Tanúsítási jelentés

Hung-TJ-016-2004

a
Marketline
webes aláíró alkalmazásról

/Axelero Rt./

Tartalom

1. A Marketline webes PKI modul legfontosabb tulajdonságainak összefoglalása

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

1.1 Architektúra

A Marketline webes PKI modul egy HTML alapú kliens alkalmazás, ami aktív Java appleteket és Javascripteket tartalmaz.

Futtatási környezetként Internet Expoler 5.5 böngészőt és ezt futtatni képes Microsoft Windows operációs rendszert követel meg.

Az elektronikus aláíró és aláírás ellenőrzési funkciókat a MultiSigno Developer függvény készletének felhasználásával valósítja meg, amit Java illesztőfelületen keresztül ér el.

Az aláíró és aláírás ellenőrző appletek elektronikus aláírással vannak ellátva.

Az aláírás-létrehozó adat (magánkulcs) külső eszközön (intelligens kártyán) található.

Az aláíró tanúsítványát a Matáv Rt. hitelesítés-szolgáltató hitelesíti.

Az aláírások ellenőrzéséhez a Matáv Rt. hitelesítés-szolgáltató szolgáltat CRL-t, 24 óránkénti frissítéssel.

1.2 Tulajdonságok

A Marketline webes PKI modul külső eszközt (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 aláírás dátuma 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 webes PKI modul tanúsítványtárnak az operációs rendszer tanúsítványtárát használja.

A Marketline webes PKI modul saját oldalán naplófunkciókat nem valósít meg.

Az aláírás kötelezettségvállalást jelent miszerint az aláíró 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 webes PKI modul, mint aláíró alkalmazás.

A tanúsítás során feltételeztük, hogy az alábbi (a Marketline webes 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 webes 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 kliens oldali modul (mint aláíró alkalmazás) megfelel-e az adott követelménynek.

Minthogy a Marketline webes 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 értékelését is a minősített rendszerek követelményeinek való megfelelőség vizsgálatával végeztük el.
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 webes aláíró alkalmazás 4 folyamatából három (bemenet ellenőrzés, felhasználói aláírás-ellenőrzés, kimenet ellenőrzés) végez automatikus aláírás-ellenőrzést, és minden általa aláírt dokumentum automatikusan ellenőrzésre is kerül (a felhasználói aláírás-ellenőrzés, illetve a kimenet ellenőrzés folyamatában).
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 valamint, Microsft Word documentumot (DOC),Microsoft Excel táblázatot (XLS), Adobe Acrobat dokumentumot (PDF), Microsoft PowerPoint prezetációt (PPT), Zip tömöritett állományokat (ZIP), Rar tömöritett állományokat (RAR), Egyszerű szövegállományokat (TXT), Rtf dokumentumokat (RTF), Web oldalakat (HTML), GIF, TIF és JPG formátumú képeket mint csatolt dokumentumok.formátumot kezel.
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 webes PKI modulban az aláírói fődokumentum mindig iDOC XML formátumú. A csatolt állományok leírását DOCMAS.xml tartalmazza. Ezek szemantikája nem függ annak megjelenítésétől. Az egyes csatolt dokumentumok megjelenítésének módját a csatolt dokumentum kiterjesztése alapján megállapítható típus határozza meg.

Konklúzió: **megfelel**

Megjegyzés: Minősített rendszer esetén nem elegendő a kiterjesztésre hagyatkozni a csatolt dokumentumok megjelenítésének módját illetően. A file formátumot a belső felépítés alapján kell meghatározni.

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 webes PKI modulban az aláírói fődokumentum mindig iDOC XML formátumú. A csatolt állományok leírását DOCMAS.xml tartalmazza. Ezek szemantikája nem függ annak megjelenítésétől. A egyes csatolt dokumentumok megjelenítésének módját a csatolt dokumentum kiterjesztése alapján megállapítható típus határozza meg.

Konklúzió: **megfelel**

Megjegyzés: Minősített rendszer esetén nem elegendő a kiterjesztésre hagyatkozni a csatolt dokumentumok megjelenítésének módját illetően. A file formátumot a belső felépítés alapján kell meghatározni.

