TANÚSÍTVÁNY (E-DSOL21T_TAN-QSCD_v2) MELLÉKLETE

Dokumentumazonosító	**E-DSOL21T_TAN-QSCD_v2.ME-01**	
Projektazonosító	**E-DSOL21T**	**Docler Solutions Kft. AyaSAM v1.1 Minősített Elektronikus aláírást létrehozó eszköz tanúsítás 2021.**
MATRIX tanúsítási igazgató	**Molnár Ádám**	
Kelt	**Budaörs, időbélyegben látható időpontban**	

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

A MATRIX Kft. a Belügyminisztérium által a 41/2016 (X.13) BM rendelet szerint Minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközök tanúsítására kijelölt tanúsító szervezet.

A kijelölés okirat a https://matrix-tanusito.hu/wp-content/uploads/2022/03/Kijelolesi_engedely_MATRIX.pdf linken érhető el.

A Docler Solutions Kft. felkérte a MATRIX Kft.-t a Docler Solutions Kft. által létrehozott ATOS Bullsequana Edge védett környezetbe implementált AyaSAM v1.1 szoftver komponens és Thales nShield HSM Family v11.72.03 nShield Connect 6000+ nCore firmware version 2.55.4 kriptográfiai modul, mint minősített elektronikus aláírást létrehozó eszköz tanúsítására.

Az elvégzett megfelelőségértékelésről részletes jelentések készültek, amelyekből az értékelés és a felhasználás körülményeire vonatkozó legfontosabb információkat jelen melléklet tartalmazza.

1.1 Érintett felek

Tanúsítás megrendelő:	**Docler Solutions Kft.**, 1101 Budapest, Expo tér 5-7.
Termék fejlesztő:	**Docler Solutions Kft.**, 1101 Budapest, Expo tér 5-7.
Kijelölt tanúsító szervezet:	**MATRIX Kft.**, 2040 Budaörs, Szabadság út 290.

2 AZ ÉRTÉKELÉS TÁRGYA

Értékelés Tárgya	**Docler Solutions Kft. által létrehozott ATOS Bullsequana Edge védett környezetbe implementált AyaSAM v1.1 szoftver komponens és Thales nShield HSM Family v11.72.03 nShield Connect 6000+ nCore firmware version 2.55.4 kriptográfiai modul, mint minősített elektronikus aláírást létrehozó eszköz**
TOE azonosító	**AyaSAM v1.1**
Biztonsági Előirányzat	Security Target for AyaSAM v1.2.0.2
Tanúsító	MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.
Fejlesztő	Docler Solutions Kft.
CC	▪ ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security Part 1. ISO, 2009 ▪ ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security Part 2. ISO, 2008 ▪ ISO/IEC 15408-3:2008 — Information technology — Security techniques — Evaluation criteria for IT security Part 3. ISO, 2008
CEM	▪ ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation
PP megfelelés (deklarált)	▪ EN 419241-2:2013 – Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing ▪ EN 419221-5:2016, Protection profiles for Trust Service Provider Cryptographic Modules - Part 5: Cryptographic Module for Trust Services (HSM)
Biztonsági osztály	▪ EAL 4 + AVA.VAN_5 kiterjesztéssel a CC alapján

2.1 Az értékelés tárgyát képező eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	MEGJELENÉS
Hardver	Thales nShield HSM Family v11.72.03 nShield Connect 6000+ nCore firmware version 2.55.4	2.55.4	eszköz
Szoftver	AyaSAM	1.1	szoftver
Hardver	ATOS BullSequana Edge (Intrusion Detection Switch) beépített Trusted Platform Module 2.0 SLB 9670 (FIPS 140-2) chippel	2.0	eszköz
Dokumentum	ST AyaSAM 1.2.0.2_220411.pdf	1.2.0.2	Elektronikus állomány (PDF)
Dokumentum	AyaSAM (ADV_FSP), (ADV_TDS) and (ADV_IMP) 1.2.0.2_220408.pdf	1.2.0.2	Elektronikus állomány (PDF)
Dokumentum	AYA SAM ARC és install 2.0.pdf	2.0	Elektronikus állomány (PDF)
Dokumentum	AyaSAM SFR-subsystem-module 1.2.0.2_220411.xlsx	1.2.0.2	Elektronikus állomány (XLSX)
Dokumentum	ALC_TAT_DSol_Ayacucho_Fejlesztő_eszközök.pdf	1.0	Elektronikus állomány (PDF)

