TANÚSÍTÁSI JELENTÉS

Hung-TJ-027-2005

az
NLCAPI3 v3.2.0

Kriptográfiai modulról

/NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft./

Készítette: HunGuard Kft.
2005. június 20.

1 AZ NLCAPI3 v3.2.0 legfontosabb tulajdonságainak összefoglalása

A tanúsított termék a NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft. által fejlesztett és forgalmazott NLCAPI3 v3.2.0 kriptográfiai modul, mint minősített és fokozott biztonságú elektronikus aláírás létrehozásához és ellenőrzéséhez, valamint időbélyeg kérelmezéséhez és ellenőrzéséhez alkalmazható programozói függvény könyvtár.

1.1 Architektúra

Az NLCAPI3 v3.2.0 egy programozói könyvtár, amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.
Az NLCAPI3 v3.2.0 teljes mértékben a Windows operációs rendszer Crypto API-jára támaszkodik, használatát lényegesen leegyszerűsíti. A Crypto API-n keresztül a Microsoft vagy más gyártók CSP-jét használja az aláírás-létrehozó eszköz funkcionalitásának elérésére. A lenyomatoló eljárások szintén a Crypto API függvényei. A tanúsítványlánc ellenőrzésére az OpenSSL 0.9.7d verziójának függvényeit használja.

1.2 Tulajdonságok

Az NLCAPI3 v3.2.0 kriptográfiai modul fejlesztők részére elektronikus aláírások készítésére azok ellenőrzésére, tanúsítványok, és időbélyegek kezelésére nyújt programozási felületet. Jellemző tulajdonságok:

- Használt aláírás formátumok:
  - PKCS7 (RFC2315);
  - XMLDSIG (RFC3275);
  - XADES-BES, XADES-T, XADES-C, XADES-XL, XAdES-A, többszörös XAdES-A (ETSI 101903)
  - Saját NetLock formátum (nem dokumentált)
- RFC3161 szerinti időbélyeg kezelés.
- MD5 és SHA1- lenyomatoló eljárások.
- X509 tanúsítványok és CRL-ek kezelése Windows tanúsítványtárban vagy BASE64 kódolt PEM és DER formátumban.
- Tanúsítvány érvényesítés RFC3280 alapján.
- Támogatott tanúsítvány kiterjesztések:
  - Key Usage
  - Basic Constraints
  - CRL Distribution Points
  - Qualified Certificate Statement (ETSI TS 101 862)

1.3 A tanúsítás tárgya és hatóköre

Jelen tanúsítás tárgya az NLCAPI3 v3.2.0 kriptográfiai modul.
A tanúsítás során feltételezzük, hogy az NLCAPI3 v3.2.0 kriptográfiai modul alapját képező Windows operációs rendszer, és annak részét képező CSP modul biztonságosan és helyesen működnek. Az NLCAPI3 v3.2.0 alapvetően a következő operációs rendszer komponensre épül:

- Microsoft Crypto API
- OpenSSL

2 Az NLCAPI3 v3.2.0 megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS CWA 14170:2004 és CEN/ISSS CWA 14171:2004 követelményrendszerekből fakadó) funkcionális és biztonsági követelményeket, melyek minősített elektronikus aláírások létrehozására és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.
Megnevezzük azokat a követelményeket, amelyek a NLCAPI3 v3.2.0 programozói könyvtárra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy az NLCAPI3 v3.2.0 programozói könyvtár megfelel-e az adott követelménynek.

2.1 Funkcionális követelmények fokozott biztonságú és minősített elektronikus aláírásokat létrehozó alkalmazások számára

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul tartalmaz elektronikus aláírás ellenőrzéshez függvényeket, tehát készíthető vele olyan aláíró alkalmazás, amely az aláírást ellenőrzi.

Konklúzió: **megfelel**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XADES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust. Az adat tartalom típus mime-type-ként adható meg az aláíró függvényeknek.

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 NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XADES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust. Az adat tartalom típus mime-type-ként adható meg az aláíró függvényeknek.

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 NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XADES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust. Az adat tartalom típus mime-type-ként adható meg az aláíró függvényeknek.

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 NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XADES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust és az aláíró tanúsítványát. A tanúsítvány megjelenítéséhez megfelelő függvényeket nyújt. Az aláírt adat típusát az alkalmazás készítőjének kell helyesen kezelnie.

Konklúzió: **megfelel**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a tanúsítvány megjelenítéséhez megfelelő függvényeket nyújt.

Konklúzió: **megfelel**

F_SAV_3*: Az aláíró alkalmazásnak le kell ellenőrizni az aláíró tanúsítványának az érvényességét az aláírás előtt.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláíró tanúsítvány érvényességének, hitelességének ellenőrzéséhez megfelelő függvényeket nyújt.

Konklúzió: **megfelel**

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

Magyarázat: Interaktív felületet követel, az NLCAPI3 v3.2.0 kriptográfiai modul fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

* Új funkcionális követelmény

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

Magyarázat: Interaktív felületet követel, az NLCAPI3 v3.2.0 kriptográfiai modul fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A XAdES-es illetőleg a PKCS7-es csomagot az NLCAPI3 v3.2.0 kriptográfiai modul megfelelően összeállítja.

Konklúzió: **megfelel**

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

Magyarázat Az NLCAPI3 v3.2.0 kriptográfiai modul elvégzi a lenyomatolást.