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 Marketline webes PKI modul helyesen jeleníti meg az iDOC XML, illetve a DOCMAS.XML dokumentumot, a csatolt állományokat külső megjelenítővel jeleníti meg.

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 Marketline webes PKI modul aláírási szabályzata az alábbi aláírási tulajdonságokat kezeli:

az aláíró tanúsítványa,

az aláírás ideje.

A Marketline webes aláíró alkalmazás (a felhasználói aláírás-ellenőrzés folyamatában) mindkét aláírási tulajdonságot megjeleníti.

Konklúzió: **megfelel**

F_SAV_2: Lehetőséget kell biztosítani az aláíró/ellenőrző számára ahhoz, hogy az aláíráshoz csatolandó/csatolt tanúsítványt átvizsgálja.
Magyarázat: A Marketline webes PKI modul a Windows tanúsítvány megjelenítőjét használva biztosít lehetőséget a tanúsítvány átvizsgálására
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 Marketline webes PKI modulban az aláírás kiváltásához többszörös felhasználói aktivitás kell. Aláírás gomb megnyomása, aláírási szándék megerősítése, külső eszköz PIN kódjának megadása
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: Az aláírás kiváltására illetve az aláírás ellenőrzésére megfelelő felület áll a felhasználó rendelkezésére.
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 külső eszköz PIN kóddal védett, amit csak a tanúsítvány tulajdonosa ismer. A PIN kódot a Marketline webes PKI modul minden aláíráshoz külön bekéri.
Konklúzió: **megfelel**

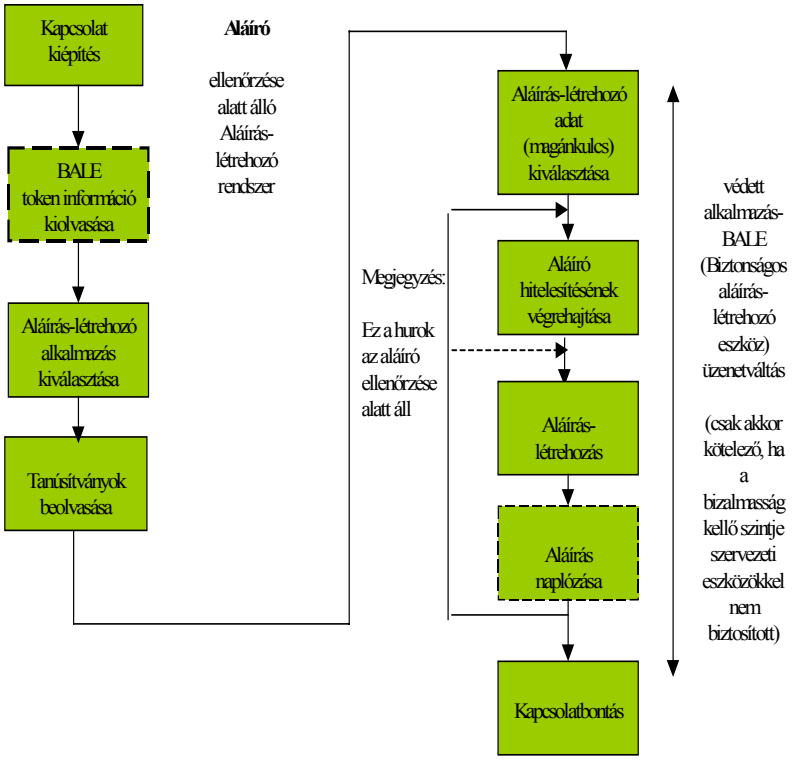
F_DTBSF_1: Ki kell alakítani a szabványos formattált aláírandó adatot az aláíró dokumentumából, az aláírási tulajdonságok felhasználásával.
Magyarázat: A Marketline webes PKI modul a MultiSigno Pack XML struktúráját használja.
Konklúzió: **megfelel**

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: Ezt a MultiSigno elvégzi.
Konklúzió: **megfelel**

F_DHC_1: Az aláírás-létrehozó folyamat kiváltása utáni első lépésként végre kell hajtani a lenyomatolást.
Magyarázat: Ezt a MultiSigno 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 az 1. ábrán jelölt minden szükséges kommunikációt.
Magyarázat: Ezt a MultiSigno végzi.
Konklúzió: **nem felel meg**
Magyarázat: Az alkalmazást futtató környezet (Internet Explorer böngésző) indítása előtt kell az intelligens kártyát az olvasóba behelyezni. Az alkalmazás az indítás után bekövetkező kártyacserét nem érzékeli.
1. számú javaslat: a kártyaolvasóba helyezett intelligens kártya lecserélését a Marketline webes PKI modulban következő verziója automatikusan kezelje le.



