TANÚSÍTVÁNY

(I-NL20T3_TAN-SW) MELLÉKLETE

Dokumentumazonosító	**TAN-SW.ME-01**	
Projektazonosító	**I-NL20T3**	**Netlock Kft. által fejlesztett SignAssist 1.11 Elektronikus aláírás létrehozó és ellenőrző alkalmazás tanúsítás 2020**
MATRIX tanúsítási igazgató	**Molnár Ádám**	
Kelt	**Budaörs, 2020. április 3.**	
 ..... MATRIX tanúsítási igazgató		

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

A MATRIX Kft. a NAH-6-0054/2019/K számon a Nemzeti Akkreditáló Hatóság (NAH) által akkreditált terméktanúsító szervezet.

A Netlock Kft. informatikai termékek fejlesztésével és forgalmazásával foglalkozó vállalkozás.

A Netlock Kft. a SignAssist 1.11 Elektronikus aláírás létrehozó és ellenőrző alkalmazás (továbbiakban: SW) 2020. március 20-án a MATRIX Kft-nek átadta.

A MATRIX Kft. az SW értékelése során a kötelező érvényű és az önként vállalt normatívák pontról pontra történő vizsgálatát végezte el.

2. AZ ÉRTÉKELÉS TÁRGYA

SignAssist 1.11 – Elektronikus aláírás létrehozó és ellenőrző alkalmazás

2.1. ÉT azonosítása

Jellemző	Érték
ÉT megnevezése	SignAssist
ÉT verzió	1.11.
Dátum	2020.03.20
Fejlesztő	Netlock Kft.
Termék típus	Elektronikus aláírás létrehozó és ellenőrző alkalmazás
Platform	Windows, Linux
CC verzió	Common Criteria version 3.1R3

PP megfelelés	EN 419111 Part 2: Signature creation application – Core PP. Part 4: Signature verification application – Core PP. A PP csomag megfelelése: EAL4 augmented with assurance component ALC_FLR.1
ST megfelelés	SignAssist 1.11 Elektronikus aláírás létrehozó és ellenőrző alkalmazás

2.2. Az értékelés tárgyát képző dokumentációk

Típus	Tárgy	Verzió	Megjelenés
Szoftver	SignAssist 1.11.	1.11	Elektronikus
Dokumentum	SignAssist 1.11 Elektronikus aláírás létrehozó és ellenőrző alkalmazás Biztonsági Előirányzat	1.11	pdf
Dokumentum	SignAssist_TDS_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_TAT_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_LCD_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_IMP_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_FSP_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_DPT_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_COV_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_CMS_v1.11.pdf	1.11	pdf
Dokumentum	SignAssist_ARC_v1.11.pdf	1.11	pdf
Dokumentum	Szoftverfejlesztési_szabályzat_20190228_applicable.pdf	1.0	pdf
Dokumentum	SignAssist 1.11 Pipeline és REST API alapú működésben használható funkciók.pdf	1.11	pdf
Dokumentum	SignAssist 1.11 - Telepítési és üzemeltetési és felhasználói dokumentáció.pdf	1.11	pdf
Dokumentum	SignAssist SAPS_1.11.pdf	1.11	pdf
Dokumentum	SignAssist 1.11 Teszteredmények_checked.xlsx	1.11	xlsx
Dokumentum	Interoperabilitási és konformancia teszt terv 1.11.pdf	1.11	pdf
Dokumentum	Interoperability and Conformance test SignAssist 1.11.pdf	1.11	pdf

2.3. A tanúsítás megrendelője

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

Székhely: 1101 Budapest, Expo tér 5-7.

Cégjegyzékszám: 01-09-563961

Adószám: 12201521-2-42

3. FUNKCIONÁLIS LEÍRÁS

A SignAssist 1.11 szoftver egy olyan DSS alapú aláíró modul/API, amivel lehetőség van HSM használatával vagy a nélkül aláíró kulcsokat és tanúsítványokat kezelni, valamint aláírásokat elhelyezni, kiterjeszteni és ellenőrizni.

