FELÜLVIZSGÁLATI JEGYZŐKÖNYV
(E-DS10F1_TANF-SW) MELLÉKLETE

Dokumentumazonosító	**E-DS10F1_TANF-SW.ME-01**	
Projektazonosító	**E-DS10F1**	**DSS Consulting Kft. SW 2. sz. fv. 2010**
MATRIX tanúsítási igazgató	**Szádeczky Tamás**	
Kelt	**Budapest, 2010.05.11.**	
……. MATRIX tanúsítási igazgató		

1. BEVEZETÉS

A DSS Consulting Kft. (továbbiakban: DSS) 2006-ban kifejlesztette a Secure Digital Sign SDK ver. 1.0 elektronikus aláírás előállító és ellenőrző modult, amelynek tanúsításával a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft-t (továbbiakban: MATRIX) bízta meg. A tanúsítási eljárás eredményeképp a MATRIX 2006. december 15-én kiadta a megfelelőséget igazoló E-DS06T_TAN-01.SW azonosítójú tanúsítványt. A modul 1.1 verziója ismét tanúsításra került E-DS07T_TAN-01.SW azonosítóval és 2010. december 18-ig tartó érvényességgel.

A DSS a MELASZ 2.0 megfelelőség érdekében továbbfejlesztette az alkalmazást, amelynek tanúsítását a MATRIX sikeresen elvégezte. A tanúsítási eljárás során a MATRIX a Secure Digital Sign SDK ver. 2.0 elektronikus aláírás előállító és ellenőrző modul (továbbiakban: SDS) elektronikus aláírási termék fokozott biztonságú aláírások létrehozására történő felhasználhatóságát vizsgálta a Common Criteria szerinti EAL2 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. AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: „DSS Consulting Kft. által kifejlesztett Secure Digital Sign SDK ver. 2.0.0.0 elektronikus aláíró és elektronikus aláírás ellenőrző modul"

2.1. Az ÉT azonosítása

Az ÉT egyértelmű azonosítása az alábbi adatok alapján lehetséges:

Jellemző	Érték
ÉT márkaneve	Secure Digital Sign SDK
ÉT verzió	2.0.0.0
Dátum	2010. 02. 24.
Fejlesztő	DSS Consulting Kft.
Termék típus	Elektronikus aláírás létrehozó és ellenőrző modul
Platform	Windows
CC verzió	3.1
PP megfelelés	nincs
ST megfelelés	nincs

2.2. Az értékelés tárgyát képező komponensek és dokumentációk

Típus	Tárgy	Verzió	Megjelenés
Szoftver	Secure Digital Sign SDK 2.0 telepítő készlet	2.0.0.0	MSI állomány
Szoftver	Tesztesetek	2.0	Elektronikus állományok
Dokumentum	ACM_CAP.2 Konfigurációs tételek	2.0	DOC állomány
Dokumentum	ADO_DEL.1 A kiszállítás eljárásai	2.0	DOC állomány
Dokumentum	ADO_IGS.1 HW telepítés, SW telepítés, beindítás eljárásai	2.0	DOC állomány
Dokumentum	ADV_FSP.1 Informális funkcionális leírás	2.0	DOC állomány
Dokumentum	ADV_HLD.1 A felsőszintű tervezés leírása	2.0	DOC állomány
Dokumentum	ADV_RCR.1 A kölcsönös megfelelés informális szemlélte	2.0	DOC állomány
Dokumentum	AGD_ADM.1 Az adminisztrátori útmutató	2.0	DOC állomány
Dokumentum	ATE_COV.1 A lefedettség bizonyítéka	2.0	DOC állomány
Dokumentum	ATE_FUN.1 Funkcionális vizsgálat	2.0	DOC állomány
Dokumentum	ATE_SOF.1 A TOE biztonsági funkció erősségértékelése	2.0	DOC állomány
Dokumentum	AVA_VLA.1 Sebezhetőség vizsgálat	2.0	DOC állomány

A tanúsítás csak az alábbi konkrét szoftverkomponensre vonatkozik:

Név	Verzió	Méret	Sha-256 Lenyomat
DSS.SDS.dll	2.0.0.0	274 432	76b80420f2e2b705e3da4437d 44c34a412d0f2f1dfe1f22826eb 49717416a8a3

2.3. A tanúsítás megrendelője

Az Értékelés Tárgyát képező elektronikus aláírási termék fejlesztője és a tanúsítás megrendelője:

DSS Consulting Kft.

1113 Budapest, Nagyszőlős u. 11-15.

info@dss.hu

3. FUNKCIONÁLIS LEÍRÁS

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 interoperabilitási elvárásoknak megfelelően az aláírás formátuma megfelel az [1]-ben (a továbbiakban a [] között lévő hivatkozásokat lásd az 5. Hivatkozások című fejezetben) 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 megfelelőség tanúsítása folyamatban van.

