TANÚSÍTÁSI JELENTÉS

HUNG-TJ-022-2004

a
Pénztár v4.0.1.12

elektronikus aláíró alkalmazásról

/Pénzügyi Szervezetek Állami Felügyelete/

Készítette: HunGuard Kft.
2004. december 14.

1. A Pénztár v4.0.1.12 legfontosabb tulajdonságainak összefoglalása

A tanúsított termék a Pénzügyi Szervezetek Állami Felügyelete által fejlesztetett Pénztár v4.0.1.12 aláíró alkalmazás.

1.1. Architektúra

A Pénztár v4.0.1.12 aláíró alkalmazás elektronikus dokumentumok elektronikus aláírással történő ellátását, és ezen aláírások kezdeti ellenőrzését támogatja.

Az aláírás 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 aláírt adat objektumot az RFC 3275 dokumentumában specifikált XMLDSig formátumban tárolja.

A Pénztár v4.0.1.12 az alábbi komponenseket valósította meg:

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

Az alábbi komponenseket az operációs rendszer standard hívásain keresztül (Crypto API) a biztonságos aláíró eszköz CSP –je valósítja meg

- Aláírót hitelesítő
- Biztonságos aláíró eszköz és az aláírás eszköz közötti kommunikátor

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, amely a CSP (Crypto Service Provider) segítségével tud kommunikálni a biztonságos aláíró eszközzel. Az aláírás folyamat során a megfelelő XML struktúrák legenerálódnak az aláírandó adatra az aláírás a CSP-n keresztül készül el.

1.2. Tulajdonságok

A Pénztár v4.0.1.12 aláíró alkalmazás feladata, foglalkoztatók és egyéni vállalkozók magánnyugdíjpénztári tagdíjbevallásának elkészítésére és azok minősített elektronikus aláírással és időbélyegzővel történő ellátása, a bevallás elküldése a pénztár szerverére és a kapott nyugta üzenet feldolgozása, az azon elhelyezett fokozott biztonságú pénztári aláírás ellenőrzése, a tartalom megjelenítése és a nyugtaüzenet mentése.

Az aláírásokon a Pénztár v4.0.1.12 kezdeti ellenőrzést hajt végre. Ehhez időbélyeget, és aktuális visszavonási listát szerez és csatol az aláírt adat objektumhoz. Érvénytelen esetben kijelzésre kerül a hiba oka, valamint az elektronikus bevallás elküldésének folyamatát a rendszer felfüggeszt. Miután az érvényes aláírási szabályzatban meghatározott késleltetésű visszavonási lista az aláírás időpontjában nem áll rendelkezésre ezért a kezdeti ellenőrzést meg kell ismételni.

Az aláírás megismételt kezdeti ellenőrzéséhez valamint utólagos ellenőrzéshez az IngridSigno 2.1.31 alkalmazás használandó.

A Pénztár v4.0.1.12 jellemző tulajdonságai:

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

1.3. A tanúsítás tárgya hatóköre

A tanúsítás tárgy maga a Pénztár v4.0.1.12 aláíró alkalmazás.

Az tanúsítás során feltételeztük, hogy az alkalmazás alapjául szolgáló Windows operációs rendszer, valamint az ennek részét képező CSP modul biztonságosan és helyesen működnek. A Pénztár v4.0.1.12 alapvetően az alábbi komponensekre épül:

- Microsoft Crypto API
- MultiSigno 2.2.b7 programozói könyvtár

2. A Pénztár v4.0.1.12 megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 követelményrendszerekből fakadó) funkcionális és biztonsági követelményeket, melyek minősített elektronikus aláírások létrehozására, és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.
Megnevezzük azokat a követelményeket, amelyek a Pénztár v4.0.1.12 aláíró alkalmazásra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy a Pénztár v4.0.1.12 aláíró 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: A Pénztár v4.0.1.12 aláíró alkalmazás minden általa aláírt elektronikus bevallási csomag esetén automatikus aláírás ellenőrzést végez. Az automatikusan kapott nyugta csomag aláírását is ellenőrzi.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás által aláírt dokumentum tartalom formátuma és annak megjelenítése kötött. 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: A Pénztár v4.0.1.12 aláíró alkalmazás által aláírt dokumentum tartalom formátuma és annak megjelenítése kötött. 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: A Pénztár v4.0.1.12 aláíró alkalmazás által aláírt dokumentum tartalom formátuma és annak megjelenítése kötött. 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: A Pénztár v4.0.1.12 aláíró 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: A Pénztár v4.0.1.12 aláíró 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: A Pénztár v4.0.1.12 aláíró alkalmazás a Windows tanúsítvány-megjelenítőjét használva ad lehetőséget az aláíró tanúsítvány megjelenítésére.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az XML bevallási csomag összeállítása után felhasználói aktivitás hatására végzi el a tényleges aláírást.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás biztosítja az aláíró/ellenőrző számára a megfelelő funkciókat.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API és a CSP feladata.

Konklúzió: **feltétellel megfelel**

1. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes bekérni az aláírót hitelesítő adatot, és azt továbbítani a biztonságos aláíró eszköz számára.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírandó XMLDSig csomagot megfelelően előállítja.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás kezdeményezi a lenyomatolást.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás elvégzi a lenyomatolást.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a lenyomatolás elvégzése után a lenyomat értékét feltölti az XMLDSig struktúrában a PKCS1 v1.5 szabvány szerint.