Az alkalmazás felhasználói felülettel nem rendelkezik, jellemzően web szolgáltatásként érhető el, a hívó alkalmazásnak szükséges szolgáltatások különböző interfészeken keresztül érhetőek el.

Ez lehetővé teszi több kulcs tárolását és használatát a hívó alkalmazásból.

A webservice segítségével lehetőség van arra, hogy a felhasználó helyi gépén telepített smart kártyán vagy gépén található tanúsítványt is felhasználjuk a folyamatban, ekkor az aláíró alkalmazás a hívó webfelület felé adja tovább az aláírási kérést és az eredmény visszaérkezte után folyik a hagyományos folyamat tovább.

A szoftver az alábbi szolgáltatásokat valósítja meg ETSI 119101 szabvány szerinti:

- **aláírás:** XADES, PADES, CADES és ASIC aláírás / bélyegzés
    - Amennyiben a művelethez minősített eszköz (SSCD/QSCD) és tanúsítvány áll rendelkezésre a létrejövő aláírás/bélyegzés a 910/2014/EU-nak megfelelő minősített aláírás / bélyegzés.
- **ellenőrzés:** XADES, PADES, CADES és ASIC aláírás/bélyegzés ellenőrzése
    - Az aláírás ellenőrzés során az aláírt dokumentumról megállapításra kerül állapota, amely érvényes (valid), érvénytelen (invalid) vagy nem megállapítható (indeterminate) lehet.
- **aláírás kiterjesztés:** Az aláírás kiterjesztése művelet, jellemzően az előző kettő művelet kombinációja

4. MEGFELELŐSÉG

4.1. Megfelelőség a normatív dokumentumoknak

Az ÉT megfelel az alábbi követelményeknek:

4.1.1. Kötelezően betartandó normatívák

- Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
- EN 419111-1:2013 Protection profiles for signature creation and verification application - Part 1: Introduction
- EN 419111-2:2013 Protection profiles for signature creation and verification application - Signature creation application – Part 2: Core PP
- EN 419111-4:2013 Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP

- - ISO/IEC 15408-1:2009 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 1. rész. ISO, 2009
- - ISO/IEC 15408-2:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 2. rész. ISO, 2008
- - ISO/IEC 15408-3:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 3. rész. ISO, 2008

4.1.1.1. A vizsgálat módszertana a következő normatíváknak megfelelő

- - ISO/IEC 18045:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés módszertana

4.1.2. Önként vállalt normatívák

- ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI) Policy and security requirements for applications for signature creation and signature validation
- SignAssist 1.11 Elektronikus aláírás létrehozó és ellenőrző alkalmazás v1.11 Biztonsági Előriányzat

Az aláírási termék megfelel a fenti követelményeknek a 4.2 és a 4.3 pontban leírt biztonságos felhasználási és működési környezetben az alábbi feltételek teljesülése mellett:

A tanúsítás kizárólag a vizsgált rendszer aktuális verziójára vonatkozik, bárminemű változás esetén a módosított verzióra jelen tanúsítvány érvénytelen.

Nem képezi a tanúsítás tárgyát a program működési környezete így az:

- Operációs rendszer,
- a felhasznált külső szoftver modulok illetve programok,
- a működéshez használt hardver elemek.

4.2. A biztonságos felhasználás feltételei

A tanúsítvány érvényessége a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesítésén múlik.

Az alábbi (biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

4.2.1. Elektronikus aláírás létrehozására és ellenőrzésére vonatkozó közös feltételek

OT.Signer Control

A TOE lehetőséget biztosítson arra, hogy a kulcs birtokos egyedi csak általa ismert jelszót használva megvalósuljon az explicit akarat kifejezés.

Az interfészek lehetőséget biztosítanak az aláírási folyamat megszakítására.

OT.Document

A TOE védi a felhasználói adatot a módosítástól.

A TOE garantálja, hogy a kiválasztott dokumentumok kerülnek aláírásra.

OT.Certificate

A TOE nem kezel SP-t.

A TOE ellenőrzi a tanúsítványt, hogy érvényességi idején belül legyen.

