TANÚSÍTVÁNY (E-EG09T-TAN.SW) MELLÉKLETE

Dokumentumazonosító	TAN-SW-01.ME-01	
Projektazonosító	E-EG09T	E-Group ICT Software Zrt. 2009.
MATRIX tanúsítási igazgató	Dr. Szőke Sándor	
Kelt	Budapest, 2009. május 15.	
	…… 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 (2.0.0.4 verzió) Aláírás-létrehozó és Kezelő Alkalmazást, amelyet 2005-ben bevizsgált a MATRIX Kft. A vizsgálat eredményeként 2006. február 23-án a MATRIX kiállította a megfelelőséget igazoló E-EG05T2-TAN.SW tanúsítványt 3 éves érvényességgel. A tanúsítás érvényessége lejárt és az E-GROUP kisebb fejlesztéseket is végzett a programon, ezért megrendelte az alkalmazás aktuális verziójának 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 éles SDX Professional ME 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 (VT)

Megnevezés: „Signed Document eXpert (SDX) Professional M Edition ver. 2.0.1 azonosítójú elektronikus aláírási termék"

2.1 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	DÁTUM	ADAT-HORDOZÓ
Szoftver	SDX Professional M Edition Telepítő készlet	2.0.1	2009.04.30	Elektronikus állomány
Szoftver	TESZT ESETEK		2009.04.28.	Elektronikus állomány
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.1 / SDX Professional M Edition. Konfigurációmenedzsment eljárások.		2009.03.03.	Elektronikus állomány
Dokumentum	ADO_DEL.1 / SDX Professional M Edition. Szállítási dokumentáció.		2009.03.03.	Elektronikus állomány
Dokumentum	ADO_IGS.2 / SDX Professional M Edition. Telepítési útmutató.		2009.01.14.	Elektronikus állomány
Dokumentum	ADV_FSP.2 / SDX Professional M Edition. Funkcionális specifikáció.		2009.03.03.	Elektronikus állomány
Dokumentum	ADV_HLD.2 / SDX Professional 1.0. Magas szintű terv.		2009.03.03.	Elektronikus állomány
Dokumentum	AGD_USR.2 / SDX Professional M Edition. Felhasználói kézikönyv.		2009.02.19.	Elektronikus állomány
Dokumentum	ALC_DVS.1 / SDX Professional M Edition. Fejlesztési környezet biztonsága.		2009.03.03.	Elektronikus állomány
Dokumentum	ATE_COV.2 / SDX Professional M Edition. A vizsgálat kiterjedtsége.		2009.03.03.	Elektronikus állomány
Dokumentum	ATE_DPT.2 / SDX Professional M Edition. A vizsgálat mélysége.		2009.03.03.	Elektronikus állomány
Dokumentum	ATE_FUN.2 / SDX Professional M Edition. Tesztelési jegyzőkönyv		2009.03.16.	Elektronikus állomány
Dokumentum	AVA_VLA.1 / SDX Professional M Edition.		2009.03.03.	Elektronikus állomány

	Sebezhetőség vizsgálat.		
Dokumentum	Nyilatkozat a fejlesztés biztonsági körülményeiről		Papír
Dokumentum	Nyilatkozat egyes önként vállalt normatíváknak való megfelelésről		Papír
Dokumentum	MELASZ megfelelőségi vizsgálat tanúsítási jelentése.-2005-0004-BME-IK	2005.12.22.	Elektronikus állomány
Dokumentum	MELASZ megfelelőségi Tanúsítvány.-MMMEAA-2006/004. 2005. december 19	2005.12.19.	Elektronikus állomány

Fejlesztő:

E-GROUP ICT Software Zrt.

