TANÚSÍTVÁNY (E-EG12T-TAN-SW) MELLÉKLETE

Dokumentumazonosító	TAN-SW-01.ME-01	
Projektazonosító	E-EG12T	E-Group ICT Software Zrt.
MATRIX tanúsítási igazgató	Hodován Attila	
Kelt	Budapest, 2013. január 21.	

.....

MATRIX tanúsítási igazgató

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

Az E-GROUP ICT Software Zrt. (továbbiakban E-GROUP) kifejlesztette a Signed Document eXpert (SDX) Professional M Edition Aláírás-létrehozó és Kezelő Alkalmazást, amelyet 2005-ben bevizsgált és kiállította a megfelelőséget igazoló tanúsítványt, amelyet 2009 május 15-én újra tanúsított 3 éves érvényességgel. A 2009-es tanúsítás érvényessége lejárt és az E-GROUP jelentősebb fejlesztéseket is végzett a programon, ezért megrendelte az alkalmazás aktuális verzió „core" moduljának újbóli bevizsgálását.

A MATRIX áttanulmányozta az E-GROUP által átadott fejlesztői dokumentumokat, elemezte a kötelezően betartandó és az önként vállalt normatíváknak való megfelelést. A fejlesztő által biztosított SDX alkalmazás segítségével ellenőrizte a fejlesztő által átadott és teszt jegyzőkönyvben is rögzített tesztesetek eredményét.

Az elvégzett vizsgálatokról részletes jelentések készültek, amelyekből a vizsgálat és a felhasználás körülményeire vonatkozó legfontosabb információkat jelen melléklet tartalmazza.

2 A VIZSGÁLAT TÁRGYA (VT)

Megnevezés: „Signed Document eXpert (SDX) „core" modul program v3.0.0 azonosítójú elektronikus aláírási termék "

2.1 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

Típus	Tárgy	Kapott fájlnév
Szoftver	Signed Document eXpert (SDX) „core” modul program v3.0.0 azonosítójú elektronikus aláírási termék (Kliens és szerver alapokon), működő környezetetel VMWare formátumban	CD
Dokumentum	E-Group ICT Software Zrt Informatikai szabályzat v.1.2	E_Group_ICT_Software_Zrt_Informatikai_szabalyzat_v.1.2.pdf
Dokumentum	E-Group Alkalmazások tervezése, fejlesztése Minőségirányítási eljárás	E_Group_Alkalmazasok_tervezese_fejlesztese.pdf
Dokumentum	E-Group Alkalmazások Tesztelés Minőségirányítási Eljárás	E_Group_Alkalmazasok_tesztelese.pdf
Dokumentum	SDX „core” modul v3.0.0 - Konfigurációmenedzsment eljárások. 2012.11.06.	_ALC_CMC_3_CMS_3_LCD_1_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Szállítási dokumentáció. 2012.11.06.	_ALC_DEL_1_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Telepítési leírás. 2012.11.06.	_AGD_PRE_1_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Funkcionális specifikáció. 2012.11.06.	_ADV_FSP_3_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Magas szintű TOE terv. 2012.11.06.	_ADV_ARC_1_TDS_2_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Felhasználói kézikönyv. 2012.11.06.	_AGD_OPE_1_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Fejlesztési környezet biztonsága. 2012.11.06	_ALC_DVS_1_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - A vizsgálat kiterjedtsége. 2012.11.06	_ATE_COV_2_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - A vizsgálat mélysége. 2012.11.06	_ATE_DPT_1_2012-11-06.pdf
Dokumentum	SDX „core” modul v3.0.0 - Tesztelési jegyzőkönyv. 2012.11.06.	_ATE_FUN_1_2012-12-03.pdf
Dokumentum	Nyilatkozat a fejlesztés biztonsági körülményeiről	E_Group_Nyilatkozat_a_fejlesztes_biztonsagi_korulmenyeirol.docx
Dokumentum	Tesztelési jegyzőkönyv és tesztesetek	E_Group_Tesztelesi_jegyzokonyv_2012-12-03.doc; log.zip
Dokumentum	MELASZ megfelelőségi Tanúsítvány.	melasz tanu_2009_egroup.pdf
Dokumentum	Megfelelőség a műszaki normatíváknak nyilatkozat.	E_Group_Nyilatkozat_a_muszaki_normativaknak_valo_megfelelosegrol.docx

Fejlesztő:

E-GROUP ICT Software Zrt.

