Tanúsítási jelentés

Hung-TJ-026-2004

a
Marketline Integrált Aláíró Modulról
v2.0

/Axelero Rt./

Tartalom

1. A Marketline Integrált Aláíró Modul legfontosabb tulajdonságainak összefoglalása

Az értékelt termék az „OTP elektronikus számlafogadás megvalósítása" projekt keretében az OTP oldalán megvalósított elektronikus aláíró alkalmazás, a **M**arketline **I**ntegrált **A**láíró **M**odul (2.0-ás verzió) /a továbbiakban **MIAM v2.0/**.

1.1 Architektúra

A MIAM v2.0 Java nyelven készített automata aláírást létrehozó és aláírást ellenőrző alkalmazás.

Az elektronikus aláíró és aláírás ellenőrzési funkciókat a MultiSigno Developer Professional (2.1 verzió) függvénykészlete felhasználásával valósítja meg, amit Java illesztő felületen keresztül ér el.

A MultiSigno Developer Professional 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.

A MIAM v2.0 futtatási környezete 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, legalább 24 óránkénti frissítéssel.

1.2 A tranzakciós környezet

A tranzakciós környezetben az OTP és beszállítói között elektronikus megrendelések és azokra küldött visszaigazolások, valamint ajánlatkérések és ajánlatok kétirányú kommunikációja zajlik a Marketline közvetítésével.

Az aláírásra és ellenőrzésre kerülő tranzakciók (dokumentumok) iDOC XML formátumúak.

Egy iDOC XML tranzakcióhoz tetszőleges formátumú csatolt dokumentum is kapcsolódhat, melyek a tranzakció részeként, azzal együtt szintén aláírásra kerülnek.

Az OTP oldali rendszerből a beszállítók felé a következő típusú tranzakciók indulnak (mely tranzakciókat a MIAM v2.0 elektronikus aláírással lát el):

- ajánlatkérés,
- megrendelés
- megrendelés módosítása és törlése.

A beszállítók oldaláról az OTP rendszerébe a következő típusú tranzakciók érkeznek (mely tranzakciók elektronikus aláírásait a MIAM v2.0 ellenőrzi):

- ajánlat,
- megrendelés visszaigazolása,
- számla.

A Marketline rendszere a tranzakciókat csak továbbítja, archiválja és naplózza, azokon nem módosít. A tranzakciókon az aláírás kapcsán formátum változtatás történik, mely a tartalmat nem befolyásolja.

1.3 Tulajdonságok

A MIAM v2.0 nem használ külső eszközt az aláírások létrehozására.

A MIAM v2.0 által létrehozott, és fogadáskor ellenőrzött aláírások formátuma az XML-Signature (RFC 3275, XML-Signature Syntax and Processing) szabványnak felel meg.

A rendszer többszörös aláírásokat nem kezel.

Az aláírások aláírt aláírási jellemzőként tartalmazzák az alábbiakat:

- aláírási szabályzat azonosító,
- az aláíráshoz felhasznált végfelhasználói tanúsítvány,

Az aláírások nem aláírt aláírási jellemzőként tartalmazzák az alábbiakat:

- időbélyegző,
- az aláírás létrehozásának időpontjában érvényes visszavonási lista,
- a visszavonási lista aláírásához használt szolgáltatói tanúsítvány.

A MIAM v2.0 eArchiv funkciója az archiválandó dokumentumokat rendszeresen ellenőrzi, és megpróbálja kicserélni az aláíró tanúsítványhoz tartozó visszavonási listát egy az aláírás ideje (az időbélyegzőben szereplő időpont) utáni kibocsátásúra. Ha ez az aláírás ideje után 48 órával sem sikerül, az adott dokumentumra hibát jelez, az archiválás sikertelen.

A MIAM v2.0 tanúsítványtárnak az operációs rendszer tanúsítványtárát használja.

