TANÚSÍTVÁNY (E-DS07T_TAN-01.SW) MELLÉKLETE

Dokumentumazonosító	TAN-01.SW.ME-01	
Projektazonosító	E-DS07T	DSS Consulting Kft. 2007.
MATRIX tanúsítási igazgató	Dr. Szőke Sándor	
Kelt	Budapest, 2007. december 18.	
	…… MATRIX tanúsítási igazgató	

TARTALOMJEGYZÉK

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

A DSS Consulting Kft. (továbbiakban: DSS) 2006-ban kifejlesztette a Secure Digital Sign SDK ver. 1.0 elektronikus aláírás előállító és ellenőrző modult, amelynek bevizsgálásával a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft-t (továbbiakban: MATRIX) bízta meg. A tanúsítási eljárás eredményeképp a MÁTRIX 2006. december 15-én kiadta a megfelelőséget igazoló E-DS06T_TAN-01.SW azonosítójú tanúsítványt és annak E-DS06T_TAN-01.SW.ME-01 azonosítójú mellékletét.

A DSS 2007-ben továbbfejlesztette az alkalmazást, amelynek vizsgálatával ismét a MATRIX Kft-t bízta meg. A tanúsítási eljárás során a MATRIX a Secure Digital Sign SDK ver. 1.1. elektronikus aláírás előállító és ellenőrző modul (továbbiakban: SDS) elektronikus aláírási termék fokozott biztonságú aláírások létrehozására történő felhasználhatóságát vizsgálta az egységes követelményrendszer (Common Criteria) szerinti EAL-2 bizonyossági szinthez hasonló mélységben.

Az audit során a MATRIX áttanulmányozta a DSS által átadott fejlesztői dokumentumokat, megvizsgálta a kötelezően betartandó és az önként vállalt normatíváknak való megfelelést. A fejlesztő által biztosított éles SDS modul és a tesztet segítő keretalkalmazás segítségével ellenőrizte a fejlesztő által átadott és teszt jegyzőkönyvben is rögzített tesztesetek eredményét és a fejlesztőktől független teszteket is végzett.

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

A tanúsítási eljárás során a MATRIX felhasználta a korábbi eljárás során létrehozott vizsgálati anyagokat is.

2 A VIZSGÁLAT TÁRGYA

2.1 A Vizsgálat Tárgyának pontos megnevezése

„Secure Digital Sign SDK ver. 1.1. elektronikus aláírás előállító és ellenőrző modul” azonosítójú elektronikus aláírási termék.

2.2 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	DÁTUM	ADAT-HORDOZÓ
Szoftver	Secure Digital Sign SDK 1.1 Telepítő készlet	1.1.2893.19777	2007.12.03.	Elektronikus állomány
Szoftver	TESZT ESETEK	---	2007.12.03.	Elektronikus állomány
Dokumentum	DSS Consulting Kft. Projektvezetési módszertan		2007.12.03.	Elektronikus állomány

	bemutatása szoftverfejlesztésekhez			
Dokumentum	DSS Consulting Kft. Szoftverfejlesztési módszertan bemutatása .NET technológiájú fejlesztésekhez		2007.12.03.	Elektronikus állomány
Dokumentum	DSS Consulting Kft. Minőségbiztosítási anyagok		2007.12.03.	Elektronikus állomány
Dokumentum	DSS Consulting Kft. ISO 9001:2000 minőségirányítási rendszer tanúsítvány		2007.12.03.	Elektronikus állomány
Dokumentum	ACM_CAP.2 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. Konfigurációs tételek.	1.1	2007.12.03.	Elektronikus állomány
Dokumentum	ADO_DEL.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. A kiszállítás eljárásai.	1.2	2007.12.03.	Elektronikus állomány
Dokumentum	ADO_IGS.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. HW telepítés, SW telepítés, beindítás eljárásai. tése.	1.3	2007.12.03.	Elektronikus állomány
Dokumentum	ADV_FSP.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. Informális funkcionális leírás.	1.3	2007.12.03.	Elektronikus állomány
Dokumentum	ADV_HLD.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. A felsőszintű tervezés leírása.	1.3	2007.12.03.	Elektronikus állomány
Dokumentum	ADV_RCR.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. A kölcsönös megfelelés informális szemlélte	1.1	2007.12.03.	Elektronikus állomány
Dokumentum	AGD_ADM.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. Az adminisztrátori útmutató.	1.2	2007.12.03.	Elektronikus állomány
Dokumentum	ATE_COV.1 Secure Digital Sign SDK ver. 1.0	1.4	2007.12.03.	Elektronikus állomány