A TOE átadja a szükséges információkat az SSCD (QSCD) fel, így az a megfelelő tanúsítványt tudja aktiválni.

Ellenőrzés során meg a TOE meggyőződik, hogy érvényességi időn belül került-e használatra. (amennyiben áll rendelkezésre hozzá időbélyeg)

OT.Signature_Attributes

A TOE nem felhasználói felületet.

A TOE nem kezel aláírási policy-t.

Amennyiben az aláírás több dokumentumra szól, a TOE ugyanazon attribútumokat állítja be hozzájuk.

OT.Signature_Policy

A TOE nem kezel SP-t,

A TOE az SDO-t a kiválasztott aláírás formátumnak és szintek megfelelően állítja elő.

A TOE nem kezel SP-t.

OT.Crypto

A TOE a következő tulajdonságokkal rendelkező kriptográfiai algoritmusokat használja:

- a hash egyedi
- a hash megfelel az előírt követelményeknek

OT.Sig_Verify

A TOE-nak ellenőrizni kell tudnia, hogy az SSCD (QSCD) által visszaadott aláírás érvényes-e. Ez megvalósulhat az aláírás véglegesítését követő visszaellenőrzéssel.

OT.Certification_Path_Validation

Ellenőrzéskor a TOE-nak ellenőrizni kell tudnia a tanúsítványláncot. Ez megvalósul az aláírás ellenőrzés során történő tanúsítványlánc ellenőrzéssel.

OT.Root_Certificate

Ellenőrzéskor a TOE-nak ellenőrizni kell tudnia a Root tanúsítványt. Ez megvalósul a tanúsítvány aláírás ellenőrzésével, vagy ez EU TL használatával.

4.2.2. A környezetre vonatkozó feltételek

OE.Platform

A TOE egy olyan számítógépre kerül telepítésre, amit korlátozott hozzáférésű területen található, és nem manipulálható észrevétlenül. A host platformért, amin az alkalmazás fut, a futtató szervezet a felelős.

Az operációs rendszer lehet Linux vagy Windows, ami a szoftver vezérléséhez szükséges IO eszközökhöz biztosít alacsony szintű (billentyű-képernyő) hozzáférést.

A használt operációs rendszer az egyes folyamatokat védi egymástól.

Továbbá feltételezett, hogy:

- A host platform védett legyen vírusoktól
- Tűzfalon keresztül megy a forgalom nyílt hálózattal.
- A host platformhoz csak adminisztrátorok férnek hozzá
- A telepítést és frissítést a host platformon adminisztrátor kezeli
- Nincs lehetőség nem megbízható alkalmazások futtatására az OS-en

OE.SSCD (QSCD)

Amennyiben SSCD (QSCD) kerül használatba vételre az tanúsított.

Az SSCD (QSCD) tartalmaz legalább egy aláíró létrehozó adatot (SCD).

Ha több elérhető SCD van, vagy előzetes megjelöléssel vagy interaktívan kiválasztható a megfelelő SCD.

OE.SSCD_communication_protected (QSCD_communication protected)

Amennyiben SSCD (QSCD) kerül használatba a környezet az SCA és az SSCD (QSCD) között biztonságos, nem kerül ki szenzitív adat vagy változtatható meg egy támadó által az SCA és az SSCD (QSCD) közötti kommunikáció során. Ez megvalósul a kommunikáció titkosításával és - ahol értelmezett - a same_origin működési korlátozással.

OE.Checker

A Cheker ellenőrzi, hogy a megkapott dokumentum formátuma megfelel-e a kívánt formának.

OE.Signer_Presence

Az aláíró a jóváhagyás és a kulcs authentikációt adat megadása között jelen van. Ez vagy előzetes megjelöléssel vagy interaktívan kiválaszthatósággal valósul meg.

OE.Output_Device

A hívó alkalmazás, amely kommunikál a végfelhasználóval, a felhasználói felülete segítségével megvalósítja a következők valamelyikét:

- megjeleníti a dokumentumok aláírás előtt
- figyelmeztet az inkompatibilitásra.