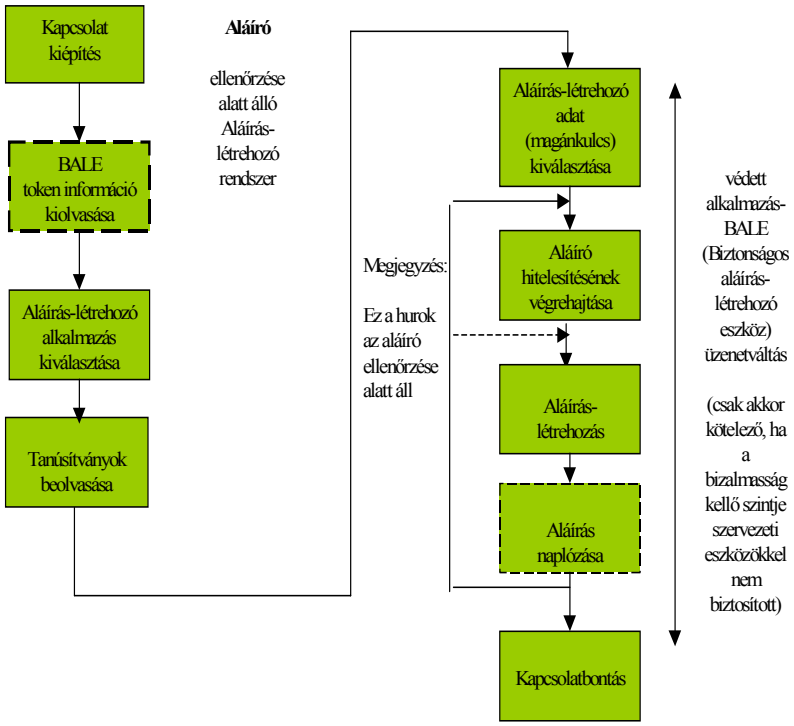
Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás minden szükséges kommunikációt végrehajt a Microsoft Crypto API-ján és a BALE eszközhöz tartozó CSP-én keresztül.

Konklúzió: **feltétellel megfelel**

2. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely aláírás létrehozó rendszer és a BALE közti minden szükséges kommunikációt végrehajt. (CWA14170 14.1 fejezet)*



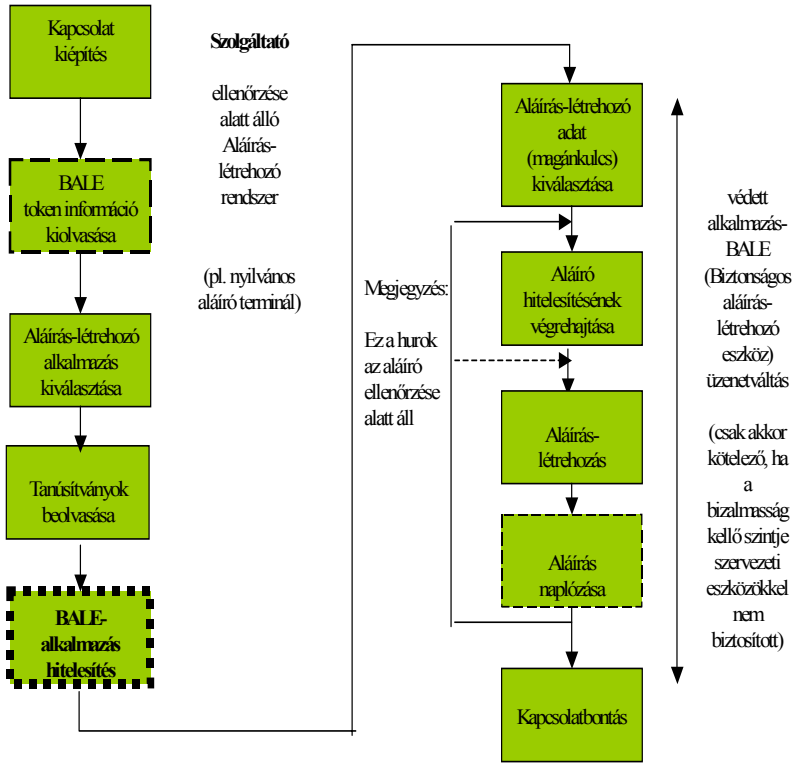
1. ábra

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

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazást nem külső szolgáltató ellenőrzése alá tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**



2. ábra

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

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-ját és a BALE-hoz tartozó CSP-t felhasználva képes fizikai interfészen keresztül aláíró eszközzel kommunikálni.

Konklúzió: **feltétellel megfelel**

3. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes fizikai interfészen keresztül a BALE-val kommunikálni.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírás-létrehozó alkalmazásnak a kiválasztása a Crypto API és a CSP feladata.

Konklúzió: **feltétellel megfelel**

4. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes kiválasztani a BALE-n levő megfelelő alkalmazást.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás támogatja a több tanúsítványból történő választást. A tanúsítványok tárolására az operációs rendszer tanúsítványtárát használja.

Konklúzió: **feltétellel megfelel**

5. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz kezelő szoftverének biztosítani kell kezelői felületet, amelyen keresztül az aláíró adathoz (privát kulcs) tartozó tanúsítvány a Microsoft tanúsítványtárába telepíthető.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírás-létrehozó adat a kiválasztása a Crypto API és a CSP feladata, az a tanúsítvány kiválasztása után automatikus.

Konklúzió: **feltétellel megfelel**

6. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes a Microsoft Tanúsítványtárából kiválasztott tanúsítványhoz tartozó aláírás létrehozó adatot (magánkulcsot) a BALE-n kiválasztani.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírót hitelesítő adat bekérése a Crypto API és a CSP feladata.

Konklúzió: **feltétellel megfelel**

7. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírót hitelesítő adatot és az aláírót hitelesítő összetevőt egy megbízható útvonalon keresztül a BALE-nak átadni.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-n és a BALE CSP-jén keresztül kiszámítatja az aláírás értékét, és eltárolja azt az XMLDSig dokumentumban.

