan és helyesen működnek. Az IngridSigno Feldolgozó Modul 2.1.31 alapvetően az alábbi komponensekre épül:

- Microsoft Crypto API
- MultiSigno 2.2.b7 programozói könyvtár

2. Az IngridSigno Feldolgozó Modul 2.1.31 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 ellenőrzésére szolgáló alkalmazásokra vonatkoznak.

Megnevezzük azokat a követelményeket, amelyek az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásra vonatkoznak.

Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelel-e az adott 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás az aláírt állírási tulajdonságok között megkeresi a tartalom formátum azonosítót. Csak akkor jeleníti az aláíró dokumentumát, ha a tartalom formátum a bevallás esetén OID: 1.3.6.1.4.1.16261.3.2.1.1.7 (Compressed XML document), egyéb aláírt objektumnál OID: 1.3.6.1.4.1.16261.3.2.1.1.1(Plain text document).

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás az aláírt állírási tulajdonságok között megkeresi a tartalom formátum azonosítót. Csak akkor jeleníti az aláíró dokumentumát, ha a tartalom formátum a bevallás esetén OID: 1.3.6.1.4.1.16261.3.2.1.1.7 (Compressed XML document), egyéb aláírt objektumnál OID: 1.3.6.1.4.1.16261.3.2.1.1.1(Plain text document).

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás az aláírt aláírási tulajdonságok között megkeresi a tartalom formátum azonosítót. Csak akkor jeleníti az aláíró dokumentumát, ha a tartalom formátum a bevallás esetén OID: 1.3.6.1.4.1.16261.3.2.1.1.7 (Compressed XML document), egyéb aláírt objektumnál OID: 1.3.6.1.4.1.16261.3.2.1.1.1 (Plain text document).

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelel a követelménynek.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás lehetőséget biztosít a következő aláírt aláírási tulajdonságok megjelenítésére: Aláírás ideje; Hivatkozás az aláírási szabályzatra; Aláírás helye; Az aláírt dokumentum tartalom formátuma, Kötelezettség vállalás típusa, Aláírói tanúsítvány, Kapcsolattartó neve, telefonszáma, e-mail címe, partner azonosító típusa, partnerazonosító.

Konklúzió: **megfelel**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionális.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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

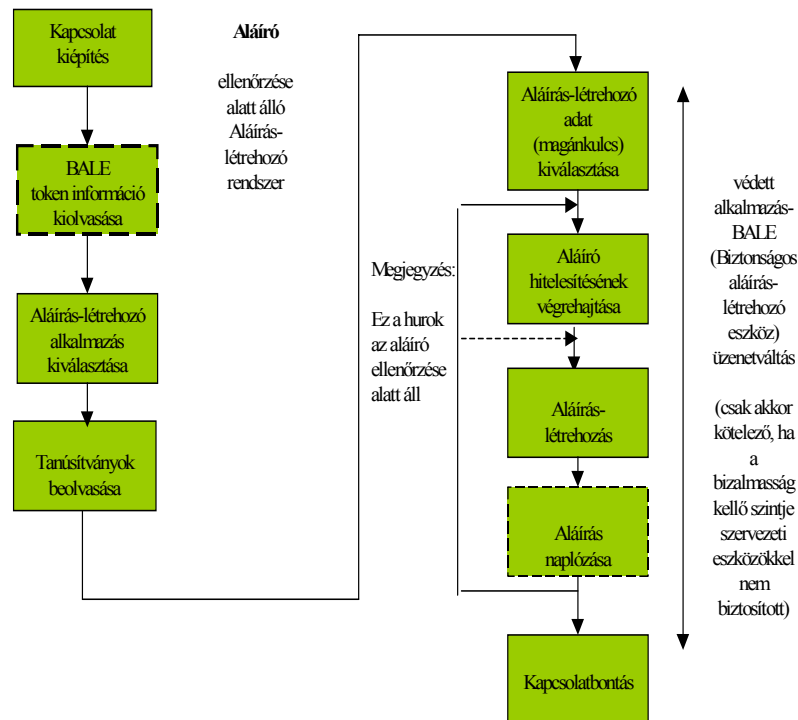
Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**



