TANÚSÍTVÁNY (I-SDA21T_TAN) MELLÉKLETE

Dokumentumazonosító	**I-SDA21T_TAN.ME-01**	
Projektazonosító	**I-SDA21T**	**SDA Informatika Zrt. által fejlesztett XadesMagic V2.0.0 ST és SW tanúsítása 2021**
MATRIX tanúsítási igazgató	**Molnár Ádám**	
Kelt	**Budaörs, 2021. július 30.**	

1 ELŐZMÉNY

A MATRIX Kft. (továbbiakban: MATRIX) a NAH-6-0054/2019/K nyilvántartási számú akkreditálási okirat 2019. 04. 18-án kiadott részletező okirat melléklete alapján a Nemzeti Akkreditálási Hivatal által megfelel elektronikus aláírási szoftverek tanúsítására, mint kijelölt független tanúsító szervezet.

Az SDA Informatika Zrt. elektronikus aláírási termékek fejlesztésével, forgalmazásával, foglalkozó vállalat.

Az SDA Informatika Zrt. a következő termék/rendszer – XadesMagic V2.0.0 BIZTONSÁGI ELŐIRÁNYZAT és SZOFTVER - tanúsításával bízta meg a MATRIX-ot.

1.1 Érintett Felek

Tanúsító szervezet	**MATRIX Kft.**, 2040 Budaörs, Szabadság út 290.
Fejlesztő / megrendelő	**SDA Informatika Zrt.,** 1111 Budapest, Budafoki út 59

2 AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: „SDA INFORMATIKA által fejlesztett XadesMagic elektronikus aláírás alkalmazás fejlesztői készlet elektronikus aláíráshoz v2.0.0. "

2.1 Az ÉT azonosítása

Jellemző	Érték
ÉT márkaneve	SDA INFORMATIKA által fejlesztett XadesMagic elektronikus aláírás alkalmazás fejlesztői készlet elektronikus aláíráshoz v2.0.0.

ÉT verzió	2.0.0.26.
Dátum	2015. június 15.
Fejlesztő	SDA Informatika Zrt.
Termék típus	Elektronikus aláírás létrehozó és ellenörző modul
Platform	Windows

2.2 Az ÉT tárgyát képző komponensek és dokumentációk

Típus	Tárgy	Verzió
dokumentum	SAPS_v1.0_ok_veglegesitve.docx	3.0
dokumentum	Security_Target_v3.0_veglegestive.docx	3.0
dokumentum	ALC_CMC_v3.0_OK_veglegesitve.docx	3.0
dokumentum	ADV_TDS_v3.0_OK_vegelgesitve.docx	3.0
dokumentum	ADV_FSP_v3.0_OK_veglegesitve.docx	3.0
dokumentum	Interop Test Cases_emagic.xlsx	1.0
dokumentum	ALC_LCD_v3.0_veglegesitve.docx	3.0
dokumentum	ALC_DVS_v3.0_OK_veglegesitve.docx	3.0
dokumentum	ALC_TAT_v1.0_OK.docx	1.0
dokumentum	EMagicFelhasznaloiDokumentacio_v20.doc	20.0
Szoftver	SDA.E-Magic.exe	3.0
dokumentum	DE_07_SDAI_Hibakezelés.pdf	1.0
dokumentum	DE_11_SDAI_Szoftverfejlesztés.pdf	1.0

3 FUNKCIONÁLIS LEÍRÁS

A TOE egy olyan Windows rendszerre készült aláíró modul, amivel lehetőség van olyan alkalmazásokat készíteni, amelyek rendelkeznek XADES aláírások létrehozására, ellenőrzésére és kiterjesztésére alkalmas funkcionalitással.

A modul felhasználói felülettel nem rendelkezik, beágyazása C# hívásokon keresztült történik. Az aláírás során használható kulcsokat a Windows operációs rendszer tanúsítványtárán keresztül lehet elérni, a modul tárolási funkcionalitást nem biztosít.

A modul által megvalósított ETSI TS 119101 funkcionalitások a következők:
- aláírás,
- aláírás kiterjesztés,
- ellenőrzés.

