Tanúsítási jelentés

Hung-TJ-015-2004

a
Marketline
integrált aláíró alkalmazásról

/Axelero Rt./

Tartalom

1. A Marketline integrált PKI modul legfontosabb tulajdonságainak összefoglalása

Az értékelt termék a „PKI Projekt” keretében fejlesztett, a Marketline Integrált Szállítói Rendszer vevő oldali elektronikus aláírási alkalmazás összetevő modul (a továbbiakban Marketline integrált PKI modul vagy Marketline integrált aláíró alkalmazás).

1.1 Architektúra

A Marketline integrált PKI modul Java nyelven készített automata aláírást létrehozó és aláírást ellenőrző alkalmazás.

Az elektronikus aláíró és aláírás ellenőrzési funkciókat a MultiSigno Developer (1.3 verzió) függvény készletének felhasználásával valósítja meg, amit Java illesztő felületen keresztül ér el.

A MultiSigno Developer fejlesztő készlet DLL elemei a Microsoft Crypto API függvényeit hívják meg. Az aláírandó/ellenőrizendő XML struktúrára az MS Crypto API-n keresztül történik az aláírás létrehozásának és ellenőrzésének aktivizálása.

Futtatási környezet: Windows 2000 server.

Az aláírások létrehozása és ellenőrzése automatizált folyamatként emberi beavatkozás nélkül történik.

Az aláírás-létrehozó adat (magánkulcs) az operációs rendszer tanúsítványtárában található.

Az aláíró tanúsítványát a MATÁV hitelesítés-szolgáltató hitelesíti.

Az aláírások ellenőrzéséhez a MATÁV hitelesítés-szolgáltató biztosít CRL-t, 24 óránkénti frissítéssel.

1.2 Tulajdonságok

A Marketline integrált PKI modul intelligens kártyát használ az aláírások létrehozására.
Az aláírandó adat formátuma mindig iDOC XML.
A csatolt dokumentumok formátuma (az aláírás szabályzatban meghatározottaknak megfelelően) az alábbi lehet:

- iDOC XML,
- Microsoft Word dokumentum (DOC),
- Microsoft Excel táblázat (XLS),
- Adobe Acrobat dokumentum (PDF),
- Microsoft PowerPoint prezetáció (PPT),
- Zip tömöritett állomány (ZIP),
- Rar tömörített állomány (RAR),
- egyszerű szövegállomány (TXT),
- Rtf dokumentum (RTF),
- Web oldal (HTML),
- GIF formátumú kép,
- TIF formátumú kép és
- JPG formátumú kép.

Az aláírás formátuma: XML-Signature.

Aláírt aláírási tulajdonságként az aláíró által állított aláírási dátum kerül az aláírásba.

Nem aláírt aláírási tulajdonságként az aláíró tanúsítványa, valamint az aláíráskor aktuális CRL kerül az aláírásba.

A rendszer időbélyegző alkalmazását nem követeli meg.

Az aláírás dátuma a rendszer dátuma, ami negyedóránál nagyobb mértékben nem térhet el a központi szerver órájától.

A Marketline integrált PKI modul tanúsítványtárnak az operációs rendszer tanúsítványtárát használja.

A Marketline integrált PKI modul mind a sikeres, mind a sikertelen aláírásokról naplóbejegyzést készít.

Az aláírás kötelezettségvállalást jelent, miszerint az aláíró (aki a Marketline integrált PKI modul alkalmazást elindító, a cég nevében eljáró személy) az aláírásával elismeri, hogy az aláírt iDOC XML dokumentumot és a csatolásokat ő készítette, hagyta jóvá és küldte el az aláírásban jelölt időpontban.

1.3 Az értékelés tárgya és hatóköre

Jelen tanúsítási jelentés tárgya maga a Marketline integrált PKI modul, mint aláíró alkalmazás.

A tanúsítás során feltételeztük, hogy az alábbi, a Marketline integrált PKI modul aláíró alkalmazás alapját képező funkciók és platformok biztonságosan és helyesen működnek:

- a MultiSigno Developer fejlesztő készlet DLL elemei (ennek biztonságos és helyes működését a HUNG-T-003-2003 számú tanúsítás is alátámasztja),
- a Microsoft Crypto API függvényei.

2. A Marketline integrált aláíró alkalmazás megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 követelményrendszereiből fakadó) funkcionális és biztonsági követelményeket, melyek minősített aláírások létrehozására és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy a Marketline integrált aláíró alkalmazás megfelel-e az adott követelménynek.

Minthogy a Marketline integrált aláíró alkalmazást nem minősített aláírásra, hanem csak fokozott biztonságú aláírásra kívánják felhasználni, megfelelő értékelési végeredmény adható akkor is, ha egyes vonatkozó követelményeknek az alkalmazás nem felel meg. A nem teljesített feltételeket külön is összegezzük a "minősített aláíráshoz szükséges, jelenleg ki nem elégített követelmények" alfejezetben.

Mivel a fokozott biztonságú aláírások létrehozását és ellenőrzését végző rendszerekre nézve nincs kidolgozott nemzetközi követelményrendszer, ezért az ilyen rendszerek tanúsítását is a minősített rendszerek követelményeinek való megfelelőség vizsgálatára alapoztuk.
Egy fokozott biztonságra megvalósított rendszer biztonságát ezáltal a minősített aláíró rendszerek követelményeihez való hasonlítással (s ezen belül pl. a teljesített követelmények aránya szerint) lehet érzékeltetni, számszerűsíteni. Ez a megfeleltetés különböző fokozott biztonságú rendszerek biztonsági szempontú összehasonlítását is lehetővé teszi.