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 webes PKI modul nem egy szolgáltató ellenőrzése alatt álló aláíró rendszer.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A biztonságos aláírás-létrehozó eszköz felé soros és/vagy USB csatlakozás van.

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 eszközalkalmazásnak 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: Csak egy tanúsítványt tartalmaz az eszköz. Ennek ellenére mivel a Windows tanúsítványtárát használja a rendszer, lehetnek más nem külső eszközön tárolt tanúsítványok is a rendszerben. A választás lehetséges.

Konklúzió: **megfelel**

Megjegyzés: Kártyacsere esetén az alkalmazás futtató környezetet újra kell indítani.

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: Csak egy magánkulcsot tartalmaz az eszköz. Ennek ellenére mivel a Windows tanúsítványtárát használja a rendszer, lehetnek más nem külső eszközön tárolt tanúsítványok is a rendszerben. A választás lehetséges.

Konklúzió: **megfelel**

Megjegyzés: Kártyacsere esetén az alkalmazást, futtató környezetet újra kell indítani.

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

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: Ezt a MultiSigno DLL – CSP (Cryptographic Service Provider) és a biztonságos aláírás-létrehozó eszköz közösen elvégzik.
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 és a biztonságos aláírás-létrehozó eszközzel) megoldja.
Konklúzió: **megfelel**

F_SSC_9: A befejezett aláírásokat naplózni kell.
Magyarázat: A rendszer kliens oldalon nem naplóz
Konklúzió: **nem felel meg** (**rendszer szinten 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 webes PKI modul nem egy szolgáltató ellenőrzése alatt álló aláíró rendszer.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SDC_1: Lehetővé kell tenni az aláíró számára az aláírói dokumentum létrehozását vagy kiválasztását.
Magyarázat: A Marketline webes PKI modul az ajánlat iDOC dokumentumot elkészíti. A csatolt dokumentumok a filerendszerből kiválaszthatók, (csak az engedélyezett kiterjesztésűek) a hozzátartozó DOCMAS.XML-t szintén a rendszer állítja össze. Az így összeállt aláírói dokumentumot a modul felkínálja aláírásra.
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 Marketline webes PKI modul a MultiSigno Pack XML struktúráját használja.
Konklúzió: **megfelel**

F_SLC_1: Minden létrehozott/ellenőrzött aláírásra egy naplóbejegyzés tárolandó.
Magyarázat: A rendszer kliens oldalon nem naplóz.
Konklúzió: **nem felel meg** (**rendszer szinten 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 rendszerre vonatkozó aláírási szabályzat alapján az aláírói tanúsítványok az aláírt dokumentumban megtalálhatóak, azt nem kell külön megszerezni. Ugyanezen aláírási szabályzat értelmében az aláíró alkalmazást támogató Matáv tanúsítvány visszavonási listákat (CRL) elérhetővé tesz, on-line tanúsítvány állapotlekérdezést nem. Ezért a fenti követelmény arra szűkül, hogy a hitelesítés-szolgáltatóval való kapcsolat felvételén keresztül képesnek kell lennie a tanúsítvány visszavonási listák letöltésére. Ez teljesül.

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 rendszerre vonatkozó aláírási szabályzat alapján:

aláírás-létrehozáshoz mindig jelen van a szükséges tanúsítvány (az aláírás-létrehozó eszközön),

aláírás-ellenőrzéshez az aláírói tanúsítványok mindig megtalálhatóak az aláírt dokumentumban.

Ezért tanúsítványok megszerzésére nincs szükség.

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 garantálja, és a rendszer 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 webes aláíró alkalmazás az aláírói dokumentumot (elküldendő iDOC dokumentumot) saját maga állítja elő. Ebben egyetlen rejtett rész sem lehet az iDOC XML struktúra miatt. A csatolt állományokat a filerendszerből olvassa be. A Marketline webes aláíró alkalmazásnak biztosítania kell azt, hogy egyetlen aláírandó adat összetevőt se cserélhessenek ki aláírás előtt.

