TANÚSÍTVÁNY (E-MS08T2_TAN-SW-01) MELLÉKLETE

Dokumentumazonosító	TAN-SW-01.ME-01	
Projektazonosító	E-MS08T2	Microsec Kft. 2008
MATRIX tanúsítási igazgató	Dr. Szőke Sándor	
Kelt	Budapest, 2009. május 28.	
	…… MATRIX tanúsítási igazgató	

TARTALOMJEGYZÉK

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

2003-ban a MICROSEC Kft. az MSZ ISO/IEC 15408 "Az informatikai biztonság értékelésének közös szempontrendszere" (Common Criteria) alapján elkészült Védelmi Profil (PP-MS-03/001 ver. 2.3) tanúsítására kérte fel a MATRIX Kft-t, amely tanúsítás eredményeképp 2003.10.03-án kiadásra került az E-MS03T_TAN.PP jelű Tanúsítvány. 2004-ben a törvényi változások, illetve a fejlesztő módosításai a vizsgált dokumentumon szükségessé tették a tanúsítás felülvizsgálatát. A felülvizsgálat során a MATRIX a Védelmi Profil (PP-MS-03/001 ver. 3.0) új verzióját megfelelőnek találta, amit a T-MS04F1_TANF.PP jelű Felülvizsgálati Jegyzőkönyv kiadásával igazolt.

A MICROSEC az elmúlt években a Védelmi Profil alapján több Biztonsági Előirányzatot és az ezeknek megfelelő alkalmazást is kifejlesztett, amelyek megfelelőségét minden esetben a MATRIX vizsgálta és tanúsította. A 2006 nyarán megkötött vállalkozási szerződés alapján a MATRIX elvállalta a „MICROSEC parancssori e-Szignó 3.1" Biztonsági előirányzatának és a program modulnak a tanúsítását. 2006 őszén MATRIX bevizsgálta az ST-MS-06/002 Biztonsági Előirányzatot, és a tanúsítási eljárás eredményeképp 2006.10.02-n kiállította az E-MS08T2_TAN-01.ST azonosítójú tanúsítványt.

2006 év végén MICROSEC megrendelte az „e-Szignó 3.1 minősített aláírás létrehozó és kezelő parancssori alkalmazás megbízható aláírás-létrehozó modulja Microsoft Windows 2000, XP, Server 2003, Solaris és Linux operációs rendszerekre" elektronikus aláírási termék bevizsgálását. A tanúsítási eljárás eredményeként MATRIX 2007. március 14-én kiállította az E-MS06T_TAN-02.SW azonosítójú tanúsítványt.

2008-ban a MICROSEC elkészítette az aláírás létrehozó modul WinCE rendszeren futó verzióját, amelynek megrendelte a tanúsítását az eredeti tanúsítvány érvényességének kiterjesztéseként.

A tanúsítási eljárás során MATRIX azt vizsgálta, hogy a termék megfelel-e a kötelezően előírt és a fejlesztő által önként vállalt normatívák által támasztott követelményeknek. A tanúsítási folyamat során MATRIX ellenőrzésképpen ismételten elvégezte a Tesztjegyzőkönyvben leírt valamennyi tesztet, s megvizsgálta, hogy az átadott eszközök és dokumentumok alapján az e-Szignó program magját képező megbízható aláírás-létrehozó modul maradéktalanul megfelel-e a Biztonsági Előirányzatban megfogalmazott célkitűzéseknek, s így közvetve az annak alapját képező normatíváknak.

2 A VIZSGÁLAT TÁRGYA

Megnevezés: „MICROSEC e-Szignó 3.1 minősített aláírás létrehozó parancssori alkalmazás Megbízható aláírás-létrehozó modulja WinCE operációs rendszerre (röviden: e-Szignó WinCE SDK)"