	elektronikus aláíró- és ellenőrző-modul. A lefedettség bizonyítéka.			
Dokumentum	ATE_FUN.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. Funkcionális vizsgálat.	1.3	2007.12.03.	Elektronikus állomány
Dokumentum	ATE_SOF.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. A TOE biztonsági funkció erősségértékelése.	1.2	2007.12.03.	Elektronikus állomány
Dokumentum	AVA_VLA.1 Secure Digital Sign SDK ver. 1.0 elektronikus aláíró- és ellenőrző-modul. Sebezhetőség vizsgálat.	1.2	2007.12.03.	Elektronikus állomány
Dokumentum	Az elektronikus aláíró és aláírás ellenőrző modulra vonatkozó követelmények.	1.1	2007.12.03.	Elektronikus állomány
Dokumentum	Nyilatkozat a fejlesztés körülményeiről, a vonatkozó biztonsági előírások betartásáról		2007.12.03.	Papír
Dokumentum	Nyilatkozat egyes normatíváknak való megfelelésről		2007.12.03.	Papír

2.3 A vizsgálat megrendelője

A Vizsgálat Tárgyát képező elektronikus aláírási terméket fejlesztette és az auditot megrendelte:

DSS Consulting Kft.
1113 Budapest, Nagyszőlős u 11-15.

3 A SECURE DIGITAL SIGN SDK BEMUTATÁSA

A DSS Consulting Kft. által fejlesztett Secure Digital Sign SDK, mint elektronikus aláírási termék elsődleges célja – megfelelve a Magyarországon hatályos elektronikus aláírásról szóló törvénynek és egyéb önként vállalt elektronikus aláírási termékekre vonatkozó normatíváknak – egy olyan fejlesztői függvénykönyvtár biztosítása, amelynek felhasználásával lehetőség nyílik az alkalmazói réteg(ek) számára, hogy hatékonyan, a lehető legkevesebb ráfordítással alkalmassá váljanak elektronikus aláírás(ok) létrehozására és ellenőrzésére.

Az SDS modul által biztosított funkciók két fő csoportra bonthatók:

- az első csoporthoz tartoznak azon funkciók, amely segítségével a modul lehetőséget biztosít szabványos elektronikus aláírások létrehozására, míg

- a második csoporthoz azon szolgáltatások tartoznak, amelyek felhasználásával a létrehozott elektronikus aláírások ellenőrizhetővé válnak, valamint a letagadhatatlanság hosszú távú bizonyítása végett archív formátumra hozhatók.

A modul által előállított elektronikus aláírással szemben támasztott interoperábilitási elvárásoknak megfelelően az aláírás formátuma megfelel az [1]-ben definiált aláírási formátumoknak mind a pillanatnyi, a rövid távú, a hosszú távú illetve az archív formátumot tekintve, ezáltal biztosítva a MELASZ-ready aláíró/ellenőrző alkalmazásokkal történő kölcsönös együttműködést.

A modul minden egyes eseményről aláírási naplót vezet, amely lehetőséget biztosít az egyes tevékenységek nyomon követésére.

3.1 Elektronikus aláírás létrehozásához kapcsolódó szolgáltatások

3.1.1 Aláírási formátum

Az SDS által létrehozott aláírási formátum megfelel a [2]-ben definiált XAdES-BES formátumnak.

Amennyiben az alkalmazói rendszer szükségessé teszi az aláírási szabályzatok kezelését, akkor az [1]-ben definiált módon nyílik lehetőség a kezelésükre és az így előálló formátum az XAdES-EPES követelményeinek is megfelel, legyen szó akár explicit akár implicit aláírási szabályzat hivatkozásról.