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, az aláíró tanúsítványát illetve aláírva az aláíró által állított aláírás dátumot.
Konklúzió: **megfelel**
2. számú javaslat: Minősített rendszer esetén időbélyegzőt kell használni.

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: 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. [2]
Magyarázat: Eszköz van, csak egy aláírást támogat a rendszer.
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 súgójában link van az aláírási szabályzatra így on-line megnézhető.
Konklúzió: **megfelel**

F_human_3: A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az "Ami megjelenik, azt írták alá." követelményt. Ha valamilyen okból az aláírói dokumentum nem jeleníthető meg pontosan a megfelelő módon, akkor ezt a felhasználói interfésznek világosan jeleznie kell.
Magyarázat: Az aláírandó iDOC dokumentumot és annak ember által értelmezhetőbb kivonatát is megmutatja a rendszer. A csatolt dokumentumokat külső megjelenítő segítségével mutatja meg. Azoknál a file tipusoknál, amelyek aktív kódot tartalmazhatnak a megjelenítés előtt figyelmeztet.
Konklúzió: **megfelel**

[2] A Marketline webes PKI modul nem támogat többszörös aláírást, ezért a követelmény második része nem vonatkozik rá.

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 befejezetlen ellenőrzés csak akkor lehetséges ha a Matáv tanúsítványa nem található a tanúsítványtárban.
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: Ha a CRL nem elérhető, azaz megsérült az elektronikus dokumentum, a rendszer hiba üzenetet küld.
Konklúzió: **megfelel**

F_human_6: A felhasználói interfészekre teljesüljenek az F_principles egyszerűségre és hibamentességre vonatkozó speciális elvárásai.
Magyarázat: A speciális elvárások teljesülnek.
Konklúzió: **megfelel**

Gépi (automatikus) ellenőrzés esetén:
Az automatizált feldolgozás esetében alkalmazói program interfészek (API-k) használhatók. Bár az ilyen interfészek kialakításának többféle módja van, ezeket két csoportba lehet sorolni:

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

F_machine_1: Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére és az elektronikus aláírás formátumának meghatározására.
Amennyiben az aláírási szabályzat explicit, akkor a szabályzat azonosítóját magából az elektronikus aláírásból kell kinyerni az 1-es típusú API-jainak felhasználásával[3].
Magyarázat: Ez a MultiSigno Developer DLL-jeire ró kötelezettséget (amiről a HUNG-T-003/2003 számú tanúsítvány alapján már tudjuk, hogy teljesül).
Konklúzió: **megfelel**

[3] A Marketline webes PKI modul nem céloz meg explicit aláírási szabályzat automatizált feldolgozását, ezért a követelmény második része nem vonatkozik rá.

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

- 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 fenti elvárások lényegi elemei teljesülnek.
Konklúzió: **megfelel**

2.2 A biztonsági követelményeknek való megfelelés

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 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 webes aláíró alkalmazás 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: Az aláírandó iDOC dokumentumot és annak ember által értelmezhetőbb kivonatát is megmutatja a rendszer. A csatolt állományok esetén külső megjelenítőt használ.

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 biztonságkritikus részek forráskód szintű ellenőrzése sem mutatott ki semmilyen tudatos vagy véletlen integritás vesztést.

Konklúzió: **megfelel**

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

Bizt_köv9, … , Bizt_köv10:
Magyarázat: A Marketline webes aláíró alkalmazás nem osztott architektúrájú alkalmazás.
Konklúzió: **nem vonatkoznak rá a követelmények**

A nem megbízható folyamatokból/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 Marketline webes aláíró alkalmazás egy szoftver alkalmazás, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek (operációs rendszer) kell biztosítania.
Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg.**
1. számú feltétel: A Marketline webes 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 4. számú javaslatot az 5 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: A felhasználói felületen nem lehet aláírást kiváltani kiválasztott dokumentum nélkül.
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.
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 a Marketline webes aláíró alkalmazás által támogatott egyetlen 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 Marketline webes aláíró alkalmazás nem kezel kötelezettségvállalás típust.