Dokumentum	ALC_CMS_DSOL_Ayacucho_Framework.pdf	1.0	Elektronikus állomány (PDF)
Dokumentum	ALC_DVS DSOL DVS _1.0_eng.pdf	1.0	Elektronikus állomány (PDF)
Dokumentum	ALC_CMC_ALC_LCD_DSOL Szoftverfejlesztési_szabályzat_1.0.pdf	1.0	Elektronikus állomány (PDF)
Dokumentum	Ayacucho Architektúra Felépítése És Telepítése(1).docx	1.0	Elektronikus állomány (DOCX)
Dokumentum	Ayacucho_SAM_Test_Coverage_2022.docx	1.0	Elektronikus állomány (DOCX)
Dokumentum	AyaSAM SFR-TSFI mátrix 1.2.0.1_220209.xlsx	1.2.0.1	Elektronikus állomány (XLSX)
Dokumentum	AyaSAM Appendix tables 1.2.0.0_211021.pdf	1.2.0.0	Elektronikus állomány (PDF)
Dokumentum	AyaSAM SFP teljesülése 1.2.0.0_211021.xlsx	1.2.0.0	Elektronikus állomány (XLSX)

MATRIX jelen tanúsítás során az Értékelés Tárgyát képező eszközökre vonatkozóan a következő tanúsítványokat fogadja be:

Név	Modell	Szoftverkomponensek verziói	Hivatkozás	Kiadás dátuma	Lejárata
nShield HSM Family v11.72.03	nShield Connect 6000+	• nCore firmware version 2.55.4, nShield Connect firmware image version 12.45.1 • Hardserver version 2.92.1 • Client libraries: Generic stub version 3.30.5, NFKM and RQCard version 1.86.1, and PKCS#11 version 2.14.1 • Client utilities version 2.54.1	OCSI/CERT/LEO/01/2019/RC	2019-09-17	-
Trusted Platform Module 2.0 SLB 9670 chip		SLB 9670 (Package PG-UQFN-32-1 or PG-VQFN-32-13) (FW: 7.83)	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3203	2018-06-20	2023-06-19

3 FUNKCIONÁLIS LEÍRÁS

Az Értékelés Tárgyának részét képező szoftver komponens megvalósít egy Signature Activation Protokollt, (SAP), amely az Értékelés Tárgyát képező dedikált ATOS BullSequana Edge (Intrusion Detection Switch) beépített Trusted Platform Module 2.0 SLB 9670 (FIPS 140-2) chippel rendelkező tamper védett környezettel rendelkezik és megbízható csatornán kerersztül kommunikál az Értékelés Tárgyának részét képező tanúsított Thales nShield HSM Family v11.72.03 nShield Connect 6000+ nCore firmware version 2.55.4 kriptográfiai modullal.

Az aláírás aktiváló adatot (SAD) használja az aláírótól, hogy aktiválja a kulcsot a kriptográfiai modulban az aláíráshoz.

A 2. fejezetben meghatározott Értékelés Tárgya egy Minősített Elektronikus Aláírást Létrehozó Eszköz.

Az ÉT megfelel az eIDAS 910/2014 EU rendelet II. melléklet *A minősített elektronikus aláírást létrehozó eszközökre vonatkozó követelmények*ben foglaltaknak.

Az Értékelés Tárgya hardver és szoftver alkotóelemekből épül fel.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

Az ÉT megfelel az alábbi követelményeknek:

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 (Továbbiakban: eIDAS);

- A Bizottság (EU) 2016/650 végrehajtási határozata (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó eletronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és a 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról;

- ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertana.
- Az ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertanban nem meghatározott értelmezési kérdések kapcsán a TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv dokumentum tartalmaz további információkat.