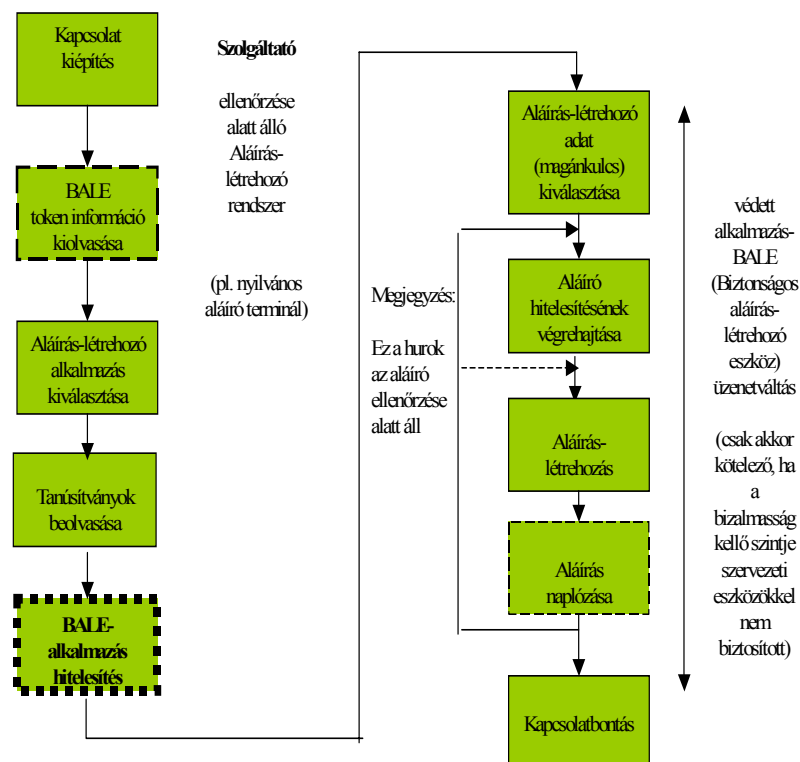
1. ábra

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

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

F_SSC_4: A biztonságos aláírás-létrehozó eszköz funkcionálitása 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

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 aláíró hitelesítő adatot az aláíró hitelesítő összetevőtől egy megbízható útvonalon keresztül, és el kell küldenie egy megfelelő parancs (utasítás) kíséretében a biztonságos aláírás-létrehozó eszköznek összehasonlításra.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

F_SSC_9: A befejezett aláírásokat naplózni kell.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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 feltételezhető-e ugyanolyan szintű bizalmasságot, mint amit a saját ellenőrzése alatt álló aláírás-létrehozó rendszer esetén elérhet.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazásnak nincs aláíró funkcionálitása.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás naplóz.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás az aláírói tanúsítványok állapotának lekérésére képes. Tanúsítványok megszerzésére nincs szükség, mivel az aláíró tanúsítványa aláírási tulajdonságként szerepel az XMLDSig 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás képes a tanúsítvány hitelességének megállapítására. Képes ellenőrizni a teljes tanúsítványláncot illetve tanúsítvány visszavonási listában való szereplését.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás az aláíró tanúsítványának érvényességének és hitelességének ellenőrzéséhez képes a megfelelő adatok (hitelesítő szolgáltató tanúsítványa, visszavonási lista) begyűjtésére.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás a kezdeti ellenőrzés folyamán minden érvényesítő adatot begyűjt és tárol az XMLDSig csomagban.

Konklúzió: **megfelel**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás a kezdeti ellenőrzés folyamán minden érvényesítő adatot begyűjt és tárol az XMLDSig csomagban.

Konklúzió: **megfelel**

Ember által történő ellenőrzés esetén:

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás támogatja a fenti elvárást.

Konklúzió: **megfelel**

F_human_2: Az aláírás-ellenőrző rendszernek interaktív eszközt kell biztosítani a felhasználó számára, hogy megnézhesse az aláírási szabályzat teljes egészét, vagy legalább az alkalmazási területre és feltételekre vonatkozó részeket.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás az elektronikus aláírási szabályzatnak megfelelően jeleníti meg az aláíró dokumentumot.