2.1 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Szoftver	MICROSEC e-Szignó WinCE SDK aláírás létrehozó és kezelő parancssori alkalmazás	3.1	2009.04.30.	elektronikus
Szoftver	Teszt esetek és teszt eredmények		2009.04.13.	elektronikus
Dokumentáció	Microsec XSign4COM fejlesztői leírás		2009.03.23.	elektronikus
Dokumentáció	Tesztjegyzőkönyv a WinCE platformra készített e-Szignó minősített aláírás létrehozó parancssori alkalmazás Megbízható aláírás-létrehozó moduljához	ver. 1.2.	2009.05.25.	elektronikus
Dokumentáció	Nyilatkozat a biztonsági körülményekről		2009.03.14.	Papír
Dokumentáció	Nyilatkozat a műszaki normatíváknak való megfelelőségről		2009.03.14.	Papír

2.2 Fejlesztő

MICROSEC Számítástechnikai Fejlesztő Kft.
1022 Budapest, Marczibányi tér 9.

3 AZ E-SZIGNÓ 3.1 WINCE SDK

3.1 A vizsgálat tárgyának bemutatása

A MICROSEC e-Szignó WinCE SDK a „Biztonsági Specifikáció Minősített elektronikus aláírás létrehozó és kezelő alkalmazáshoz” (azonosító: PP-MS-03/001) című Védelmi Profil, és az ennek megfelelő „Biztonsági Előirányzat Minősített elektronikus aláírás létrehozó és kezelő parancssori alkalmazáshoz” (azonosító: ST-MS-06/002) című Biztonsági Előirányzat alapján került létrehozásra.

A minősített aláírás létrehozó és kezelő alkalmazás két komponensre osztható fel: az Aláírás létrehozásához szükséges műveleteket tartalmazó Megbízható aláírás-létrehozó modulra és a felhasználóval folytatott „párbeszédek” vezérlését végző Felhasználói felületre. A vizsgálat célja a Megbízható aláírás-létrehozó modul megfelelőségének kiértékelése volt.

3.2 A megbízható aláírás-létrehozó modul működése

A Megbízható aláírás-létrehozó modul az XSign4COM.dll-ből valamint több Dynamic Link Library (.dll) állományból áll (a részletes leírás a Rendszertervben illetve a Biztonsági Előirányzatban található). A működéshez szükséges egy megfelelő licensz állomány (server_reg.xml), és rendelkezésre kell állniuk a felhasználni kívánt tanúsítványoknak illetve aláírói kulcsoknak a Windows tanúsítványtárában a megfelelő helyre telepítve.

A megbízható aláírás-létrehozó modul függvényei egy megfelelően implementált program révén használhatóak.

A Megbízható aláírás-létrehozó modul függvényeinek végrehajtását befolyásolni lehet különböző lokális vagy globális beállítások megadásával, az értékek beállítására a függvényeket használó programban van lehetőség. A globális beállítások hatással vannak (a program befejezéséig) minden végrehajtott függvényre, míg a lokális beállításokkal az aktuális függvényvégrehajtást lehet befolyásolni.

Minősített aláírás létrehozása mindig a Felhasználói felület segítségével történik, amely biztosítja az Aláíró számára a szükséges interakciós folyamatot (Aláírás előhívás; Aláírói dokumentum, Aláírói tanúsítvány felmutatása stb.). Minősített aláírás létrehozásához mindig Biztonságos Aláírás Létrehozó Eszközre (BALE) van szükség. Az e-Szignó által támogatott elektronikus aláírás formátumok közül mind az e-aktában létrehozott, mind a Különálló aláírás, mind a Beágyazott aláírás esetében van lehetőség minősített aláírás létrehozására.

Az e-Szignó WinCE SDK megbízható aláírás-létrehozó modul a parancssori (aláírás létrehozó és kezelő) modul funkcióinak a minősített aláírás létrehozásához szükséges részhalmazát valósítja meg. Az aláírás ellenőrzéssel kapcsolatos funkciók nem kerültek implementálásra jelen modulban, így az ellenőrzési adatokat is tartalmazó aláírási formátumok nem kerülhetnek létrehozásra, azaz jelen modul csak a XAdES-EPES és XAdES-T aláírási formátumokat használja.