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: Fődokumentumként iDOC XML dokumentum formátum megengedett. A csatolt dokumentumok formátumát a DOCMAS.xml-ben tárolt file-név kiterjesztése határozza meg.

Konklúzió: **megfelel**

Megjegyzés: Minősített rendszer esetén nem elegendő a kiterjesztésre hagyatkozni a csatolt dokumentumok megjelenítésének módját illetően. A file formátumot a belső felépítés alapján kell meghatározni.

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.

Magyarázat: Fődokumentumként iDOC XML dokumentum formátum megengedett. A csatolt állományok lehetséges formátumait az aláírási szabályzat tartalmazza

Konklúzió: **megfelel**

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

Magyarázat: A Marketline webes aláíró alkalmazás központi modulja ellenőrzi az iDOC formátumát és csak abban az esetben teszi elérhetővé a kliens számára, ha nincs formátum probléma. A nem elfogadott formátumú csatolt file-okat nem engedi kiválasztani a modul.

Konklúzió: **megfelel**

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

Magyarázat: Fődokumentumként iDOC XML dokumentum formátum megengedett. A csatolt állományok lehetséges formátumait az aláírási szabályzat tartalmazza.

Konklúzió: **megfelel**

Bizt_köv20: A használati útmutatóban jelezni kell, hogy milyen lehetséges következménnyel jár, ha az aláíró tévesen választja ki a tartalom formátumot.
Magyarázat: A rendszer nem teszi lehetővé, hogy nem megengedett file formátumot csatoljon.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv21: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha olyan aláírói dokumentumot kíván aláírni, amelynek tartalom formátumát nem támogatja.
Magyarázat: A rendszer nem teszi lehetővé, hogy nem megengedett file formátumot csatoljon.
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 biztonságkritikus részek forráskód szintű ellenőrzése sem mutatott ki semmilyen tudatos vagy véletlen eltérést a megmutatott és a felhasznált dokumentumok között.
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).
Magyarázat: Aláírt aláírási jellemző az aláírás dátuma, és ez megjelenítésre kerül.
Konklúzió: **megfelel**

Bizt_köv24: Az aláíró dokumentumát megjelenítő összetevőnek nem szabad lehetővé tennie az aláíró számára, hogy az aláírói dokumentum bármely részét megváltoztassa.
Magyarázat: A különböző ajánlatokat és egyéb adatokat a felhasználó egy másik appleten keresztül adja meg a rendszernek. Aláíráskor már csak ellenőrizheti az elkészült iDOC XML adattartalmát.
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.
Magyarázat:A Marketline webes aláíró alkalmazás aláírás előtt megjeleníti a teljes iDOC XML dokumentumot. A iDOC kivonatoló csak segítő eszköz a felhasználó számára. A csatolt dokumentumokat külső megjelenítővel lehet megnézni.
Konklúzió: **megfelel**

Az aláíró dokumentumára vonatkozó egyértelműségi követelmény:

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

Magyarázat: Fődokumentumként iDOC XML dokumentum formátum megengedett. A csatolt dokumentumok formátumát a DOCMAS.xml-ben tárolt file-név kiterjesztése határozza meg.

Konklúzió: **megfelel**

Megjegyzés: Minősített rendszer esetén nem elegendő a kiterjesztésre hagyatkozni a csatolt dokumentumok megjelenítésének módját illetően. A file formátumot a belső felépítés alapján kell meghatározni.

A nem megjelenítés-érzékeny aláírói dokumentumokra vonatkozó követelmény:

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

Magyarázat: Fődokumentumként iDOC XML dokumentum formátum megengedett. A csatolt dokumentumok formátumát a DOCMAS.xml-ben tárolt file-név kiterjesztése határozza meg.

Konklúzió: **megfelel**

Megjegyzés: Minősített rendszer esetén nem elegendő a kiterjesztésre hagyatkozni a csatolt dokumentumok megjelenítésének módját illetően. A file formátumot a belső felépítés alapján kell meghatározni.