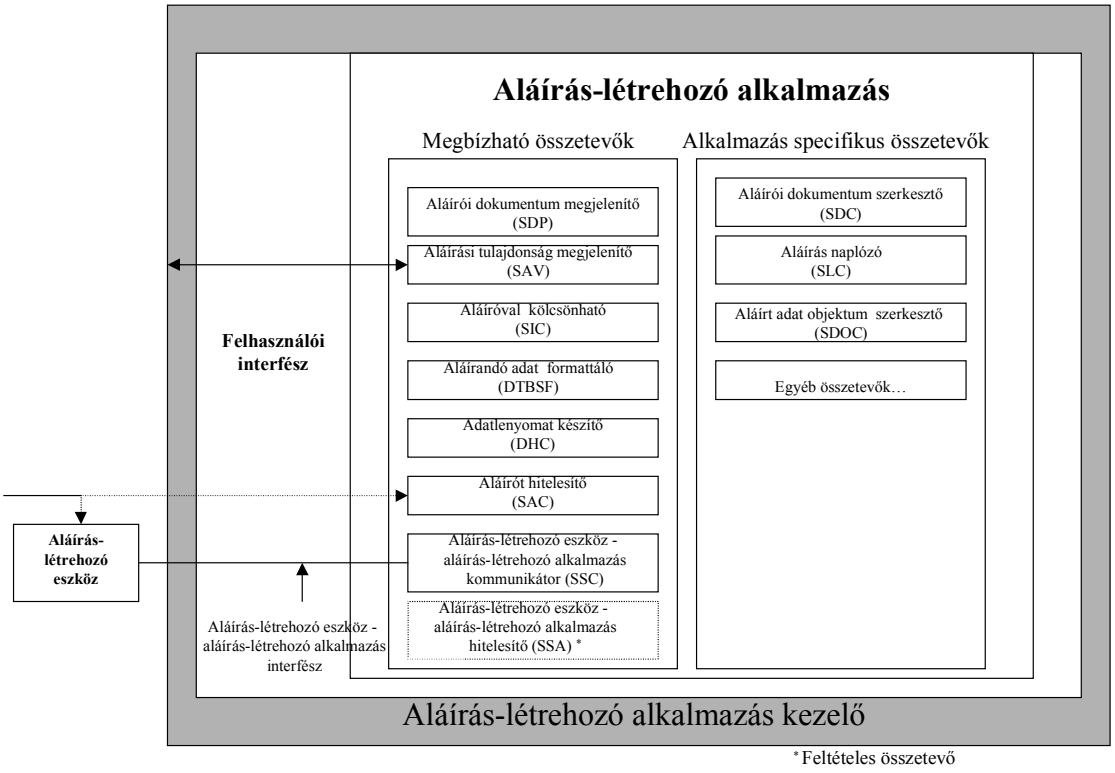
A MIAM v2.0 mind a sikeres, mind a sikertelen aláírásokról naplóbejegyzést készít.

1.4 Az értékelés tárgya és hatóköre

Jelen tanúsítás (és az alapját képező biztonsági értékelés) tárgya a MIAM v2.0, mely egyéb programokkal együttműködve megvalósítja az aláíró alkalmazásoktól elvárt funkcionalitást.

Az értékelés tárgya hatókörének pontos meghatározása érdekében tekintsük az 1. ábrát, melyen egy általános aláírás-létrehozó alkalmazás összetevői szerepelnek (a CWA 14170:2004 irányadó követelményrendszernek megfelelően).

1. ábra: Egy aláírás-létrehozó alkalmazás összetevői



Az 1. ábrán látható összetevők feladata az alábbi:

- aláírói dokumentum megjelenítő összetevő /SDP (Signer's document presenter)/:
  annak az aláírói dokumentumnak a megjelenítésére szolgál, amelyet az aláíró választ ki az aláíróval kölcsönható összetevőn keresztül.
- aláírási tulajdonság megjelenítő /SAV (Signature attribute viewer)/:
  azoknak az aláírási tulajdonságoknak az áttekintésére szolgál, amelyeket az aláíró választ ki az aláíróval kölcsönható összetevőn keresztül az aláírói dokumentummal együtt. Lehetőséget biztosít az aláíró tanúsítványának megjelenítésére is.
- aláíróval kölcsönható összetevő /SIC (Signer's interaction component)/:
  ezen keresztül lép az aláíró kölcsönhatásba az aláírás-létrehozó alkalmazással az aláírás-létrehozási folyamat vezérlésének céljából. Visszajelzést is ad a felhasználónak (pl. hibaüzeneteket küld, kijelzi a folyamatok eredményének állapotát és egyéb kiegészítő információkat ad). Ez a felület szolgál minden kölcsönhatásra az aláíró és az aláírás-létrehozó alkalmazás között, beleértve az aláírói dokumentum és az aláírási tulajdonságok kiválasztását vagy megadását.
- aláírandó adat formattáló /DTBSF (Data To Be Signed formatter)/:
  megformázza és elrendezi az aláírói dokumentumot vagy annak egy lenyomatát az aláírási tulajdonságokkal együtt, és az eredményt továbbítja az adatlenyomat készítő összetevőhöz.