Konklúzió: **megfelel**

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

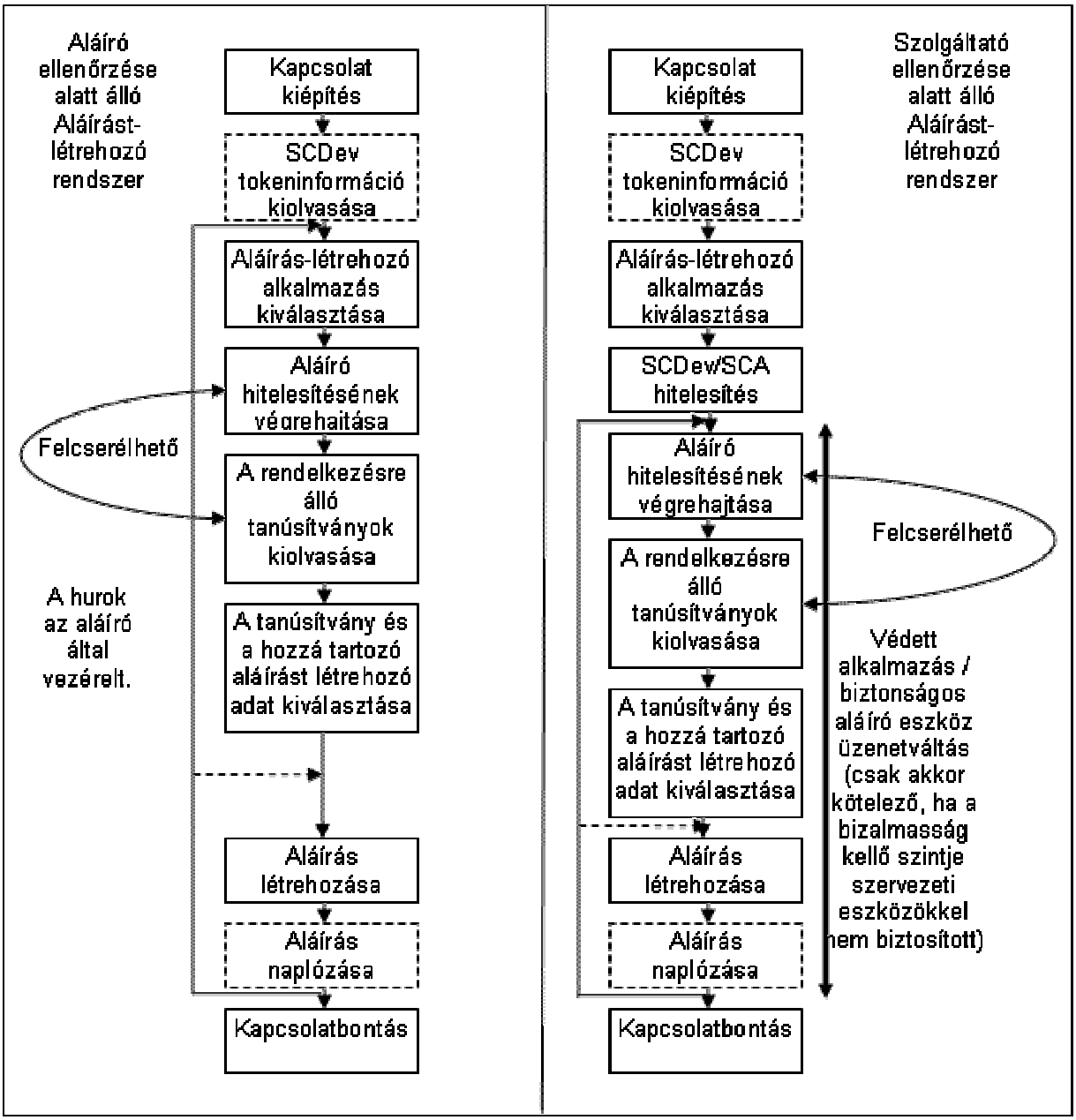
Magyarázat Az NLCAPI3 v3.2.0 kriptográfiai modul megfelelően felhívja a Microsoft Windows CryptoAPI lenyomatoló függvényét .

Konklúzió: **megfelel**

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

Magyarázat Az NLCAPI3 v3.2.0 kriptográfiai modul megfelelően felhívja a Microsoft Windows CryptoAPI aláíró függvényét, ami elvégzi a feltöltést.

Konklúzió: **megfelel**



3. ábra: Megvalósítandó együttműködési sorozat az aláírás-létrehozó rendszer és az aláírás-létrehozó eszköz között

F_SSC_1: Egy aláíró ellenőrzése alatti aláírás-létrehozó rendszer és az aláírás-létrehozó eszköz között végre kell hajtani a 3. ábrán jelölt minden szükséges kommunikációt.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

F_SSC_2: Egy szolgáltató ellenőrzése alatti aláírás-létrehozó rendszer és az aláírás-létrehozó eszköz között végre kell hajtani a 3. ábrán jelölt minden szükséges kommunikációt.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

F_SSC_4: Az aláírás-létrehozó eszköz funkcionalitása megvalósítható egy olyan platformon (pl. intelligens kártya), amely egy vagy több aláírás-létrehozó eszköz funkciót (amelyeket gyakran 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 NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul nem ellenőrzi a környezetét. Ez nem is feladata. A környezet biztonságát az operációs rendszerrel kell megteremteni.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul paraméterkén kapja meg, hogy mely dokumentumot írja alá.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A biztonságos aláírás-létrehozó eszköz kimeneti adatát az NLCAPI3 v3.2.0 kriptográfiai modul XAdES illetőleg PKCS7 csomagba helyesen rakja be.

Konklúzió: **megfelel**

F_I/O-1: Ha aláírás-létrehozásnál az 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 NLCAPI3 v3.2.0 kriptográfiai modul a Windows tanúsítványtárát használja a tanúsítványok eléréséhez. Itt a teljes tanúsítvány megtalálható.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláíró tanúsítvány érvényességének, hitelességének ellenőrzéséhez megfelelő függvényeket nyújt.

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 NLCAPI3 v3.2.0 kriptográfiai modul biztosítja a fenti elvárást.

Konklúzió: **megfelel**

2.2 Funkcionális követelmények fokozott biztonságú és minősített elektronikus aláírásokat ellenőrző alkalmazások számára

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul nem egy konkrét aláírási szabályzatra készült. A fejlesztő készlettel különböző aláírási szabályzatok kielégíthetők.

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 NLCAPI3 v3.2.0 kriptográfiai modul XAdES aláírási formátumot képes kibővíteni a teljes körű érvényességi adatokkal

Konklúzió: **megfelel**

F_ISV_3[*] A kezdeti ellenőrzés során a CWA 14171:2004 5.7 pontban felsorolt szabályokat be kell tartani.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul támogatja az ETSI TS 101 862 (Qualified Certificate Profile) dokumentumban specifikált `Qualified Certificate Statement` *mezőt. A tanúsítványlánc érvényességének ellenőrzéséhez az RFC 3280 dokumentum 6. fejezetében leírt algoritmust használja. Az időbélyeget az RFC 3161 szerint kezeli.*

Konklúzió: **feltétellel megfelel**

1. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a CRL-t más tanúsítvánnyal ellenőrzik, mint a végfelhasználó tanúsítványokat. Ezért csak olyan környezetben szabad alkalmazni, amelyben önkibocsátott (self issued) tanúsítvány a tanúsítványláncban nem fordul elő, valamint amelyben a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni.*

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul nem egy konkrét aláírási szabályzatra készült. A fejlesztő készlettel különböző aláírási szabályzatok kielégíthetők. Utólagos ellenőrzésre a XAdES kiterjesztett aláírási formátumok alkalmasak.