- 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
- EN 419 241-2:2019 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
- EN 419221-5:2016, Protection profiles for Trust Service Provider Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
- FIPS 140-2: Security Requirements for Cryptographic Modules

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,
- A 2.1 fejezetben hivatkozott ST AyaSAM 1.2.0.2 dokumentumban foglalt működési környezetre (7 Security Objectives) vonatkozó követelmények betartása mellett.

4.2 Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége.

Általánosan

Ez a szakasz azonosítja és definiálja a biztonsági célokat a TOE-nál és a működési környezetét.

A biztonsági célok reflektálnak az azonosított veszélyekre és figyelembe veszik a feltételezéseket.

Biztonsági előirányzat a TOE részére:

Az alábbi biztonsági célok leírják a TOE által biztosított biztonsági funkciókat.

Enrolment/Regisztráció

OT.SIGNER_PROTECTION:

A TOE biztosítja, hogy az R.Signerhez kapcsolódó adatok sértetlenek legyenek és ha szükséges, bizalmasságát védje.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA:

A TOE-nak biztonságosan kell tudnia kezelni a signature authentication data-át, a R.Reference_Signer_ Authentication_Data-t, mint az R.Signer részét.

OT.SIGNER_KEY_PAIR_GENERATION:

A TOE-nak tudnia kell biztonságosan használni a kriptográfiai modult az aláíró kulcspárok generálásához az R.Signing_Key_Id-t és R.SVD-t R.Signer-hez történő hozzárendelésre.

OT.SVD:

A TOE-nak biztosítania kell, hogy az R.SVD, ami az R.Signer-hez kötött nem módosul mielőtt tanúsított.

Felhasználó kezelés

OT.PRIVILEGED_USER_MANAGEMENT:

A TOE-nak biztosítani kell, hogy bármely módosítás a R.Privileged_User-ben és az R.Reference_Privileged_User_Authentication_Data-ban kizárólag privilegizált felhasználók kontrollja alatt történjen.

OT.PRIVILEGED_USER_AUTHENTICATION:

A TOE-nak biztosítania kell, hogy a privilegizált felhasználónak autentikálnia kell magát, mielőtt bármilyen műveletet a TOE-n végrehajtana.

Ez alól kivétel lehet az az eset, amikor egy kezdeti privilegizált felhasználó a telepítés során létrejön.

OT.PRIVILEGED_USER_PROTECTION:

A TOE-nak biztosítania kell, hogy R.Privileged_User asszociált adatának integritása védett és ha szükséges bizalmassága őrzött.

OT.SIGNER_MANAGEMENT:

A TOE-nak biztosítania kell, hogy bármilyen módosítása az R.Signer, R.Reference_Signer_Authentication_Data, R.Signing_Key_Id és az R.SVD-nek az Aláíró vagy Privilegizált felhasználó kontrollja alatt történjen.

Használat

OT.SAD_VERIFICATION:

A TOE-nak ellenőriznie kell a SAD-ot. Ennek ellenőriznie kell a kapcsolatot a SAD elemei között és biztosítania szükséges, hogy az aláíró erősen autentikált.

Ahol a TOE az SAD-ban található hitelesítési adatokból jogosultsági adatokat származtat, és ezt használja az aláíró kulcs aktiválásához a kriptográfiai modulban, ez a funkció függhet a kriptográfiai modul által biztosított vezérlőktől.

Az autentikáció előírásai az EN 419241-1 SRA_SAP.1.1 találhatók.

OT.SAP:

A TOE-nak a szerver oldali végpontját a Signature Activation Protocol (SAP)-nak implementálnia szükséges, ami a következőket biztosítja:

- Aláíró authentikációja
- Az átvitt SAD integritását.
- Legalább a SAD azon elemeinek a bizalmasságát, amelyek érzékeny adatokat tartalamznak.
- Védekezés valamely lépések visszajátszása, megkerülése, hamisítása ellen.