A főbb funkcionalitások, amelyek a vizsgált verzióban nem kerültek implementálásra:

- Visszavonás ellenőrzés OCSP és CRL alapon. Ennek következtében a XAdES-T típusú aláírásnál bonyolultabb aláírás típusok nem hozhatók létre.
- Tömörítetlen dokumentum beillesztés. Emiatt MELASZ-Ready formátumú aláírás nem hozható létre.
- Aláírás jellemzők megadása, úgymint:
  - Explicit aláírási szabályzat
  - Aláírás helye
  - Aláíró szerepe
  - Kötelezettség vállalás típusa
- Ellenjegyzés létrehozása
- Aláírás előtti időbélyeg létrehozása

A szűkítés nem érinti a minősített aláírás létrehozásához szükséges funkciók körét. A meg nem valósított funkciókra vonatkozó követelményeknek nem kell megfelelni, így az ezekkel kapcsolatos vizsgálatok sem kerültek elvégzésre.

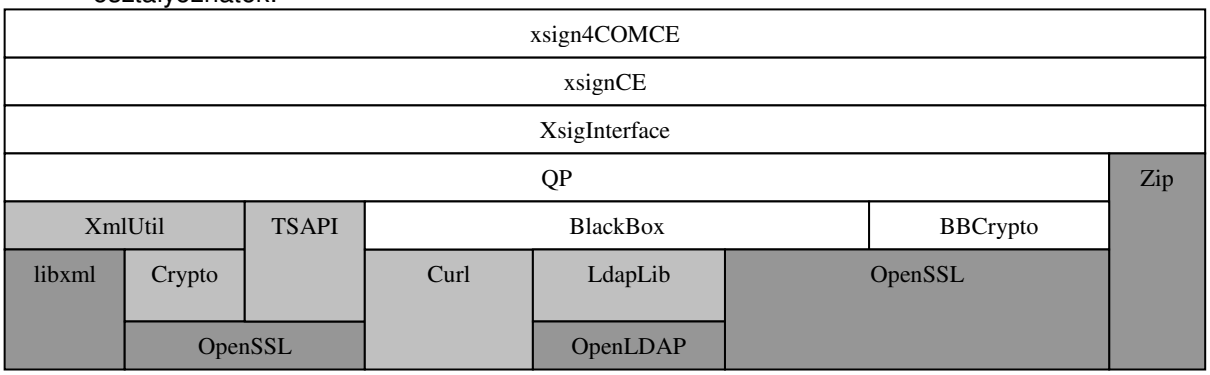
3.3 Megbízható aláírás-létrehozó modul szoftver igénye

Az e-Szignó alkalmazás Megbízható aláírás-létrehozó modulja WindowsCE platformon futtatható.

A Megbízható aláírás-létrehozó modul által használt modulok vagy a fenti operációs rendszer részét képezik, vagy a telepítő csomag tartalmazza őket.

3.4 A Megbízható aláírás-létrehozó modul felépítése

A Megbízható aláírás-létrehozó modul számos alrendszerből – függvénykönyvtárból – áll (1. ábra). A függvénykönyvtárak legegyszerűbben funkcionalitásuk szerint osztályozhatók.



1. ábra A megbízható aláírás-létrehozó modul szerkezete

XML feldolgozás

libxml Alapvető XML feldolgozási funkcionalitás, C nyelven megvalósítva.

XAdES formátum

XmlUtil A XAdES alapját képező XMLDSIG feldolgozását végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezelés nélkül.

QP A XAdES által definiált kiegészítő aláírási tulajdonságok kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel. (Neve a XAdES formátumban fő szerepet játszó QualifyingProperties XML elem nevéből származik.)

E-akta formátum kezelése

XsigInterface Az e-aktán végezhető műveleteket tartalmazó függvénykönyvtár, C++ nyelven megvalósítva, részleges kivételkezeléssel.

xsignCE Az XsigInterface-re épülő C függvénykönyvtár.

Xsign4COMCE Az xsignCE-re épülő C++ függvénykönyvtár COM interfésszel, teljes kivételkezeléssel.

Kriptográfiai szolgáltatások

OpenSSL	Az aláírások és a titkosítás kezelését, az időbélyegek feldolgozását, tanúsítványok és OCSP válaszok, tanúsítványlánc ellenőrzését végző függvénykönyvtár, C nyelven megvalósítva. A HTTP kommunikációra is használatos.