1117 Budapest, Hauszmann Alajos u. 3.

3 AZ SDX PROFESSIONAL M EDITION BEMUTATÁSA

Az E-GROUP ICT Software Zrt 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 Professional M Edition – az SDX termékcsalád legfontosabb kliens oldali 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 folyamatot kezel:

- Elektronikus dokumentumok **hitelesítése** – elektronikus aláírással és időbélyeggel való ellátása – 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 .SDXM kiterjesztésű állományba kerül(nek), amelyek megfelelnek a MELASZ által definiált egységes magyar aláírási formátumnak az „Egységes MELASZ formátum (MELASZ Munkacsoport Megállapodás)” 1.00 verziójának. A formátumot az Informatikai és Hírközlési Minisztérium ajánlásként fogadta el, mint „IHM ajánlás a közigazgatásban alkalmazható elektronikus aláírás műszaki specifikációjáról”. Ezen együttműködési képessége alapján probléma nélkül alkalmazható a Ket. – a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény – által előírt eljárások kialakításában.

- Elektronikusan aláírt dokumentumokat tartalmazó .SDXM állományok **hitelességének ellenőrzése** során az alkalmazás az aláírás összes komponensének teljes körű ellenőrzése alapján eldönti, hogy az aláírás hiteles-e

A folyamat mindkét funkció esetén az aláírás létrehozására és ellenőrzésére vonatkozó előírásokat definiáló Elektronikus Aláírási Szabályzat (EASZ) követelményeinek megfelelően működik. Az SDX Professional 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.

Az SDX Professional program működése során nagy mértékben támaszkodik a Microsoft Windows operációs rendszer erőforrásaira, eszközeire, számos funkciót 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 (Cryptographic Service Provider) modul segítségével végzi.

Az SDX Professional Windows operációs rendszereken fut, szolgáltatásai az intéző/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 operációs rendszer felhasználói felületébe integrált működés,
- X.509 tanúsítványok kezelése,
- RFC3161 szerinti időbélyeg szolgáltatás támogatása,
- CRL vagy OCSP alapú tanúsítvány kezelés és ellenőrzés,
- XAdES formátumú .SDXM dokumentum használata,
- „MELASZ-ready” megfelelőség,
- egymásba ágyazott, többszörös aláírás struktúrák támogatása,
- XML formátumú, szabványos Elektronikus Aláírás Szabályzatok használata,
- hitelesített dokumentum archiválása a hosszú távú hitelesség ellenőrzés számára szükséges érvényesítő adatok elmentésével,
- ALE és BALE kezelés a MS Crypto API felhasználásával,
- az alkalmazás programkomponenseinek védelme elektronikus aláírással, valamint futás időbeni ellenőrzésével.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

A „Signed Document eXpert (SDX) Professional M Edition ver. 2.0.1 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
    - 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
    - Megfelelés az algoritmikus követelményeknek
      Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917-x/2008 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,
    - RFC 2560: On-line Certificate Status Protocol - OCSP,
    - 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 SDX Professional az alábbi operációs rendszereken fut:

- Windows NT 4.0 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 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. A Windows 2000 és a Windows XP Professional SP2 CC EAL4+ tanúsítással rendelkezik. A tanúsítással rendelkező operációs 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 fokozottabban kell ügyelni a rendszer fizikai biztonságára és az alkalmazott üzemeltetési védelmi intézkedések szigorú betartására.

4.2.1.2 A bevizsgált program komponensek azonosítása

A futtatható program komponensek azonos tárgykódból (object) két különböző módon kerülhetnek összeállításra (link). A két módozat abban különbözik, hogy a Windows operációs rendszerhez tartozó MFC (Microsoft Foundation Class Library) komponensek milyen módon kapcsolódnak az alkalmazáshoz. Az egyik az ún. dinamikus kapcsolódás (link), a másik pedig a statikus.

A vizsgált program verzió csak a dinamikusan kapcsolódó program komponenseket tartalmazza.

A tanúsítás érvényessége csak az alábbi, vizsgált programverzióra vonatkozik.