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

Az SDS elektronikus aláíró alkalmazás a CWA 14170 és CWA 14171 ajánlásokban szereplő komponensek egy részhalmazát implementálja a saját kódjában, működése során nagymértékben 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 az MS Crypto API számára szabványos felületen elérhetővé tevő CSP (Cryptographic Service Provider) modul segítségével végzi.

Az SDS fokozott biztonságú elektronikus aláíró és ellenőrző modul a következő modulok funkcionalitását használja fel:

Függvénykönyvtár	Függőség tárgya
crypt32.dll	MS Windows Crypto API, a Windows operációs rendszer része, az aláíráshoz kapcsolódó alacsony szintű funkciókat ezen a komponensen keresztül valósítja meg
advapi32.dll	a Windows operációs rendszer része, biztonsági és registry funkciók elérésére használja fel a modul
vjslib.dll	a .Net keretrendszer, illetve a J# Újraeloszthető Csomag része
mscorlib.dll	a .Net keretrendszer központi eleme
System.Xml.dll	XML funkcionalitást megvalósító könyvtár
System.dll	a .Net keretrendszerben futtatandó programok alapfunkcionalitását biztosító könyvtár
System.Security.dll	egyes biztonsági funkciók megvalósítására felhasznált függvénykönyvtár, a .Net keretrendszer része

4. MEGFELELŐSÉG

4.1. Megfelelőség a normatív dokumentumoknak

Az ÉT megfelel az alábbi követelményeknek:

4.1.1. 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;

4.1.2. 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,

- Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
- CWA 14170:2004 – Security Requirements for Signature Creation Applications,
- CWA 14171:2004 – Procedures for Electronic Signature Verification.

A fejlesztő, vagy más szervezetek által igazolt megfelelés:

- RFC 3275: XML-Signature Syntax and Processing,
- ETSI TS 101 903 V1.4.1 (2009-06): XML Advanced Electronic Signatures (XAdES),
- RFC 5280: 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),
- MELASZ Munkacsoport Megállapodás, v2.0, 2008. december. Egységes MELASZ formátum elektronikus aláírásokra,
- Biztonsági körülmények, környezet.

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

A tanúsítás kizárólag a bevizsgált rendszerre 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 32 bites 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,

Windows Server 2008,

Windows Vista,

Windows 7.

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. 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 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.

4.2.4. 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 normatívákból nyerhető:

- Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917/2008 határozata.

- ETSI TS 102 176-1 Algorithms and Parameters for Secure Electronic Signatures

A specifikációk rendszeresen megújításra kerülnek, 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 a Common Criteria szerinti 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	Azonosító	Garancia összetevők
A konfiguráció menedzselése	ACM_CAP.2	Konfigurációs tételek
Kiszállítás és üzemeltetés	ADO_DEL.1	A kiszállítás eljárásai
	ADO_IGS.1	HW-telepítés, SW-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. 2.0 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 szinthez hasonló, ami a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét jelenti.

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

5. HIVATKOZÁSOK

Az Értékelési Jelentésben a következő dokumentumokra hivatkoztunk:

Szám	Dokumentum
[1]	MELASZ Munkacsoport Megállapodás, v2.0, 2008 december, Egységes MELASZ formátum elektronikus aláírásokra
[2]	ETSI TS 101 903 V1.4.1 (2009-06), XML Advanced Electronic Signatures (XAdES)
[3]	Network Working Group, RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[4]	Network Working Groups, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[5]	ETSI TS 101 861 V1.3.1 (2006-01), Time stamping profile

6. RÖVIDÍTÉSEK

Az Értékelési Jelentésben a következő rövidítéseket használtuk általános jelleggel:

Rövidítés	Magyarázat
ALE	Aláírás Létrehozó Eszköz – olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza (Eat. 2. § 3.)
BE	Biztonsági Előirányzat – egy megvalósítandó termék biztonsági rendszerterve
CC	Common Criteria for Information Technology Security Evaluation – Az informatikai biztonság értékelésének közös szempontrendszere
DSS	DSS Consulting Kft., az elektronikus aláírási termék fejlesztője
Eat.	2001. évi XXXV. törvény az elektronikus aláírásról
ÉT	Értékelés Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza
MATRIX	MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft., a tanúsító szervezet
PP	Protection Profile – a Védelmi Profil eredeti, angol elnevezése
ST	Security Target – a Biztonsági Előirányzat eredeti, angol elnevezése
TOE	Target Of Evaluation – az Értékelés Tárgya eredeti, angol elnevezése
VP	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere
VT	Vizsgálat Tárgya (ld. ÉT)