A rejtett szövegre és aktív kódra vonatkozó követelmény:

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

Magyarázat: Fődokumentumként iDOC XML dokumentum formátum megengedett. A csatolt dokumentumok formátumát a DOCMAS.xml-ben tárolt file-név kiterjesztése határozza meg. A rendszernek paraméterként megadható, hogy mely file formátumok tartalmazhatnak aktív kódot.

Konklúzió: **megfelel**

Megjegyzés: Minősített rendszer esetén nem elegendő a kiterjesztésre hagyatkozni a csatolt dokumentumok megjelenítésének módját illetően. A file formátumot a belső felépítés alapján kell meghatározni.

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.

Magyarázat: Lehetőség van az aláíró tanúsítvány megjelenítésére. A képernyő tartalmazza az aláírás dátumát.

*Konklúzió: **megfelel***

Bizt_köv30: Az aláírás tulajdonságokat megjelenítő folyamatnak biztosítania kell, hogy az aláírónak megjelenített aláírás tulajdonság ugyanaz, mint ami az aláírás folyamatában aláírásra kerül majd, és amit az aláíró kiválasztott az aláíráshoz.
Magyarázat: A rendszerdátum, mint aláírt aláírási tulajdonság kerül bele az elektronikus dokumentumba..
Konklúzió: **megfelel**

Bizt_köv31: Az aláírás tulajdonságok sértetlenségét és hitelességét meg kell védeni.
Magyarázat: Az aláírás dátuma aláírt aláírási tulajdonság.
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.
Magyarázat: Az aláírási tulajdonságok az aláíró tanúsítvány, az aláíráskor érvényes CRL, illetve az aláírás dátuma. Ezekben sem rejtett szövegek sem aktív kódrészek nincsenek.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv33: Az aláírás tulajdonság megjelenítő folyamatnak figyelmeztetnie kell az aláírót bármely, az aláírás tulajdonságokba beágyazott rejtett vagy aktív komponens (pl. word processzor makró) jelenlétére. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.
Magyarázat: Az aláírási tulajdonságok az aláíró tanúsítvány, az aláíráskor érvényes CRL, illetve az aláírás dátuma. Ezekben sem rejtett szövegek sem aktív kódrészek nincsenek.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv34: Az aláírás tulajdonság megjelenítő összetevőnek lehetővé kell tennie az aláíró számára, hogy átvizsgálja a kiválasztott, aláírandó adatokhoz csatolandó tanúsítvány fő összetevőit.
Magyarázat: A Marketline webes aláíró alkalmazás a Windows tanúsítvány megjelenítőjét használva biztosít lehetőséget a tanúsítvány átvizsgálására
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 Marketline webes aláíró alkalmazásban az aláírás kiváltásához többszörös felhasználói aktivitás kell. Aláírás gomb megnyomása, aláírási szándék megerősítése, külső eszköz PIN kódjának megadása

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: Nincs időkorlát.

Konklúzió: **nem felel meg**

3. számú javaslat: A minősített aláírást kezelő rendszerben be lehessen állítani egy korlátot arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet.

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: Nincs időkorlát.

Konklúzió: **nem felel meg**

3. számú javaslat: A következő verzióban be lehessen állítani egy korlátot arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet.

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 PIN kód beírásához megfelelő dialógus ablak jelenik meg.

Konklúzió: **megfelel**

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: Ezt az operációs rendszer, a CSP segítségével önállóan elvégzi Ez viszont jelen értékelési jelentés tárgyán kívül áll.

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: Angol nyelvű üzenet jelenik meg,
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: Három ismétlés után a kártya blokkolódik. Angol nyelvű üzenet jelenik meg,
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 megbízható útvonal kiépítése a CSP feladata (amennyiben az aláírás-létrehozó eszköz támogatja ezt). Ez viszont jelen értékelési jelentés tárgyán kívül áll.
Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv43: Biztosítani kell egy olyan funkciót, amellyel a tudáson alapuló hitelesítő adatok lecserélhetőek (hacsak ez nincs tiltva egy aláírás-létrehozó alkalmazás típus esetében az alkalmazás szolgáltatójának biztonsági szabályzatában).
Magyarázat: A PIN kód lecserélésére van lehetőség.
Konklúzió: **megfelel**

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 PIN kód beírásakor a bevitel ablakban csillagok jelennek meg. Így megakadályozza az illetéktelen leolvasást.
Konklúzió: **megfelel**