- adat-lenyomat készítő összetevő /DHC (Data hashing component)/:
  az aláírandó adat reprezentáns előállítására szolgál (amely a lenyomatolást teljesen, vagy részlegesen elvégzi, esetleg egyáltalán nem végzi el, a 3. ábrán szemléltetett munkamegosztás, illetve a biztonságos aláírás-létrehozó eszköz elvárásainak megfelelően). Ha a biztonságos aláírás-létrehozó eszköz végzi teljesen a lenyomatolási eljárást, akkor ennek az összetevőnek a feladata csak abból áll, hogy az aláírandó adat reprezentánst változatlan formában az biztonságos aláírás-létrehozó eszközhöz továbbítja.
- aláírót hitelesítő összetevő /SAC (Signer's authentication component), pl. egy PIN pad-es intelligens kártyaolvasó egység/:
  arra szolgál, hogy bemutassa az aláírónak a tudáson alapuló hitelesítő adatait és/vagy biometrikus jellemzőit, továbbá az aláíró hitelesítő adatait olyan módon készítse elő, hogy azok összevethetők legyenek az aláírónak a biztonságos aláírás-létrehozó eszközön tárolt hitelesítő adataival.
- az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikátor /SSC (SSCD/SCA Communicator)/:
  az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kölcsönhatást kezeli.
- a biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikációt hitelesítő /SSA (SSCD/SCA Communicator authenticator)/:
  ez a feltételesen jelen lévő összetevő egy megbízható útvonalat épít ki az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás között.
- aláírói dokumentum szerkesztő /SDC (Signer's document composer)/: (pl. szöveg szerkesztő)
  ez az alkalmazás specifikus összetevő[1] (tek az aláírói dokumentum létrehozására, beolvasására vagy kijelölésére szolgál.
- aláírás naplózó összetevő /SLC (Signature logging component)/:
  ez az alkalmazás specifikus összetevő bizonyos információkat rögzít az aláírás-létrehozó alkalmazás által létrehozott aláírásokról.
- aláírt adat objektum szerkesztő /SDOC (Signed data object composer)/:
  ez az alkalmazás specifikus összetevő a formattált aláírandó adat összetevőket összekapcsolja az aláírás-létrehozó eszköz által szolgáltatott elektronikus aláírást reprezentáló bitfolyammal, és kiadja az aláírási folyamat eredményét (vagyis aláírt adat objektumot) az aláírt adat objektum típusaként specifikált szabvány formátumban (az ETSI által specifikált elektronikus aláírás formátumoknak megfelelően).
- hitelesítés-szolgáltatóval kölcsönható összetevő /CSPC (Certificate Service Provider interaction component)/:
  ez az egyéb alkalmazás specifikus összetevő a hitelesítés-szolgáltatóval való kölcsönhatásba lépést biztosítja, pl. fogadja az aláírói tanúsítványokat (ha ezeket nem tárolják a biztonságos aláírás-létrehozó eszközben) vagy időbélyegeket (ha ezt az aláírási szabályzat előírja).

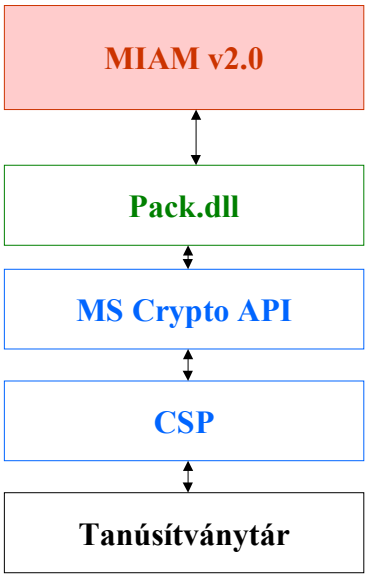
[1] tehát csak bizonyos alkalmazásokban jelen lévő

A fenti összetevőket a vizsgált rendszerben több különböző program komponens valósítja meg.

A MIAM v2.0 program a MultiSigno Developer Professional (Pack.dll) fejlesztő készlet elemeit hívja meg az aláírás létrehozásának és ellenőrzésének folyamatában.

A MultiSigno Developer Professional teljes mértékben a Windows operációs rendszer erőforrásaira, eszközeire támaszkodik. A Crypto API függvényeit használja, amely a Windows CSP-jét használja. Az aláírás létrehozása során a megfelelő XML struktúrák legenerálódnak, majd az aláírandó XML elemre Microsoft Crypto API-n keresztül készül el a digitális aláírás.

A 2. ábra a jelen értékelés tárgyának (MIAM v2.0) helyét szemlélteti az aláírás létrehozást és ellenőrzést végző rendszerben:



Csak a piros háttérszínnel jelölt MIAM v2.0 a jelen értékelés tárgya, amely a teljes aláírás-létrehozás és aláírás-ellenőrzés folyamatának csak egy részét végzi el.

Ebből következően nem a MIAM v2.0 valósítja meg az 1. ábrán szereplő általános aláírás-létrehozó alkalmazás összetevők mindegyikét, hanem ráépül a MultiSigno Pack.dll-jére és a Microsoft Crypto API-jára és CSP-jének szolgáltatásaira.