2.1 A funkcionális követelményeknek való megfelelés

F_SCA_1: Minden aláírás-létrehozó rendszer tartalmazzon egy (teljes) aláírás-ellenőrző rendszert is.
Magyarázat: A Marketline integrált aláíró alkalmazás a beérkező dokumentumok és minden általa aláírt dokumentum esetén automatikus aláírás-ellenőrzést végez.
Konklúzió: **megfelel**

F_SDP_1: Minden aláírói dokumentumnak közvetett módon tartalmaznia kell egy tartalom-formátumot, amely meghatározza azokat a részleteket, ahogyan a dokumentumot az ellenőrző számára meg kell jeleníteni, vagy ahogyan fel kell használni.
Magyarázat: A rendszer iDOC XML formátumú aláírandó dokumentumot, valamint az alábbi formátumú csatolt dokumentumokat kezeli: Microsft Word dokumentum (DOC), Microsoft Excel táblázat (XLS), Adobe Acrobat dokumentum (PDF), Microsoft PowerPoint prezetáció (PPT), Zip tömöritett állomány (ZIP), Rar tömöritett állomány (RAR), Egyszerű szövegállomány (TXT), Rtf dokumentum (RTF), Web oldal (HTML), GIF, TIF és JPG formátumú képek.
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 Marketline integrált PKI modulban az aláírói fődokumentum mindig iDOC XML formátumú. Ennek szemantikája nem függ annak megjelenítésétől. Az egyes csatolt dokumentumok megjelenítésének módját a csatolt dokumentum kiterjesztése alapján megállapítható típus határozza meg. A rendszer nem tartalmaz megjelenítő modult.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SDP_3: Amennyiben az aláírói dokumentum szemantikája függ annak megjelenítésétől, akkor az aláírónak elegendő információval kell ellátnia az aláírás ellenőrzőjét a dokumentum pontos megjelenítéséhez.
Magyarázat: A Marketline integrált PKI modulban az aláírói fődokumentum mindig iDOC XML formátumú. Ennek szemantikája nem függ annak megjelenítésétől. Az egyes csatolt dokumentumok megjelenítésének módját a csatolt dokumentum kiterjesztése alapján megállapítható típus határozza meg. A rendszer nem tartalmaz megjelenítő modult.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SDP_4: Az ellenőrzési folyamatok helyesen értelmezzék a F_SDP_1 által megkövetelt információt, illetve ezek alapján egyértelműen és helyesen jelenítsék azt meg az ellenőrző számára.
Magyarázat: A Marketline integrált PKI modul az aláírások ellenőrzését automatizált folyamatként emberi beavatkozás nélkül végzi. Helyesen értelmez, de nem jelenít meg semmit az ellenőrző számára.
Konklúzió: **nem vonatkozik rá a követelmény**

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

az aláíró tanúsítványa,

az aláíró dokumentumának tartalom-formátuma (ha szerepel),

az aláírási szabályzat (ha szerepel),

a kötelezettségvállalás típusa (ha szerepel).

Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként emberi beavatkozás nélkül végzi. Megjelenítő modult nem tartalmaz.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SAV_2: Lehetőséget kell biztosítani az aláíró/ellenőrző számára ahhoz, hogy az aláíráshoz csatolandó/csatolt tanúsítványt átvizsgálja.
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SIC_1: Egy aláírás létrehozása előtt meg kell győződni arról, hogy az aláíró valóban létre kíván-e hozni egy minősített elektronikus aláírást.
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SIC_2: Az aláíró/ellenőrző számára vezérlő funkciók szükségesek, melyen keresztül irányíthatja az aláírási/ellenőrzési folyamatot és az aláírás-alkalmazás tevékenységét.
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SIC_3: Egy elektronikus aláírás létrehozása előtt a biztonságos aláírás-létrehozó eszköznek és az aláírás-létrehozó alkalmazásnak is meg kell győződnie arról, hogy az aláíró a biztonságos aláírás-létrehozó eszköz tulajdonosa (vagy jogosult használója).
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként emberi beavatkozás nélkül végzi és nem használ biztonságos aláíró eszközt .
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 Marketline integrált PKI modul a MultiSigno Pack XML struktúráját használja.
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 MultiSigno elvégzi ezt a feladatot.
Konklúzió: **megfelel**

F_DHC_1: Az aláírás-létrehozó folyamat kiváltása utáni első lépésként végre kell hajtani a lenyomatolást.
Magyarázat: Ezt a MultiSigno felhívására a CSP (Cryptographic Service Provider) elvégzi.
Konklúzió: **megfelel**

F_DHC_2: Második lépéseként végre kell hajtani a lenyomat formattálását (feltöltését).
Magyarázat: Ezt a MultiSigno felhívására a CSP elvégzi.
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: Jelen esetben ez a helyzet, de a BALE helyett az operációs rendszer által védett fájlban van a magánkulcs.
Konklúzió: **nem felel meg**
1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni.
Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.

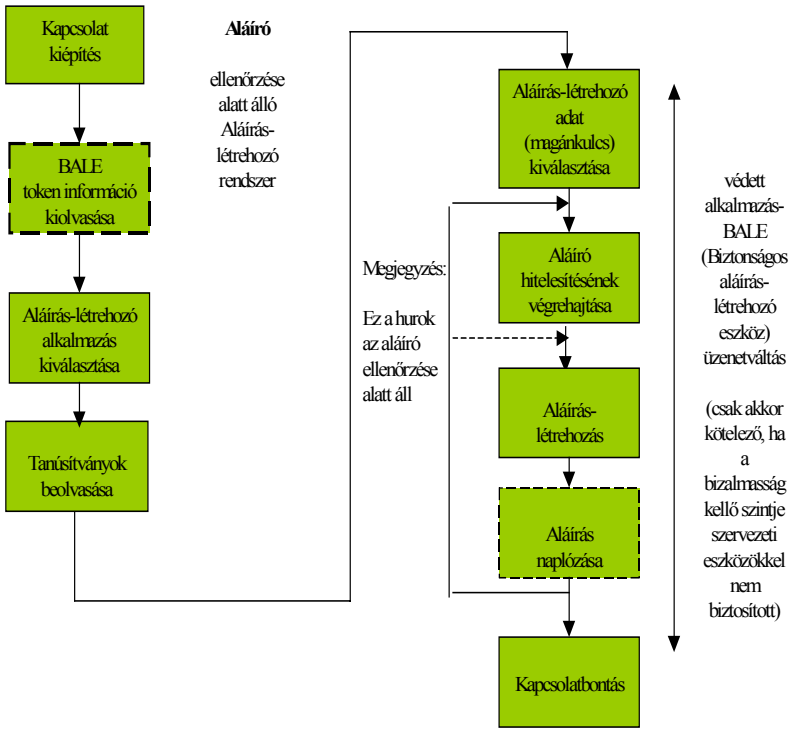
F_SSC_2: Egy szolgáltató ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 2. ábrán[1] jelölt minden szükséges kommunikációt.