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 PIN kód lecserélésére van lehetőség.
Konklúzió: ***megfelel***

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

Bizt_köv46, …, Bizt_köv47:
Magyarázat: A Marketline webes 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 webes 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" (szabványos és elterjedt) lenyomatoló algoritmus használatát lenyomatolásra.
Magyarázat: A Marketline webes aláíró alkalmazás által használt MultiSigno Pack.dll MD5-et használ.
Konklúzió: **megfelel**

Bizt_köv50: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy "elfogadott" (szabványos és elterjedt) elektronikus aláírás input formátum (feltöltési módszer) használatát.
Magyarázat: A Marketline webes 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 webes 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: 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 biztonságos aláírás-létrehozó eszköz felé soros és/vagy USB csatlakozás van.
Konklúzió: **megfelel**

Bizt_köv53:

Magyarázat: Az 53. követelmény csak a vezeték nélküli összeköttetést használó alkalmazásokra vonatkozik. A Marketline webes aláíró alkalmazás nem ilyen, ezért ez a követelmény nem vonatozik rá.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A dokumentációból nem derül ki, hogy a kártya támogat-e más alkalmazásokat illetve több aláíró adat tárolást. A tesztelés során erre utaló jelet nem tapasztaltunk. A CSP elvileg támogatja.

Konklúzió: **megfelel**

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

Magyarázat: Lévén a Marketline webes PKI modul 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.**

2. számú feltétel: A Marketline webes 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 megbízható útvonal kiépítése, s eközben az entitások hitelesítése a CSP feladata (amennyiben az aláírás-létrehozó eszköz támogatja ezt). Ez viszont jelen értékelési jelentés tárgyán kívül áll.

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 Marketline webes 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 (pl. az operációs rendszernek) kell biztosítania.

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

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

- ***vírusok ne ronthassák el a Marketline webes PKI aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket (DLL, CSP), 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 Marketline webes PKI modul 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.**

4. számú feltétel: A Marketline webes 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.

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

Magyarázat: Az appletek elektronikus aláírással vannak ellátva, amelyeket letöltés után a Marketline webes PKI modulon kívüli alkalmazással ellenőriznek.

Konklúzió: **megfelel**

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 webes PKI 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.

3. A Marketline webes aláíró alkalmazás követelményeknek való megfelelése

3.1 A Marketline webes 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	**megfelel**
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**megfelel**
F_SSC_1	**nem felel meg** /lásd az 1. számú javaslatot/ /fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
F_SSC_2	nem vonatkozik rá a követelmény
F_SSC_3	**megfelel**
F_SSC_4	nem vonatkozik rá a követelmény
F_SSC_5	**megfelel**
F_SSC_6	**megfelel**
F_SSC_7	**megfelel**
F_SSC_8	**megfelel**
F_SSC_9	**nem felel meg (rendszer szinten megfelel)**
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	**megfelel**
F_SDOC_1	**megfelel**
F_SLC_1	**nem felel meg (rendszer szinten megfelel)**
F_SCPC_1	**megfelel**
F_I/O_1	nem vonatkozik rá a követelmény
F_I/O_2	**megfelel**
F_I/O_3	**megfelel**
F_ISV_1	**megfelel**
F_ISV_2	**megfelel**
F_USV_1	**megfelel**
F_human_1	**megfelel**
F_human_2	**megfelel**
F_human_3	**megfelel**
F_human_4	**megfelel**
F_human_5	**megfelel**
F_human_6	**megfelel**
F_machine_1	**megfelel**
F_machine_2	**megfelel**
F_general_1	**megfelel**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	**megfelel**