Konklúzió: **megfelel**

[*] Új funkcionális követelmény

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: Az NLCAPI3 v3.2.0 kriptográfiai modul közvetlenül nem tud kommunikálni a felhasználóval, de eszközt biztosít az aláírások ellenőrzésére.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul közvetlenül nem tud kommunikálni a felhasználóval, de eszközt biztosít az aláírások ellenőrzésére.

Konklúzió: **nem vonatkozik rá a követelmény**

F_human_3: A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az “Ami megjelenik, azt írták alá.” követelményt. Ha valamilyen okból az aláírói dokumentum nem jeleníthető meg pontosan a megfelelő módon, akkor ezt a felhasználói interfésznek világosan jeleznie kell.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul közvetlenül nem tud kommunikálni a felhasználóval, de eszközt biztosít az aláírások ellenőrzésére.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul közvetlenül nem tud kommunikálni a felhasználóval, de eszközt biztosít az aláírások ellenőrzésére, és megjelenítésére.

Konklúzió: **megfelel**

F_human_5: „Befejezetlen ellenőrzés” állapot esetén az aláírás-ellenőrző alkalmazásnak javasolnia kell a felhasználó számára, hogy szerezze be azt az információt, ami az aláírást érvényessé teszi hosszú távra.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

F_human_7: 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 NLCAPI3 v3.2.0 kriptográfiai modul hiba vagy hiányosság esetén többféle hibaüzenetet ad vissza. Ezekből, a hibaüzenetekből a fejlesztő készletet használó aláíró alkalmazás képes kikeverni a felsorolt állapotokat.

Konklúzió: **megfelel**

Gépi (automatikus) ellenőrzés esetén:

Az automatizált feldolgozás esetében alkalmazói program interfészek (API-k) használhatók. Bár az ilyen interfészek kialakításának többféle módja van, ezeket két csoportba lehet sorolni:
az 1-es típusú API-k arra szolgálnak, hogy az elektronikus aláírásban tárolt adatokat kigyűjtsék.
A 2-es típusú API-k az elektronikus aláírás ellenőrzésére és az érvényesítő adatok beszerzésére szolgálnak.

F_machine_1: Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére és az elektronikus aláírás formátumának meghatározására.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul önmagában nem képes automatikusan ellenőrizni az aláírt adat objektumot, de az abban tárolt adatokat képes visszaadni a fejlesztő készletet használó aláíró alkalmazás számára.

Konklúzió: **megfelel**

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

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul nem képes automatikusan ellenőrizni az aláírt adat objektumot, de meg vannak valósítva az aláírás ellenőrző függvények és az érvényesítő adatlekérő függvények.

Konklúzió: **megfelel**

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

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

2.3 Funkcionális követelmények fokozott biztonságú és minősített elektronikus aláírásokat létrehozó és ellenőrző alkalmazások számára

F_protocol: Az aláírás-létrehozó 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 NLCAPI3 v3.2.0 kriptográfiai modul szabványos protokollokat használ.

Konklúzió: **megfelel**

F_format: Az aláírás-létrehozó alkalmazásnak képesnek kell lennie szabványos formátumok kezelésére az alábbi területeken:

- szabványos aláírási formátumok;
- szabványos tanúsítvány formátumok.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul szabványos formátumokat használ. Aláírási formátumként XAdES vagy PKCS7, tanúsítvány formátumként X509v3.

Konklúzió: **megfelel**

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

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

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

- félreérthetetlen felhasználói útmutatót kell szolgáltatnia arra nézve, hogy hogyan kell a rendszert installálni, konfigurálni és használni;
- ön-leírónak kell lennie abban az értelemben, hogy minden párbeszéd-lépésnek azonnal érthetőnek kell lennie vagy a

rendszertől kapott visszajelzéseken keresztül, vagy úgy, hogy az ellenőrző kérésére a rendszer magyarázatot ad;

- meg kell felelnie a felhasználók szokásos elvárásainak, azaz tudásuknak, képzettségüknek, tapasztalatuknak és az általánosan elfogadott konvencióknak;
- adaptálhatónak kell lennie, azaz támogatnia kell a felhasználók egyéni igényeit és preferenciáit;
- hibatűrőnek kell lennie úgy, hogy a nyilvánvaló input hibák ellenére az eredményt el lehessen érni minimális javításokkal.
- tájékoztató hiba üzeneteket kell küldenie, a felhasználó továbbhaladása érdekében;
- visszajelzéseket kell szolgáltatnia, mely megerősíti a felhasználó által végrehajtott tevékenység helyességét (vagy helytelenségét);
- a hibaüzenetek legyenek kellően informatívak, adjanak eligazítást a hiba okáról, a szükséges teendőkről (pl. a “Hibakód: 213” hibaüzenet nem igazán segítőkész);
- szabatos és minden részletre kiterjedő terminológia helyett hétköznapi kifejezéseket kell használni (a technikai kifejezéseket ugyanis a legtöbb felhasználó nem érti, és nem is kell értenie);
- alkalmaznia kell a színek használatára vonatkozó konvenciókat (pl. piros = hiba, zöld = továbbhaladás/siker);
- minden időpontban képesnek kell lennie arra, hogy az éppen végrehajtás alatt álló műveletet félbeszakítsa és vagy visszatérjen a főmenübe, vagy teljesen kilépjen a rendszerből;
- a felhasználói egyének számára biztosítania kell a magántitok jelleget (pl. azáltal, hogy az információkat nem teszi mások számára hozzáférhetővé a felhasználói interfészen keresztül).
- A műveletek helyes időzítésével elegendő időt kell biztosítani minden felhasználónak a folyamatok befejezéséhez (figyelembe véve azt a tényt is, hogy az emberek olvasási és reagálási és reagálási képességei különbözők).