Magyarázat: A Marketline integrált PKI modul nem áll egy külső szolgáltató ellenőrzése alatt.

Konklúzió: **nem vonatkozik rá a követelmény**

1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni.

Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.



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

[1] Mivel a követelmény nem vonatkozik az értékelés tárgyára, ezért az ábrát mellőzzük

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

Magyarázat: A Marketline integrált PKI modul fizikai interfészen keresztül kommunikál az aláírást végző intelligens kártyával.

Konklúzió: **megfelel**

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

Magyarázat: A MultiSigno Developer elvileg támogat több-alkalmazásos platformot is, de ilyenkor az aktivizálandó magánkulcshoz tartozó tanúsítványt be kell hozzá előzetesen állítani. Jelen esetben az alkalmazás nem is az intelligens kártyán fut, ezért kiválasztásra sincs szükség.

Konklúzió: **Nem vonatkozik rá a követelmény**

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

Magyarázat: A Marketline integrált PKI rendszerében nincs biztonságos aláírás-létrehozó eszköz, helyette a Windows tanúsítványtárát használja a rendszer. A tanúsítványtár elvileg több tanúsítványt is tartalmazhat. A Marketline integrált aláíró alkalmazás a tanúsítvány kiválasztásakor leellenőrzi, hogy valóban azt használja-e aláírásra, és képes több tanúsítványból is kiválasztani az aláíráshoz szükségeset.

Konklúzió: **megfelel**

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

Magyarázat: A Marketline integrált PKI rendszerében nincs biztonságos aláírás-létrehozó eszköz, helyette a Windows tanúsítványtárát használja a rendszer. A tanúsítványtár elvileg több magánkulcsot is tartalmazhat. Ebből az alkalmazás a paraméterfájlban megadtat, választja ki automatikusan.

Konklúzió: **nem felel meg** (az 1. számú feltétel teljesítése esetén: **Nem vonatkozik rá a követelmény)**

1. számú feltétel: A magánkulcsok és tanúsítványok számítógépre táplálásakor (a Windows 2000 operációs rendszer védett tárába, illetve tanúsítványtárába) a Kulcskezelési szabályzat (V2.0) 5.2 és 6.3 pontjaiban meghatározott szabályokat be kell tartani. A működtetés során folyamatosan biztosítani kell azt is, hogy illetéktelen módon a magánkulcsokat és tanúsítványokat ne cseréljék ki, a tárakat pedig más magánkulccsal, tanúsítvánnyal illetéktelenül ne egészítsék ki.

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: Jelen esetben a fentieket úgy kell értelmezni, hogy az aláíró alkalmazásnak speciális jogosultságot kell adni, hogy hozzáférhessen és aktivizálhassa az aláíró magánkulcsot.
Konklúzió: **megfelel**
F_SSC_8: Az aláírás létrehozó folyamat utolsó lépéseként ki kell számíttatni (a biztonságos aláírás-létrehozó eszköz által megvalósítva) magát az aláírást.
Magyarázat: Ezt a feladatot a MultiSigno (az alapját képező CSP-vel de BALE nélkül) megoldja.
Konklúzió: **megfelel**

F_SSC_9: A befejezett aláírásokat naplózni kell.
Magyarázat: A rendszer mind a sikeres, mind a sikertelen aláírásokat naplózza.
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 Marketline integrált aláíró alkalmazás nem áll egy külső szolgáltató ellenőrzése alatt.
Konklúzió: ***nem vonatkozik rá a követelmény***

F_SDC_1: Lehetővé kell tenni az aláíró számára az aláírói dokumentum létrehozását vagy kiválasztását.
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.
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 Marketline integrált PKI modul a Multisigno Pack XML struktúráját használja.
Konklúzió: **megfelel**

F_SLC_1: Minden létrehozott/ellenőrzött aláírásra egy napló bejegyzés tárolandó.
Magyarázat: A rendszer mind a sikeres, mind a sikertelen aláírásokat naplózza.
Konklúzió: **megfelel**

F_SCPC_1: A hitelesítés-szolgáltatóval való kapcsolat felvételén keresztül képesnek kell lennie az alábbiakra:

- az aláírói tanúsítványok megszerzése,
- az aláírói tanúsítványok állapotának lekérése.

Magyarázat: A rendszerben az aláírásnak mindig része (nem aláírt aláírási tulajdonságként) az aláíró tanúsítványa, ezt ezért nem kell külön lekérdezni. A tanúsítvány visszavonási listát viszont igen, s ezt a Marketline integrált aláíró alkalmazás meg is teszi. (Az OCSP-t a Marketline integrált aláíró alkalmazás nem támogatja.)
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 rendszerben az aláírásnak mindig része (nem aláírt aláírási tulajdonságként) az aláíró tanúsítványa, ezt ezért nem kell külön lekérdezni.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A Tanúsítványok hitelességét a MATÁV hitelesítés-szolgáltató garantálja, a rendszer pedig mindig ellenőrzi.