1062 Budapest Váci út 1-3.

3 AZ SDX „CORE” MODUL V3.0.0 BEMUTATÁSA

Az E-GROUP által kifejlesztett, PKI alapokon nyugvó SDX (Signed Document eXpert) termékcsalád az elektronikus dokumentumok hitelesítését, hitelességének ellenőrzését, tikosítását és időbélyeggel való ellátását biztosító kliens- és szerveroldali komponensekből áll. Az SDX „core” modul v3.0.0 – az SDX termékcsalád legfontosabb modulja, az első magyarországi minősített elektronikus aláíró alkalmazás továbbfejlesztése – egy Elektronikus Aláírás-létrehozó és Kezelő Alkalmazás, amely elektronikus dokumentumok elektronikus aláírását és elektronikusan aláírt dokumentumok aláírásának teljes körű ellenőrzését támogatja. Alapvetően két fő funkciója van a SDX „core” modul -nak :

- Elektronikus aláírás-létrehozó funkció
- Elektronikus aláírás-ellenőrző funkció

A folyamat mindkét funkció esetén az aláírás létrehozására és ellenőrzésére vonatkozó előírásokat definiáló Elektronikus Aláírási Szabályzat (EASZ) követelményeinek megfelelően működik. Az SDX egy EASZ független alkalmazás, ami azt jelenti, hogy az elvégzendő folyamatokhoz és döntésekhez szükséges paraméterek nincsenek a program kódjában rögzítetten kódolva, hanem külső állományból „paraméterezhető” a működés, azaz bármilyen későbbiekben meghatározott EASZ probléma nélkül használható az alkalmazásban, az EASZ bármikor megváltoztatható az alkalmazás változása nélkül és a felhasználó előírásaihoz igazítható. Az alkalmazandó EASZ egy XML struktúrában, szabványos, formalizált nyelven áll rendelkezésre, így ugyanaz a program akár aláírásonként eltérő feladatokat láthat el.

3.1 A SDX aláírás-ellenőrző funkció komponenseinek azonosítása

Az SDX aláíró alkalmazás „core” (engine) modulja a CWA 14171–ben előírt komponenseknek egy részhalmazát implementálja a saját kódjában, a nem SDX-ben implementált komponenseket a Microsoft CryptoAPI (amely az MS Windows operációs rendszer része) és ezen keresztül a Cryptographic Service Provider (CSP) alrendszer (BALE, olvasó ill. aláíró kulcsok kezelésére pl. a BALE gyártó által biztosított) tartalmazza. A tanúsítványok megjelenítésére a környezet az MS CryptoAPI kiegészítését a CAPICOM felületet használhatja. (Ez már az újabb Windows operációs rendszerek része, a korábbiakhoz pedig kiegészítésként installálható Microsoft által készített komponens.)

SDX által megvalósított komponensek:

SDP: Az SDP komponens vezérli az aláírt dokumentum megjelenítését. Az SDX „core” (engine) modulja nem tartalmaz ehhez kapcsolódó függvényeket, az aláírt dokumentum megjelenítése a környezet feladata.

SAV: Az aláírói tulajdonságok megjelenítésére szolgál. Az SDX „core” (engine) modulja nem tartalmaz ehhez kapcsolódó függvényeket, az aláíráshoz használandó, vagy felhasznált adatok tulajdonságai az interfészen keresztül megadandók, illetve kinyerhetők, de azok megjelenítése a környezet feladata.

VIC: Ez a felhasználói felülete, interfésze az SDX alkalmazásnak. Az SDX „core” (engine) modulja nem tartalmaz GUI-jellegű felhasználó interfészt, a kivezetett függvények meghívása, az interfészen a paraméterek átadása a környezet feladata.