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

2.4 Biztonsági követelmények fokozott biztonságú és minősített elektronikus aláírásokat létrehozó alkalmazások számára

2.4.1 Követelmények az aláírás-létrehozó alkalmazás (SCA) egészére

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

A következő két követelmény csak minősített elektronikus aláírás létrehozásánál (biztonságos aláírás-létrehozó eszköz használata esetén) kötelező.

S_SCA_1 (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 NLCAPI3 v3.2.0 kriptográfiai modul teljesíti a követelményt.

Konklúzió: **megfelelt**

S_SCA_2 (Bizt_köv2): Az aláírás-létrehozó alkalmazásnak meg kell őriznie az aláírandó adat komponensek, a formattált aláírandó adat és az aláírót hitelesítő adatok bizalmasságát.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul teljesíti a követelményt.

Konklúzió: **megfelelt**

Nyilvános aláírás-létrehozó alkalmazásokra vonatkozó követelmények

A következő két követelmény csak nyilvános aláírás-létrehozó alkalmazásokra vonatkozik.

S_SCA_3 (Bizt_köv3): Az aláírás-létrehozó alkalmazásnak biztonságosan törölnie kell az aláíráshoz kapcsolódó összes adatot az aláírási folyamat befejeződése után.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul teljesíti a követelményt.

Konklúzió: **megfelelt**

[*] Az értékelések összehasonlíthatóságának fenntartása érdekében a követelmények régi címkéjét zárójelben jelezzük.

S_SCA_4 (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: Az NLCAPI3 v3.2.0 kriptográfiai modul teljesíti a követelményt.

Konklúzió: **megfelelt**

Az aláírandó adat és az aláírási tulajdonságok helyességének követelményei

S_SCA_5 (Bizt_köv7): Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy az aláírónak bemutatott aláírandó adat ugyanaz, mint amit az aláíró kiválasztott.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SCA_6 (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: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

S_SCA_7 (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: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SCA_8 (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: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

A nem megbízható folyamatokból és kommunikációs portokból adódó követelmény

S_SCA_9 (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: Az NLCAPI3 v3.2.0 kriptográfiai modul, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek kell biztosítani

Konklúzió: **feltétellel megfelel**

2. számú feltétel *Az NLCAPI3 v3.2.0 kriptográfiai modullal fejlesztett 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

S_SCA_10 (Bizt_köv12): Az aláírandó adatnak tartalmaznia kell egy aláírói dokumentumot. (Egy “üres” dokumentumhoz ne lehessen aláírást előállítani).

Megjegyzés: Az NLCAPI3 v3.2.0 kriptográfiai modullal 0 hosszú fájlt nem lehet alá írni.

Konklúzió: **megfelel**

S_SCA_11 (Bizt_köv13): Az aláírandó adatnak tartalmaznia kell az aláírónak azt a tanúsítványát (vagy az arra vonatkozó hivatkozást és a tanúsítvány lenyomat értékét), amely az elektronikus aláírás létrehozásánál a biztonságos aláírás-létrehozó eszköz által felhasznált aláírás-létrehozó adathoz kapcsolódik, s amely az aláíró szándékának megfelel.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XAdES formátum esetén, aláírt aláírási tulajdonságként eltárolja aláíró tanúsítványát.

Konklúzió: **megfelel**

S_SCA_12 (Bizt_köv16):Az aláírandó adatnak tartalmaznia kell az aláírói dokumentum adat tartalom típusát, ha az más módon nem meghatározott.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XAdES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust.

Konklúzió: **megfelel**

2.4.2 Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP)

A tartalom formátumra vonatkozó követelmények:

S_SDP_1 (Bizt_köv17): Az aláíró dokumentumát megjelenítő összetevőnek lehetővé kell tennie az aláírói dokumentum adat tartalom típusának csatolását vagy közvetett módon az aláírási szabályzat részeként, vagy pedig egy közvetlen aláírás tulajdonságként.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XAdES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust.

Konklúzió: **megfelel**

S_SDP_2 (Bizt_köv18): Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha a dokumentum nem felel meg az adat tartalom típussal meghatározott szintaxisnak, és lehetővé kell tennie az aláíró számára, hogy félbeszakítsa az aláírási folyamatot.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_3 (Bizt_köv19): A használati útmutatóban jelezni kell, hogy milyen adat tartalom típusok helyes kezelésére alkalmas az aláíró dokumentumát megjelenítő összetevő.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_4 (Bizt_köv20): A használati útmutatóban jelezni kell, hogy milyen lehetséges következménnyel jár, ha az aláíró tévesen választja ki az adat tartalom típust.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_5 (Bizt_köv21): Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha olyan aláírói dokumentumot kíván aláírni, amelynek adat tartalom típusát nem támogatja.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_6 (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: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_7 (Bizt_köv23): A megjelenítő folyamatnak tájékoztatnia kell az aláírót, hogy egyéb aláírt adatok vannak beágyazva az aláírói dokumentumba (az aláíró dokumentumát megjelenítő összetevő opcionálisan kapcsolódhat egy aláírás ellenőrző rendszerrel az ilyen aláírások ellenőrzésére).

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_8 (Bizt_köv24): Az aláíró dokumentumát megjelenítő összetevőnek nem szabad lehetővé tennie az aláíró számára, hogy az aláírói dokumentum bármely részét megváltoztassa.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SDP_9 (Bizt_köv25): Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha nem képes az aláírói dokumentum minden részének a helyes adat tartalom típusnak megfelelő megjelenítésére.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

Az aláíró dokumentumára vonatkozó egyértelműségi követelmény:

S_SDP_10 (Bizt_köv26): Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy adat tartalom típus 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 NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XAdES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust. Az adat tartalom típus mime-type-ként adható meg az aláíró függvényeknek.

Konklúzió: **megfelel**

A nem megjelenítés-érzékeny aláírói dokumentumokra vonatkozó követelmény:

S_SDP_11 (Bizt_köv27): Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy adat tartalom típus tulajdonság csatolását az aláírandó adatokhoz annak biztosítására, hogy az aláíró dokumentum szemantikáját csak egyféleképpen lehessen értelmezni.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XAdES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust. Az adat tartalom típus mime-type-ként adható meg az aláíró függvényeknek.