3.1.2 Aláírói tulajdonságok

Az aláíró személye és az ahhoz kapcsolható aláírási tulajdonságok kezelése az [1]-ben definiált módón történik. A modul által támogatott aláírási tulajdonságok:

- SignatureProductionPlace – aláírás létrejöttének helye,
- SignerRole, ClaimedRoles – állított aláírói szerepkörök.

Az aláíró személyét igazoló aláírói tanúsítványok az operációs rendszer tanúsítványtárolójából kerülnek feldolgozásra. Amennyiben egy adott aláírói tanúsítvány ALE illetve BALE eszközön került kibocsátásra, az aláírói modul lehetőséget biztosít a kártyán tárolt titkos kulcs elérésére, illetve a kártya által előállított aláírási érték felhasználására.

Az aláírói dokumentum formátumára a modul nem tesz megkötést, azaz tetszőleges formátumú adathalmaz aláírható, viszont a helyes megjelenítés érdekében az adatformátum pontos meghatározása szükséges.

3.1.3 Visszavonási információk

A modul lehetőséget biztosít az egyes elektronikus aláírásokhoz felhasznált hitelesítés szolgáltatótól származó aláírói tanúsítványokhoz tartozó visszavonási információk elérésére. Ezen információk megszerzésére két lehetőséget biztosít az SDS. Az egyik lehetőség a visszavonási listák (CRL) formájában elérhető információk beszerzése és feldolgozása, míg a második lehetséges mód az OCSP-n keresztüli visszavonási információ on-line lekérdezése. Az implementáció során követett szabványok a [3] és [4] dokumentumokban találhatók.

3.2 Elektronikus aláírás ellenőrzéséhez kapcsolódó szolgáltatások

3.2.1 Megbízható időpont kezelése

Az SDS által létrehozott elektronikus aláírások letagadhatatlanságának egyik feltétele egy megbízható időpont igazolása, amely biztosítja, hogy az aláírás a kérdéses időpont előtt készült. A modul ezen információ begyűjtését hiteles időbélyegzés szolgáltatótól származó időbélyeg kezelésével éri el. Az időbélyegzés szolgáltatóval történő kommunikáció az [5] dokumentumban foglaltak szerint történik. Az időbélyeg kérése, illetve az időbélyeg kérő személyének igazolása authentikációs tanúsítvány, felhasználó név és jelszó páros vagy egyedi URL alapján biztosított. Sikeres időbélyeg kérést követően a modul által előálló aláírási formátum megfelel a [2]-ben definiált XAdES-T formátumnak.

3.2.2 Érvényesség hosszú távú biztosítása

Az aláíráshoz a kezdeti ellenőrzés során begyűjtött kiegészítő információk csatolásával illetve a visszavonási információkra történő hivatkozások beillesztésével a modul teljesíti a [2]-ben definiált XAdES-C aláírási formátumra vonatkozó követelményeket.

A kivárási idő letelte után a modul lehetőséget biztosít az előálló aláírások archív formátumra való bővítésére. A bővítés két lépésben történik. Első fázisban az XAdES-C formátumban szereplő visszavonási információkra történő hivatkozásokon keresztül elérhető adatok és az aláírói tanúsítvány teljes hitelesítési láncában szereplő tanúsítványok kerülnek beillesztésre, majd az aláírás során használt kriptográfiai algoritmusok és az alkalmazott kulcsok kompromittálódása esetén bekövetkező fenyegetést kiküszöbölő archív időbélyeg kerül csatolásra az aláíráshoz. Amennyiben az összes kiegészítő információ rendelkezésre áll, az SDS által létrehozott aláírási formátum megfelel a [2]-ben definiált XAdES-A formátumnak.

3.3 Működési környezet

Az SDS program modul 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,
- az elektronikus aláírás elvégzését és az ehhez kapcsolódó egyes funkciókat az ALE eszköz, illetve az azt a MS Crypto API számára szabványos felületen elérhetővé tevő CSP (Cryptographic Service Provider) modul segítségével végzi.