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 Marketline integrált aláíró alkalmazás az aláírói dokumentumot (elküldendő iDOC dokumentumot) egy külső I/O interfészen keresztül kapja az SAP MM modultól. Ebben egyetlen rejtett rész sem lehet az iDOC XML struktúra miatt. Ugyanakkor a Marketline integrált aláíró alkalmazásnak kell biztosítania azt, hogy egyetlen aláírandó adat összetevőt se cserélhessenek ki aláírás előtt. Ezt a Windows szerveren futó többi alkalmazás irányából az operációs rendszer (W2K) biztosítja, belülről pedig maga a Marketline integrált PKI modul.

Konklúzió: **megfelel**

F_ISV_1: Az érvényesítő adatokat az ellenőrzőnek be kell gyűjtenie, és az aláírási szabályzat minden követelményét teljesítenie kell.

Magyarázat: A rendszer minden ellenőrzés előtt a Pack XML struktúrában lévő CRL-t bemásolja a Windows tanúsítványtárába, illetve ellenőrzi az aláírás dátumával kapcsolatos aláírási szabályzat előírásait.

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 formattált aláírt adat tartalmazza az aláíráskor CRL-t illetve aláírva az aláíró által állított aláírás dátumot.

Konklúzió: **megfelel**

2. számú javaslat: A minősített aláírásokat kezelő rendszerben időbélyegzőt használjanak.

F_USV_1: A kezdeti ellenőrzés során begyűjtött érvényesítő adatok ellenőrzésénél az aláírási szabályzat minden követelményét teljesíteni kell.

Magyarázat: A formattált aláírt adat tartalmazza az aláíráskor CRL-t, illetve aláírva az aláíró által állított aláírás dátumot.

Konklúzió: **megfelel**

Ember által történő ellenőrzés esetén:
F_human_1: ---
F_human_2: ---
F_human_3: ---
F_human_4: ---
F_human_5: ---
F_human_6: ---
Magyarázatok: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúziók: **nem vonatkoznak rájuk a követelmények**

Gépi (automatikus) ellenőrzés esetén:
F_machine_1: Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére és az elektronikus aláírás formátumának meghatározására.
Magyarázat: Ezt a MultiSigno Developer DLL-jeire ró kötelezettséget (amiről a HUNG-T-003/2003 számú tanúsítvány alapján már tudjuk, hogy teljesül).
Konklúzió: **megfelel**

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

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

Magyarázat: Ez a MultiSigno Developer DLL-jeire ró kötelezettséget (amiről a HUNG-T-003/2003 számú tanúsítvány alapján már tudjuk, hogy teljesül).
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: A Marketline integrált aláíró alkalmazás megfelel a rá vonatkozó aláírási szabályzatnak. Ebben az aláírási szabályzatban pedig minden feldolgozási szabály világosan meghatározott.
Konklúzió: **megfelel**

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

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

Magyarázat: Egyedül a CRL érintett, ami szabványos LDAP.
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: Szabványos az aláírás formátuma (PKCS #1) és a tanúsítvány formátuma (X509v3) is.
Konklúzió: **megfelel**

F_principles: A felhasználói (aláírói, aláírás-ellenőrzői) felületek tervezésekor a következő elveket kell figyelembe venni: …….
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: ***nem vonatkozik rá a követelmény***

2.2 A biztonsági követelményeknek való megfelelés

2.2.1 Követelmények az aláírás-létrehozó alkalmazás (SCA) egészére

<u>Az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz közötti megbízható útvonalra vonatkozó követelmények:</u>

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 biztonságkritikus részek forráskód szintű ellenőrzése sem mutatott ki semmilyen tudatos vagy véletlen integritás vesztést.
Konklúzió: **megfelel**

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 biztonságkritikus részek forráskód szintű ellenőrzése sem mutatott ki semmilyen tudatos vagy véletlen integritás vesztést.
Konklúzió: **megfelel**

Bizt_köv3: … Bizt_köv6:
Magyarázat: A 3.-6. követelmények csak a nyilvános aláíró alkalmazásokra vonatkoznak (melyek egy szolgáltató ellenőrzése alatt állnak). A Marketline integrált PKI modul nem ilyen.
Konklúzió: **nem vonatkoznak rá a követelmények**

Bizt_köv7: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy az aláírónak bemutatott aláírandó adat ugyanaz, mint amit az aláíró kiválasztott.
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv8: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy a formattált aláírandó adat és aláírandó adat reprezentáns előállításához felhasznált aláírandó adat komponensek ugyanazok, mint amelyeket az aláírónak bemutattak a bemutatási eljárás során, és amelyeket a felhasználó kiválasztott.
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkozik rá a követelmény**

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

Bizt_köv9: … Bizt_köv10:
Magyarázat: A Marketline integrált PKI modul nem osztott architektúrájú alkalmazás.
Konklúzió: **nem vonatkoznak rájuk a követelmények**

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: Mivel a Marketline integrált PKI modul egy szoftveralkalmazás, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek (operációs rendszer) kell biztosítania.
Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg.**
2. számú feltétel: A Marketline integrált 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.
Megjegyzés: A "védett" környezet biztosításához szükséges 5. számú feltételt és 3. számú javaslatot a 4. fejezet részletezi.