Konklúzió: **megfelel**

A rejtett szövegre és aktív kódra vonatkozó követelmény:

S_SDP_12 (Bizt_köv28): Amennyiben az aláíró dokumentumát megjelenítő összetevő nem csak egy statikus dokumentum formátum aláírását teszi lehetővé:

- az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót a rejtett kódok jelenlétére,
- egy olyan aláírói dokumentum megjelenítőnek kell elérhetőnek lennie, mely függetlenül a forrás megbízhatóságától, figyelmeztet azokra a rejtett kódok által végrehajtott módosulásokra, amelyek az aláíró dokumentumán aláírás után keletkeztek.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

2.4.3 Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV)

S_SAV_1 (Bizt_köv29): Az aláírás tulajdonság megjelenítési folyamatának lehetővé kell tennie az aláíró számára az aláírás tulajdonságok megtekintését.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláírt adat objektumban PKCS7 és XAdES formátum esetén, aláírt aláírási tulajdonságként eltárolja az adat tartalom típust és az aláíró tanúsítványát. A tanúsítvány megjelenítéséhez megfelelő függvényeket nyújt. Az aláírt adat típusát az alkalmazás készítőjének kell helyesen kezelnie.

Konklúzió: **megfelel**

S_SAV_2 (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: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAV_3 (Bizt_köv31): Az aláírás tulajdonságok sértetlenségét és hitelességét meg kell védeni.

Megjegyzés: Az NLCAPI3 v3.2.0 kriptográfiai modullal készített aláírt adat objektumban az aláírt aláírási tulajdonságokat maga az aláírás védi, a nem aláírt aláírási tulajdonságok önmagukat védik.

Konklúzió: **megfelel**

S_SAV_4 (Bizt_köv32): Az aláírót figyelmeztetni kell az aláírás tulajdonságokban jelenlévő bármilyen rejtett szövegről, makróról vagy aktív kódról.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAV_5 (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.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAV_6[*]: Az aláírás tulajdonság megjelenítő folyamatnak, függetlenül a forrás megbízhatóságától, figyelmeztetni kell azokra a rejtett kódok által a tulajdonságokon végrehajtott módosulásokra, amelyek az aláíró dokumentumán aláírás után keletkeztek.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

[*] Új biztonsági követelmény

S_SAV_7*: Az aláírás-létrehozó alkalmazásnak ellenőrizni kell az aláíró tanúsítvány érvényességi idejét és visszavonási állapotát, a megfelelő tanúsítvány állapot információk elérésével. Amennyiben az aláíró tanúsítványa az aláírás időpontjában nem érvényes, akkor meg kell tagadni a tanúsítványhoz tartozó aláírást létrehozó adat felhasználását.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul az aláíró tanúsítvány érvényességének, hitelességének ellenőrzéséhez megfelelő függvényeket nyújt.

Konklúzió: **megfelel**

S_SAV_8 (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 NLCAPI3 v3.2.0 kriptográfiai modul a tanúsítvány megjelenítéséhez megfelelő függvényeket nyújt.

Konklúzió: **megfelel**

2.4.4 Követelmények az aláíróval kölcsönható összetevőre (SIC)

Az aláírás kiváltására vonatkozó követelmények

S_SIC_1 (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: Interaktív felületet követel, az NLCAPI3 v3.2.0 kriptográfiai modul fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

Az inaktivitási időkorlátra vonatkozó biztonsági követelmények

S_SIC_2 (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 NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SIC_3 (Bizt_köv37): Ha az időkorlát letelik, az aláírót újra kell hitelesíteni.

Magyarázat: Interaktív felületet követel, az NLCAPI3 v3.2.0 kriptográfiai modul fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

* Új biztonsági követelmény

S_SIC_4*: Az aláíróval kölcsönható összetevőnek olyan egyértelmű, az alkalmazás által megvalósítható utasításokat kell adni az aláírónak, amelyek megakadályozzák a rossz használatot és kivédik az ebből eredő veszélyeket.

Magyarázat: Interaktív felületet követel, az NLCAPI3 v3.2.0 kriptográfiai modul fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SIC_5*: A megjelenítő képernyőn törölni kell az aláíró személyes adatait egy olyan időtartam leteltével, mely a normál működéshez elég. Az aláírói adatok helyét más „semleges" adatokkal felül kell írni az eredeti adatok kiolvasásának megakadályozása érdekében.

Magyarázat: Interaktív felületet követel, az NLCAPI3 v3.2.0 kriptográfiai modul fölé írt alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

2.4.5 Követelmények az aláírót hitelesítő összetevőre (SAC)

A tudáson alapuló aláírót hitelesítő adatokra vonatkozó követelmények

S_SAC_1 (Bizt_köv38): Az aláírás-létrehozó alkalmazásnak eszközt kell biztosítania a felhasználó számára ahhoz, hogy az megadhassa az aláírót hitelesítő adatot ezen keresztül az aláírás-létrehozó eszköz számára.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_2 (Bizt_köv39): Amennyiben a hitelesítő adatokat az aláírás létrehozó alkalmazáson belül kezelik, az aláírás-létrehozó alkalmazásnak meg kell őriznie az aláírót hitelesítő adatok bizalmasságát, és biztonságosan törölnie kell azokat, amint azokra nincs már szükség.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_3 (Bizt_köv40): Ha az aláírni szándékozó korlátozott számban helytelen hitelesítő adatot ad meg, akkor egy hibajelzést kell adni az aláíró részére, és ismételt hitelesítést kell engedélyezni kivéve akkor ha az aláíró hitelesítési módszer nem blokkolta korábban az aláírást-létrehozó eszközt. Az aláírni szándékozó részére egy megfelelő üzenetet kell küldeni. A hiba típusáról tilos információt adni.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

* Új biztonsági követelmény

S_SAC_4[*]: Bár a biztonsági ellenintézkedéseket az aláírás-létrehozó eszköznek kell megvalósítania, de az aláírást-létrehozó alkalmazás nem akadályozhatja meg a PIN/jelszó eszköz általi kezelését. Ennek megfelelően:

- biztosítani kell az aláíró eszköz által támogatott PIN vagy jelszó teljes hosszának alkalmazhatóságát,
- nem szabad megakadályozni az aláírót abban, hogy szándékosan módosíthassa saját PIN-jét/jelszavát.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_5[**] (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 NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_6 (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: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_7 (Bizt_köv44): A megadott PIN kódot vagy jelszót nem szabad kijelezni, bár egy számjegy vagy karakter begépelését vissza kell jelezni egy megfelelő jellel, amely nem fedi fel magát a PIN-t vagy a jelszót.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_8 (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 az aláírás-létrehozó eszköznek.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

[*] Új biztonsági követelmény
[**] Ez a követelmény csak minősített aláírás esetén kötelező.