3.4 Az SDS program modul főbb tulajdonságai

- fejlesztői függvénykönyvtár elektronikus aláírási termékek fejlesztéséhez,
- felhasználható otthoni és irodai környezetben,
- X.509 tanúsítványok kezelése,
- CRL vagy OCSP alapú tanúsítvány kezelés és ellenőrzés,

- XAdES formátumú 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.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

A „Secure Digital Sign SDK ver. 1.1 elektronikus aláíró- és ellenőrző-modul elektronikus aláírási termék" megfelel az alábbi követelményeknek:

- Kötelezően betartandó normatívák:
  - 2001. évi XXXV. törvény az elektronikus aláírásról,
  - 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- Önként vállalt normatívák:
  - MATRIX által vizsgált megfelelés:
    - 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 14170:2004 (E) – Security Requirements for Signature Creation Applications,
    - CWA 14171:2004 (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),
    - RFC 3280: Certificate and Certificate Revocation List (CRL) Profile

- RFC 2560: Online Certificate Status Protocol (OCSP)
- RFC 3161: Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)
- 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. Mivel az SDS modult nem önálló működésre tervezték, tipikus felhasználása esetén egy programfejlesztő integrálja saját elektromos aláíró alkalmazásába. Az alkalmazás fejlesztésénél figyelembe kell venni az alábbi feltételeket, amelyek betartása szükséges a modul helyes és biztonságos működéséhez.

4.2.1 Hardver és szoftver környezet

A vizsgált aláírási termék csak olyan környezetben használható elektronikus aláírások létrehozására, amelynek minden eleme kielégíti az általánosan 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 alkalmazás megfelelő használatához.

4.2.1.1 Operációs rendszer

Az SDS az alábbi operációs rendszereken használható:

- Windows 98,
- Windows 98 Second Edition,
- Windows Millenium Edition,
- Windows 2000 Service Pack 3,
- Windows XP Service Pack 2,
- Windows Server 2003.

4.2.1.2 Egyéb program komponensek

Az SDS modul működéséhez szükséges egyéb komponensek:

- Microsoft .NET Framework Version 2.0 Redistributable Package (x86) verzió: 2.0,
- Visual J# Redistributable Package verzió: 2.0,
- Microsoft Internet Explorer verzió: 5.01 (vagy későbbi)
- Microsoft Crypto API (a Windows operációs rendszer része)
- Víruskereső szoftver (amely képes megvédeni a modul és az egyéb felhasznált komponensek integritását, de legalább képes jelezni az integritás sérülését)

Az egyes programokat, program komponenseket megfelelően biztonságos forrásból kell beszerezni, a telepítés és üzemeltetés során pontosan be kell tartani a telepítési és felhasználói útmutatóban megfogalmazott utasításokat, követelményeket.

4.2.1.3 A bevizsgált program komponensek azonosítása

A tanúsítás érvényessége csak az alábbi, vizsgált programverzióra vonatkozik:

NÉV	VERZIÓ	MÉRET	SHA-256 LENYOMAT
DSS.SDS.dll	1.1.2893.19777	245 760	c33f0bb35d93744e 9116437cf3e476c3 b90af277e6395c4f e86f34186997fb21

A bevizsgálás során felhasznált egyéb komponensek azonosítása:

NÉV	VERZIÓ	MÉRET	SHA-256 LENYOMAT
DSS.SDSTest.exe	1.0.2524.34317	94 208	a937db74e9cdabf9 8320d706f9982fd9 e388f7b18f5cf9a0 4cc92bfc538c910e
DSS.DSM.Config.XML	---	5 026	6dc4453c1f217c91 5e1e6f373dd45b08 16fdd1145efd2054 b4685494461166a8

4.2.1.4 Hálózati működés

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

4.2.2 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.

4.2.3 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.