Az értékelés feltételezte, hogy a MIAM v2.0 alapját képező alábbi funkciók és platformok biztonságosan és helyesen működnek:

- a MultiSigno Developer Professional (Pack.dll) aláíró alkalmazás fejlesztő készlet DLL elemei (ennek biztonságos és helyes működését a HUNG-T-010-2003 számú tanúsítás is alátámasztja),
- a Microsoft Crypto API függvényei,
- a Windows CSP.

2. A MIAM v2.0 megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS/E-Sign CWA 14170:2004 és CEN/ISSS/E-Sign CWA 14171:2004 követelményrendszereiből fakadó) funkcionális és biztonsági követelményeket, melyek elektronikus aláírások létrehozására és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.

Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy a MIAM v2.0 megfelel-e az adott követelménynek.

2.1 A funkcionális követelményeknek való megfelelés

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

Magyarázat: A MIAM v2.0 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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

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 MIAM v2.0 automata rendszer, nem jeleníti meg az aláírási tulajdonságokat.

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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat..

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer, a felhasználói szándék kinyilvánítása közvetetten az alkalmazás elindításával történik.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 automata rendszer, melyben nincs közvetlen kommunikáció az aláíróval.

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 MIAM v2.0 automata rendszer, melyben nincs közvetlen kommunikáció az aláíróval.

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 MIAM v2.0 az XMLDSig csomagot megfelelően előállítja.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 kezdeményezi a lenyomatolást.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 elvégzi a lenyomatolást.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 a lenyomatolás elvégzése után a lenyomat értékét feltölti az XMLDSig struktúrában a PKCS1 v1.5 szabvány szerint.

Konklúzió: **megfelel**

F_SSC_1: Egy aláíró ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 1. ábrán jelölt[2] minden szükséges kommunikációt.

Magyarázat: A MIAM v2.0 nem használ biztonságos aláíró eszközt, csak fokozott biztonságú aláírást hoz létre.

Konklúzió: **nem vonatkozik rá a követelmény**

[2] Mivel a követelmény nem vonatkozik a MIAM v2.0 aláíró alkalmazásra, az ábrát mellőzzük.

F_SSC_2: Egy szolgáltató ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 2. ábrán jelölt[3] minden szükséges kommunikációt.

Magyarázat: A MIAM v2.0 nem külső szolgáltató ellenőrzése alá lett tervezve.

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 MIAM v2.0 nem használ biztonságos aláíró eszközt, csak fokozott biztonságú aláírást hoz létre.

Konklúzió: **nem vonatkozik rá a követelmény**

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 MIAM v2.0 nem használ biztonságos aláíró eszközt.

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 MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

[3] Mivel a követelmény nem vonatkozik a MIAM v2.0 aláíró alkalmazásra, 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: A MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

F_SSC_9: A befejezett aláírásokat naplózni kell.

Magyarázat: Bár a MIAM v2.0 nem használ biztonságos aláíró eszközt, a befejezett 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 MIAM v2.0 nem külső szolgáltató ellenőrzése alá lett tervezve.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 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 MIAM v2.0 nem használ biztonságos aláírás eszközt. Az aláírást szoftver úton állítja elő a Microsoft Crypto API segítségével. Az aláírás kimeneti adatát ugyanakkor megfelelően helyezi az XMLDSig csomagba.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 naplózza az aláírások készítését és ellenőrzését sikeres és sikertelen esetben egyaránt.

Konklúzió: **megfelel**

F_SCPC_1: A hitelesítés-szolgáltatóval való kapcsolat felvételén keresztül képesnek kell lennie az alábbiakra:
az aláírói tanúsítványok megszerzése,
az aláírói tanúsítványok állapotának lekérése.

Magyarázat: Az aláírói tanúsítványok a Microsoft tanúsítványtárában vagy az XML csomagban helyezkednek el, így nincs szükség a megszerzésükre.
A MIAM v2.0 képes a tanúsítványok állapotának ellenőrzésére vagy a helyben levő CRL segítségével, vagy a hitelesítés-szolgáltatótól letöltött CRL segítségével (Az aláírt dokumentumban lévő CRL-t a MIAM v2.0 nem használja fel.)

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: Aláírás létrehozásakor a MIAM v2.0 a Windows tanúsítványtárát használja a tanúsítványok eléréséhez. Itt a teljes tanúsítvány megtalálható. Ellenőrzéshez az aláíró tanúsítványát tartalmazza az aláírt adat objektum.

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 MIAM v2.0 képes a tanúsítvány hitelességének megállapítására. Képes ellenőrizni a teljes tanúsítványláncot illetve tanúsítvány visszavonási listában való szereplését.