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

S_SAC_9 (Bizt_köv46): Megbízható útvonalat kell biztosítani a biometrikus adatok továbbítására a biometrikus érzékelő egység és a biztonságos aláírás-létrehozó eszköz közé.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_10 (Bizt_köv47): A biometrikus érzékelőknek biztosítaniuk kell a felhasználó biometrikus adatainak védelmét visszajátszásos támadások elkerülésére.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_11*: A felhasználó és a biometrikus adat összerendelését, az aláírást létrehozó alkalmazáson kívül kell megvalósítani.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SAC_12*: A biometrikus adat ellenőrzését, az aláírást létrehozó alkalmazáson kívül kell megvalósítani.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

2.4.6 Követelmények az aláírandó adat formattáló összetevőre (DTBSF)

S_DTBSF_1 (Bizt_köv48): Az aláírás-létrehozó alkalmazásnak annak érdekében, hogy az aláíró által kiválasztott helyes aláírandó adat formátum keletkezzen, ellenőrizni kell valamennyi rendelkezésre álló adat érvényességét, hitelességét és teljességét.

Magyarázat: A XAdES-es illetőleg a PKCS7-es csomagot az NLCAPI3 v3.2.0 kriptográfiai modul megfelelően összeállítja.

Konklúzió: **megfelel**

* Új biztonsági követelmény

2.4.7 Követelmények az adat lenyomat készítő összetevőre (DHC)

S_DHC_1 (Bizt_köv49): Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy csak az ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures dokumentumban specifikált lenyomatoló algoritmust használ lenyomatolásra.

Magyarázat Az NLCAPI3 v3.2.0 kriptográfiai modul MD5 és SHA-1 lenyomattoló algoritmusokat ismer és használ..

Konklúzió: **feltétellel megfelel**

3. számú feltétel: *Fokozott vagy minősített elektronikus aláírások létrehozásánál az MD5 lenyomatoló algoritmus nem használható.*

S_DHC_2 (Bizt_köv50): Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy csak az ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures dokumentumban specifikált input formátumot (feltöltési módszer) használ.

Magyarázat Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Windows CryptoAPI függvényein keresztül pkcs1-v1_5 feltöltési módszert használ.

Konklúzió: **megfelel**

S_DHC_3 (Bizt_köv51): Az aláírás-létrehozó alkalmazásnak biztosítania kell a helyes aláírandó adat reprezentáns előállítását az elektronikus aláíráshoz.

Magyarázat Az NLCAPI3 v3.2.0 kriptográfiai modul megfelelően felhívja a Microsoft Windows CryptoAPI lenyomatoló függvényét .

Konklúzió: **megfelel**

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

S_SSC_1 (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 aláírás-létrehozó eszköz típusok megfelelő működésének biztosítása érdekében.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SSC_2 (Bizt_köv53): Amennyiben vezeték nélküli vagy más „sugárzó” összeköttetést használnak az aláírás-létrehozó alkalmazás és az aláírás-létrehozó eszköz között, az SSC komponensnek megfelelő eszközöket kell biztosítania a lehallgatás és a zavarás megakadályozása érdekében.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SSC_3 (Bizt_köv54): Az SSC összetevőnek biztosítania kell az aláírás-létrehozó eszköz helyes funkcionalitásának kiválasztását, amennyiben az 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 az aláírás-létrehozó eszközön tárolva.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

S_SSC_4 (Bizt_köv55): Az SSC-t védeni kell a jogosulatlan módosításokkal szemben.

Magyarázat: Az NLCAPI3 v3.2.0 kriptográfiai modul a Microsoft Crypto API-jára támaszkodik. Az aláírás-létrehozó eszközzel való kommunikáció a Crypto API feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

2.4.9 Követelmény az SCDev/SCA hitelesítő összetevőre (SSA)

Az alábbi követelménynek csak azoknál a szolgáltató ellenőrzése alatt álló alkalmazásoknál kell megfelelni, ahol a bizalom szükséges szintje szervezeti eszközökkel nem biztosított.

S_SSA_1 (Bizt_köv56: Nyilvános környezetben az SCA-nak támogatnia kell az aláírás-létrehozó alkalmazás és az 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 NLCAPI3 v3.2.0 kriptográfiai modulnak nem feladata az aláírás-létrehozó alkalmazás és az aláírás-létrehozó eszköz között az entitások hitelesítését biztosítani.

Konklúzió: **nem vonatkozik rá a követelmény**

2.4.10 Követelmény az aláíró dokumentumát szerkesztőre (SDC)

S_SDC_1[*]: Az aláíró dokumentumát szerkesztő összetevő tiltsa rejtett kódok hozzáadását az aláíró dokumentumához.

Magyarázat: Ez az NLCAPI3 v3.2.0 kriptográfiai modul használó aláíró alkalmazás feladata.

Konklúzió: **nem vonatkozik rá a követelmény**

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

S_I/O_1 (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 NLCAPI3 v3.2.0 kriptográfiai modul szoftver alkalmazás, önállóan nem képes megvédenie sem saját, sem egyes moduljainak integritását. Rendelkezik ugyan aláírással, de nem lehet feladata a kommunikációs összetevő módosítással szembeni védelme. Ezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítani.

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

4. számú feltétel: *Bár az NLCAPI3 v3.2.0 kriptográfiai modul rendelkezik önvédelmi funkcióval, 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.*

S_I/O_2 (Bizt_köv58): Az SCA-nak védenie kell funkcionális összetevőinek sértetlenségét, és meg kell akadályozni, hogy behatolók elrontsák ezeket.

Magyarázat: Lévén az NLCAPI3 v3.2.0 kriptográfiai modul szoftver alkalmazás, önállóan nem képes megvédenie sem saját, sem egyes moduljainak integritását. Ezért nem lehet feladata a kommunikációs összetevő módosítással szembeni védelme. Ezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítani.