Konklúzió: **feltétellel megfelel**

8. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírandó adat reprezentánst átadni a BALE-nak, valamint képes visszavenni az elektronikus aláírást.*

F_SSC_9: A befejezett aláírásokat naplózni kell.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás napló bejegyzést készít az aláírásról és annak automatikus ellenőrzéséről is.

Konklúzió: **megfelel**

F_SSA_1: Ha az aláírás-létrehozás egy - szolgáltató ellenőrzése alatt álló – aláírás-létrehozó rendszeren történik meg, akkor az aláírónak képesnek kell lennie annak megállapítására, hogy feltételezhet-e ugyanolyan szintű bizalmasságot, mint amit a saját ellenőrzése alatt álló aláírás-létrehozó rendszer esetén elérhet.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazást nem külső szolgáltató ellenőrzése alá tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás egy XML bevallási csomagot ír alá, a csomag összeállítását a felhasználó végzi, mielőtt még aláírhatná azt.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a BALE által létrehozott aláírást megfelelően beteszi az XMLDSig csomagba.

*Konklúzió: **megfelel***

F_SLC_1: Minden létrehozott/ellenőrzött aláírásra egy naplóbejegyzés tárolandó.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás naplóbejegyzést készít az aláírásról és annak automatikus ellenőrzéséről, és a válasz nyugta csomag automatikus ellenőrzéséről.

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 aláírói tanúsítványok a Microsoft tanúsítványtárában vagy az XML csomagban helyezkednek el, így nincs szükség a megszerzésükre. A Pénztár v4.0.1.12 aláíró program képes a tanúsítványok állapotának ellenőrzésére vagy a helyben levő CRL segítségével, vagy a letöltött CRL segítségével.

Konklúzió: **megfelel**

F_I/O-1: Ha aláírás-létrehozásnál a biztonságos aláírás-létrehozó eszköz nem tartalmaz minden szükséges tanúsítványt az aláírási folyamathoz (mert csak a tanúsítvány azonosítókat tartalmazza), vagy ha aláírás-ellenőrzésnél az aláírótól nem érkezett meg a szükséges tanúsítvány (csak annak azonosítója), akkor az aláírás-alkalmazásnak képesnek kell lennie arra, hogy ezeket a tanúsítványokat megszerezze (lekérdezze a hitelesítés-szolgáltatótól).

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Windows tanúsítványtárát használja a tanúsítványok eléréséhez. Az aláírói tanúsítványok a Microsoft tanúsítványtárában vagy az XML csomagban helyezkednek el, így nincs szükség a megszerzésükre.

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 aláírói tanúsítványok a Microsoft tanúsítványtárában vagy az XML csomagban helyezkednek el, így nincs szükség a megszerzésükre. A Pénztár v4.0.1.12 aláíró program 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: A Pénztár v4.0.1.12 aláíró alkalmazás biztosítja a fenti elvárást.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírás időpontjában elérhető minden érvényesítő adatot begyűjt.

Konklúzió: **megfelel**

F_ISV-2: Ha szükség lehet utólagos ellenőrzésre, az érvényesítő adatoknak tartalmazniuk kell annak bizonyítékát, hogy a felhasznált tanúsítvány lánc érvényes volt az aláírás létrehozásának időpontjában.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a kezdeti ellenőrzés folyamán minden érvényesítő adatot begyűjt. Az utólagos ellenőrzést IngridSigno v2.1.31 alkalmazás végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem alkalmas utólagos ellenőrzés elvégzésére, nem is feladata. Az utólagos ellenőrzést IngridSigno v2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás végzi.

Konklúzió: **nem vonatkozik rá a 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: A Pénztár v4.0.1.12 aláíró alkalmazás támogatja a fenti elvárást.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás támogatja a fenti elvárást.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az elektronikus aláírási szabályzatnak megfelelően jeleníti meg az aláíró dokumentumot az aláírás előtt.

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: A Pénztár v4.0.1.12 aláíró alkalmazás érvényes vagy érvénytelen ellenőrzés állapotot ismer, utólagos ellenőrzést nem végez. Az érvénytelen állapot kijelzése az érvénytelenség okával történik. Utólagos ellenőrzés az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazással történik.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem alkalmas utólagos ellenőrzés elvégzésére, nem is feladata. Az utólagos ellenőrzést és az adatok begyűjtését az IngridSigno Feldolgozó Modul 2.1.31 minősített elektronikus aláírás ellenőrző alkalmazás végzi. Az utólagos ellenőrzéshez csak a soron következő visszavonási listát kell beszerezni.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás teljesíti a fenti elvárást.

Konklúzió: **megfelel**

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

F_machine_1: Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére és az elektronikus aláírás formátumának meghatározására.
Amennyiben az aláírási szabályzat explicit, akkor a szabályzat azonosítóját magából az elektronikus aláírásból kell kinyerni az 1-es típusú API-jainak felhasználásával.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazást nem automatikus ellenőrzésre tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

F_machine_2: A 2-es típusú API-k az elektronikus aláírások hitelesítését és/vagy ellenőrzését kell lehetővé tenniük, illetve be kell szerezniük az aláírói információkat, az output állapotot és az érvényesítő adatokat.
Az automatizált feldolgozás esetében alkalmazói program interfészek (API-k) használhatók. Bár az ilyen interfészek kialakításának többféle módja van, ezeket két csoportba lehet sorolni:

- az 1-es típusú API-k arra szolgálnak, hogy az elektronikus aláírásban tárolt adatokat kigyűjtsék.
- A 2-es típusú API-k az elektronikus aláírás ellenőrzésére és az érvényesítő adatok beszerzésére szolgálnak.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazást nem automatikus ellenőrzésre tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás aláírás ellenőrzés során teljesíti az elektronikus aláírási szabályzatban foglaltakat.