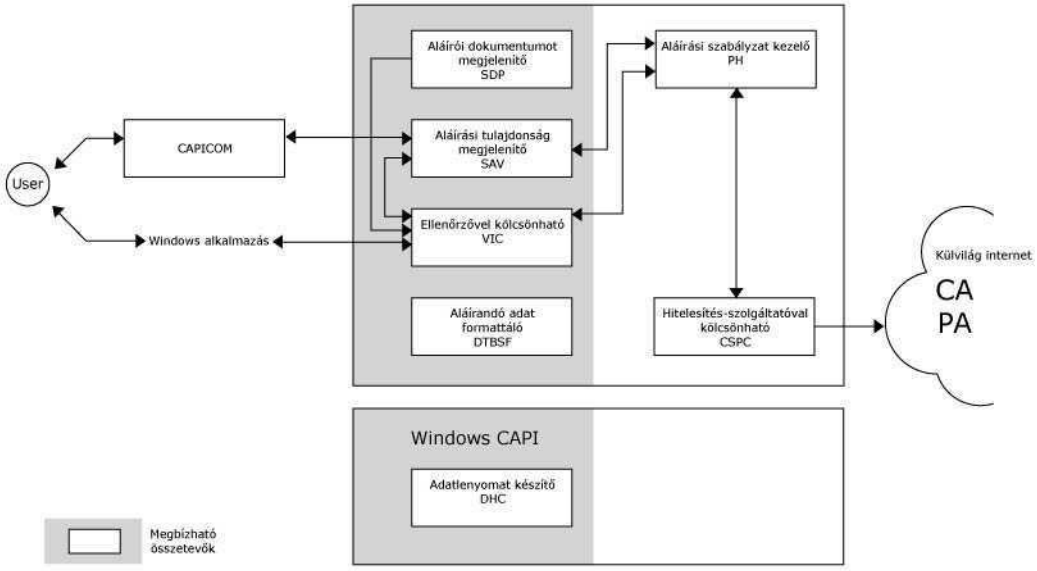
DTBSF: Az ETSI 101 903 szabványnak megfelelően előállítja és formázza az aláírásra kerülő adatokat. (<SignedInfo> előállítása)

CSPC: Ez a komponens vezérli a külső, aláírással kapcsolatos szolgáltatókkal való adatcserét. Ilyen pl. Hitelesítés szolgáltató – visszavonási lista, CA tanúsítvány, időpecsét stb.; EASZ szolgáltató – EASZ letöltés.

PH: (Policy Handler) EASZ kezelő komponens. Együtt működve a többi komponenssel biztosítja, hogy az egész aláírási folyamat az EASZ-ben előírtaknak megfelelően történik, és ezzel garantálja, hogy a létrejött aláírt dokumentum az EASZ-nek teljes mértékben megfelel.

Felhasznált egyéb komponensek:

DHC: A MS CAPI-n keresztül, a CSP alrendszer valósítja meg.



3.2 SDX aláírás-létrehozó funkció komponenseinek azonosítása

Az SDX aláíró alkalmazás „core” (engine) modulja a CWA 14170–ben előírt komponenseknek egy részhalmazát implementálja a saját kódjában, a nem SDX-ben implementált komponenseket a Microsoft CryptoAPI (amely az MS Windows operációs rendszer része) és ezen keresztül a Cryptographic Service Provider (CSP) alrendszer (BALE, olvasó ill. aláíró kulcsok kezelésére pl. a BALE gyártó által biztosított) tartalmazza. A tanúsítványok megjelenítésére a környezet az MS CryptoAPI kiegészítését a CAPICOM felületet használhatja. (Ez már az újabb Windows operációs rendszerek része, a korábbiakhoz pedig kiegészítésként installálható Microsoft által készített komponens.)

SDX által megvalósított komponensek:

SDP: Az SDP komponens vezérli az aláírói dokumentum megjelenítését. Az SDX „core” (engine) modulja nem tartalmaz ehhez kapcsolódó függvényeket, az aláírandó dokumentum megjelenítése és aláírásra történő átadása a környezet feladata.

SAV: Az aláírói tulajdonságok megjelenítésére szolgál. Az SDX „core” (engine) modulja nem tartalmaz ehhez kapcsolódó függvényeket, az aláíráshoz használandó, vagy felhasznált adatok tulajdonságai az interfészen keresztül megadandók, illetve kinyerhetők, de azok megjelenítése a környezet feladata.

SIC: Ez a felhasználói felülete, interfésze az SDX alkalmazásnak. Az SDX „core” (engine) modulja nem tartalmaz GUI-jellegű felhasználó interfészt, a kivezetett függvények meghívása, az interfészen a paraméterek átadása a környezet feladata. (kivétel az aláíró azonosító adat bevitel pl. PIN)

DTBSF: Az ETSI 101 903 szabványnak megfelelően előállítja és formázza az aláírásra kerülő adatokat. (<SignedInfo> előállítása)

SDC: Az aláírói dokumentum kiválasztását és megnyitását valósítja meg szerkesztésre. Az SDX alkalmazás nem ad lehetőséget az aláírói dokumentum szerkesztésére.