3.2 A Marketline webes 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	**megfelel**
Bizt_köv8	**megfelel**
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_köv14	nem vonatkozik rá a követelmény
Bizt_köv15	nem vonatkozik rá a követelmény
Bizt_köv16	**megfelel**
Bizt_köv17	**megfelel**
Bizt_köv18	**megfelel**
Bizt_köv19	**megfelel**
Bizt_köv20	nem vonatkozik rá a követelmény
Bizt_köv21	nem vonatkozik rá a követelmény
Bizt_köv22	**megfelel**
Bizt_köv23	**megfelel**
Bizt_köv24	**megfelel**
Bizt_köv25	**megfelel**
Bizt_köv26	**megfelel**
Bizt_köv27	**megfelel**
Bizt_köv28	**megfelel**
Bizt_köv29	**megfelel**
Bizt_köv30	**megfelel**
Bizt_köv31	**megfelel**
Bizt_köv32	nem vonatkozik rá a követelmény
Bizt_köv33	nem vonatkozik rá a követelmény
Bizt_köv34	**megfelel**
Bizt_köv35	**megfelel**
Bizt_köv36	**nem felel meg** /lásd a 3. számú javaslatot/ / fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv37	**nem felel meg** /lásd a 3. számú javaslatot/ / fokozott biztonságú aláírásokra elfogadható a megvalósult megoldás is/
Bizt_köv38	**megfelel**
Bizt_köv39	nem vonatkozik rá a követelmény
Bizt_köv40	**megfelel**
Bizt_köv41	**megfelel**
Bizt_köv42	nem vonatkozik rá a követelmény
Bizt_köv43	**megfelel**
Bizt_köv44	**megfelel**
Bizt_köv45	**megfelel**
Bizt_köv46	nem vonatkozik rá a követelmény

Biztonsági követelmény	Teljesülés
Bizt_köv47	nem vonatkozik rá a követelmény
Bizt_köv48	**megfelel**
Bizt_köv49	**megfelel**
Bizt_köv50	**megfelel**
Bizt_köv51	**megfelel**
Bizt_köv52	**megfelel**
Bizt_köv53	nem vonatkozik rá a követelmény
Bizt_köv54	**megfelel**
Bizt_köv55	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
Bizt_köv58	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
Bizt_köv59	**megfelel**
Bizt_köv60	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**

4. A tanúsítási jelentés eredménye

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltétel teljesülése esetén a Marketline webes 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, a kliens érvényes aláírásával ellátott dokumentumok mehetnek át** (a fogadó 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 webes aláíró alkalmazás által kezelt aláírások fokozott biztonságához.

1. számú feltétel
A Marketline webes 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

2. számú feltétel
A Marketline webes 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

3. számú feltétel
A Marketline webes aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:
- vírusok ne ronthassák el a Marketline webes 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 webes aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a Marketline webes aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva hogy behatolók elrontsák ezt.

Érintett biztonsági követelmény: Bizt_köv58

5. számú feltétel
A Marketline webes 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.

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 kártyaolvasóba helyezett intelligens kártya lecserélését a Marketline webes aláíró alkalmazás következő verziója automatikusan kezelje le.

Érintett funkcionális követelmény: F_SSC-1

2. számú javaslat
Időbélyegzőt kell használni.

Érintett funkcionális követelmény: F_ISV-2

3. számú javaslat:
A következő verzióban be lehessen állítani egy korlátot arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet.

Érintett biztonsági követelmény: Bizt_köv36, Bizt_köv37

4. számú javaslat

A Marketline webes PKI modul számára az alábbiakkal lehet biztonságos területet megvalósítani, az 1.- 5. számú feltételeket teljesíteni:

1. A Marketline webes PKI modult 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:
17. a sikeres illetve sikertelen bejelentkezéseket,
18. a sikeres illetve sikertelen fiókkezelést
19. a sikeres illetve sikertelen rendszereseményeket.
20. A napló file-okat archiválni kell.
21. Antivírus programot kell alkalmazni, illetve folyamatosan frissíteni kell ennek vírus adatbázisát.
22. Rendszeresen ellenőrizni kell a Microsoft honlapján a kiadott javító csomagokat, szükség esetén installálni kell azokat.
23. Rendszeresen ellenőrizni kell a rendszert a Microsoft által kiadott Baseline Security Analyzer segítségével. A létrejött report file-t archiválni kell.

Érintett biztonsági követelmények: Bizt_köv11, Bizt_köv57, Bizt_köv58, Bizt_köv60

5. A követelményeknek való megfelelést ellenőrző független értékelés 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 webes 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 webes aláíró alkalmazás biztonsági funkcióinak értékelt erőssége

Még ha az értékelés tárgyának (jelen esetben a Marketline webes 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

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, kliens 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/ kliens 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