Az aláíró authentikációja feltételezett, hogy az EN 419241-1 SCAL.2 szerint történik. Ez azt jelenti, hogy az aláíró azonosítása a következő módokon történhet:

- Két direkt vagy indirekt séma kombinációja szerint.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION:

A TOE-nak biztosítania kell, hogy a signature authentication data védett a támadások ellen, amikor átvitelre kerül a TOE-ba, ami kompromittálná az autentikációra történő használatát.

OT.DTBSR_INTEGRITY:

A TOE-nak biztosítania kell, hogy az R.DTBS/R integritása védett, amikor átvitelre kerül a TOE-ba.

OT.SIGNATURE_INTEGRITY:

A TOE-nak biztosítania kell, hogy az aláírás nem módosítható a TOE-ban.

OT.CRYPTO:

A TOE csak olyan algoritmusokat, kulcshosszokat és hozzájuk tartozó paramétereket használhat, amelyeket a hatóságok elismertek. Ez vonatkozik a véletlen számok generálására, a kulcspárok generálására és az aláírásokra egyaránt, akár csak az integritásának és bizalmasságának védelme a TOE elemeknek.

Rendszer

OT.RANDOM:

A TOE számára generált véletlen számoknak, ami a kulcsokhoz, protokollokhoz és másik véletlen szám generátor seed adatként használ, meg kell felelniük a vonatkozó előírásoknak, hogy a random ne legyen kitalálható és rendelkezzen a szükséges entrópiával.

OT.SYSTEM_PROTECTION:

A TOE-nak biztosítani kell, hogy az R.TSF_DATA módosítása Privilegizált felhasználó által azonosított legyen, és a jogosulatlan módosítás észlelhető legyen.

OT.AUDIT_PROTECTION:

A TOE-nak biztosítani kell, hogy az R.AUDIT módosítása észlelhető legyen.

Biztonsági előírások a működtető környezet számára

OE.SVD_AUTHENTICITY:

A működtető környezetnek biztosítani kell az SVD integritását a TOE-től a CA felé történő átvitel során.

OE.CA_REQUEST_CERTIFICATE:

A működtető környezetnek kell biztosítania, hogy a minősített bizalmi szolgáltató, aki üzemelteti a rendszert minősített legyen, és megfeleljen az eIDAS rá vonatkozó követelményeinek.

A működtetőnek olyan folyamatot kell használnia tanúsítvány igénylésre, beleértve az SVD-t, aláíró információt és CA aláírást, oly módon, ami demonstrálja, hogy az aláíró van a kontroljában a kulcsnak, amihez az SVD-t bemutatták tanúsításra. A kérelem integritása védett kell legyen.

OE.CERTIFICATE_VERFICATION:

A működtető környezetnek hitelesítenie kell, hogy a tanúsítvány az R.SVD-hez tartalmazza-e az R.SVD-t.

OE.SIGNER_AUTHENTICATION_DATA:

Az aláíró menedzsment autentikációs faktor adatok a TOE-n kívül biztonságosan kezelendők.

OE.DELEGATED_AUTHENTICATION

Ha a TOE támogatja a delegált azonosítást és konfigurált is a használatára, akkor az SSA és TOE telepítő bizalmi szolgáltatónak be kell tartania az EN 419241-1 SRA_SAP.1.1 követelményeket.

Továbbá a bizalmi szolgáltatónak biztosítania kell, hogy:

- a delegált fél megfelel az összes releváns követelmények, szabványok és az eIDAS regisztrációs követelményeinek; vagy

- a delegált azonosítási folyamat olyan elektronikus azonosító eszközt használ, ami szerepel a Bizottság listáján, mint az eIDAS 9. cikk szerinti eszköz.

Ha az aláíró kizárólag a delegált fél által kerül azonosításra, a bizalmi szolgáltatónak biztosítania kell, hogy a titkos kulcs, ami azonosításra használt a TOE felé, tanúsított kriptográfiai eszközbe kerüljön, úgy, hogy konzisztens legyen az EN 419241-1 SRG_KM.1.1 követelménnyel.