Konklúzió: **megfelel**

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

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a szabványos protokollokat használ.

Konklúzió: **megfelel**

F_format: Mind az aláírás-létrehozó, mind az aláírás-ellenőrzési alkalmazásnak képesnek kell lennie szabványos formátumok kezelésére az alábbi területeken:

- szabványos aláírási formátumok;
- szabványos tanúsítvány formátumok.

Magyarázat: A Pénztár v4.0.1.12 aláíró 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 biztosítania;
- megfelelő állapotjelzéseket és hibaüzeneteket kell küldenie a felhasználó számára.

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

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

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazást teljesíti a fenti elvárást.

Konklúzió: **megfelel**

2.2. Biztonsági követelmények minősített elektronikus aláírásokat létrehozó/ellenőrző alkalmazások számára

2.2.1. Követelmények az aláírás-létrehozó alkalmazás (SCA) egészére

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

Bizt_köv1: Az aláírás-létrehozó alkalmazásnak meg kell őriznie a következők sértetlenségét:

- aláírandó adat (DTBS), formattált aláírandó adat (DTBSF), aláírandó adat reprezentáns (DTBSR) és minden egyéb, az aláíró által szolgáltatott információ,
- az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között áramló valamennyi protokoll adat.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-n és a BALE CSP-jén keresztül éri el a biztonságos aláírás létrehozó eszközt. Önmagában a fenti adatok sértetlenségét megőrzi, a BALE eszköz, csak az aláírandó adat reprezentánst kapja meg.

Konklúzió: **feltétellel megfelel**

9. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-n és a BALE CSP-jén keresztül éri el a biztonságos aláírás létrehozó eszközt. Önmagában a fenti adatok bizalmasságát megőrzi.

Konklúzió: **feltétellel megfelel**

10. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes megőrizni az aláírót hitelesítő adatok bizalmasságát.*

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

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a megjelenítő funkciónak közvetlenül az XML bevallási csomagból adja át a megjelenítőnek a bevallási adatokat.

Konklúzió: **megfelel**

Bizt_köv8: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy a formattált aláírandó adat és aláírandó adat reprezentáns előállításához felhasznált aláírandó adat komponensek ugyanazok, mint amelyeket az aláírónak bemutattak a bemutatási eljárás során, és amelyeket a felhasználó kiválasztott.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírás folyamán a XML csomagban lévő a bevallási XML dokumentumot írja alá.

Konklúzió: **megfelel**

<u>Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények</u>

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem osztott architektúrájú aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem osztott architektúrájú aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

A nem megbízható folyamatokból és kommunikációs portokból adódó követelmény

Bizt_köv11: Meg kell gátolni, hogy az aláírási folyamatba beavatkozhassanak olyan nem-megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

Magyarázat: Lévén a Pénztár v4.0.1.12 egy szoftveralkalmazás, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek (operációs rendszer) kell biztosítani

Konklúzió: **feltétellel megfelel**

11. számú feltétel *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.*

Az aláírandó adatra vonatkozó követelmények

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás egy XML bevallási csomagot ír alá, ami nem lehet üres.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás az XMLDSig csomagban tárolja az aláíró tanúsítványát. Ezen kívül tárolja az aláíró tanúsítványának lenyomatát, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás az XMLDSig csomagban tárolja a hivatkozást az aláírási szabályzatra, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás az XMLDSig csomagban tárolja a kötelezettségvállalás típusát, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás az XMLDSig csomagban tárolja a tartalom formátumot, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

2.2.2. Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP)

A tartalom formátumra vonatkozó követelmények:

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás az XMLDSig csomagban tárolja 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.

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás maga állítja össze az aláírásra szánt XML bevallási csomagot.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás csak XML bevallási csomagokat ír alá és csak ezeket tudja megjeleníteni.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró csak bevallási XML csomagokat ír alá és csak ezeket tudja megjeleníteni.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró csak XML bevallási csomagokat ír alá és csak ezeket tudja megjeleníteni.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv22: Az aláíró dokumentumát megjelenítő összetevőnek biztosítania kell, hogy az aláírónak megmutatott aláírói dokumentum ugyanaz, mint amit az aláírási folyamat fog használni, és ugyanaz, mint amit az aláíró választott ki aláírásra.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírás előtti megtekintéskor az XMLDSig csomagból adja át a XML bevallási csomagot a megjelenítőnek.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás által készített és kezelt bevallási XML csomag szerkezete az elektronikus aláírási szabályzatban rögzített, nem lehet benne le nem kezelt aláírt adat.

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.

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás csak megjeleníti a bevallási XML csomagot, nem ad lehetőséget az adatok módosítására.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró csak bevallási XML csomagokat ír alá és csak ezeket tudja megjeleníteni. A megjelenítés módja az elektronikus aláírási szabályzatban rögzített.

Konklúzió: **nem vonatkozik rá a követelmény**

Az aláíró dokumentumára vonatkozó egyértelműségi követelmény:

Bizt_köv26: Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy tartalom formátum tulajdonság csatolását az aláírandó adatokhoz annak biztosítására, hogy az aláíró dokumentumának megjelenítése egyértelmű legyen. Vagyis pontosan úgy lehessen azt a későbbiekben megjeleníteni, mint ahogyan az aláírónak a megjelenítési folyamat során.

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás csak bevallási XML csomagokat ír alá és csak ezeket tudja megjeleníteni. Az XMLDSig csomagban tárolja a tartalom formátumot, mint aláírt aláírási tulajdonság. A megjelenítés módja az elektronikus aláírási szabályzatban rögzített.