4.2.1.2.1 A DINAMIKUSAN kapcsolódó program komponensek azonosítása

telepítés helye	NÉV	VERZIÓ	MÉRET	SHA256 LENYOMAT
system32 *	SDX_Abt.dll	2.0.1.35	699.392	ead0b00bd4978e4c 20961b63436c147e 793239884c581216 a1596b1604fd2223
system32 *	SDX_Dlg.dll	2.0.1.32	1.005.928	6aa1f39965581b37 c347de94ec2ffeb2 ffd3938f3c0dbc99 28c38bf5194a5da8
system32 *	SDX_Vfy.dll	2.0.1.36	827.240	5574095d3dd91c19 d6cc798f1fd822c6 bfd68c8fee1599ba 7631d46c038549f7
system32 *	SDXEN.dll	2.0.1.35	69.120	810557fd37a4acf1 fbdb97c643a42600 020649c4e693a1f7 176907afcb941bf7
system32 *	SDXFreeM.exe	2.0.1.38	179.200	46c1350571c79dbb c45cf4709ee14d6f aa68634fe41cc811 6bf9b47cc75a5f95
system32 *	SDXHU.dll	2.0.1.34	73.728	dd0dc5108c9474d2 1c24f1721360f24b 28721b06997e3445 617e29345068ade9
system32	OCSPdll.dll	2.0.1.36	66.560	8aa76ebb3c7c8677 010f39905189913c 687f4c9e77ec4b14 85f6691ba995db2f
system32	SDX_EncDlg.dll	2.0.1.35	252.264	68cf3868896cbea1 36d196a4e6ebbcdc c1b60439cc93b6aa 365172644123 91a0
system32	SDX_Parts.dl	1.0.0.1	35.840	e404ad261f7b21b6 d2ba6d067d29d53d 83dce8a360cebbac 1820625373f10d0c
system32	SDXVN.dll	1.0.0.24	75.264	929f1661f7e8fa74

				9717f8b04278dd17 b0701db33b3a2f80 d980150b4be3cf74
system32	Signer.dll	2.0.1.11	698.728	ad38fbbd5989527a 4e8796bd4e19e227 5beabda49af21655 a173ae458228db24
program files	CertUpdate.exe	---	78.848	e7ad51c64b36d814 484bc1a7432fd9d5 87e142cd31747826 18ba24fc26e74cde
program files	SDX_Browser.dll	2.0.1.34	668.672	948a9852fb4ef95a 3933f1d73415e645 4bcb4f82e405f1d6 15acb679b31480f2
program files	SDX_Language.exe	1.0.0.1	24.064	4e3ae9779da9d275 b7bb6b082b161f85 707cda162128cc9b 637727ce840cd138
program files	SDX_Prop.dll	2.0.1.16	148.840	79840ac1e8068827 ac1d7b15225a48d6 d1414d2cbd88b91d 9026a5d4811d5aad
program files	SDX_SignAx.dll	1.0.0.28	448.000	404578b16f53d35a 8ad1ee8762b75c29 72869f5898d3023b 0a8414a74eae576a
program files	SDX_Starter.exe	---	72.192	b263880f8ad92d44 2f0354e27a8479f4 a05d250803a47903 9ec10744cbeae1ec
program files	SDXFreeM.exe	2.0.1.38	179.200	46c1350571c79dbb c45cf4709ee14d6f aa68634fe41cc811 6bf9b47cc75a5f95
program files	SDXGroupEditor.exe	1.0.0.21	147.968	f0e9d5803b4a3ac5 287af7e1f8ef02f0 95f08515ad0f565e e0a8af73888b25af

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.

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:

- A aláírási termék használatát biztosító rendszer által tartalmazott hardver, szoftver és firmware elemeket megfelelően kell védeni az illetéktelen fizikai módosítások ellen.
- A aláírási termék által használt kommunikációs csatornákat megfelelően védeni kell az illetéktelen fizikai módosítások ellen.
- A 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 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 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:

– ACM osztály:	A konfigurációmenedzselés	ACM_CAP.1
– ADO osztály:	Kiszállítás és üzemeltetés	ADO_DEL.1 ADO_IGS. 2
– ADV osztály:	Fejlesztés	ADV_FSP.2 ADV_HLD.2
– AGD osztály:	Útmutató dokumentumok	AGD_USR.2
– ALC osztály:	Az életciklus támogatása	ALC_DVS.1
– ATE osztály:	Vizsgálatok (tesztek)	ATE_COV.2 ATE_DPT.2 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 ICT Software Zrt által fejlesztett SDX Professional M Edition 2.0.1 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