Konklúzió: **megfelel**

F_I/O-3: Ha az aláírói dokumentumot, vagy annak egy részét, vagy az aláírási tulajdonságokat egy input/output interfészen keresztül adják meg, az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy egyetlen rejtett rész se játszhasson szerepet, és hogy egyetlen aláírandó adat összetevőt se cserélhessenek ki.

Magyarázat: A MIAM v2.0 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 MIAM v2.0 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 biztosítja, belülről pedig maga a MIAM v2.0 alkalmazás.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 eArchív funkciója minden érvényesítő adatot begyűjt.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 archiváló funkciója, az aláírást követően 24 órával később megismétli a kezdeti ellenőrzést. Ekkor már rendelkezésre áll az aláírás ellenőrzéshez szükséges visszavonási lista. Ezt a CRL-t a MIAM v2.0 elhelyezi az XMLDSig struktúrába, így az utólagos ellenőrzés számára minden ellenőrző adat biztosított.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 nem végez utólagos ellenőrzést, de az utóellenőrzéshez szükséges kezdeti ellenőrzés elvégzi, s ennek eredményét archiválja. A rendszerben (szükség esetén) az utólagos ellenőrzést a beszállítói oldalon működő webes aláíró alkalmazások segítségével lehet elvégezni.

Konklúzió: **nem vonatkozik rá a követelmény**

Ember által történő ellenőrzés esetén:

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

Magyarázat: A MIAM v2.0 az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

F_human_4: Az aláíró azonosítójának, vagyis az állítólagos aláíró nevének vagy felvett nevének megjeleníthetőnek kell lenni. Az adott nevet az aláíró tanúsítványában szereplő, "megkülönböztető név" információjából kell venni. Ha az aláíró nem bocsátotta rendelkezésre a tanúsítványt, a hitelesítés-szolgáltató nevét kell megjeleníteni ehelyett, és ha ez a név elfogadható, akkor az adott tanúsítványt a hálózati interfész felhasználásával be kell szerezni. Az említett névnek csak a tanúsítványt kibocsátó hitelesítés-szolgáltató számára van jelentése, ezért a hitelesítés-szolgáltató nevét az aláíró nevével együtt ki kell jelezni.
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 MIAM v2.0 az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 az aláírások létrehozását és ellenőrzését automatizált folyamatként, emberi beavatkozás nélkül végzi.

Konklúzió: **nem vonatkozik rá a követelmény**

Gépi (automatikus) ellenőrzés esetén:

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

Magyarázat: A MIAM v2.0 teljesíti a követelményt.

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: A MIAM v2.0 teljesíti a követelményt.

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 MIAM v2.0 megfelel a rá vonatkozó aláírási szabályzatnak. Az aláírási szabályzatban 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: A MIAM v2.0 szabványos protokollokat használ.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 szabványos formátumokat használ. Aláírási formátum: XMLDSig, tanúsítvány formátum: X509v3, időbélyegző formátum: RFC3161.

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 MIAM v2.0 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

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 MIAM v2.0 önmagában teljesíti a követelményt. BALE eszközt nem használ.

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 MIAM v2.0 teljesíti a követelményt.

Konklúzió: **megfelel**

A következő 4 követelmény csak a nyilvános aláírás-létrehozó alkalmazásokra vonatkozik.

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

Magyarázat: A MIAM v2.0 nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem nyilvános aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

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 MIAM v2.0 automata rendszer nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

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

Magyarázat: A MIAM v2.0 nem osztott architektúrájú aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem osztott architektúrájú aláíró alkalmazás.

Konklúzió: **nem vonatkozik rá a követelmény**

A nem megbízható folyamatokból és kommunikációs portokból adódó követelmény

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

Magyarázat: Lévén a MIAM v2.0 egy szoftver módon megvalósított alkalmazás, önállóan nem képes megvédenie saját integritását. Ezt a működési környezetnek (operációs rendszer, hálózati védelem) kell biztosítani.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg**
(lásd 1. számú feltétel)

1. számú feltétel A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

Az aláírandó adatra vonatkozó követelmények

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

Magyarázat: A MIAM v2.0 automatizmusa nem teszi lehetővé üres dokumentum aláírását.

Konklúzió: **megfelel**

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

Megjegyzés: A MIAM v2.0 az XMLDSig csomagban tárolja az aláíró tanúsítványát. Ezen kívül tárolja az aláíró tanúsítványának lenyomatát, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A MIAM v2.0 az XMLDSig csomagban tárolja a hivatkozást az aláírási szabályzatra, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A MIAM v2.0 az XMLDSig csomagban tárolja a kötelezettségvállalás típusát, mint aláírt aláírási tulajdonság. A kötelezettségvállalás az aláírási szabályzatban egyértelműen meghatározott.