Konklúzió: **megfelel**

A nem megjelenítés-érzékeny aláírói dokumentumokra vonatkozó követelmény:

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás csak bevallási XML csomagokat ír alá és csak ezeket tudja megjeleníteni. Az XMLDSig csomagban tárolja a tartalom formátumot, mint aláírt aláírási tulajdonság. A megjelenítés módja az elektronikus aláírási szabályzatban rögzített.

Konklúzió: **megfelel**

A rejtett szövegre és aktív kódra vonatkozó követelmény:

Bizt_köv28: Az aláírás-létrehozó alkalmazásnak figyelmeztetnie kell az aláírót a rejtett szövegek, makrók vagy aktív kódok jelenlétére. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás csak bevallási XML csomagokat ír alá és csak ezeket tudja megjeleníteni. Az XML csomag nem tartalmazhat aktív kódot vagy rejtett szövegrészt.

Konklúzió: **megfelel**

2.2.3. Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV)

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás lehetőséget ad az aláírási tulajdonságok megtekintésére: 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**

Bizt_köv30: Az aláírás tulajdonságokat megjelenítő folyamatnak biztosítania kell, hogy az aláírónak megjelenített aláírás tulajdonság ugyanaz, mint ami az aláírás folyamatában aláírásra kerül majd, és amit az aláíró kiválasztott az aláíráshoz.

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás biztosítja az aláírt aláírási tulajdonságok hitelességét és sértetlenségét, azokat az XMLDSig csomagból veszi ki bemutatásra.

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazásban az aláírt aláírási tulajdonságokat maga az aláírás védi, a nem aláírt aláírási tulajdonságok önmagukat védik.

Konklúzió: **megfelel**

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.

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás aláírási tulajdonságai nem tartalmaznak rejtett szöveget vagy aktív kódot

Konklúzió: **megfelel**

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

Megjegyzés: A Pénztár v4.0.1.12 aláíró alkalmazás aláírási tulajdonságai nem tartalmaznak rejtett szöveget vagy aktív kódot.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Windows tanúsítvány-megjelenítőjét használva ad lehetőséget az aláíró tanúsítvány megjelenítésére.

Konklúzió: **megfelel**

2.2.4. Követelmények az aláíróval kölcsönható összetevőre (SIC)

Az aláírás kiváltására vonatkozó követelmények

Bizt_köv35: Az aláírási folyamat megkezdése előtt az aláíróval kölcsönható összetevőnek egy olyan nem nyilvánvaló, az aláírás-létrehozó alkalmazással folytatott, aláírás kiváltási cselekvést kell elvárnia az aláírótól, amely véletlenül valószínűleg nem következne be.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírás funkció kiváltására a bevallási csomag elkészítése után aktív felhasználói beavatkozást vár.

Konklúzió: **megfelel**

Az inaktivitási időkorlátra vonatkozó biztonsági követelmények

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás előbb bekéri a felhasználótól az aláírói akarat kinyilvánítását, és ezt követően adja át a CSP-nek aláírásra az aláírandó adat reprezentánst. Így amikor a CSP bekéri az aláíró hitelesítő adatot, az aláírónak nincs módja várni az aláírás kiváltásával.

Konklúzió: **megfelel**

Bizt_köv37: Ha az időkorlát letelik, az egész aláírási folyamatot félbe kell szakítani, az aláírótól az aláírási folyamat újraindítását követelve meg, hitelesítő adatainak újra megadását is beleértve. Az újraindítás szükségességéről tájékoztatni kell az aláírót.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás előbb bekéri a felhasználótól az aláírói akarat kinyilvánítását, és ezt követően adja át a CSP-nek aláírásra az aláírandó adat reprezentánst. Így amikor a CSP bekéri az aláíró hitelesítő adatot, az aláírónak nincs módja várni az aláírás kiváltásával.

Konklúzió: **megfelel**

2.2.5. Követelmények az aláírót hitelesítő összetevőre (SAC)

A tudáson alapuló aláírót hitelesítő adatokra vonatkozó követelmények

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírót hitelesítő adat bekérése ezek feladata.

Konklúzió: **feltétellel megfelel**

1. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes bekérni az aláírót hitelesítő adatot és azt továbbítani a biztonságos aláíró eszköz számára.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírót hitelesítő adat bizalmasságának megőrzése ezek feladata.

Konklúzió: **feltétellel megfelel**

12. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely megőrzi az aláírót hitelesítő adatok bizalmasságát, és biztonságosan törli azokat, amikor már nincs azokra szükség.*

Bizt_köv40: Ha az aláírni szándékozó egy korlátot meghaladó számban helytelen hitelesítő adatot ad meg, akkor az újrapróbálkozást le kell tiltani, egyúttal hibajelzést kell adni az aláíró részére, ha az aláíró hitelesítési módszert már nem blokkolta korábban a biztonságos aláírás-létrehozó eszköz. Az aláírni szándékozó részére egy megfelelő üzenetet kell küldeni.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. A helytelen próbálkozások utáni letiltás ezek feladata. Ezt a kritériumot maga a BALE teljesíti.

Konklúzió: **megfelel**

Bizt_köv41: Ha az aláírni szándékozó ismételten helytelen hitelesítő adatot ad meg (pl. három egymást követő alkalommal), a biztonságos aláírás-létrehozó eszköznek félbe kell szakítania az aláíró hitelesítését, és erről informálnia kell az aláírás-létrehozó alkalmazást, amelynek az aláíró részére egy megfelelő üzenetet kell küldeni.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírási folyamat félbeszakítása ezek feladata. Ezt a kritériumot maga a BALE teljesíti.