SDOC: Az ETSI 101 903 szabványnak megfelelően előállítja és formázza az aláírást kiszámító alrendszer számára az aláírandó adatokat. (<SignedInfo> transzformálása)

SLC: Az SDX alkalmazás tartalmaz naplózó funkciót: szabványos syslog-alapút (log4net) és debug üzeneteket (Sysinternals DebugView). A naplóba bejegyzésre kerül minden aláíráshoz: az aláírás időpontja, az aláíró tanúsítvány lenyomata, az aláírt dokumentum lenyomata, EASZ hivatkozás).

CSPC: Ez a komponens vezérli a külső, aláírással kapcsolatos szolgáltatókkal való adatcserét. Ilyen pl. Hitelesítés szolgáltató – visszavonási lista, CA tanúsítvány, időpecsét stb.; EASZ szolgáltató – EASZ letöltés.

PH: (Policy Handler) EASZ kezelő komponens. Együtt működve a többi komponenssel biztosítja, hogy az egész aláírási folyamat az EASZ-ben előírtaknak megfelelően történik, és ezzel garantálja, hogy a létrejött aláírt dokumentum az EASZ-nek teljes mértékben megfelel.

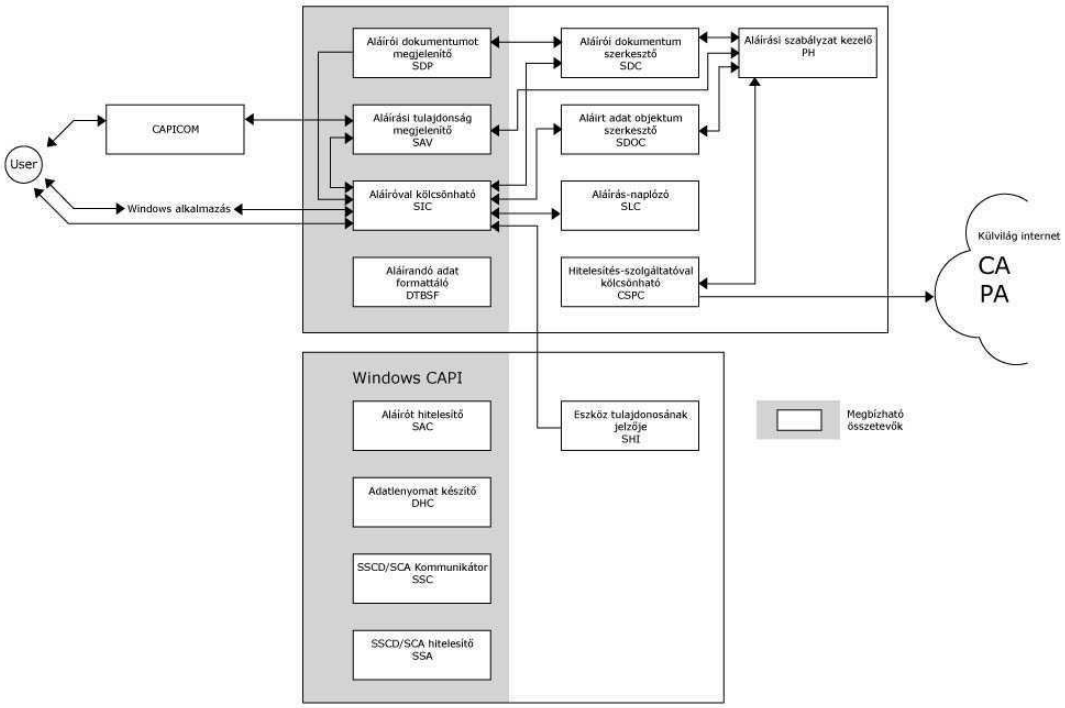
Felhasznált egyéb komponensek:

SAC: A MS CAPI-n keresztül, a CSP alrendszer valósítja meg.

DHC: A MS CAPI-n keresztül, a CSP alrendszer valósítja meg.

SSC: A MS CAPI-n keresztül, a CSP alrendszer valósítja meg.

SSA: A MS CAPI-n keresztül, a CSP alrendszer valósítja meg.