A minősített bizalmi szolgáltató auditja az EN 419241-1 szerint bizonyítékot kell szolgáltasson, hogy bármely delegált fél betartja az EN 419241-1 SRA_SAP.1.1. követelményeit és opcionálisan az SRG_KM.1.1 követelményét, abban az esetben, ha az aláíró kizárólag a delegált féllel kerül azonosításra.

OE.DEVICE:

Az eszköz, computer/tablet/smart phone, ami a SIC-et tartalmaz és amit az aláíró a TOE-val interakcióra használ, védett kell legyen veszélyes kód ellen. Részt kell vennie a SIC

használatával, mint a lokális része SAP-nak és számolhatja a SAD-ot az EN 419241-1 szerint. Használható még az aláírandó dokumentum megtekintésére is.

OE.ENV:

A TSP, mely telepíti az SSA-t és a TOE-t egy minősített bizalmi szolgáltató, aki audtiált a 910/2014 [eIDAS] 3. cikk (20) szerint és megfelel az eIDAS által előírt követelményeknek. Az auditnak vizsgálnia kell a környezeti előírásokat is.

A TOE-nak védett környezetben kell működnie, ami csak a jogosult privilegizált felhasználóknak teszi lehetővé a hozzáférést. A TOE hardver és szoftver környezet (beleértve a kliens applikációkat is) Adminisztrátorok által telepítendő, biztonságos állapotban, ami mitigálja a telepítési környezetre vonatkozó kockázatokat:

- Védekezés a TOE vagy bármilyen külső eszközének elvesztése vagy ellopása ellen,

- A tamper észlelése és elhárítása (beleértve az oldalcsatornás próbálkozásokat, vagy a TOE fizikailag elválaszott vagy hardver részeivel történő kapcsolati próbálkozásokat is.)

- Védelem a TOE sugárzása ellen (pl. elektromágneses sugárzás)

- Védelem a jogosulatlan szoftver és a konfigurációs változtatások ellen a TOE és a hardver esetében

- Egységes szintű védelem minden TOE példánynak, ami ugyanazon asseteket tartalmazza. (pl. amikor a kulcs, mint backup vagy magas rendelkezésreállási okokból több mint egy példányban található meg a TOE-ban)

OE.CRYPTOMODULE_CERTIFIED:

A TOE-t szeparált fizikai határok között kell implementálni, mivel a TOE kriptográfiai modultól függ, ami kriptográfiai funkciókat és véletlenszám generálást lát el. A fizikai határnak a TOE-t fizikailag védenie kell és meg kell fellenie az FPT_PHP.1 és FPT_PHP.3 követelményeknek az EN 419221-5 szerint.

Abban az esetben, ha az ST megfelel ennek a PP-nek és az EN 419221-5 szabványnak a PP-Claim szakasz szerint, az ST tanúsítása kiterjed erre a követelményre az Üzemeltetési Környezetre vonatkozóan.

OE.TW4S_CONFORMANT:

A TOE-t egy minősített bizalmi szolgáltatónak az EN 419241-1 szabványnak megfelelő környezetben kell működtetnie.

4.2.1 A termék használata

Működés közben a megfelelő termék használat érdekében az alábbi előírásoknak kell megfelelni:

A bizalmi szolgáltatóra vonatkozó általános előírások:

- A bizalmi szolgáltató köteles betartani a hatóság algoritmusokra és paramétereire vonatkozó hatályos határozatát.

- A bizalmi szolgáltatónak folyamatosan figyelnie kell az algoritmikus követelmények változásait, és szükség esetén fel kell készülnie a használat módjának megváltoztatására vagy extrém esetben az eszközök tömeges cseréjére.

Amennyiben az ÉT-t minősített elektronikus aláírások létrehozására kívánják felhasználni, teljesíteni kell az alábbi követelményeket:

- A bizalmi szolgáltató köteles az eIDAS 910/2014 EU rendelet II. mellékletében meghatározott feltételeknek megfelelni.