4.2.4 Algoritmusok és kapcsolódó paraméterek

Az alkalmazás csak a mindenkor érvényes szabályzásnak megfelelő algoritmusokkal és paraméterekkel használható. Az elektronikus aláíráshoz használható kriptográfiai algoritmusokat egységesen szabályozzák az Európai Unióban, aktuális információ az alábbi normatívából nyerhető:

ETSI TS 102 176-1 V2.0.0 (2007-11) Technical Specification
Electronic Signatures and Infrastructures (ESI);
Algorithms and Parameters for Secure Electronic Signatures;
Part 1: Hash functions and asymmetric algorithms

A specifikáció rendszeresen megújításra kerül, ezért a felhasználónak folyamatosan figyelemmel kell kísérnie az elektronikus aláírás létrehozatalához használható kriptográfiai algoritmusokra vonatkozó normatívák változását, s az annak megfelelő algoritmusokat és paramétereket kell használnia!

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 EAL2 szintű volt, ami mérsékelt garanciát biztosít a fejlesztő számára a tervezői

fázisban alkalmazott pozitív biztonsági megközelítésből anélkül, hogy a már meglévő és alapos fejlesztői gyakorlatot lényegesen megváltoztatná.

A vizsgálat az alábbi garancia összetevőkre terjedt ki:

Garanciaosztály	Garancia összetevők	
A konfiguráció menedzselése	ACM_CAP.2	Konfigurációs tételek
Kiszállítás és üzemeltetés	ADO_DEL.1	A kiszállítás eljárásai
	ADO_IGS.1	HV-telepítés, SV-telepítés, beindítás eljárásai
Fejlesztés	ADV_FSP.1	Informális funkcionális előírás
	ADV_HLD.1	A felsőszintű tervezés leírása
	ADV_RCR.1	A kölcsönös megfelelés informális szemléltetése
Útmutató dokumentumok	AGD_ADM.1	Az adminisztrátori útmutató
	AGD_USR.1	A felhasználói útmutató
Vizsgálatok	ATE_COV.1	A lefedettség bizonyítéka
	ATE_FUN.1	Funkcionális vizsgálat
	ATE_IND.2	Független vizsgálat – mintán
A sebezhetőség felmérése	AVA_SOF.1	A TOE biztonsági funkció erősségértékelése
	AVA_VLA.1	A sebezhetőség fejlesztői elemzése

A fejlesztő nem készítette el külön dokumentumként az AGD_USR.1 Felhasználói útmutatót, mivel az alkalmazást nem végfelhasználóknak szánták. A modul integrálásához szükséges valamennyi információ megtalálható az AGD_ADM.1 Adminisztrátori útmutatóban.

4.4 Biztonsági garancia szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a DSS Consulting Kft. által kifejlesztett „Secure Digital Sign SDK ver. 1.1 elektronikus aláírás előállító és ellenőrző modul" azonosítójú elektronikus aláírási termék megfelel a normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben és felhasználható fokozott biztonságú elektronikus aláírások létrehozására, az aláírások érvényességének ellenőrzésére.

A megfelelés biztonsági garancia szintje a **Common Criteria** értékelési rendszere szerinti **EAL 2** szintnek felel meg, ami a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét jelenti.[1]

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

[1] A kiadott tanúsítvány nem kerül automatikusan elfogadásra külföldön, mivel a MATRIX nem rendelkezik a CCRA körben érvényes tanúsítvány kibocsátói jogosítvánnyal.

5 HIVATKOZÁSOK

[1] MELASZ Munkacsoport Megállapodás, v1.0, 2005 szeptember,
Egységes MELASZ formátum elektronikus aláírásokra

[2] ETSI TS 101 903 V1.3.2 (2006-03),
XML Advanced Electronic Signatures (XAdES)

[3] Network Working Group, RFC 3280,
Certificate and Certificate Revocation List (CRL) Profile

[4] Network Working Groups, RFC 2560,
Online Certificate Status Protocol - OCSP

[5] ETSI TS 101 861 V1.3.1 (2006-01),
Time stamping profile

6 RÖVIDÍTÉSEK

ALA	Aláíró alkalmazás
BALE	Biztonságos Aláírás-Létrehozó Eszköz
CC	(Common Criteria) MSZ ISO/IEC 15408. Az informatikai biztonság értékelésének közös szempontrendszere
DSS	DSS Consulting Kft.
MATRIX	MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.
SDS	Secure Digital Sign SDK ver. 1.1 elektronikus aláírás előállító és ellenőrző modul
VT	Vizsgálat Tárgya

Dokumentum vége