Konklúzió: **megfelel**

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

Megjegyzés: A MIAM v2.0 az XMLDSig csomagban tárolja az aláírói dokumentum tartalom formátumot, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

2.2.2. Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP)

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: A MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer, nincs közvetlen kommunikáció az aláíróval.

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 MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

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 MIAM v2.0 automata rendszer nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Megjegyzés: A MIAM v2.0 az XMLDSig csomagban tárolja az aláírói dokumentum tartalom formátumot, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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

Megjegyzés: A MIAM v2.0 az XMLDSig csomagban tárolja az aláírói dokumentum tartalom formátumot, mint aláírt aláírási tulajdonság.

Konklúzió: **megfelel**

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: A MIAM v2.0 automata rendszer, nem jeleníti meg a dokumentumokat.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.3. Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV)

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

Magyarázat: A MIAM v2.0 automata rendszer, nem jeleníti meg az aláírási tulajdonságokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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 MIAM v2.0 automata rendszer, nem jeleníti meg az aláírási tulajdonságokat.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Megjegyzés: A MIAM v2.0 esetén az aláírt aláírási tulajdonságokat maga az aláírás védi, a nem aláírt aláírási tulajdonságok pedig önmagukat védik (szintén aláírással).

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: A MIAM v2.0 aláírási tulajdonságai nem tartalmaznak rejtett szöveget vagy aktív kódot.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 aláírási tulajdonságai nem tartalmaznak rejtett szöveget vagy aktív kódot.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 automata rendszer, nem jeleníti meg az aláírási tulajdonságokat.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.4. Követelmények az aláíróval kölcsönható összetevőre (SIC)

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 MIAM v2.0 automata rendszer, a felhasználói szándék kinyilvánítása közvetetten az alkalmazás elindításával történik.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 a Microsoft Crypto API-jára támaszkodik. Az aláírásnál nem küld aláírót hitelesítő adatot.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 a Microsoft Crypto API-jára támaszkodik. Az aláírásnál nem küld aláírót hitelesítő adatot.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.5. Követelmények az aláírót hitelesítő összetevőre (SAC)

A tudáson alapuló aláírót hitelesítő adatokra vonatkozó követelmények

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

Magyarázat: A MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

Konklúzió: **nem vonatkozik rá a követelmény**

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 MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

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 MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

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 MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

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: A MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

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 MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

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 MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

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 MIAM v2.0 nem alkalmaz aláírót hitelesítő adatot.

Konklúzió: **nem vonatkozik rá a követelmény**

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

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

Magyarázat: A MIAM v2.0 nem alkalmaz biometrikus aláírót hitelesítő adatot.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem alkalmaz biometrikus aláírót hitelesítő adatot.

Konklúzió: **nem vonatkozik rá a követelmény**

2.2.6. Követelmények az aláírandó adat formattáló összetevőre (DTBSF)

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

Magyarázat: A MIAM v2.0 az XMLDSig csomagot megfelelően előállítja.

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 MIAM v2.0 lenyomatolásra az SHA-1 algoritmust 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 MIAM v2.0 az aláírt adatra a megkövetelt feltöltési módszert alkalmazza.

Konklúzió: **megfelel**

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

Magyarázat: A MIAM v2.0 az aláírandó adat reprezentánst helyesen állítja elő.

Konklúzió: **megfelel**

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

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

Magyarázat: A MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

Bizt_köv54: Az SSC[4] 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 MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Magyarázat: A MIAM v2.0 nem használ biztonságos aláíró eszközt.

Konklúzió: **nem vonatkozik rá a követelmény**

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

Bizt_köv56: Az SSA[5]-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 MIAM v2.0 nem külső szolgáltató ellenőrzése alá lett tervezve.

Konklúzió: **nem vonatkozik rá a követelmény**

[4] SSC: a biztonságos aláírás-létrehozó eszköz (**S**SCD) és az aláírás-létrehozó alkalmazás (**S**CA) közötti kommunikáció összetevő

[5] SSA: a biztonságos aláírás-létrehozó eszköz (**S**SCD) és az aláírás-létrehozó alkalmazás (**S**CA) közötti kommunikációt hitelesítő összetevő

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 MIAM v2.0 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, működési környezetnek) kell biztosítania.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg** (lásd 2. számú feltétel)

2. számú feltétel: A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

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

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

Magyarázat: Lévén a MIAM v2.0 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** (lásd 3. számú feltétel)

3. számú feltétel: A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a MIAM v2.0 funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

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

Magyarázat: A MIAM v2.0 nem tartalmaz importált komponenseket.

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 szoftver modul számára a biztonságos területet a működtetési környezetnek kell biztosítania.