RSA-SHA1 aláírások kezelése:

Crypto	Az aláírások kezelését végző, OpenSSL-re épülő függvénykönyvtár, C++ nyelven megvalósítva, kivételkezelés nélkül. A PKCS #11 modulok és az OpenSSL engine kezelését is ez végzi.

Az X.509 infrastruktúra formátumainak kezelése

BBCrypto	A tanúsítványok, CRL-ek és OCSP válaszok kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel. Az OpenSSL-t használja.
TSAPI	Az időbélyegek kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezelés nélkül. Az OpenSSL-t használja.
BlackBox	A tanúsítványok ellenőrzését (tanúsítványlánc és visszavonás-ellenőrzés) végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel. A OpenSSL-t használja.
BBUtil	Segédfüggvények, C++ nyelven megvalósítva, kivételkezeléssel.

Hálózati kommunikáció

OpenLDAP	Az LDAP kapcsolódáskor használatos függvénykönyvtár, C nyelven megvalósítva.
LdapLib	Az OpenLDAP-ra épülő C++ burkoló („wrapper”) könyvtár. Kivételkezelést nem alkalmaz.
CURL	A HTTP kommunikációra használt C++ könyvtár. Kivételkezelést alkalmaz.

Tömörítés

Zip	A PKZIP algoritmusú tömörítés implementációja Windows operációs rendszeren, C és C++ nyelven megvalósítva, kivételkezelés nélkül.

Egyéb

Trio	A többnyelvűséghez elengedhetetlen változó sorrendű paraméterekkel használható szövegformázó függvénykönyvtár, C nyelven megvalósítva.
XadesSignerLocale	A WinCE SDK nyelvenkénti üzenettábláját tartalmazza, valamint

ez végzi az UTF-8 és a lokális karakterkészlet (pl. ISO-8859-2) közötti konverziót.

A fent felsorolt függvénykönyvtárakból a fordítást követően több különböző modul jön létre, amelyeket a telepítő csomag is tartalmaz.

3.5 Hardver környezet

A VT működése során a következő külső hardver komponensek jelenlétét igényli:

- Minősített aláírás létrehozásához:
  - Biztonságos Aláírás-Létrehozó Eszköz
- Tanúsítványok beszerzéséhez; Időpecsét készítéshez:
  - TCP/IP hálózati összeköttetés a Hitelesítés-szolgáltató illetve az Időbélyegző szolgáltató eléréséhez.

3.6 Támogatott Aláírói dokumentum formátumok

Az e-Szignó három kategóriába sorolja az Aláírói dokumentumokat azok formátuma, s az ettől függő megbízhatóságának mértéke alapján.

Elektronikus állomány: Bármilyen elektronikus formátumban létező adathalmaz.

Elektronikus dokumentum: Olyan elektronikus állomány, amelynek ismert a formátuma, azonban nem zárható ki, hogy aktív elemet tartalmaz, és így nem garantálható, hogy mindig mindenhol ugyanúgy lehet megjeleníteni.

Elektronikus irat: Olyan elektronikus dokumentum, amely nem tartalmaz aktív elemet, valamint egyértelműen ismert a használandó megjelenítő alkalmazás; így garantálható, hogy minden megjelenítéskor ugyanazt a képet (tartalmat) mutatja.

Az e-Szignó 3.1 a következő formátumú állományokat kezeli:

Formátum	Specifikáció
text/plain	RFC2646, ISO 8859-2
text/xml	RFC 3023, W3C XML V1.0
application/pdf	Adobe PDF V1.5
text/rtf	\rtf\ansi\ansicpg1250\uc1\deff0\stshfd
text/html	RFC2854, HTML V4.0
application/msword	Microsoft Word 97 V8.0
image/jpeg	JFIF V1.02 1992
image/tiff	RFC2302 , TIFF V6.0
image/png	PNG V1.0 1996
image/gif	GIF 89a
image/bmp	Windows Bitmap Format

application/zip	PKWARE 98
application/x-zip-compressed	PKWARE 98
application/eszigno	MICROSEC e-Szignó 2.0
application/eszigno3	MICROSEC e-Szignó 3.0

