TANÚSÍTVÁNY (E-EG05T-TAN.SW) MELLÉKLETE

Dokumentumazonosító:	TAN.SW.ME-01	
Projektazonosító:	E-EG05T	E-Group Rt. 2005
MATRIX tanúsítási igazgató:	Dr. Szőke Sándor	
Kelt:	Budapest, 2005. augusztus 25.	
	..... MATRIX tanúsítási igazgató	

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

Az E-Group Magyarország Rt. által kifejlesztett Signed Document eXpert (SDX) Professional ver. 1.0. Elektronikus Aláírás-létrehozó és Kezelő Alkalmazást (továbbiakban: SDX Professional vagy ALA) a Hunguard Kft. bevizsgálta, és a vizsgálat eredményeképpen a vonatkozó normatíváknak való megfelelőséget igazoló tanúsítványt (HUNG-T-017/2004) állított ki 2004. február 15-én. A programon végzett funkcionális és biztonsági részeket is érintő fejlesztések szükségessé tették az alkalmazás továbbfejlesztett verziójának vizsgálatát, amelynek elvégzésével az E-Group Rt. a Mátrix Kft.-t bízta meg.

A Mátrix Kft. áttanulmányozta az E-Group Rt. által átadott fejlesztői dokumentumokat, elemezte a kötelezően betartandó és az önként vállalt normatíváknak való megfelelést. A fejlesztő által biztosított éles SDX Professional alkalmazás segítségével ellenőrizte a fejlesztő által átadott és teszt jegyzőkönyvben is rögzített tesztesetek eredményét és a fejlesztőktől független teszteket is végzett.

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

2 A VIZSGÁLAT TÁRGYA

Megnevezés: „Signed Document eXpert (SDX) Professional ver. 1.0.0.157 elektronikus aláírási termék"

2.1 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	DÁTUM	ADAT-HORDOZÓ
Szoftver	SDX Professional Edition Telepítő készlet	1.0.0.157	2005.07.25.	CD
Dokumentum	E-Group Magyarország Rt. Informatikai szabályzat	v.1.0		Papír
Dokumentum	E-Group Alkalmazások tervezése, fejlesztése. Minőségirányítási eljárás ME-07-06	v.01.12.	2002.05.03.	Papír
Dokumentum	E-Group Alkalmazások tervezése, fejlesztése. Minőségirányítási eljárás ME-07-06	v.01.14.	2003.11.14.	Papír
Dokumentum	E-Group Alkalmazások Tesztelés Minőségirányítási Eljárás ME-07-08	v.01.42.	2002.05.07.	Papír
Dokumentum	ACM_CAP.3 / SDX Professional 1.0. Konfigurációmenedzsment eljárások.		2003.11.14.	CD+papír
Dokumentum	ADO_DEL.1 / SDX Professional 1.0. Szállítási dokumentáció.		2003.11.14.	CD+papír
Dokumentum	ADO_IGS.1 / SDX Professional 1.0. Telepítési útmutató.		2005.07.25..	CD+papír
Dokumentum	ADV_FSP.1 / SDX Professional 1.0. Funkcionális specifikáció.		2005.07.25.	CD+papír
Dokumentum	ADV_HLD.2 / SDX Professional 1.0. Magas szintű terv.		2003.11.14.	CD+papír
Dokumentum	AGD_USR.1 / SDX Professional 1.0. Felhasználói kézikönyv.		2005.07.25.	CD+papír
Dokumentum	ALC_DVS.1 / SDX Professional 1.0. Fejlesztési környezet biztonsága.		2003.08.19.	CD+papír
Dokumentum	ATE_COV.2 / SDX Professional 1.0. A vizsgálat kiterjedtsége.		2005.07.25.	CD+papír
Dokumentum	ATE_DPT.1 / SDX Professional 1.0. A vizsgálat mélysége.		2005.07.25.	CD+papír
Dokumentum	ATE_FUN.2 / SDX Professional 1.0 Functional Tests		2005.07.25.	CD+papír
Dokumentum	AVA_VLA.1 / SDX Professional 1.0. Sebezhetőség vizsgálat.		2003.12.04.	CD+papír
Dokumentum	Nyilatkozat a biztonsági körülményekről		2005.08.02.	Papír

Fejlesztő:

E-Group Magyarország Rt.

1117 Budapest, Hauszmann Alajos u. 3.

3 AZ SDX PROFESSIONAL BEMUTATÁSA

A Signed Document eXpert (SDX) Professional egy Elektronikus Aláírás-létrehozó és Kezelő Alkalmazás, amely elektronikus dokumentumok elektronikus aláírását és elektronikusan aláírt dokumentumok aláírásának teljes körű ellenőrzését támogatja. A segítségével elvégezhető feladatok:

- Dokumentumok elektronikus aláírása során a kiválasztott dokumentum(ok) a választható aláírási szabályzat szerint a kiválasztott tanúsítvány felhasználásával aláírásra kerül(nek), az aláírt dokumentum(ok) egy szabványos, XAdES formátumú .SDX kiterjesztésű állományba kerül(nek)

- Elektronikusan aláírt dokumentumokat tartalmazó .SDX állományok hitelességének ellenőrzése során az alkalmazás az aláírás összes komponensének teljeskörű on-line ellenőrzése alapján eldönti, hogy az aláírás hiteles-e

A program mindkét funkció esetén a megfelelő Elektronikus Aláírási Szabályzat (EASZ) követelményeinek megfelelően működik. Az SDX Professional egy EASZ független alkalmazás, ami azt jelenti, hogy az elvégzendő feladatok nincsenek a program kódjában rögzítetten kódolva, hanem külső állományból „paraméterezhetően" a működés 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.

A program működése során egyes funkciókat külső programok illetve program komponensek meghívásával valósít meg.