Szoftver modul, mely más szoftver részeként Windows operációs rendszeren fut, és aláírásra, ellenőrzésre és kiterjesztésre képes.

A TOE használat

A TOE a következő formátumú aláírásokat tudja létrehozni, ellenőrizni és kiterjeszteni:

- XADES-B-B

- XADES-B-T
- XADES-B-LT
- XADES-B-LTA

Amennyiben a használt kulcs megfelelő tároló eszközön található, akkor az aláírás létrehozást képes minősített szinten végezni, ezáltal a 910/2014/EU előírásainak megfelelő minősített aláírást létrehozni.

Az ellenőrzés során a TOE eldönti, hogy az aláírás:
- érvényes,
- érvénytelen,
- nem meghatározható.

A kiterjesztés az aláírás funkció speciális esete, amit többnyire megelőz egy ellenőrzés folyamat is.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

CC conformance	Ez a Security Target CC Part 2 Extended és CC Part 3 konform, A Common Criteria version 3.1R3 -nak megfelelően készült
CC package conformance:	EAL4 augmented with assurance component ALC_FLR.1
PP conformance	A Security Target konform a következő előírásokkal: EN 419111 Part 2: Signature creation application – Core PP. EN 419111 Part 4: Signature verification application – Core PP. A PP conformancia mindkét esetben: EAL4 augmented with assurance component ALC_FLR.1
PP conformance típus	demonstrálható, az alapként szolgáló összes PP összes követelménye átvett

Az ÉT megfelel az alábbi követelményeknek:

- ISO/IEC 15408 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1–3. rész az alábbiak szerint:
- ISO/IEC 15408-1:2009 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1. rész. ISO, 2009
- ISO/IEC 15408-2:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 2. rész. ISO, 2008
- ISO/IEC 15408-3:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 3. rész. ISO, 2008

4.2 Biztonságos felhasználás feltételei

4.3 Működési környezet

Az aláírás és ellenőrzés során a következő táblázatban összefoglalt célok vonatkoznak a TOE környezetére:

Megnevezés	Scope	Biztonsági célok
OE.Platform	S/V	A vonatkozó feltételezések megvalósulása szükséges. Lásd a 3.4. fejezetben.
OE.SSCD	S	A vonatkozó feltételezések megvalósulása szükséges. Lásd a 3.4. fejezetben.
OE.SSCD_communication_protected	S	Ha SSCD használt, az SCA és az SSCD közötti adatátvitel védett kell legyen.
OE.Signer_Presence	S	Az aláírónak jelen kell lennie az a jóváhagyás és a kulcs authentikációs adat megadása közötti időben.
OE.Output_Device	S/V	A környezetnek rendelkeznie kell olyan output eszközzel, ami lehetővé teszi, hogy vagy pontosan megjelenjen az aláírandó dokumentum, vagy figyelmezteti az aláírót a lehetséges hibákra és az inkompatibilitásra. Ha a dokumentum már aláírt, az aláírónak kell legyen eszköze a korábbi aláírók azonosításra és ellenőrzésére.
OE.Checker	S/V	A környezetnek biztosítania kell egy modult, ami eldönti, hogy az aláírandó vagy ellenőrzendő dokumentum szemantikája megfelel-e szükséges formátumnak.
OE.Signer	S	A vonatkozó feltételezések megvalósulása szükséges. Lásd a 3.4. fejezetben.
OE.CSP (TSP)	S	A vonatkozó feltételezések megvalósulása szükséges. Lásd a 3.4. fejezetben.
OE.Root_Certificate	V	Biztosítani kell, hogy legalább egy érvényes root tanúsítvány elérhető legyen.
OE.Verifier	V	A vonatkozó feltételezések megvalósulása szükséges. Lásd a 3.4. fejezetben.

4.4 Értékelési módszertan

Az értékelés vizsgálatai a következő metodológia szerint történnek:

- ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation

4.5 Biztonsági garancia szint

Az értékelés tárgyára vonatkozó meghatározott Biztonsági garancia szint:

EAL4 augmented with assurance component ALC_FLR.1

Dokumentum vége