Konklúzió: **megfelel**

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

A kezdeti aláírás-ellenőrzési folyamat kimenő állapota az alábbiak egyike legyen:

- „érvényes” állapot (sikeres ellenőrzés),
- „érvénytelen” állapot (sikertelen ellenőrzés),
- „befejezetlen ellenőrzés” állapot (befejezetlen ellenőrzés)

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelel a feltételnek.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelel a feltételnek.

Konklúzió: **megfelel**

F_human_6: A felhasználói interfészekre teljesüljenek az F_principles egyszerűsége és hibamentessége vonatkozó speciális elvárásai.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazást képes az elektronikus aláírásban tárolt információk kinyerésére.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelel a feltételnek.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás szabványos formátumokat kezel. Aláírási formátumként XMLDSig, 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 biztosítani;
- 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 biztosítani 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

/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 befejezése után.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző 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 (aláíró hitelesítő adatok, aláírandó adat, formattált aláírandó adat) egyetlen olyan partner számára sem, akit az aláíró nem jogosított fel erre.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző 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 aláíró hitelesítő adatokat.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

Bizt_köv9: Minden aláíró 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző 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 beavatkozassanak olyan nem-megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

Az aláírandó adatra vonatkozó követelmények

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás, XMLDSig csomagból állapítja meg a tartalom formátumot, 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.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazást teljesíti a követelményt.

Konklúzió: **megfelel**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv23: A megjelenítő folyamatnak tájékoztatnia kell az aláírót, hogy egyéb aláírt adatok vannak beágyazva az aláírói dokumentumba (az aláíró dokumentumát megjelenítő összetevőnek kapcsolódnia kell egy aláírás ellenőrző rendszerrel az ilyen aláírások ellenőrzésére).

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás, az elektronikus aláírási szabályzatban rögzített módon jeleníti meg az aláíró dokumentumát.

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.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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.

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

A biometrikus, aláíró 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.7. Követelmények az adat lenyomat készítő összetevőre (DHC)

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv53: Amennyiben vezetékek 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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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: Az IngridSigno Feldolgozó Modul 2.1.31 , minősített elektronikus aláírás ellenőrző alkalmazás.

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 az IngridSigno Feldolgozó Modul 2.1.31 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**

1. számú feltétel: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

- *vírusok ne ronthassák el az minősített elektronikus aláírás ellenőrző 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 az IngridSigno Feldolgozó Modul 2.1.31 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**.

2. számú feltétel: *Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző 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**.

3. számú feltétel: *Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazást, valamint valamennyi aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

3. Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelelése a követelményeknek

3.1. Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
F_SIC_2	megfelel
F_SIC_3	nem vonatkozik rá a követelmény
F_DTBSF_1	nem vonatkozik rá a követelmény
F_DTBSF_2	nem vonatkozik rá a követelmény
F_DHC_1	nem vonatkozik rá a követelmény
F_DHC_2	nem vonatkozik rá a követelmény
F_SSC_1	nem vonatkozik rá a követelmény
F_SSC_2	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
F_SSC_9	nem vonatkozik rá a követelmény
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	nem vonatkozik rá a követelmény
F_SDOC_1	nem vonatkozik rá a követelmény
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	megfelel
F_human_2	megfelel
F_human_3	megfelel
F_human_4	megfelel
F_human_5	megfelel
F_human_6	megfelel
F_machine_1	megfelel
F_machine_2	megfelel
F_general_1	megfelel
F_protocol	megfelel
F_format	megfelel
F_principles	megfelel

