

# TANÚSÍTVÁNY

## (I-DSOL20T1\_TAN-SW) MELLÉKLETE

Dokumentumazonosító	TAN-SW.ME-01	
Projektazonosító	I-DSOL20T1	DOCLER SOLUTIONS Kft. által fejlesztett Cloud Sign 1.1.0.0 tanúsítás 2020
MATRIX tanúsítási igazgató	Molnár Ádám	
Kelt	Budaörs, 2020. április 23.	
<p>.....</p> <p>MATRIX tanúsítási igazgató</p>		

### 1. A TANÚSÍTÁS KÖRÜLMÉNYEI

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

A Docler Solutions Kft. informatikai termékek fejlesztésével és forgalmazásával foglalkozó vállalkozás.

A Docler Solutions Kft. Cloud Sign 1.1.0.0 felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modult a MATRIX Kft.-nek átadta.

A MATRIX Kft. a Cloud Sign 1.1.0.0 felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modul értékelése során a kötelező érvényű és az önként vállalt normatívák pontról pontra történő vizsgálatát végezte el.

### 2. AZ ÉRTÉKELÉS TÁRGYA

Cloud Sign 1.1.0.0 felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modul

#### 2.1. ÉT azonosítása

Jellemző	Érték
ÉT megnevezése	Cloud Sign
ÉT verzió	1.0.0.0
Dátum	2020.04.17
Fejlesztő	Docler Solutions Kft..
Termék típus	felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modul
Platform	Windows, Linux
CC verzió	Common Criteria version 3.1R3

<b>PP megfelelés</b>	EN 419241-1:2018 Trustworthy Systems Supporting Server Signing. Part 1: General System Security Requirements A PP csomag megfelelése: EAL4 augmented with assurance component ALC_DVS.2 és AVA_VAN.5
<b>ST megfelelés</b>	Cloud Sign 1.1.0.0 felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modul biztonsági előírányzat

## 2.2. Az értékelés tárgyát képező dokumentációk

Típus	Tárgy	Verzió	Megjelenés
<b>Szoftver</b>	Cloud Sign 1.0.0.0	1.0.0.0	Elektronikus
<b>Dokumentum</b>	Security Target CloudSign 419241-1 1.2.pdf	1.2	pdf
<b>Dokumentum</b>	Sign and Enrollment audit - TOE Design Document - Microservice szint-20200310.pdf	2020-03-10	pdf
<b>Dokumentum</b>	Sign and Enrollment audit - Functional specification (ADV_FSP), Basic modular design (ADV_TDS) and Implementation representation (ADV_IMP)-20200310.pdf	2020-03-10	pdf
<b>Dokumentum</b>	ALC_TAT_DSol_Fejesztő_eszközök.docx	1.0	pdf
<b>Dokumentum</b>	ALC_FLR_DSol_Változáskezelési_szabályzat.pdf	1.0	pdf
<b>Dokumentum</b>	ALC_FLR_DSol Incidenskezelési szabályzat.pdf	1.0	pdf
<b>Dokumentum</b>	ALC_DVS_DSOL DVS (English).pdf	1.0	pdf
<b>Dokumentum</b>	ALC_CMS_DSOL_CloudSign.pdf	1.0	pdf
<b>Dokumentum</b>	ALC_CMC_ALC_LCD_DSOL Szoftverfejlesztési_szabályzat.pdf	1.0	pdf
<b>Dokumentum</b>	CloudSign_1.1.0.0_SIGN_Functional_test_results.pdf	2020-02-05	pdf
<b>Dokumentum</b>	AGD_OPT_CloudSign_VideoRA and SIGN_Installation and administration instructions.pdf	1.0	pdf
<b>Dokumentum</b>	APT_DPT_CloudSign 1.1.0.0_SIGN_Test_Deepness.pdf	1.0	pdf
<b>Dokumentum</b>	APT_COV_CloudSign 1.1.0.0_SIGN_Test_Coverage.pdf	1.0	pdf
<b>Dokumentum</b>	CloudSign 1.1.0.0_pentest_vulnerabilities_solutions.pdf	1.0	pdf
<b>Dokumentum</b>	DSol_RACA_CLOUDSIGN_APP_USER_GUIDE_v3.pdf	V3.0	pdf

## 2.3. A tanúsítás megrendelője

Docler Solutions Korlátolt Felelősségű Társaság

Székhely: 1101 Budapest, Expo tér 5-7.