Konklúzió: védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg** (lásd 4. számú feltétel)

4. számú feltétel: A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a MIAM v2.0 alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

3. A MIAM v2.0 megfelelése a követelményeknek

3.1 A MIAM v2.0 megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	nem vonatkozik rá a követelmény
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	**megfelel**
F_SIC_2	nem vonatkozik rá a követelmény
F_SIC_3	nem vonatkozik rá a követelmény
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**megfelel**
F_SSC_1	nem vonatkozik rá a követelmény
F_SSC_2	nem vonatkozik rá a követelmény
F_SSC_3	nem vonatkozik rá a követelmény
F_SSC_4	nem vonatkozik rá a követelmény
F_SSC_5	nem vonatkozik rá a követelmény
F_SSC_6	nem vonatkozik rá a követelmény
F_SSC_7	nem vonatkozik rá a követelmény
F_SSC_8	nem vonatkozik rá a követelmény
F_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	nem vonatkozik rá a követelmény
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 MIAM v2.0 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** **(lásd 1. számú feltétel)**
Bizt_köv12	**megfelel**
Bizt_köv13	**megfelel**
Bizt_köv14	**megfelel**
Bizt_köv15	**megfelel**
Bizt_köv17	nem vonatkozik rá a követelmény
Bizt_köv18	nem vonatkozik rá a követelmény
Bizt_köv19	nem vonatkozik rá a követelmény
Bizt_köv20	nem vonatkozik rá a követelmény
Bizt_köv21	nem vonatkozik rá a követelmény
Bizt_köv22	nem vonatkozik rá a követelmény
Bizt_köv23	nem vonatkozik rá a követelmény
Bizt_köv24	nem vonatkozik rá a követelmény
Bizt_köv25	nem vonatkozik rá a követelmény
Bizt_köv26	**megfelel**
Bizt_köv27	**megfelel**
Bizt_köv28	nem vonatkozik rá a követelmény
Bizt_köv29	nem vonatkozik rá a követelmény
Bizt_köv30	nem vonatkozik rá a követelmény
Bizt_köv31	**megfelel**
Bizt_köv32	**megfelel**
Bizt_köv33	**megfelel**
Bizt_köv34	nem vonatkozik rá a követelmény
Bizt_köv35	**megfelel**
Bizt_köv36	nem vonatkozik rá a követelmény
Bizt_köv37	nem vonatkozik rá a követelmény
Bizt_köv38	nem vonatkozik rá a követelmény
Bizt_köv39	nem vonatkozik rá a követelmény
Bizt_köv40	nem vonatkozik rá a követelmény
Bizt_köv41	nem vonatkozik rá a követelmény
Bizt_köv42	nem vonatkozik rá a követelmény
Bizt_köv43	nem vonatkozik rá a követelmény
Bizt_köv44	nem vonatkozik rá a követelmény
Bizt_köv45	nem vonatkozik rá a követelmény
Bizt_köv46	nem vonatkozik rá a követelmény
Bizt_köv47	nem vonatkozik rá a követelmény
Bizt_köv48	**megfelel**
Bizt_köv49	**megfelel**

Bizt_köv50	**megfelel**
Bizt_köv51	**megfelel**
Bizt_köv52	nem vonatkozik rá a követelmény
Bizt_köv53	nem vonatkozik rá a követelmény
Bizt_köv54	nem vonatkozik rá a követelmény
Bizt_köv55	nem vonatkozik rá a követelmény
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg** **(lásd 2. számú feltétel)**
Bizt_köv58	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg** **(lásd 3. számú feltétel)**
Bizt_köv59	nem vonatkozik rá a követelmény
Bizt_köv60	Védett környezetben: **megfelel**, védtelen környezetben: **nem felel meg** **(lásd 4. számú feltétel)**

4. A Tanúsítási jelentés eredménye, érvényességi feltételei

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltétel teljesülése esetén a MIAM v2.0 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 MIAM v2.0 által kezelt aláírások fokozott biztonságához.

1. számú feltétel *A MIAM v2.0 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 MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

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

Érintett biztonsági követelmény: Bizt_köv57

3. számú feltétel: A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a MIAM v2.0 funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

Érintett biztonsági követelmény: Bizt_köv58

4. számú feltétel: A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a MIAM v2.0 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

A MIAM v2.0 aláíró alkalmazás számára az alábbiakkal lehet biztonságos területet megvalósítani, az 1. – 4. számú feltételeket teljesíteni:

1. A MIAM v2.0 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 file-okat 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 file-t archiválni kell.

5. A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az MSZ ISO/IEC 15408:2002 /Közös szempontok, Common Criteria/ **EAL 2**-es szintjéhez hasonló volt. /Az EAL2 a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét biztosítja./

A fejlesztőktől független ellenőrző vizsgálatról értékelési jelentés készült (lásd 6.2.2). Jelen tanúsítási jelentés alapvetően az ebben megfogalmazott és dokumentált eredményekre épül.