Az aláírandó adatra vonatkozó követelmények

Bizt_köv12: Az aláírandó adatnak tartalmaznia kell egy aláírói dokumentumot. (Egy "üres" dokumentumhoz ne lehessen aláírást előállítani).
Magyarázat: Az automatizmus nem tesz lehetővé üres dokumentum aláírását.
Konklúzió: **megfelel**

Bizt_köv13: Az aláírandó adatnak tartalmaznia kell az aláírónak azt a tanúsítvány-azonosítóját, amely az elektronikus aláírás létrehozásánál a biztonságos aláírás-létrehozó eszköz által felhasznált aláírás-létrehozó adathoz kapcsolódik, s amely az aláíró szándékának megfelel.
Magyarázat: Az aláírással együtt mindig a teljes (hitelesítés-szolgáltató által aláírt) tanúsítvány is átjut, az aláírási szabályzat értelmében. Ezért a tanúsítvány-azonosító külön aláírására nincs szükség.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv14: Az aláírandó adatnak tartalmaznia kell egy hivatkozást az aláírási szabályzatra.
Magyarázat: A szerződés aláírásakor minden felhasználó megismerheti az egyetlen, A Marketline integrált aláíró alkalmazás vevő oldali modul által támogatott aláírási szabályt.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv15: Az aláírandó adatnak tartalmaznia kell a kötelezettségvállalás típus tulajdonságot, ha az aláírási szabályzat egynél több kötelezettségvállalás típust határoz meg.
Magyarázat: A rendszerben nincs kötelezettségvállalás típus.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv16: Ha az alkalmazás vagy az érvényben lévő biztonsági szabályzat egynél több aláírói dokumentum tartalom formátumot enged meg, az aláírandó adatnak tartalmaznia kell az aláírói dokumentum tartalom formátumot.
Magyarázat: A rendszerben csak egy megengedett formátum típus van.
Konklúzió: **nem vonatkozik rá a követelmény**

2.2.2. Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP)

Bizt_köv17, …, Bizt_köv28:
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkoznak rájuk a követelmények**

2.2.3. Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV)

Bizt_köv29, … , Bizt_köv34:
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkoznak rájuk a követelmények**

2.2.4. Követelmények az aláíróval kölcsönható összetevőre (SIC)

Bizt_köv35, …. , Bizt_köv37:
Magyarázat: A Marketline integrált PKI modul az aláírások létrehozását automatizált folyamatként, emberi beavatkozás nélkül végzi.
Konklúzió: **nem vonatkoznak rá a követelmények**

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: Nincs BALE, nincs külön eszköz az aláírót hitelesítő adat megadására sem.
Konklúzió: **nem felel meg**
1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni. Ez biztosítja majd az itt elvárt eszközt is.
Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.

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 magánkulcs aktivizálásához szükséges hitelesítő adat jelenleg a Marketline integrált PKI alkalmazáson kívül kerül megadásra. Ezért ezt a követelményt a hitelesítő adatot fogadó operációs rendszernek kell teljesítenie.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv40: Ha az aláírni szándékozó egy korlátot meghaladó számban helytelen hitelesítő adatot ad meg, akkor az újrapróbálkozást le kell tiltani, egyúttal hibajelzést kell adni az aláíró részére, ha az aláíró hitelesítési módszert már nem blokkolta korábban a biztonságos aláírás-létrehozó eszköz. Az aláírni szándékozó részére egy megfelelő üzenetet kell küldeni.
Magyarázat: A magánkulcs aktivizálásához szükséges hitelesítő adat jelenleg a Marketline integrált aláíró alkalmazáson kívül kerül megadásra. Ezért ezt a követelményt a hitelesítő adatot fogadó operációs rendszernek kell teljesítenie.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv41: Ha az aláírni szándékozó ismételten helytelen hitelesítő adatot ad meg (pl. három egymást követő alkalommal), a biztonságos aláírás-létrehozó eszköznek félbe kell szakítania az aláíró hitelesítését, és erről informálnia kell az aláírás-létrehozó alkalmazást, amelynek az aláíró részére egy megfelelő üzenetet kell küldeni.
Magyarázat: A magánkulcs aktivizálásához szükséges hitelesítő adat jelenleg a Marketline integrált aláíró alkalmazáson kívül kerül megadásra. Ezért ezt a követelményt a hitelesítő adatot fogadó operációs rendszernek kell teljesítenie.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv42: Egy megbízható útvonalat kell biztosítani a PIN/jelszó továbbítására a PIN pad (vagy billentyűzet) és a biztonságos aláírás-létrehozó eszköz között az aláírás-létrehozó alkalmazáson keresztül.
Magyarázat: Nincs BALE, nincs megbízható útvonal sem a PIN kód megadására.
Konklúzió: **nem felel meg**
1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni. Ez biztosítja majd az itt elvárt megbízható útvonalat is.
Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.

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 magánkulcs aktivizálásához szükséges hitelesítő adat a megvalósított rendszerben a magánkulcsot aktivizáló központi oldali aláíró alkalmazást elindító felhasználó bejelentkezési jelszava. Ennek megadása a Marketline integrált PKI modulon kívül kerül megadásra. Ezért ezt a követelményt a felhasználói jelszót fogadó operációs rendszer teljesíti.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv44: A megadott PIN kódot (vagy jelszót) nem szabad kijelezni, bár egy számjegy vagy karakter begépelését vissza kell jelezni egy megfelelő jellel (pl. egy csillag karakterrel), amely nem fedi fel magát a PIN-t (vagy a jelszót).
Magyarázat: A magánkulcs aktivizálásához szükséges hitelesítő adat jelenleg a Marketline integrált aláíró alkalmazáson kívül kerül megadásra. Ezért ezt a követelményt a hitelesítő adatot fogadó operációs rendszernek kell teljesítenie.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv45: Az aláírás-létrehozó alkalmazásnak meg kell követelnie az új PIN kód (jelszó) kétszeri megadását, és ellenőriznie kell ezek azonosságát, mielőtt az új PIN kódot (jelszót) továbbítaná a biztonságos aláírás-létrehozó eszköznek.
Magyarázat: A magánkulcs aktivizálásához szükséges hitelesítő adat jelenleg a Marketline integrált aláíró alkalmazáson kívül kerül megadásra. Ezért ezt a követelményt a hitelesítő adatot fogadó operációs rendszernek kell teljesítenie.
Konklúzió: **nem vonatkozik rá a követelmény**

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

Bizt_köv46,…,Bizt_köv47:
Magyarázat: A Marketline integrált aláíró alkalmazás nem kezel biometrikus hitelesítő adatot.
Konklúzió: **nem vonatkoznak rá a követelmények**