4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

A „Signed Document eXpert (SDX) „core” modul program v3.0.0 azonosítójú elektronikus aláírási termék" megfelel az alábbi követelményeknek:

- Kötelezően betartandó normatívák
  - 2001. évi XXXV. törvény az elektronikus aláírásról,
- Önként vállalt normatívák
  - MATRIX által vizsgált megfelelés
    - A Miniszterelnöki Hivatalt vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
    - Megfelelés az algoritmikus követelményeknek
      Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság EF/26838-x/2011 határozata.
    - Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
    - CWA 14170:2001 (E) – Security Requirements for Signature Creation Applications,

- CWA 14171:2001 (E) – Procedures for Electronic Signature Verification.

- Fejlesztő, vagy más szervezetek által igazolt megfelelés
  - RFC 3275: XML-Signature Syntax and Processing,
  - ETSI TS 101 903 V1.2.2 (2004-04): XML Advanced Electronic Signatures (XAdES),
  - ETSI TR 102 038 V1.1.1 (2002-04): XML format for Signature Policies,
  - MMM 001:2005. Egységes MELASZ formátum elektronikus aláírásokra. Verzió:1.0.

Az aláírási termék megfelel a fenti követelményeknek a 4.2 pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

- A tanúsítás kizárólag a bevizsgált program modulokra vonatkozik, bárminemű változtatás esetén a módosított verzióra jelen tanúsítás érvénytelen.
- Nem képezi a tanúsítás tárgyát a program működési környezete, így az
  - operációs rendszer,
  - a felhasznált külső szoftver modulok illetve programok,
  - a működéshez szükséges hardver elemek.

4.2 Működési környezet

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

4.2.1 Hardver és szoftver környezet

A vizsgált aláírási termék 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.

4.2.1.1 Operációs rendszer

Az „Signed Document eXpert (SDX) „core” modul az alábbi operációs rendszereken fut:

- Microsoft Windows XP (minimum Service Pack 3)
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003

- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

Minden operációs rendszerben az elérhető legmagasabb Service Pack változat alkalmazása ajánlott.

A vizsgált aláírási termék az alap operációs rendszeri szolgáltatásokon túlmenően a kriptográfiai műveletek végzésekor jelentős mértékben támaszkodik a Microsoft Crypto API által megvalósított függvényekre.

A vizsgált aláírási termék biztonságos használatának előfeltétele, hogy az operációs rendszert megfelelően biztonságos konfigurációban használjuk.

4.2.1.2 A bevizsgált program komponensek azonosítása

A tanúsítás érvényessége csak az alábbi, vizsgált programverzióra vonatkozik.

telepítés helye	NÉV	MÉRET	SHA256 LENYOMAT
system32 *	SDX2Engine.dll	965.056	867010bc2894a28f8832a89ed0582f7e9e39ab9269c60db4346dfa911a44b14e

4.2.1.3 BALE eszköz

Az SDX alkalmazás minősített aláírás létrehozására csak olyan biztonságos aláírás-létrehozó eszközzel (BALE) használható, amely szerepel a Nemzeti Média- és Hírközlési Hatóság (NMHH) 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 CSP modul megbízhatóságára. A BALE csak olyan CSP-vel használható, amelyet a BALE gyártója szállít, vagy amelynek fejlesztője garantálja a CSP biztonságos működését.

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

Intelligens kártya (Smartcard) alkalmazás esetén előnyben kell részesíteni az olyan CSP használatát, amely a BALE-t képes saját Pinpad-dal rendelkező (Class 2) olvasóval használni, ezzel mellőzve a könnyen támadható normál billentyűzet használatát.

Minősített elektronikus aláírás létrehozatalához kizárólag megfelelően megszemélyesített BALE használható.

4.2.1.4 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.

4.2.2 Személyi védelem

Hivatali felhasználás esetén az üzemeltetés során a személyi védelem tekintetében az alábbi intézkedések betartásáról kell gondoskodni:

- Hozzáértő adminisztrátorokat és felhasználókat kell az aláírási termék és az általa tartalmazott titkos adatok kezelésére alkalmazni.
- Az összes adminisztrátor és felhasználó magas szinten ismerje a biztonsági szabályzatot, amely szerint az aláírási termék 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 az aláírási termék 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.).

4.2.3 A fizikai védelem

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

- Az aláírási termék használatát biztosító rendszer által tartalmazott hardver, szoftver és firmware elemeket megfelelően kell védeni az illetéktelen fizikai módosítások ellen.
- Az aláírási termék által használt kommunikációs csatornákat megfelelően védeni kell az illetéktelen fizikai módosítások ellen.
- Az aláírási termék által használt kommunikációs csatornákat megfelelő módon védeni kell az illetéktelen lehallgatás ellen. Lehallgatás alatt logikai (pl. kémprogramok) és fizikai (EMC) módszerekkel végzett adatgyűjtés értendő.