OE.Signer

Az aláírók megbízhatók és követik a TOE-vel együtt szállított dokumentációk útmutatásait.

OE.CSP (TSP)

Az SCA által használt tanúsítvány a 910/2014/EU rendelet szerinti fokozott vagy minősített szolgáltatótól kell, hogy származzék.

OE.Root_Certificate

Ellenőrzéskor a TOE-nak legalább egy érvényes Root tanúsítvánnyal rendelkeznie kell, amelyet ellenőriz. Ez megvalósul a tanúsítvány aláírás ellenőrzésével, vagy ez EU TL használatával.

OE.Verifier

Ellenőrzéskor az ellenőrzők, a végfelhasználók követik a TOE-vel együtt szállított dokumentációk útmutatásait.

4.3. Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége. Mivel az ÉT-t, nem önálló működésre tervezték, tipikus felhasználása esetén egy programfejlesztő integrálja saját elektronikus aláíró vagy ilyen funkcionalitással is rendelkező alkalmazásba. Az alkalmazás fejlesztésénél figyelembe kell venni az alábbi feltételeket, amelyek betartása szükséges a modul helyes és biztonságos működéséhez.

4.3.1. Hardver és szoftver környezet

Az értékelt aláírási termék csak olyan működési környezetben használható elektronikus aláírások létrehozására, amelynek minden eleme kielégíti az általánosan elvárható biztonsági követelményeket, és együttesen egy megfelelően biztonságos informatikai rendszert hoznak létre. Az értékelésnek nem tárgya a környezet elemeinek vizsgálata, az itt megfogalmazott követelmények iránymutató jellegűek az alkalmazás megfelelő használatához.

4.3.2. 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 logika (pl.: kémprogramok) és fizikai (EMC) módszerekkel végzett adatgyűjtés értendő.

4.3.3. 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 felhasználók az internetről is letölthetik a terméket, ebben az esetben biztosítani kell számukra az ellenőrzési lehetőséget, hogy a program megbízható forrásból származik.

- A telepítést csak megfelelően előkészített, biztonságos környezetben szabad megkezdeni, a telepítési útmutatóban rögzített pontos lépések betartásával.

- A terméket ajánlott rendszeresen frissíteni az új verziókra.

4.3.4. 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:

- Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. ETSI TS102 176-1 V2.1.1 2011-07.

- ETSI, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices (ETSI TS102 176-2) V1.2.1. 2005-07.

- (ESI); Cryptographic Suites

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.

4.4. Értékelési módszertan

Az értékelés nyelvezete az ISO/IEC 15408-ban meghatározott, az értékelés módszertanának alapját az ISO/IEC 15408 használt módszertani ajánlás képezi.

A tanúsítási eljárás során elvégzett, fejlesztőktől független értékelés az ISO/IEC 15408 szerinti EAL4 szint volt. Az EAL4 jelentős garancianövekedést jelent az EAL3-hoz képest azzal, hogy a biztonsági funkciók és mechanizmusok és/vagy eljárások vizsgálatának sokkal teljesebb lefedettségét követeli, ami bizonyos mértékű bizalmat teremt abban, hogy a fejlesztés során a TOE-t nem hamisítják meg.

4.5. Biztonsági garancia szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy az Netlock Kft. által kifejlesztett „SignAssist 1.11 Elektronikus aláírás létrehozó és ellenőrző alkalmazás" megfelel a normatív dokumentumokban foglalt követelményeknek.

A megfelelés biztonsági garancia szintje az ISO/IEC 15408 értékelési rendszere szerinti EAL 4 + ALC_FLR.1 szint.

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

4.6. Rövidítések

Rövidítés	Tartalom
BE	Biztonsági Előirányzat
CC	Common Criteria for Information Technology Security Evaluation- Az informatikai biztonság értékelésének közös szempontrendszere

ÉT	ÉT Értékelés Tárgya - az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza
PP	Protection Profile – Védelmi profil
ST	Security target – Biztonsági Előirányzat
TOE	Target of Evaluation – az értékelés tárgya
VP	Védelmi profil – Protection Profile

Dokumentum vége