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

5. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az NLCAPI3 v3.2.0 kriptográfiai modul funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

[*] Új biztonsági követelmény

S_I/O_3 (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 NLCAPI3 v3.2.0 kriptográfiai modul nincs importált komponens.

Konklúzió: **nem vonatkozik rá a követelmény**

2.5 Biztonsági követelmények fokozott biztonságú és minősített elektronikus aláírásokat ellenőrző alkalmazások számára

S_VER_1 (Bizt_köv60) Az aláírás-ellenőrzés folyamattal kölcsönhatásba lépő összes összetevőt egy biztonságos területen kell megvalósítani.

Biztonságos területet (azaz egy olyan területet, melyen belül speciális ellenintézkedésekkel védekeznek a feldolgozott és tárolt adatok, illetve a folyamatok sikeres manipulálása ellen) technikailag (tehát nem adminisztratív, vagy egyéb nem-technikai módszerekkel) az alábbi három különböző módon lehet megvalósítani:

- Egy szoftver modulban, melyben a biztonsági ellenintézkedések szoftverben vannak megvalósítva. Az így elérhető biztonság a működtető környezet biztonságától függ. Az adatok és folyamatok szoftver úton megvalósított biztonsági intézkedésekkel történő védelmének elégségessége erősen vitatott a szakértők között, különösen egy standard operációs rendszerű PC-ben.

- Egy módosítást-jelző modulban, ahol a biztonsági ellenintézkedéseket olyan módon valósítják meg, hogy a manipuláció ugyan nem akadályozható meg, de a felhasználó észlelheti azt. Ez azt jelenti, hogy a felhasználó védve van a biztonságos területen manipulált komponensek véletlen használatától. Egy standard operációs rendszerű PC-ben a módosítást észlelő modul megvalósítása jelenleg csak kiegészítő hardver alkalmazásával oldható meg. (Megjegyezzük, hogy ez a modul nem a biztonságos aláírás-létrehozó eszköz, hanem az azt felhívó eszköz.)

- Egy módosításnak ellenálló modulban, ahol a biztonsági ellenintézkedéseket olyan módon valósítják meg, hogy a manipuláció reális erőfeszítésekkel nem megvalósítható. /A manipuláláshoz szükséges erőfeszítéseknek arányban kell állnia az általa elérhető előnyökkel./ A módosításnak ellenálló modulok jelenleg csak speciális hardver felhasználásával valósíthatók meg.

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**.

6. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az NLCAPI3 v3.2.0 kriptográfiai modul, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

3 Az NLCAPI3 v3.2.0 kriptográfiai modul megfelelése a követelményeknek.

3.1 Az NLCAPI3 v3.2.0 kriptográfiai modul 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_SAV_3	megfelel
F_SIC_1	nem vonatkozik rá a követelmény
F_SIC_2	nem vonatkozik rá a követelmény
F_SIC_3	nem vonatkozik rá a követelmény
F_DTBSF_1	megfelel
F_DTBSF_2	megfelel
F_DHC_1	megfelel
F_DHC_2	megfelel
F_SSC_1	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_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	nem vonatkozik rá a követelmény
F_SDOC_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_ISV-3	feltétellel megfelel
F_USV-1	megfelel
F_human_1	nem vonatkozik rá a követelmény
F_human_2	nem vonatkozik rá a követelmény
F_human_3	nem vonatkozik rá a követelmény
F_human_4	megfelel
F_human_5	nem vonatkozik rá a követelmény
F_human_6	nem vonatkozik rá a követelmény
F_human_7	megfelel
F_machine_1	megfelel
F_machine_2	megfelel
F_general_1	nem vonatkozik rá a követelmény
F_protocol	megfelel
F_format	megfelel
F_principles	nem vonatkozik rá a követelmény

3.2 A NLCAPI3 v3.2.0 kriptográfiai modul megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
S_SCA_1	megfelel
S_SCA_2	megfelel
S_SCA_3	megfelel
S_SCA_4	megfelel
S_SCA_5	nem vonatkozik rá a követelmény
S_SCA_6	nem vonatkozik rá a követelmény
S_SCA_7	nem vonatkozik rá a követelmény
S_SCA_8	nem vonatkozik rá a követelmény
S_SCA_9	feltétellel megfelel
S_SCA_10	megfelel
S_SCA_11	megfelel
S_SCA_12	megfelel
S_SDP_1	megfelel
S_SDP_2	nem vonatkozik rá a követelmény
S_SDP_3	nem vonatkozik rá a követelmény
S_SDP_4	nem vonatkozik rá a követelmény
S_SDP_5	nem vonatkozik rá a követelmény
S_SDP_6	nem vonatkozik rá a követelmény
S_SDP_7	nem vonatkozik rá a követelmény
S_SDP_8	nem vonatkozik rá a követelmény
S_SDP_9	nem vonatkozik rá a követelmény
S_SDP_10	megfelel
S_SDP_11	megfelel
S_SDP_12	nem vonatkozik rá a követelmény
S_SAV_1	megfelel
S_SAV_2	nem vonatkozik rá a követelmény
S_SAV_3	megfelel
S_SAV_4	nem vonatkozik rá a követelmény
S_SAV_5	nem vonatkozik rá a követelmény
S_SAV_6	nem vonatkozik rá a követelmény
S_SAV_7	megfelel
S_SAV_8	megfelel
S_SIC_1	nem vonatkozik rá a követelmény
S_SIC_2	nem vonatkozik rá a követelmény
S_SIC_3	nem vonatkozik rá a követelmény
S_SIC_4	nem vonatkozik rá a követelmény
S_SIC_5	nem vonatkozik rá a követelmény
S_SAC_1	nem vonatkozik rá a követelmény
S_SAC_2	nem vonatkozik rá a követelmény
S_SAC_3	nem vonatkozik rá a követelmény
S_SAC_4	nem vonatkozik rá a követelmény
S_SAC_5	nem vonatkozik rá a követelmény
S_SAC_6	nem vonatkozik rá a követelmény
S_SAC_7	nem vonatkozik rá a követelmény
S_SAC_8	nem vonatkozik rá a követelmény
S_SAC_9	nem vonatkozik rá a követelmény
S_SAC_10	nem vonatkozik rá a követelmény
S_SAC_11	nem vonatkozik rá a követelmény
S_SAC_12	nem vonatkozik rá a követelmény
S_DTBSF_1	megfelel
S_DHC_1	feltétellel megfelel
S_DHC_2	megfelel
S_DHC_3	megfelel