Cégjegyzékszám: 01-09-337339

Adószám: 26652793242

### 3. FUNKCIONÁLIS LEÍRÁS

A **TOE** szoftver egy olyan DSS alapú aláíró modul/API, amivel lehetőség van távoli HSM használatával aláíró kulcsokat és tanúsítványokat kezelni, valamint aláírásokat elhelyezni, kiterjeszteni és ellenőrizni.

Az alkalmazás REST felületet biztosít a hívó alkalmazások számára, illetve REST felületen keresztül kommunikál a hozzá illesztett default SCA webfelület. A működés lehetővé teszi több kulcs tárolását és használatát a hívó alkalmazásból.

A TOE segítségével továbbá lehetőség tetszőleges alkalmazás használatára aláírásra CSP interfészen keresztül.

Ez esetben figyelembe kell venni a használni kívánt aláíró alkalmazás korlátozásait, miszerint az alkalmazás során nem szabványos formátumokat is előállíthat.

A fő folyamatok amit a TOE kezel:

- Regisztrációs, felhasználó, és felhasználói adat Menedzsment
- CRS és válaszok kezelése
- Aláírás kérések kezelése
- Azonosítás és autentikáció 241-1 SCAL 2 szinten.

A szoftver, megfelelő HSM-mel (és ha a HSM tanúsítása igényli, SAM-mal) alkalmas minősített aláírás távoli létrehozására.

Module-PP Név	Típus	Leírás
SERVER-SIDE AUTHENTICATION	Alternative	Ez a modul tartalmaz minden funkciót, ami szükséges, ha az aláíró azonosítása a HSM/SAM-mal történik.

#### Formátumok

A TOE aláírás létrehozása műveletkor képes XADES, PADES, CADES és ASIC aláírást/bélyegzést létrehozni.

Amennyiben a művelethez minősített eszköz (SSCD/QSCD) és tanúsítvány áll rendelkezésre a létrejövő aláírás/bélyegzés a 910/2014/EU-nak megfelelő minősített aláírás/bélyegzés.

#### Szükséges nem TOE hardver/szoftver

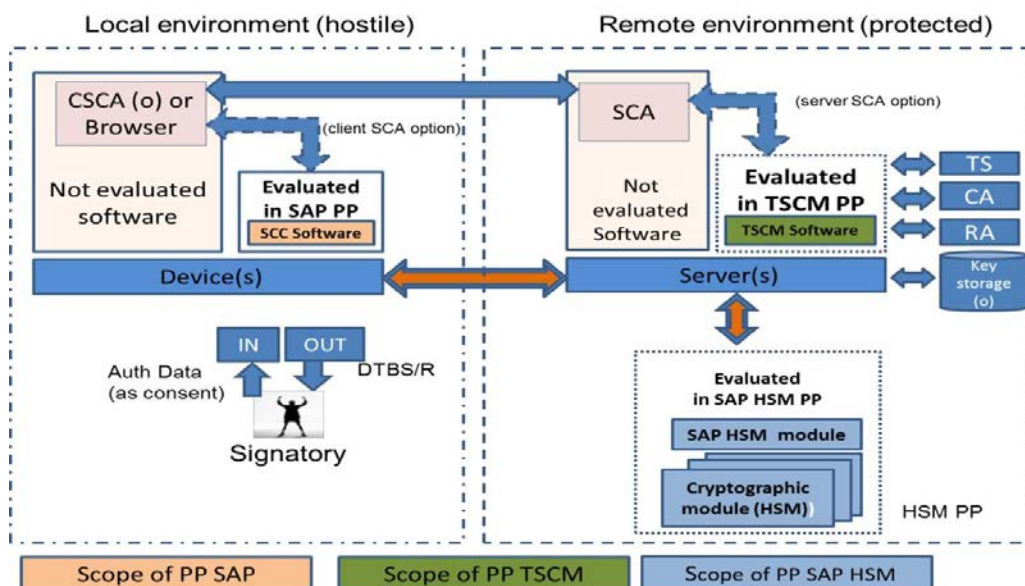
Az alkalmazás használata során a következő hardver/szoftver elemeket igényli:

1. szerver  
A TOE kerül rá telepítésre
2. tanúsított HSM  
Article 30 vagy EN 419221-5 tanúsítás
3. tanúsított SAM (opcionális, a HSM tanúsítása határozza meg)