A támogatott formátumok közül azokat, amelyek biztosan nem tartalmazhatnak aktív elemet, valamint amelyekhez a VT tartalmaz biztonságos (beépített) megjelenítő programot, támogatott biztonságos formátumnak nevezzük. A támogatott biztonságos formátumok a következők:

Formátum	**Specifikáció**
text/plain	RFC2646, ISO 8859-2
text/rtf	\rtf\ansi\ansicpg1250\uc1\deff0\stshfd
application/eszigno3	MICROSEC e-Szignó 3.0

Egy ismeretlen formátumú állomány kategóriája mindig Elektronikus adat.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

Az elvégzett vizsgálatok és a beszerzett nyilatkozatok alapján a vizsgált alkalmazás megfelel az alábbi normatív követelményeknek:

- Kötelezően betartandó normatívák a MATRIX által bevizsgálva.
  - 2001. évi XXXV. törvény az elektronikus aláírásról,
  - 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
  - Megfelelés az algoritmikus követelményeknek
    Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917-x/2008 határozata.
- Megfelelés az önként vállalt normatíváknak.
  - MATRIX által bevizsgált normatívák:
    - MSZ ISO/IEC 15408: Az informatikai biztonság értékelésének közös szempontjai

      1. 15408-1:2002 1. rész: Bevezetés és általános modell,

2. 15408-2:2003 2. rész: A biztonság funkcionális követelményei,

3. 15408-3:2003 3. rész: A biztonság garanciális követelményei,

- Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
- A Miniszterelnöki Hivatalt vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
- CWA 14170:2001 (E) – Security Requirements for Signature Creation Applications,
- CWA 14171:2001 (E) – Procedures for Electronic Signature Verification.
- A Megbízó által készített Biztonsági Előirányzat (ST-MS-06/002 ver. 1.0),

o Fejlesztő által igazolt megfelelések:

- RFC 3275: XML-Signature Syntax and Processing,
- ETSI TS 101 903 V1.2.2 (2004-04): XML Advanced Electronic Signatures (XAdES),
- 20/2004. (IV. 21.) PM rendelet az elektronikus számláról,
- 7/2005. (VII. 18.) IHM rendelet a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól,
- 12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól,
- 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól,
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára, 2005. november 1.
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára, 2005. november 1.
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára, 2005. november 22.
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírási szabályzatok készítésére, 2005. november 22.

A biztonságos aláírás létrehozó modul megfelel a fenti követelményeknek a 4.3 pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

- A tanúsítás kizárólag a 4.2 pontban részletezett, bevizsgált verziószámú program modulokra vonatkozik,
- Nem képezi a tanúsítás részét a program működési környezete, mint például az
  - operációs rendszer,
  - a felhasznált külső szoftver modulok illetve programok,
  - a működéshez szükséges hardver elemek.

4.2 A bevizsgált program komponensek azonosítása

4.2.1 A Windows CE környezet program komponensei

Program modul	Verzió	Méret	Leírás	Szerzői jog	SHA-256 lenyomat
XSign4COMCE.dll	1.0.1.6	632 320	COM-os interfész dll	Microsec Kft.	01cd354010e00341 aac1830115657f5c b7b6993cfddeac61 16805bbe52637f5c
xsignCE.dll	1.0.1.7	382 976	C interfész dll	Microsec Kft.	6207b003a54f5441 b30f25f3ded65f89 ce2aee4924693178 299787fa73381c02
XadesSignerCE.dll	1.1.12.4	4 590 592	Aláíró alkalmazás belső felülete	Microsec Kft.	fe90b4e3ebd54fac acc91ac4954a0caf 30be2229974a16b0 80f96dc39288069d
XadesSignerLocale_HUN.dll	1.1.0.14	47 104	Üzenetek, helyi kódolás magyarul.	Microsec Kft.	ae22495cb01e7da2 7b5876c913010620 f666d0226025daa2 044bf3922c710738
libiconv.dll	1.9.0.0	976 384	Karakter kódoló könyvtár	Open source	3ece9a0c6879c569 4c3ec6cd546d14cd 7499cc197c6cc74e ab3c0fa19dd722ca
libxml2.dll		1 867 776	XML feldolgozó könyvtár	Open source	1ae30c9f29ff234d 1bca754aaf2a4de6 5fb61851d548f89f 78e40df836c2aa45

A tanúsítás csak a vizsgált programverzióra vonatkozik.