4.2.4 Szállítás és telepítés

Az alkalmazás telepítésével kapcsolatos biztonsági előírások:

- A program telepítőkészletét 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.

4.2.5 Algoritmusok és kapcsolódó paraméterek

Az elvégzett vizsgálat alapján megállapítható, hogy a tanúsítvány 3 éves érvényességi időtartama alatt a vizsgált alkalmazás által támogatott alábbi kriptográfiai algoritmuskészlet jelenlegi ismereteink szerint megfelelően biztonságos marad:

- sha256 lenyomatképző függvény
- emsa-pkcs1-v1.5 feltöltő algoritmus
- RSA aláíró algoritmus 2048 bites kulccsal

Az sha1 lenyomatképző függvény és az 1024 bites RSA kulcs használata jelenleg még nem tiltott, de a támadási módszerek fejlődésével fel kell készülni ezen algoritmusok és paraméterek használatának megszüntetésére.

A szolgáltatónak és a felhasználónak folyamatosan figyelnie kell a felhasználható kriptográfiai algoritmusokkal kapcsolatos határozatokat, és az elektronikus aláírás használata során a megfelelő algoritmusokat előíró Elektronikus Aláírási Szabályzatot (EASZ) kell használniuk.

A fentiek alapján javasolt az sha256 lenyomatképző függvény és a 2048 bites RSA kulcs használata új tanúsítványok kiadása és új aláírások létrehozása esetén.

4.3 Értékelési módszertan

Az értékelés nyelvezete a Közös Szempontrendszerben meghatározott, az értékelés módszertanának alapját a Közös Szempontrendszerhez használt módszertani ajánlás képzi.

A tanúsítási eljárás során elvégzett, fejlesztőktől független értékelő vizsgálat az MSZ ISO/IEC 15408 EAL3 szint által megkövetelthez hasonló tartalmú és mélységű volt, ami a lehető legnagyobb garanciát biztosítja a fejlesztő számára a tervezői fázisban alkalmazott pozitív biztonsági megközelítésből anélkül, hogy a már meglévő és alapos fejlesztői gyakorlatot lényegesen megváltoztatná.

A fejlesztő által a vizsgálatra átadott részletes dokumentumok elemzése és az elvégzett független működési tesztek eredményeit szakterületi audit jelentésekben foglaltuk össze, amelyek főbb megállapításait és az azokban megfogalmazott környezeti követelményeket tartalmazza a jelen értékelési jelentés.

A vizsgálat az alábbi garancia összetevőkre terjedt ki:

ADV osztály: Fejlesztés

ADV_ARC.1

ADV_FSP.3

ADV_TDS.2

AGD osztály: **Útmutató dokumentumok**

AGD_OPE.1

AGD_PRE.1

ALC osztály: **Az életciklus támogatása**

ALC_CMC.3

ALC_CMS.3

ALC_DEL.1

ALC_DVS.1

ALC_LCD.1

ATE osztály: **Vizsgálatok (tesztek)**

ATE_COV.2

ATE_DPT.1

ATE_FUN.1

ATE_IND.2 (auditor)

AVA osztály: **A sebezhetőség felmérése**

AVA_VAN.2 (auditor)

4.4 Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy az E-GROUP ICT Software Zrt által fejlesztett Signed Document eXpert (SDX) „core" modul program v3.0.0 azonosítójú elektronikus aláírási termék megfelel a normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben.

A megfelelés biztonsági garancia szintje a **Common Criteria** értékelési rendszere szerinti **EAL 3** szinthez hasonló, ami a fejlesztőktől függetlenül garantált biztonság közepes szintjét jelenti.

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

5 RÖVIDÍTÉSEK

Rövidítés	Tartalom
ALA	Aláírás Létrehozó Alkalmazás
BALE	Biztonságos Aláírás-Létrehozó Eszköz
CC	(Common Criteria) MSZ ISO/IEC 15408. Az informatikai biztonság értékelésének közös szempontrendszere
EASZ	Elektronikus Aláírási Szabályzat
TOE	Target of Evaluation – a VT eredeti, angol nyelvű megfelelője
VT	Vizsgálat Tárgya

Dokumentum vége