- Az aláírandó/aláírt dokumentumok megjelenítésére a megfelelő külső programokat használja. Az idegen, nem bevizsgált programok alkalmazásában rejlő veszélyforrásra minden esetben felhívja a felhasználó figyelmét.

- A kriptográfiai műveletek elvégzésére a MS Crypto API függvényeit használja,

- A minősített aláírás elvégzését és az ehhez kapcsolódó egyes funkciókat a BALE eszköz, illetve az azt a MS Crypto API számára szabványos felületen elérhetővé tevő CSP modul segítségével végzi.

Az SDX Professional Windows operációs rendszereken fut, szolgáltatásai a böngésző (Explorer) menüjén keresztül érhetők el a feldolgozni kívánt állomány(ok) kijelölése után.

Az SDX Professional főbb tulajdonságai:

- önálló alkalmazás otthoni és irodai környezetre,

- MS Windows böngészőbe integrált működés,

- X.509 tanúsítványok kezelése,
- RFC3161 szerinti időbélyeg szolgáltatás támogatása,
- CRL és OCSP alapú tanúsítvány ellenőrzés,
- XAdES formátumú .SDX dokumentum használata,
- egymásba ágyazott, többszörös aláírás struktúrák támogatása,
- XML formátumú, szabványos Elektronikus Aláírás Szabályzatok használata,
- BALE kezelés a MS Crypto API felhasználásával,
- az alkalmazás programkomponenseinek védelme elektronikus aláírással.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

A „Signed Document eXpert (SDX) Professional ver. 1.0.0.157 elektronikus aláírási termék" megfelel az alábbi követelményeknek:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról,
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
- EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures,
- CWA 14170:2001 E – Security Requirements for Signature Creation Applications,
- CWA 14171:2001 E – Procedures for Electronic Signature Verification,
- 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.

Az aláírás létrehozó modul 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 részét 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 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.

4.2.1.1 Operációs rendszer

Az SDX Professional az alábbi operációs rendszereken fut:

– Windows 98 OSR2,

– Windows NT Service Pack 5, vagy magasabb változat,

– Windows 2000 összes változat

– Windows XP összes változat

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

Az alkalmazás futtatásához szükséges minimum böngésző verzió:

– Microsoft Internet Explorer 6.0

Ajánlott a 128 bites böngésző verzió alkalmazása.

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

A VT biztonságos használatának előfeltétele, hogy az operációs rendszert megfelelően biztonságos konfigurációban használjuk. A Windows 2000 EAL4+ tanúsítással rendelkezik, a Windows XP Professional jelenleg biztonsági tanúsítás alatt áll. A tanúsítással rendelkező

rendszereket a biztonságos működtetés érdekében a tanúsításban megfogalmazott feltételek betartásával kell telepíteni és üzemeltetni.

A fentiektől eltérő Windows operációs rendszer is használható, ez esetben azonban csak szoftveres úton nem garantálható az operációs rendszer megfelelősége az adott feladatra. Ilyen esetben fokozottabban kell ügyelni a rendszer fizikai biztonságára és az alkalmazott üzemeltetési védelmi intézkedések szigorú betartására.

4.2.1.2 A bevizsgált program komponensek azonosítása

NÉV	VERZIÓ	MÉRET	SHA1 LENYOMAT
SDX.dll	1.0.0.157	280 200	4a1c8c2a80b8d6859839 4d70f913991781977f93
SDXFree.exe	1.0.0.128	300 680	dc9bdd80d41c995ee3f1 b9556f98785fcb764b0e
SDXShellProp.dll	1.0.0.27	149 128	c350b44973450ade7b19 391d3e725d5d6a63675d
Signer.dll	1.0.0.105	91 784	fce0431e6a96ae3a2d09 e93ff5e0868857685df7

A tanúsítás érvényessége csak a vizsgált programverziókra vonatkozik.

4.2.1.3 BALE eszköz

Az SDX Professional alkalmazás 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 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.

A minősített elektronikus aláírás létrehozatalhoz 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 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.).

4.2.3 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.

4.2.4 Szállítás és telepítés

Az alkalmazás telepítésével kapcsolatos biztonsági előírások:

- 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.

4.2.5 Algoritmusok és kapcsolódó paraméterek

Az alkalmazott Aláírási Szabályzatnak garantálnia kell, hogy az aláírás létrehozása során az alábbi algoritmusok illetve függvények kerülnek felhasználásra:

Az aláírandó adathalmaz lenyomatának létrehozására (hash) használt függvény:

Sha-1 FIPS PUB 180-1. (1995) / ISO/IEC 10118-3 (1998).

A kitöltő adatok hozzáadására használt függvény:

emsa-pkcs-v1_5 RSA Laboratories, .PKCS #1 v2.0 (1998).

Aláíró algoritmus:

RSA min. 1024 bites kulcsméret

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:

ACM osztály:	A konfigurációmenedzselés	ACM_CAP.3
ADO osztály:	Kiszállítás és üzemeltetés	ADO_DEL.1 ADO_IGS. 1
ADV osztály:	Fejlesztés	ADV_FSP.1 ADV_HLD.2
AGD osztály:	Útmutató dokumentumok	AGD_USR.1
ALC osztály:	Az életciklus támogatása	ALC_DVS.1
ATE osztály:	Vizsgálatok (tesztek)	ATE_COV.2 ATE_DPT.1 ATE_FUN.2

AVA osztály: A sebezhetőség felmérése AVA_VLA.1

4.4 Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy az E-Group Rt. által fejlesztett SDX Professional 1.0.0.157 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

ALA	Aláíró alkalmazás
BALE	Biztonságos Aláírás-Létrehozó Eszköz
CC	(Common Criteria) MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere
VT	Vizsgálat Tárgya

Dokumentum vége