S_SSC_1	nem vonatkozik rá a követelmény
S_SSC_2	nem vonatkozik rá a követelmény
S_SSC_3	nem vonatkozik rá a követelmény
S_SSC_4	nem vonatkozik rá a követelmény
S_SSA_1	nem vonatkozik rá a követelmény
S_SDC_1	nem vonatkozik rá a követelmény
S_I/O_1	védett környezetben: megfelel, védtelen környezetben: nem felel meg
S_I/O_2	védett környezetben: megfelel, védtelen környezetben: nem felel meg
S_I/O_3	nem vonatkozik rá a követelmény
S_VER_1	védett környezetben: megfelel, védtelen környezetben: nem felel meg

4 A tanúsítási jelentés eredménye, érvényességi feltételei.

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltételek teljesülése esetén az NLCAPI3 v3.2.0 kriptográfiai modul alkalmas Minősített elektronikus aláíró és ellenőrző alkalmazások fejlesztésére. A feltételek nem a megvalósított programozói könyvtárra vonatkoznak, hanem annak telepítésére, környezetére, illetve az alkalmazható Elektronikus Aláírási Szabályzatra vonatkoznak.

4.2 Érvényességi feltételek

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az NLCAPI3 v3.2.0 kriptográfiai modullal kifejlesztett elektronikus aláíró alkalmazások által kezelt aláírások biztonságához.

1. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a CRL-t más tanúsítvánnyal ellenőrzik, mint a végfelhasználó tanúsítványokat. Ezért csak olyan környezetben szabad alkalmazni, amelyben önkibocsátott (self issued) tanúsítvány a tanúsítványláncban nem fordul elő, valamint amelyben a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni.*

Érintett funkcionális követelmény: F_ISV_3

2. számú feltétel *Az NLCAPI3 v3.2.0 kriptográfiai modullal fejlesztett 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: S_SCA_9

3. számú feltétel: *Fokozott vagy minősített elektronikus aláírások létrehozásánál az MD5 lenyomatoló algoritmus nem használható.*

Érintett biztonsági követelmény: S_DHC_1

4. számú feltétel: *Bár az NLCAPI3 v3.2.0 kriptográfiai modul rendelkezik önvédelmi funkcióval, 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: S_I/O_1

5. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az NLCAPI3 v3.2.0 kriptográfiai modul funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

Érintett biztonsági követelmény: S_I/O_2

6. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az NLCAPI3 v3.2.0 kriptográfiai modul, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

Érintett biztonsági követelmény: S_VER_1

4.3 Automatikus érvényesség

Bizonyos Funkcionális és Biztonsági követelmények automatikusan teljesülnek az NLCAPI3 v3.2.0 kriptográfiai modul fejlesztett elektronikus aláíró alkalmazásokra. Feltéve, hogy a programozói könyvtárat helyesen használják. Az alkalmazásra automatikusan teljesülő követelmények a következők:

F_DTBSF_1
F_DTBSF_2
F_DHC_1
F_DHC_2
F_SDOC_1
F_protocol
F_format
S_SCA_10
S_SCA_11
S_DHC_1
S_DHC_2
S_DHC_3

5 A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

Jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 15408 /Common Criteria/ EAL 3-es szintjéhez hasonló volt. / Az EAL 3 a fejlesztőktől függetlenül garantált biztonság fokozott szintjét biztosítja, mely elegendő a fokozott biztonságú elektronikus aláíráshoz használható aláírási termékekre. /

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

Az értékelés az alábbi garancia osztályokra terjedt ki:

- fejlesztés
- útmutató dokumentumok
- tesztek

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

6 A tanúsításhoz figyelembe vett egyéb dokumentumok

6.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. Évi XXXV.törvény

CEN/ISSS/E-Sign; Area G1 14170:2004 munkacsoport egyezmény: Security Requirements fro Signature Creation System

CEN/ISSS/E-Sign; Area G2 14171:2004 munkacsoport egyezmény: Procedures for Elecronic 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

ETSI TS 101 862 v1.3.2 Qualified Certificate profile

ETSI SR 002 176 v1.1.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

RFC3061 Time-Stamp Protocol (TSP)

RFC3275 XML Digital Signatures (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

PKCS #7: Cryptographic Message Syntax Standard

6.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1 A tanúsításhoz figyelembe vett fejlesztői dokumentumok

- NLCAPI 3 funkcióspecifikáció v1.0
- NLCAPI 3 magas szintű terv v1.0
- NLCAPI 3 felhasználói dokumentáció
- NLCAPI 3 tesztelési dokumentáció v1.0

6.2.2 A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés az NLCAPI3 V3.2.0 kriptográfiai modulról, mint elektronikus aláíró és ellenőrző alkalmazás kifejlesztésére alkalmas programozói könyvtárról (Készítette HunGuard Kft.)

7 Rövidítések

API (application programing interface)

CRL (certification revocation list) tanúsítvány visszavonási lista

CSP (cryptograpic service provider) kriptográfiai szolgáltató

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

DTBS (Data To Be Signed) aláírandó adat

DTBSF (DTBS formatter) aláírandó adat formattáló

EAL (Evaluation Assurance Level)

ÉJ értékelési jelentés

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

PKI (Public Key Infrastructure)

PIN (Personal Identification Number)

SAC (Signer's authentication component) aláírót hitelesítő összetevő

SAV (Signature attribute viewer) aláírási tulajdonság megjelenítő

SCA (Signature creation application) aláírás-létrehozó alkalmazás

SCS (Signature creation system) aláírás-létrehozó rendszer

SDC (Signer's document composer) aláírói dokumentum szerkesztő

SDOC (Signed data object composer) aláírt adat objektum szerkesztő

SDP (Signer's document presenter) aláírói dokumentumot megjelenítő

SDX (Signed Document eXpert)

SIC (Signer's interaction component) aláíróval kölcsönható összetevő

SLC (Signature logging component) aláírás-naplózási összetevő

SSA (SSCD/SCA Communicator authenticator) az SSCD/SCA közötti kommunikációt hitelesítő összetevő

SSC (SSCD/SCA Communicator):az SSCD és SCA közötti kommunikáció összetevője

SSCD (Secure signature creation device) biztonságos aláírás-létrehozó eszköz