Konklúzió: **megfelel**

Bizt_köv42: Egy megbízható útvonalat kell biztosítani a PIN/jelszó továbbítására a PIN pad (vagy billentyűzet) és a biztonságos aláírás-létrehozó eszköz között az aláírás-létrehozó alkalmazáson keresztül.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. A megbízható útvonal kiépítése a CSP feladata.

Konklúzió: **feltétellel megfelel**

7. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírót hitelesítő adatot és az aláírót hitelesítő összetevőt egy megbízható útvonalon keresztül a BALE-nak átadni.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem biztosít PIN kód csere lehetőséget, erre a BALE eszközök saját kezelő szoftverét használja a rendszer.

Konklúzió: **feltétellel megfelel**

13. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz telepíteni kell a BALE eszköz kezelő szoftverét, amely biztosítja a tudáson alapuló hitelesítő adatok lecserélhetőségét.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. A PIN kód bekérése és képernyőn történő visszajelzése ezek feladata.

Konklúzió: **feltétellel megfelel**

14. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely nem jeleníti meg a tudáson alapuló hitelesítő adatot a képernyőn.*

Bizt_köv45: Az aláírás-létrehozó alkalmazásnak meg kell követelnie az új PIN kód (jelszó) kétszeri megadását, és ellenőriznie kell ezek azonosságát, mielőtt az új PIN kódot (jelszót) továbbítaná a biztonságos aláírás-létrehozó eszköznek.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás nem biztosít PIN kód csere lehetőséget, erre a BALE eszközök saját kezelő szoftverét ajánlja a rendszer.

Konklúzió: **feltétellel megfelel**

15. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz kezelő szoftverének biztosítani kell PIN kód lecserélésénél az új PIN kód kétszeri megadását, a helytelen adatbevitel elkerülése érdekében.*

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a CSP feladata.

Konklúzió: **feltétellel megfelel**

7. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírót hitelesítő adatot és az aláírót hitelesítő összetevőt egy megbízható útvonalon keresztül a BALE-nak átadni.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Az aláírót hitelesítő biometrikus adat kezelése a CSP feladata.

Konklúzió: **feltétellel megfelel**

16. számú feltétel: *Amennyiben a Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz biometrikus hitelesítő adatokat használ olyan CSP-t kell alkalmazni, amely ezen adatok kriptográfiai védelmét biztosítja.*

2.2.6. Követelmények az aláírandó adat formattáló összetevőre (DTBSF)

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az XMLDSig csomagot megfelelően állítja elő.

Konklúzió: **megfelel**

2.2.7. Követelmények az adat lenyomat készítő összetevőre (DHC)

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás SHA1 lenyomatoló algoritmust használ.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírt adatra a megkövetelt feltöltési módszert alkalmazza.

Konklúzió: **megfelel**

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás az aláírandó adat reprezentánst helyesen állítja elő.

Konklúzió: **megfelel**

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

Bizt_köv52: Az aláírás-létrehozó rendszernek támogatnia kell a fizikai interfész minden fontos részletét egy meghatározott tartományon belül, vagy egy meghatározott jellegzetességgel, az általa támogatott biztonságos aláírás-létrehozó eszköz típusok megfelelő működésének biztosítása érdekében.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. Ezen keresztül képes fizikai interfészen keresztül aláíró eszközzel kommunikálni.

Konklúzió: **feltétellel megfelel**

3. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes fizikai interfészen keresztül a BALE-val kommunikálni.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik. A lehallgatás és zavarás elleni védelem a CSP feladata.

Konklúzió: **feltétellel megfelel**

17. számú feltétel: *Amennyiben a Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz vezeték nélküli összeköttetést használ, olyan CSP-t kell alkalmazni, amely a lehallgatás és a zavarás elleni védelmet biztosítja.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazás a Microsoft Crypto API-jára és a BALE CSP-jére támaszkodik.

Konklúzió: **feltétellel megfelel**

4. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes kiválasztani a BALE-n levő megfelelő alkalmazást.*

6. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes a Microsoft Tanúsítványtárából kiválasztott tanúsítványhoz tartozó aláírás létrehozó adatot (magánkulcsot) a BALE-n kiválasztani.*

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

Magyarázat: Lévén a Pénztár v4.0.1.12 egy szoftver alkalmazás, önállóan nem képes megvédenie sem saját, sem egyes moduljainak integritását. Ezért nem lehet feladata a kommunikációs összetevő módosítással szembeni védelme. Ezt a működési környezetnek (pl. az operációs rendszernek) kell biztosítania.

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

18. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírás-létrehozó eszközzel kommunikáló összetevőt (CSP) ne lehessen jogosulatlanul módosítani.*

2.2.9. Követelmények az SSCD/SCA hitelesítő összetevőre (SSA)

Bizt_köv56: Az SSA-nak támogatnia kell az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között az entitások hitelesítését, hogy megbízható jelzést adhasson az aláírónak egy sikeres hitelesítésről, és védenie kell az ezt követő kommunikációt egy biztonságos üzenetközvetítéssel.

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazást nem külső szolgáltató ellenőrzése alá tervezték.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Bizt_köv57: Intézkedéseket kell tenni annak biztosítására, hogy vírusok ne ronthassák el az SCA összetevőket, és hogy az esetlegesen vírussal fertőzött SCA összetevők megfelelően helyre legyenek állítva.

Magyarázat: Lévén a Pénztár v4.0.1.12 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**

19. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:*

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

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

Magyarázat: Lévén a Pénztár v4.0.1.12 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**.

20. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A Pénztár v4.0.1.12 aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva hogy behatolók elrontsák ezt.*

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

Magyarázat: A Pénztár v4.0.1.12 aláíró alkalmazásban nincs importált komponens.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.11. Követelmények az aláírás-rendszer védelmére (biztonságos terület)

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

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

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

21. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a Pénztár v4.0.1.12 aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

3. A Pénztár v4.0.1.12 aláíró alkalmazás megfelelése a követelményeknek

3.1. A Pénztár v4.0.1.12 aláíró alkalmazás megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	megfelel
F_SDP_1	megfelel
F_SDP_2	megfelel
F_SDP_3	megfelel
F_SDP_4	megfelel
F_SAV_1	megfelel
F_SAV_2	megfelel
F_SIC_1	megfelel
F_SIC_2	megfelel
F_SIC_3	feltétellel megfelel
F_DTBSF_1	megfelel
F_DTBSF_2	megfelel
F_DHC_1	megfelel
F_DHC_2	megfelel
F_SSC_1	feltétellel megfelel
F_SSC_2	nem vonatkozik rá a követelmény
F_SSC_3	feltétellel megfelel
F_SSC_4	feltétellel megfelel
F_SSC_5	feltétellel megfelel
F_SSC_6	feltétellel megfelel
F_SSC_7	feltétellel megfelel
F_SSC_8	feltétellel megfelel
F_SSC_9	megfelel
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	megfelel
F_SDOC_1	megfelel
F_SLC_1	megfelel
F_SCPC_1	megfelel
F_I/O-1	nem vonatkozik rá a követelmény
F_I/O-2	megfelel
F_I/O-3	megfelel
F_ISV-1	megfelel
F_ISV-2	nem vonatkozik rá a követelmény
F_USV-1	nem vonatkozik rá a követelmény
F_human_1	megfelel
F_human_2	megfelel
F_human_3	megfelel
F_human_4	megfelel
F_human_5	nem vonatkozik rá a követelmény
F_human_6	megfelel
F_machine_1	nem vonatkozik rá a követelmény
F_machine_2	nem vonatkozik rá a követelmény
F_general_1	megfelel
F_protocol	megfelel
F_format	megfelel
F_principles	megfelel

3.2. A Pénztár v4.0.1.12 aláíró alkalmazás megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	feltétellel megfelel
Bizt_köv2	feltétellel megfelel
Bizt_köv3	nem vonatkozik rá a követelmény
Bizt_köv4	nem vonatkozik rá a követelmény
Bizt_köv5	nem vonatkozik rá a követelmény
Bizt_köv6	nem vonatkozik rá a követelmény
Bizt_köv7	megfelel
Bizt_köv8	megfelel
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	feltétellel megfelel
Bizt_köv12	megfelel
Bizt_köv13	megfelel
Bizt_köv14	megfelel
Bizt_köv15	megfelel
Bizt_köv16	megfelel
Bizt_köv17	megfelel
Bizt_köv18	nem vonatkozik rá a követelmény
Bizt_köv19	megfelel
Bizt_köv20	nem vonatkozik rá a követelmény
Bizt_köv21	nem vonatkozik rá a követelmény
Bizt_köv22	megfelel
Bizt_köv23	nem vonatkozik rá a követelmény
Bizt_köv24	megfelel
Bizt_köv25	nem vonatkozik rá a követelmény
Bizt_köv26	megfelel
Bizt_köv27	megfelel
Bizt_köv28	megfelel
Bizt_köv29	megfelel
Bizt_köv30	megfelel
Bizt_köv31	megfelel
Bizt_köv32	megfelel
Bizt_köv33	megfelel
Bizt_köv34	megfelel
Bizt_köv35	megfelel
Bizt_köv36	megfelel
Bizt_köv37	megfelel
Bizt_köv38	feltétellel megfelel
Bizt_köv39	feltétellel megfelel
Bizt_köv40	megfelel
Bizt_köv41	megfelel
Bizt_köv42	feltétellel megfelel
Bizt_köv43	feltétellel megfelel
Bizt_köv44	feltétellel megfelel
Bizt_köv45	feltétellel megfelel
Bizt_köv46	feltétellel megfelel
Bizt_köv47	feltétellel megfelel
Bizt_köv48	megfelel
Bizt_köv49	megfelel
Bizt_köv50	megfelel
Bizt_köv51	megfelel

Bizt_köv52	feltétellel megfelel
Bizt_köv53	feltétellel megfelel
Bizt_köv54	feltétellel megfelel
Bizt_köv55	feltétellel megfelel
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	feltétellel megfelel
Bizt_köv58	feltétellel megfelel
Bizt_köv59	nem vonatkozik rá a követelmény
Bizt_köv60	feltétellel megfelel

4. A tanúsítási jelentés eredménye, érvényességi feltételei

4.1. Eredmények

A 4.2 alfejezetben megfogalmazott feltételek teljesülése esetén a Pénztár v4.0.1.12 aláíró alkalmazás alkalmas minősített elektronikus aláírások létrehozására és kezdeti ellenőrzésére.
A feltételek nem a megvalósított aláíró alkalmazás komponensekre vonatkoznak, hanem azok telepítésére, működési környezetére vonatkoznak.