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 Marketline integrált aláíró alkalmazás a MultiSigno Pack XML struktúráját használja.
Konklúzió: **megfelel**

2.2.7. Követelmények az adat lenyomat készítő összetevőre (DHC)

Bizt_köv49: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy “elfogadott” lenyomatoló algoritmus használatát lenyomatolásra.
Magyarázat: A Marketline integrált aláíró alkalmazás által használt MultiSigno Pack.dll az MD5-öt használja.
Konklúzió: **megfelel**

Bizt_köv50: Az aláírás-létrehozó alkalmazásnak biztosítania kell az “emsa-pkcs1-v1_5” elektronikus aláírás input formátum (feltöltési módszer) kizárólagos használatát.
Magyarázat: A Marketline integrált aláíró alkalmazás által használt MultiSigno Pack.dll szabványos feltöltést használ.
Konklúzió: **megfelel**

Bizt_köv51: Az aláírás-létrehozó alkalmazásnak biztosítania kell a helyes aláírandó adat reprezentáns előállítását az elektronikus aláíráshoz.
Magyarázat A Marketline integrált aláíró alkalmazás által használt MultiSigno és a CSP biztosítja ezt.
Konklúzió: **megfelel**

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

Bizt_köv52: …
Magyarázat: Nincs BALE, nincs kommunikációs összetevő sem.
Konklúzió: **nem felel meg**
1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni. Ez esetben biztosíthatóak lesznek az itt elvárt követelmények is.
Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.

Bizt_köv53:…
Magyarázat: Az 53. követelmény csak a vezeték nélküli összeköttetést használó alkalmazásokra vonatkozik. A Marketline integrált PKI modul nem ilyen, ezért ez a követelmény nem vonatozik rá.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv54,…,Bizt_köv55:
Magyarázat: Nincs BALE, nincs kommunikációs összetevő sem.
Konklúzió: **nem felel meg**
1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni. Ez esetben biztosíthatóak lesznek az itt elvárt követelmények is.
Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.

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

Bizt_köv56: ---
Magyarázat: Nincs BALE, nincs hitelesítő összetevő sem.
Konklúzió: **nem felel meg**
1. számú javaslat: a minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni. Ez esetben biztosítható lesz az itt elvárt követelmény is.
Megjegyzés: Fokozott biztonságú aláírások esetén (az 5.2 alfejezetben meghatározott 1. – 5. feltételek teljesítése esetén) elfogadható ez a megoldás is.

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: Mivel a Marketline integrált PKI modul egy szoftver alkalmazás, önállóan nem képes megvédenie saját integritását. Nem lehet feladata a vírusok elleni védelem és a helyreállítás sem. Mindezt a működési környezetnek (operációs rendszer) kell biztosítania.

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

3. számú feltétel: A Marketline integrált 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 (DLL, CSP), valamint***
- ***az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.***

Megjegyzés: A "védett" környezet biztosításához szükséges 5. számú feltételt és 3. számú javaslatot a 4. fejezet részletezi.

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

Magyarázat: Mivel a Marketline integrált PKI modul egy szoftver alkalmazás, önállóan nem képes megvédenie saját integritását. Nem lehet feladata a behatolók elleni védekezés sem. Mindezt a működési környezetnek (operációs rendszer) kell biztosítania.

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

5. számú javaslat: A minősített aláírásokat kezelő rendszerben legalább azt az ellenintézkedést meg kell valósítani, hogy a Marketline integrált aláíró alkalmazás ellenőrizze le az általa meghívott függvénytár (dll) integritását és hitelességét.

4. számú feltétel: A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva hogy behatolók elrontsák ezt.

Megjegyzés: A "védett" környezet biztosításához szükséges 5. számú feltételt és 3. számú javaslatot a 4. fejezet részletezi.

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 aláíró alkalmazás összes eleme előre telepített.

Konklúzió: **nem vonatkozik rá a követelmény**

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

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

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

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

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

Megjegyzés: A "védett" környezet biztosításához szükséges 5. számú feltételt és 3. számú javaslatot a 4. fejezet részletezi.

3. A Marketline integrált PKI modul megfelelése a követelményeknek

3.1 A Marketline integrált PKI modul megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	**megfelel**
F_SDP_2	nem vonatkozik rá a követelmény
F_SDP_3	nem vonatkozik rá a követelmény
F_SDP_4	nem vonatkozik rá a követelmény
F_SAV_1	nem vonatkozik rá a követelmény
F_SAV_2	nem vonatkozik rá a követelmény
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 felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
F_SSC_2	nem vonatkozik rá a követelmény
F_SSC_3	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
F_SSC_4	nem vonatkozik rá a követelmény
F_SSC_5	**megfelel**
F_SSC_6	**nem felel meg** (az 1. számú feltétel teljesítése esetén: **Nem vonatkozik rá a követelmény**)
F_SSC_7	**megfelel**
F_SSC_8	**megfelel**
F_SSC_9	**megfelel**
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	nem vonatkozik rá a követelmény
F_SDOC_1	**megfelel**
F_SLC_1	**megfelel**
F_SCPC_1	**megfelel**
F_I/O_1	nem vonatkozik rá a követelmény
F_I/O_2	**megfelel**
F_I/O_3	**megfelel**
F_ISV_1	**megfelel**
F_ISV_2	**megfelel**
F_USV_1	**megfelel**
F_human_1	nem vonatkozik rá a követelmény
F_human_2	nem vonatkozik rá a követelmény
F_human_3	nem vonatkozik rá a követelmény
F_human_4	nem vonatkozik rá a követelmény
F_human_5	nem vonatkozik rá a követelmény
F_human_6	nem vonatkozik rá a követelmény
F_machine_1	**megfelel**
F_machine_2	**megfelel**
F_general_1	**megfelel**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	nem vonatkozik rá a követelmény