4.3 Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége.

4.3.1 Hardver és szoftver környezet

A VT csak olyan környezetben használható minősített aláírások létrehozására, amelynek minden eleme kielégíti az elvárható biztonsági követelményeket, és együttesen egy megfelelően biztonságos informatikai rendszert hoznak létre. A vizsgálatnak nem tárgya a környezet egyes elemeinek vizsgálata, az itt megfogalmazott követelmények iránymutató jellegűek az eszköz megfelelő használatához.

4.3.1.1 Operációs rendszer

Az e-Szignó alkalmazás Megbízható aláírás-létrehozó modulja WindowsCE platformon futtatható.

A vizsgált aláírási termék biztonságos használatának előfeltétele, hogy az operációs rendszert megfelelően biztonságos konfigurációban használjuk. Előnyben kell részesíteni az IT biztonsági tanúsítással rendelkező operációs rendszereket, pld. a Windows Mobile 5.0 és 6.1 CC EAL2+ tanúsítással rendelkezik. A tanúsítással rendelkező operációs rendszereket a biztonságos működtetés érdekében a tanúsításban megfogalmazott feltételek betartásával kell telepíteni és üzemeltetni.

Common Criteria tanúsítással nem rendelkező operációs rendszer is használható, ilyen esetben azonban fokozottan kell ügyelni a rendszer fizikai biztonságára és az alkalmazott üzemeltetési védelmi intézkedések szigorú betartására.

4.3.1.2 Microsoft Visual Studio futtató környezet könyvtárai

A Microsoft C++ fejlesztő környezet könyvtárai nem rendelkeznek tanúsítással, nem rendelkezünk a fejlesztés körülményeire vonatkozó információkkal, a VT fejlesztőjének nincs ráhatása a modulok kialakítására, így a tanúsítás nem terjed ki ezen modulok működésére.

A Microsoft könyvtárak használatánál figyelembe kell venni, hogy egy neves – magát a Windows operációs rendszert is előállító – szoftvercég széleskörűen felhasznált termékének részei, amelyeknek esetleg jelentkező hibáit folyamatosan javítják, és a javítócsomagokat publikálják. A megjelenő javításokat folyamatosan figyelni kell, és változás esetén a javított könyvtárak felhasználásával új javító illetve telepítő csomagot kell kiadni.

A változások nyomon követése a fejlesztő feladata és felelőssége.

4.3.1.3 Netscape könyvtárak

A Netscape könyvtárak nem rendelkeznek tanúsítással, nem rendelkezünk a fejlesztésük körülményeire vonatkozó információkkal, ezért a tanúsítás nem terjed ki ezen modulok működésére

A használat során figyelembe kell venni, hogy a Netscape egy neves szoftverfejlesztő cég, aki meghatározó szerephez jutott a PKI technológiák alkalmazása és elterjesztése

terén, s a kérdéses könyvtárak forráskódját a Mozilla projekt kapcsán nyilvánosságra hozta. Bárki szabadon letöltheti, megvizsgálhatja és felhasználhatja a publikált kódokat, beépítheti saját programjaiba. A nagy nyilvánosságnak köszönhetően az esetleges programhibák, a kódban lévő rejtett csapdák valószínűleg már felderítésre kerültek. Bár a programot nem a MICROSEC írta, a forráskód rendelkezésére áll, amiből maga állította elő megfelelően biztonságos körülmények között a felhasznált könyvtárakat, s ezt bármikor reprodukálni tudja.

A publikált javításokat, fejlesztéseket folyamatosan figyelni kell, és változás esetén a javított könyvtárak felhasználásával új javító illetve telepítő csomagot kell kiadni. Feltárt hiba esetén a MICROSEC is képes az esetleges javítás elvégzésére.