3.2. Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	nem vonatkozik rá a követelmény
Bizt_köv2	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
Bizt_köv8	nem vonatkozik rá a követelmény
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	nem vonatkozik rá a követelmény
Bizt_köv12	nem vonatkozik rá a követelmény
Bizt_köv13	nem vonatkozik rá a követelmény
Bizt_köv14	nem vonatkozik rá a követelmény
Bizt_köv15	nem vonatkozik rá a követelmény
Bizt_köv16	nem vonatkozik rá a követelmény
Bizt_köv17	megfelel
Bizt_köv18	nem vonatkozik rá a követelmény
Bizt_köv19	megfelel
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	nem vonatkozik rá a követelmény
Bizt_köv27	nem vonatkozik rá a követelmény
Bizt_köv28	nem vonatkozik rá a követelmény
Bizt_köv29	megfelel
Bizt_köv30	nem vonatkozik rá a követelmény
Bizt_köv31	nem vonatkozik rá a követelmény
Bizt_köv32	nem vonatkozik rá a követelmény
Bizt_köv33	nem vonatkozik rá a követelmény
Bizt_köv34	megfelel
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	nem vonatkozik rá a követelmény
Bizt_köv49	nem vonatkozik rá a követelmény
Bizt_köv50	nem vonatkozik rá a követelmény

Bizt_köv51	nem vonatkozik rá a követelmény
Bizt_köv52	nem vonatkozik rá a követelmény
Bizt_köv53	nem vonatkozik rá a követelmény
Bizt_köv54	nem vonatkozik rá a követelmény
Bizt_köv55	nem vonatkozik rá a követelmény
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 az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás alkalmas OID: 1.3.6.1.4.1.16261.3.2.1.2.3 EASZ alapján készített minősített biztonságú elektronikus aláírások kezdeti és utólagos ellenőrzésére.

A feltételek nem a megvalósított minősített elektronikus aláírás ellenőrző alkalmazásra vonatkoznak, hanem annak telepítésére és környezetére

4.2. Érvényességi feltételek:

1. számú feltétel: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

- vírusok ne ronthatják el az minősített elektronikus aláírás ellenőrző alkalmazást és az általa meghívott egyéb aláíró összetevőket valamint
- az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

Érintett biztonsági követelmény: Bizt_köv57

2. számú feltétel: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva hogy behatolók elrontsák ezt.

Érintett biztonsági követelmény: Bizt_köv58

3. számú feltétel: Az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazást, valamint valamennyi 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 15408 /Common Criteria/ EAL 3-as szintjéhez hasonló volt. /Az EAL3 a fejlesztőktől független garantált biztonság közepes 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 értékelés az alábbi garanciaosztályokra terjedt ki:

- kiszállítás és működtetés
- fejlesztés
- útmutató
- tesztek

Az értékelés során, a fentiekén kívül a fejlesztőktől független minta tesztelésre, illetve áthatolás 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 14170:2001 munkacsoport egyezmény: Security Requirements for Signature Creation System

CEN/ISSS/E-Sign; Area G2 14171:2001 munkacsoport egyezmény: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign; Area V 14172-4:2001 munkacsoport egyezmény: Signature Creation Application and Procedures for Electronic Signature Verification

ETSI TS 101 733 v1.4.0 Electronic Signature Formats

RFC3039 Qualified Certificates Profile

RFC3061 Time-Stamp Protocol (TSP)

RFC3275 XML-Signature Syntax and Processing (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

6.2. A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1. A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- IngridSigno 2.1 telepítési és üzemeltetés kézikönyv 2004. szeptember 01.
- Követelményspecifikáció PSZÁF elektronikus tagdíjbevallás projekt
2004. augusztus 02.
- Rendszerterv PSZÁF elektronikus tagdíjbevallás projekt 2004. augusztus 12.
- IngridSigno 2.1 felhasználói kézikönyv 2004. október 01.
- Elektronikus Aláírási Szabályzat OID: 1.3.6.1.4.1.16261.3.2.1.2.3
- Tesztelési terv 2004. szeptember 01.
- Tesztelési tervkiegészítés 2004 szeptember 21.
- Tesztelési jegyzőkönyv 2004. szeptember 28.
- Fejlesztői nyilatkozatok (2004 november 08; 2004 november 30;
2004 december 08)

6.2.2. A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentum

- Értékelési jelentés az IngridSigno Feldolgozó Modul 2.1.24 aláíró alkalmazásról (készítette: HunGuard Kft)

7. Rövidítések

API (application programming interface)

CRL (certification revocation list) tanúsítvány visszavonási lista

CSP (cryptographic 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 certification status protocol) valós idejű tanúsítvány állapot protokoll

PKI (Public Key Infrastructure)

PIN (Personal Identification Number)

SAC (Signer's authentication component) aláíró 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