3.2 A Marketline integrált aláíró alkalmazás megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	**megfelel**
Bizt_köv2	**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	nem vonatkozik rá a követelmény
Bizt_köv8	nem vonatkozik rá a követelmény
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
Bizt_köv12	**megfelel**
Bizt_köv13	nem vonatkozik rá a követelmény
…….	…….
Bizt_köv37	nem vonatkozik rá a követelmény
Bizt_köv38	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv39	nem vonatkozik rá a követelmény
Bizt_köv40	nem vonatkozik rá a követelmény
Bizt_köv41	nem vonatkozik rá a követelmény
Bizt_köv42	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv43	nem vonatkozik rá a követelmény
Bizt_köv44	nem vonatkozik rá a követelmény
Bizt_köv45	nem vonatkozik rá a követelmény
Bizt_köv46	nem vonatkozik rá a követelmény
Bizt_köv47	nem vonatkozik rá a követelmény
Bizt_köv48	**megfelel**
Bizt_köv49	**megfelel**
Bizt_köv50	**megfelel**
Bizt_köv51	**megfelel**
Bizt_köv52	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv53	nem vonatkozik rá a követelmény
Bizt_köv54	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv55	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv56	**nem felel meg** /de az 1. – 5. feltételek teljesítése esetén fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv57	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
Bizt_köv58	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
Bizt_köv59	nem vonatkozik rá a követelmény
Bizt_köv60	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**

4. A Tanúsítási jelentés eredménye, érvényességi feltételei

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltétel teljesülése esetén a Marketline integrált PKI modul (mint aláíró alkalmazás) alkalmas fokozott biztonságú aláírások létrehozására és ellenőrzésére (a feltételek nem a megvalósított aláíró alkalmazásra, hanem annak telepítésére, illetve környezetére vonatkoznak).

Ennek alapján megállapítható az is, hogy **a rendszerben csak hiteles, az aláíró cég nevében hivatalosan eljáró személy érvényes aláírásával ellátott dokumentumok mehetnek át** (a szállítói oldalon sikeres ellenőrzési eredményt biztosítva).

4.2 Érvényességi feltételek

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a Marketline integrált aláíró alkalmazás által kezelt aláírások fokozott biztonságához.

1. számú feltétel
A magánkulcsok és tanúsítványok számítógépre táplálásakor (a Windows 2000 operációs rendszer védett tárába, illetve tanúsítványtárába) a Kulcskezelési szabályzat (V2.0) 5.2 és 6.3 pontjaiban meghatározott szabályokat be kell tartani. A működtetés során folyamatosan biztosítani kell azt is, hogy illetéktelen módon a magánkulcsokat és tanúsítványokat ne cseréljék ki, a tárakat pedig más magánkulccsal, tanúsítvánnyal illetéktelenül ne egészítsék ki.

Érintett funkcionális követelmény: F_SSC_6

2. számú feltétel
A Marketline integrált 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

3. számú feltétel
A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

- vírusok ne ronthassák el a Marketline integrált aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket (DLL, CSP), valamint
- az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

Érintett biztonsági követelmény: Bizt_köv57

4. számú feltétel
A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

Érintett biztonsági követelmény: Bizt_köv58

5. számú feltétel
A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy **biztonságos területen** valósítsák meg.
/lásd még a 3. számú javaslatot is erről a kérdésről/

Érintett biztonsági követelmény: Bizt_köv60

4.3 Javaslatok

Az alábbi javaslatok megfogadása szükséges ahhoz, hogy a rendszer minősített aláírások létrehozására és ellenőrzésére is alkalmassá váljon.

1. számú javaslat
A minősített aláírást megvalósító rendszerben a magánkulcsot egy biztonságos aláírás-létrehozó eszközben (ami lehet egy biztonságos aláírás-létrehozó eszközként is tanúsított hardver kriptográfiai modul) kell kezelni.

Érintett funkcionális követelmények:	F_SSC_1, F_SSC_3
Érintett biztonsági követelmények:	Bizt_köv38, Bizt_köv42, Bizt_köv52, Bizt_köv54, Bizt_köv55, Bizt_köv56

2. számú javaslat
Minősített rendszer esetén időbélyegzőt kell használni.

Érintett funkcionális követelmény: F_ISV-2

3. számú javaslat

A Marketline integrált aláíró alkalmazás számára az alábbiakkal lehet biztonságos területet megvalósítani, a 2. – 5. számú feltételeket teljesíteni:

1. A Marketline integrált aláíró alkalmazást futtató számítógépet fizikailag védett környezetben kell elhelyezni.
2. A fizikai hozzáférést korlátozni kell. Csak az arra előztessen feljogosított személy férhessen közvetlenül a számítógéphez.
3. A fizikai hozzáférést regisztrálni kell. A fizikai hozzáférést (pl. egy beléptető rendszer segítségével) letagadhatatlanná kell tenni.
4. A számítógépen futó Windows 2000 Server installációja ne upgrade legyen. (Mások az alap biztonsági beállítások).
5. A számítógép a hálózat felé szolgatatást ne nyújtson. A nem szükséges szolgáltatásokat le kell tiltani (pl.: IIS, FTP, NNTP SMTP, Server, SNMP).

6. Át kell nevezni az adminisztrátor felhasználói fiókot.
7. A Guest felhasználó tiltott legyen.
8. A felhasználók csak erős jelszót használhassanak.
9. Felhasználói fiókzárolást alkalmazni kell.
10. Meg kell vonni a Program Nyomon követés felhasználói jogot minden felhasználótól.
11. A számítógép ne tartalmazzon hordozható adathordozó írására alkalmas eszközt. (floppy, USB Drive).
12. A merevlemez NTFS fájl rendszert használjon.
13. A fájl hozzáférés beállításokat a default server template használatával kell beállítani.
14. Tiltani kell a registry hozzáférést távoli gépről.
15. Az aláíró magánkulcsa ne legyen exportálható.
16. Az operációs rendszer naplózza:
    a. A sikeres illetve sikertelen bejelentkezéseket,
    b. A sikeres illetve sikertelen fiókkezelést
    c. A sikeres illetve sikertelen rendszereseményeket.
17. A napló fájlokat archiválni kell.
18. Antivírus programot kell alkalmazni, illetve folyamatosan frissíteni kell ennek vírus adatbázisát.
19. Rendszeresen ellenőrizni kell a Microsoft honlapján a kiadott javító csomagokat, szükség esetén installálni kell azokat.
20. Rendszeresen ellenőrizni kell a rendszert a Microsoft által kiadott Baseline Security Analyzer segítségével. A létrejött report fájlt archiválni kell.