A fejlesztőktől független ellenőrzés az alábbi vizsgálatokat jelentette:

1. Az ellenőrző vizsgálat a MIAM v2.0 biztonsági viselkedésének megértése érdekében elemezte a biztonsági funkciókat, ehhez felhasználta az alábbi fejlesztői dokumentációkat:
   - **Koncepcionális Terv** - OTP - Marketline elektronikus számlafogadás megvalósítása (2003. december 23.)
   - **Bevezetési Terv** - OTP - Marketline elektronikus számlafogadás megvalósítása (2004. február 27.)
   - **PKI koncepció** az OTP – Marketline e-szla projekthez (2004. február 27.)
   - **Elektronikus Számla Interface - Specifikáció** - Verzió 1.0 - Document Rev. 1.0. (2004. január 21.)
   - **Elektronikus Számla válasz** (INVOICERESPONSE) **specifikáció** - Verzió 1.0) (2004. január 26.)
   - **Üzemeltetési Leírás** /az OTP R/3 rendszerét és a Marketline Integrált Szállítói Rendszert összekötő és digitálisan aláíró rendszerkomponensek üzemeltetésére (elektronikus számlával kiegészült verzió)/ (2004. október 18.)
2. Az értékelés kitért az aláírást és aláírás ellenőrzést végző modul fejlesztési környezetének, valamint a fejlesztők által a konfigurációkezelésre és verziókezelésre alkalmazott eljárások vizsgálatára is. Ez a vizsgálat a fejlesztőkkel folytatott konzultációkra és az alábbi dokumentumra épült:
   - **Fejlesztési környezet** - OTP - Marketline Szállítói rendszer - elektronikus aláírás projekt - Aláírási modul (2004. február 2.)
3. Az értékelés kitért az aláírást és aláírás ellenőrzést végző modulra, illetve az ennek működtetési környezetére vonatkozó szabályzatok vizsgálatára is. Ennek az értékelési feladatnak annak megállapítása volt a célja, hogy az értékelés tárgya megfelel-e a szabályzatokban leírtaknak, illetve biztosítja-e a szabályzatban leírtak támogatását. Az alábbi szabályzatokban foglaltakat kellett megvizsgálni:
   - Marketline Integrált Szállítói Rendszer **Aláírási szabályzat** - Verzió 4.0 (2004 október 20.)
   - OTP Integrált Szállítói Rendszer **Kulcskezelési szabályzat** - Verzió 2.0, 2003. december 1./
4. Az értékelők a fejlesztőktől független tesztelést végeztek.

6. A tanúsításhoz figyelembe vett dokumentumok

6.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign 14170:2004	CEN Workshop Agreement: Security requirements for signature creation applications /May 2004/
CEN/ISSS/E-Sign 14171:2004	CEN Workshop Agreement: General guidelines for electronic signature verification /May 2004/
RFC 3161	Internet X.509 PKI - Time-Stamp Protocol
RFC 3275	XML-Signature Syntax and Processing
RFC 3280	Internet X.509 PKI - Certificate and Certificate Revocation List (CRL) Profile

6.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1 A tanúsításhoz figyelembe vett egyéb fejlesztői dokumentumok

Kérdőív a tanúsítás kérelmezéséhez

Koncepcionális Terv - OTP - Marketline elektronikus számlafogadás megvalósítása (2003. december 23.)

Bevezetési Terv - OTP - Marketline elektronikus számlafogadás megvalósítása (2004. február 27.)

PKI koncepció az OTP – Marketline e-szla projekthez (2004. február 27.)

Elektronikus Számla Interface - Specifikáció - Verzió 1.0 - Document Rev. 1.0. (2004. január 21.)

Elektronikus Számla válasz (INVOICERESPONSE) specifikáció - Verzió 1.0) (2004. január 26.)

Üzemeltetési Leírás /az OTP R/3 rendszerét és a Marketline Integrált Szállítói Rendszert összekötő és digitálisan aláíró rendszerkomponensek üzemeltetésére (elektronikus számlával kiegészült verzió)/ (2004. október 18.)

Fejlesztési környezet - OTP - Marketline Szállítói rendszer - elektronikus aláírás projekt - Aláírási modul (2004. február 2.)

Marketline ISzR Aláírási szabályzat - Verzió 4.0 (2004 október 20.)

OTP ISzR Kulcskezelési szabályzat - Verzió 1.0 (2003 március 31.)

6.2.2 A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés az „OTP elektronikus számlafogadás megvalósítása" projekt keretében az OTP oldalán megvalósított Marketline Integrált Aláíró Modulról (verzió: 2.0) /2004. 11.08/

7. 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