A változások nyomon követése a fejlesztő feladata és felelőssége.

4.3.1.4 BALE eszköz

A Biztonságos aláírás-létrehozó modul minősített aláírás létrehozására csak olyan biztonságos aláírás-létrehozó eszközzel (BALE) használható, amely szerepel a Nemzeti Hírközlési Hatóság (NHH) vagy más Európai Uniós tagállam megfelelő hatósága által hivatalosan közzétett nyilvántartásban.

A BALE kiválasztása során különös figyelmet kell fordítani a BALE-t az operációs rendszer kriptográfiai szolgáltatásaihoz illesztő meghajtó modul megbízhatóságára. A BALE csak olyan meghajtóval használható, amelyet a BALE gyártója szállít, vagy amelynek fejlesztője hitelt érdemlően garantálja a modul biztonságos működését.

Az alkalmazott összeállításnak garantálnia kell a megfelelően biztonságos csatorna kialakítását a BALE és az aláíró alkalmazás között az aláírandó adatok átadásához.

Smartcard alkalmazás esetén előnyben kell részesíteni az olyan megoldás használatát, amely a BALE-t képes Pinpad-dal rendelkező (Class 2) olvasóval használni, ezzel kizárva az esetleg hozzáférhető billentyűzet használatát.

4.3.1.5 Hálózati működés

Mivel az alkalmazás az ellátandó feladatok jellegéből adódóan nyilvános hálózatra kapcsolódik, kiemelt figyelmet kell fordítani az egész számítógép védelmére a hálózaton terjedő rosszindulatú programok támadásainak detektálása, kivédése érdekében.

4.3.2 Személyi védelem

Az üzemeltetés során a személyi védelem tekintetében az alábbi intézkedések betartásáról kell gondoskodni:

- Hozzáértő adminisztrátorokat és felhasználókat kell a VT és a VT által tartalmazott titkos adatok kezelésére alkalmazni.
- Az összes adminisztrátor és felhasználó magas szinten ismerje a biztonsági szabályzatot, amely szerint a VT működik.
- A hozzáférés megszüntetése (pl. a felhasználó munkaviszonya megszűnik) során megfelelő eljárások fussanak le a hozzáférés megszüntetése és egyéb jogosultsági komponensek eltávolítása érdekében.

- Az adminisztrátorokat és felhasználókat időben és megfelelő módon kell tájékoztatni azokról a biztonsági közleményekről, amelyekben a VT üzemeltetését veszélyeztető tényezők leírásra kerülnek, így minimalizálva a bizalmas információk elvesztésének, illegális felhasználásának, illegális módosításának kockázatát.

- Az adminisztrátorokat és felhasználókat ki kell oktatni a szociális hírszerzés elleni védekezés módszereiről (pl. nem megbízhatóan hitelesített – telefonon érdeklődő – személyek felé adatszolgáltatás tiltása stb.).

- Az adminisztrátorok és felhasználók felvétele során ügyelni kell a megbízható személyek kiválasztására (pl. erkölcsi bizonyítvány stb.).

1.1.1 A fizikai védelem

Az üzemeltetés során a fizikai védelem tekintetében az alábbi intézkedések betartásáról kell gondoskodni:

- A VT által tartalmazott hardver, szoftver és firmware elemeket megfelelően kell védeni az illetéktelen fizikai módosítások ellen.

- A VT által használt kommunikációs csatornákat megfelelően védeni kell az illetéktelen fizikai módosítások ellen.

- A VT által használt kommunikációs csatornákat megfelelő módon védeni kell az illetéktelen lehallgatás ellen. Lehallgatás alatt logikai (pl. kémprogramok) és fizikai (EMC) módszerekkel végzett adatgyűjtés értendő.

1.1.2 Szállítás és telepítés

A program telepítő készletét nem módosítható, biztonságos adathordozón kell a felhasználónak átadni. Az átadás-átvételt hitelt érdemlő módon igazolni kell az átadás pontos időpontjának rögzítésével.