Érintett biztonsági követelmények: Bizt_köv11, Bizt_köv57, Bizt_köv58, Bizt_köv60

5. A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

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

A fejlesztőktől független ellenőrző vizsgálatról értékelési jelentések készültek (lásd 7.2.2 alatt) Jelen tanúsítási jelentés alapvetően az ezekben megfogalmazott és dokumentált eredményekre épül.

A fejlesztőktől független ellenőrzés alábbi vizsgálatokat jelentették:

Az ellenőrző vizsgálat a Marketline integrált aláíró alkalmazás biztonsági viselkedésének megértése érdekében elemezte a biztonsági funkciókat, felhasználva ehhez különböző fejlesztői dokumentációkat.

Ezeken kívül:

- funkcionális teszteket végzett,
- áttekintette a fejlesztők által végzett tesztelést, elemezte ennek teljes körűségét,
- a fejlesztőktől független minta tesztelést végzett,
- megvizsgálta a legfontosabb biztonságkritikus forrás kód részleteket,
- értékelte az alkalmazott biztonsági mechanizmusok erősségét.

6. A Marketline integrált aláíró alkalmazás biztonsági funkcióinak értékelt erőssége

Még ha az értékelés tárgyának (jelen esetben a Marketline integrált aláíró alkalmazásnak) a biztonsági funkcióit nem is lehet megkerülni, kiiktatni vagy tönkretenni, akkor is lehet lehetőség kijátszani azokat, ha a mögöttes biztonsági mechanizmusok sebezhetőek. E funkciók biztonsági viselkedése minősíthető a mechanizmusok biztonsági viselkedésének mennyiségi vagy statisztikai alapú elemzési eredményeinek felhasználásával és az ilyen mechanizmusok legyőzésére vonatkozó erőfeszítések segítségével.

A biztonsági funkciókat a biztonsági mechanizmusok valósítják meg. Például egy jelszókezelő mechanizmus az azonosítás és hitelesítés biztonsági funkciók megvalósításában használható fel.

A biztonsági funkciók erősségének elemzése a biztonsági mechanizmusok szintjén zajlott.

/A biztonsági mechanizmus erőssége értékelése keretében azt vizsgálták meg, hogy az értékelés tárgya által megvalósított biztonsági mechanizmusok mennyire képesek ellenállni egy képzett támadó közvetlen támadásának, illetve a támadónak milyen szintű erőforrásokra szaktudásra és lehetőségekre van szüksége a sikeres támadás megvalósításhoz. Itt annak mérésről van szó, hogy a mechanizmus mennyire képes a védelem megkerülése mellett a közvetlen támadásokat is megakadályozni.

A biztonsági mechanizmus erősségét alap, közepes és magas szintű minősítésekkel osztályozzák.

- *Alap szintű* a védelmi mechanizmus erőssége, ha bizonyíthatóan védelmet nyújt a biztonság véletlen megsértése ellen, de kellő ismeretekkel rendelkező támadók hatálytalaníthatják
- *Közepes szintű* a védelmi mechanizmus erőssége, ha bizonyíthatóan védelmet nyújt korlátozott erőforrással és lehetőséggel rendelkező támadók ellen
- *Magas szintű* a védelmi mechanizmus erőssége, ha a védelmet bizonyíthatóan csak olyan támadó képes hatálytalanítani, aki magas szintű szaktudással, erőforrással és lehetőséggel rendelkezik. Ilyen erősségű védelmi mechanizmus mellett a sikeres támadás valószínűsége rendkívül csekély./

A biztonsági mechanizmusok erősségének elemzése az alábbi eredményt adta:

A biztonsági funkciók erőssége: **közepes szintű**

7. A tanúsításhoz figyelembe vett dokumentumok

7.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign; Area G1, 14170 munkacsoport egyezmény: Security Requirements for Signature Creation Systems

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

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

7.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

7.2.1 A tanúsításhoz figyelembe vett egyéb fejlesztői dokumentumok

Kérelem a tanúsítás elvégzésére

Kérdőív a tanúsítás kérelmezéséhez

7.2.2 A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés a „PKI Projekt” keretében fejlesztett, csatolt dokumentumok kezelésével kiegészített, központi oldali elektronikus aláírási alkalmazás összetevőre /2003. 06.24/

Értékelési jelentés kiegészítés a „PKI Projekt” keretében fejlesztett, csatolt dokumentumok kezelésével kiegészített, /hitelesítés-szolgáltató váltás miatt módosított/ központi oldali elektronikus aláírási alkalmazás összetevőre /2004.01.12/

8. Rövidítések

API	Application Programming Interface
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DHC	Data Hashing Component
DLL	Dynamic Link Library
DTBS	Data To Be Signed
DTBSF	DTBS Formatter
EAL	Evaluation Assurance Level
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastucture
PIN	Personal Identification Number
SAC	Signer's Authentication Component
SAV	Signature Attribute Viewer
SCA	Signature Creation Application
SDC	Signer's Document Composer
SDOC	Signed Data Object Composer
SDP	Signer's Document Presenter
SIC	Signer's Interaction Component
SLC	Signature Logging Component
SSA	SSCD/SCA Communicator Authenticator
SSC	SSCD/SCA Communicator
SSCD	Secure Signature Creation Device
TJ	Tanúsítási jelentés