4.2. Érvényességi feltételek:

1. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes bekérni az aláírót hitelesítő adatot és azt továbbítani a biztonságos aláíró eszköz számára.*

Érintett funkcionális követelmény: F_SIC_3

Érintett biztonsági követelmény: Bizt_köv38

2. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely aláírás létrehozó rendszer és a BALE közti minden szükséges kommunikációt végrehajt. (CWA14170 14.1 fejezet)*

Érintett funkcionális követelmény: F_SSC_1

3. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes fizikai interfészen keresztül a BALE-val kommunikálni.*

Érintett funkcionális követelmény: F_SSC_3

Érintett biztonsági követelmény: Bizt_köv52

4. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes kiválasztani a BALE-n levő megfelelő alkalmazást.*

Érintett funkcionális követelmény: F_SSC_4

Érintett biztonsági követelmény: Bizt_köv54

5. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz kezelő szoftverének biztosítani kell kezelői felületet, amelyen keresztül az aláíró adathoz (privát kulcs) tartozó tanúsítvány a Microsoft tanúsítványtárába telepíthető.*

Érintett funkcionális követelmény: F_SSC_5

6. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes a Microsoft Tanúsítványtárából kiválasztott tanúsítványhoz tartozó aláírás létrehozó adatot (magánkulcsot) a BALE-n kiválasztani.*

Érintett funkcionális követelmény: F_SSC_6

Érintett biztonsági követelmény: Bizt_köv54

7. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírót hitelesítő adatot és az aláírót hitelesítő összetevőt egy megbízható útvonalon keresztül a BALE-nak átadni.*

Érintett funkcionális követelmény: F_SSC_7

Érintett biztonsági követelmény: Bizt_köv42
Bizt_köv46

8. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírandó adat reprezentánst átadni a BALE-nak, valamint képes visszavenni az elektronikus aláírást.*

Érintett funkcionális követelmény: F_SSC_8

9. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.*

Érintett biztonsági követelmény: Bizt_köv1

10. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes megőrizni az aláírót hitelesítő adatok bizalmasságát.*

Érintett biztonsági követelmény: Bizt_köv2

11. számú feltétel *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.*

Érintett biztonsági követelmény: Bizt_köv11

12. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely megőrzi az aláírót hitelesítő adatok bizalmasságát, és biztonságosan törli azokat, amikor már nincs azokra szükség.*

Érintett biztonsági követelmény: Bizt_köv39

13. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz telepíteni kell a BALE*

eszköz kezelő szoftverét, amely biztosítja a tudáson alapuló hitelesítő adatok lecserélhetőségét.

Érintett biztonsági követelmény: Bizt_köv43

14. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely nem jeleníti meg a tudáson alapuló hitelesítő adatot a képernyőn.*

Érintett biztonsági követelmény: Bizt_köv44

15. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz kezelő szoftverének biztosítani kell PIN kód lecserélésénél az új PIN kód kétszeri megadását, a helytelen adatbevitel elkerülése érdekében.*

Érintett biztonsági követelmény: Bizt_köv45

16. számú feltétel: *Amennyiben a Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz biometrikus hitelesítő adatokat használ olyan CSP-t kell alkalmazni, amely ezen adatok kriptográfiai védelmét biztosítja.*

Érintett biztonsági követelmény: Bizt_köv47

17. számú feltétel: *Amennyiben a Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz vezeték nélküli összeköttetést használ, olyan CSP-t kell alkalmazni, amely a lehallgatás és a zavarás elleni védelmet biztosítja.*

Érintett biztonsági követelmény: Bizt_köv53

18. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírás-létrehozó eszközzel kommunikáló összetevőt (CSP) ne lehessen jogosulatlanul módosítani.*

Érintett biztonsági követelmény: Bizt_köv55

19. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:*

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

Érintett biztonsági követelmény: Bizt_köv57

20. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A Pénztár v4.0.1.12 aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva hogy behatolók elrontsák ezt.*

Érintett biztonsági követelmény: Bizt_köv58

21. számú feltétel: *A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a Pénztár v4.0.1.12 aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

Érintett biztonsági követelmény: Bizt_köv60

5. A követelményeknek való megfelelést ellenőrző vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 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 fentieken kívül a fejlesztőktől független minta tesztelésre, illetve áthatolás tesztelésre is sor került.

6. A tanúsításhoz figyelembe vett egyéb dokumentumok

6.1. Termék megfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. Évi XXXV. törvény

CEN/ISSS/E-Sign; Area G1 14170:2001 munkacsoport egyezmény: Security Requirements fro 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
- Pénztár v4.0.1.12 telepítési és üzemeltetési kézikönyv 2004. október 28.
- Követelményspecifikáció PSZÁF elektronikus tagdíjbevallás projekt 2004. augusztus 02.
- Rendszerterv PSZÁF elektronikus tagdíjbevallás projekt 2004. augusztus 12.
- Elektronikus Aláírási Szabályzat OID: 1.3.6.1.4.1.16261.3.2.1.2.3
- Felhasználói kézikönyv (küldő oldal) 2004. november 08.
- 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 a Pénztár v4.0.1.12 aláíró alkalmazásról (készítette: HunGuard Kft)

7. Rövidítések

API (application programing interface)

CRL (certification revocation list) tanúsítvány visszavonási lista

CSP (cryptograpic service provider) kriptográfiai szolgáltató

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

DTBS (Data To Be Signed) aláírandó adat

DTBSF (DTBS formatter) aláírandó adat formattáló

EAL (Evaluation Assurance Level)

ÉJ értékelési jelentés

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

PKI (Public Key Infrastructure)

PIN (Personal Identification Number)

SAC (Signer's authentication component) aláírót hitelesítő összetevő

SAV (Signature attribute viewer) aláírási tulajdonság megjelenítő

SCA (Signature creation application) aláírás-létrehozó alkalmazás

SCS (Signature creation system) aláírás-létrehozó rendszer

SDC (Signer's document composer) aláírói dokumentum szerkesztő

SDOC (Signed data object composer) aláírt adat objektum szerkesztő

SDP (Signer's document presenter) aláírói dokumentumot megjelenítő

SDX (Signed Document eXpert)

SIC (Signer's interaction component) aláíróval kölcsönható összetevő

SLC (Signature logging component) aláírás-naplózási összetevő

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

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

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