A telepítést csak a megfelelően előkészített, biztonságos környezetben szabad megkezdeni az átadott adathordozó segítségével, a telepítési útmutatóban rögzített lépések pontos betartásával.

Az eredeti adathordozó felhasználásával rendszeresen ellenőrizni kell a számítógépre telepített program integritását.

1.1.3 Felhasználói felület

A Megbízható aláírás-létrehozó modul biztonságos üzemeltetéséhez a szoftver felhasználói felületének biztosítania kell a Biztonsági Előirányzatban rögzített körülményeket.

4.4 Algoritmusok és kapcsolódó paraméterek

A vizsgált alkalmazás által támogatott kriptográfia algoritmuskészlet az alábbi komponensekből áll:

- sha1 lenyomatképző függvény,

- emsa-pkcs1-v1.5 feltöltő algoritmus,
- RSA 1024 bites aláíró algoritmus.

A Vizsgálat Tárgyára nem vonatkoznak a kulcs-előállítási és véletlen-szám generálási algoritmusok követelményei.

Az érvényes előírások szerint az sha1 lenyomatképző függvény felhasználása jelenleg már nem ajánlott, bár nem is tiltott, mivel konkrét eredményes támadást még nem észleltek.

A feltöltő algoritmusok esetén nem látott napvilágot információ feltörési kísérletekkel illetve az algoritmusok gyengülésével kapcsolatban, így valamennyi feltöltő algoritmus biztonságosnak tekinthető a tanúsítvány tervezett érvényességi időtartama alatt.

2009-ben már nem ajánlott az 1024 bites RSA kulcsok használata, de mivel sikeres támadásról nincs információ, nem is tiltott. Meglévő, engedélyezett alkalmazásoknál az 1024 bites kulcsok megfelelő körültekintéssel még tovább használhatók.

Összefoglalásképpen megállapítható, hogy a vizsgált alkalmazás által támogatott kriptográfia algoritmuskészlet és az alkalmazott paraméterek a meglévő tanúsítvány kiterjesztéseként kiállított új tanúsítvány kevesebb, mint 1 éves érvényességi időtartama alatt jelenlegi ismereteink szerint megfelelően biztonságos marad. Az SHA1 lenyomatképző függvény és az 1024 bites RSA kulcs használata jelenleg még biztonságosnak tekinthető, de a támadási módszerek fejlődésével fel kell készülni a gyengébb algoritmusok és paraméterek használatának szükség szerinti soron kívüli megszüntetésére. A szolgáltatónak és a felhasználónak folyamatosan figyelnie kell a felhasználható kriptográfiai algoritmusokkal kapcsolatos határozatokat, és az elektronikus aláírás használata során a megfelelő algoritmusokat és paramétereket kell használniuk.

4.5 Biztonsági garancia szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a „MICROSEC e-Szignó 3.1 minősített aláírás létrehozó parancssori alkalmazás Megbízható aláírás-létrehozó modulja WinCE operációs rendszerre (röviden: e-Szignó WinCE SDK)" megfelel a normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben.

A megfelelés biztonsági garancia szintje megfelel a Common Criteria értékelési rendszere szerinti EAL 3+ szintnek az ALC_FLR (A termék felfedezett hibáinak javítása) garanciacsaládnak való megfelelés vállalásával.1

A megfelelőségre vonatkozó megállapítást a témakör biztonságát érintő jelentős tudományos felfedezés, illetve új verzió kiadása esetén felül kell vizsgálni.

5 RÖVIDÍTÉSEK

Rövidítés	Tartalom
BE	Biztonsági Előirányzat - egy megvalósítandó termék biztonsági rendszerterve
CC	Common Criteria - MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere

1 Az EAL szint tájékoztató jellegű, CCRA hatókörben nem automatikusan elfogadott.

Rövidítés	Tartalom
PP	Protection Profile – a Védelmi Profil eredeti, angol elnevezése
ST	Security Target – a Biztonsági Előirányzat eredeti, angol elnevezése
TOE	Target Of Evaluation – a Vizsgálat Tárgya eredeti, angol elnevezése
VP	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere
VT	Vizsgálat Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza

Dokumentum vége