4. standard PC és/vagy mobilkészülék,  
Az ügyfél az aláírásokat egy kommunikációs eszköz birtokában hajtja végre. A webfelületen dokumentumokat tölthet fel, le, és végezhet rajtuk aláírásokat.
5. telepített NLCSP driver (opcionális, NLCSP használata esetén),  
Ahhoz, hogy az ügyfél NLSIGN-nal tetszőleges CSP technológiát ismerő alkalmazással alá tudjon írni az NLSIGN CSP driverjei is szükségesek.
6. ügyfél aláíró szoftvere (opcionális, NLCSP használata esetén),  
Ahhoz, hogy az ügyfél NLSIGN-nal tetszőleges CSP technológiát ismerő alkalmazással alá tudjon írni a CSP technológiával, aláíró szoftverre is szüksége van) a chipkártya hardver és driverjei is szükségesek.  
(az aláírás minősített/nem minősített voltát az eszköz minősítése határozza meg.)

### TOE és környezete

A PP szerint, a TOE és környezete a következőképp kell felépülni (amiben még nem szerepel a SAM).



1. ábra - Az EN 419241-1 szerinti TOE és környezete

### A TOE biztonsági funkciói

A TOE 5 biztonsági funkcióval rendelkezik, melyek a következők:

1. Kriptográfiai támogatás
2. Felhasználói adatvédelem
3. Azonosítás
4. Biztonság menedzsment
5. A biztonsági funkciók védelme

Ebből aláírás esetén mind, míg ellenőrzés esetén az első 3 releváns az ellenőrzés jellege miatt.

## 4. MEGFELELŐSÉG

### 4.1. Megfelelőség a normatív dokumentumoknak

Az ÉT megfelel az alábbi követelményeknek:

#### **4.1.1. Kötelezően betartandó normatívák**

- - 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
- EN 419241-1:2018 Trustworthy Systems Supporting Server Signing. Part 1: General System Security Requirements
- Cloud Sign 1.1.0.0 felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modul biztonsági előírányzat

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, bármilyen 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 előírányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesítésén múlik.

Az alábbi (biztonsági előírányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak, és a TSP-nek meg kell valósítania azt.

##### **OE.TSP Trusted Service Provider**

A bizalmi szolgáltatónak EN319401 és EN319431 vagy ezekkel ekvivalens szerint kell működtetni a TOE-t.

##### **OE.SECENV Protected environment**

**A TOE-t fizikailag védett környezetben kell működtetni.**

## **OE.HOST\_REVIEW Hosting platform review**

A futtató rendszert rendszeresen ellenőrizni kell a nem engedélyezett alkalmazások kapcsán.

## **OE.SVD\_Auth Authenticity of the SVD**

A környezetnek kell biztosítani, hogy a publikus kulcs a kiadóhoz eljuttatása biztonságos.

## **OE.CGA\_QCert Generation of qualified certificates**

A tanúsítványkiadónak minősített tanúsítványt kell létrehoznia, ami a következőket tartalmazza:

- A publikus kulcsát az SCD-nek a TOE-ban,
- A TSP digitális aláírást a tanúsítványon.

## **OE.DTBS\_Intend SCA sends data intended to be signed**

Az aláírónak megbízható SCA-t kell használnia, ami a következőket tudja:

- generálni DTBS/R-t arról, amit megmutatott.
- elküldi a DTBS/R-t a TOE felé

## **OE.DTBS\_Protect SCA protects the data intended to be signed**

Az aláíró által használt SCA védi a DTBS/R-t a továbbítás során.

## **OE.SAP\_HSM Use of a certified SAP HSM**

Tanúsított HSM használata

## **OE.SCC Use of a certified SCC**

Tanúsított Sole Control Component használata (241-2 szerint SAM vagy tanúsított 241-1 szoftver komponense)

## **OE.SECURE CHANNEL User device – Server secure channel**

Biztonságos csatorna a felhasználó és a TOE között, ami védi azintegritást és az titkosságát a csatornának. (Megfelelő SSL beállítások.)

## **OE.CRYPTO Use of cryptography**

HSM modul használata, ami a tanúsítási előírásoknak megfelelően konfigurált.

## **OE.SIGNATORY Security obligation of the signatory**

Az aláíró aktiváló adatát, eszközét, jelszavát, bizalmasan kezeli.

## **OE.AUDIT\_REVIEW Review of the audit trail**

Az auditorok rendszeresen áttekintik az audit logokat, bizonyítékokat és jelentik, a megfelelő helyre, ha incidens történt.

### 4.3. Működési környezet

A fenti megfelelés 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, fejlesztőtől 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\_DVS.2 és AVA\_VAN.5 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**