Amennyiben az aláírói kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, teljesülniük kell az alábbi követelményeknek:

- a kulcspárt előállító kriptográfiai eszköznek tanúsítvánnyal igazoltan meg kell felelnie az alábbi normatív dokumentumokban foglaltaknak:
    - 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;
    - A Bizottság (EU) 2016/650 végrehajtási határozata (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó eletronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és a 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról;
- a kulcspárt biztonságos módon kell az aláírás-létrehozó eszközbe juttatni, az alábbi értelemben: a kriptográfiai eszköz és az aláírás létrehozó eszköz között biztonságos útvonalnak kell lennie, melynek forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával
- a kulcspárnak az aláírás-létrehozó eszközben történt elhelyezése után az aláírás-létrehozó eszközön kívüli magánkulcsot biztonságos módon meg kell semmisíteni.

A végfelhasználókra vonatkozó általános követelmények:

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt úgy használja, hogy a visszaélés és manipulálás megakadályozható legyen.
- Az aláíró kulcs birtokosa az aláírás létrehozó funkciót kizárólag olyan adatok vonatkozásában alkalmazhatja, amelyek integritását és hitelességét garantálja.
- Az aláíró kulcs birtokosa az aláírás létrehozó eszközre vonatkozó aktivizáló adatait (pl. PIN) bizalmasan kezelje.
- Az aláíró kulcs birtokosa rendszeres időközönként módosítsa az aláírás létrehozó eszközre vonatkozó aktivizáló adatait.
- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt kizárólag az eIDAS rendelet előírásainak megfelelő aláírás alkalmazás komponenssel együtt alkalmazhatja.

- Ha a MALE konfiguráció különbséget tud tenni megbízható és nem megbízható aláírási környezet között, akkor a MALE felhasználó felelőssége a környezet megbízhatóságának megállapítása.

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt kizárólag olyan aláírás alkalmazás komponenssel használhatja, amely az eIDAS rendelet II. mellékletének 2. pontjában foglalt előírásainak megfelelően képes a felhasználó által értelmezhető formában megjeleníteni az aláírandó dokumentumot.

- Az aláíró kulcs birtokosának be kell tartania a vonatkozó dokumentációkban foglalt felhasználókra vonatkozó szabályokat.

A védelemre vonatkozó általános követelmények:

- 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.

- A program telepítő készletét nem módosítható, biztonságos adathordozón kell a felhasználónak átadni.

- 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.

4.3 Algoritmusok és kapcsolódó paraméterek

Az elvégzett értékelés alapján összefoglalásként megállapítható, hogy az ÉT által támogatott kriptográfiai algoritmuskészletek a következők:

- SHA256 lenyomatképző függvény;
- RSA aláíró algoritmus 2048 bites kulccsal;
- ECC 384 bit kulcshossz és algoritmus paraméterrel;
- ETSI TS 119 312 szabványban előírt követelmények

Az ÉT felhasználójának folyamatosan figyelnie kell az algoritmikus követelmények változásait, és szükség esetén fel kell készülnie a használat módjának megváltoztatására, vagy extrém esetben az eszköz cseréjére.

4.4 Értékelési módszertan

Az értékelés módszertanának alapját az ISO/IEC 15408-hoz használt módszertan képzi. Az értékelés nyelvezete az ISO/IEC 15408-ban meghatározott. A tanúsítás teljes módszertani leírása a TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv című dokumentumban található.

A fejlesztő által az értékelésre átadott részletes dokumentumok elemzését és értékelés eredményeit szakterületi jelentésekben foglaltuk össze, amelyek főbb megállapításait és az azokban megfogalmazott környezeti követelményeket tartalmazza az értékelési jelentés és a tanúsítvány melléklete (jelen dokumentum).

A fejlesztő által átadott részletes dokumentumok vizsgálatának módszertana a következő normatíváknak megfelelő:

ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertana. A módszertanban nem meghatározott értelmezési kérdések kapcsán a TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv dokumentum tartalmaz további információkat.

A Védelmi Profil és a kapcsolódó Biztonsági előirányzat a következő normatíváknak felel meg:

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

- EN 419 241-2:2019 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

4.5 Biztonsági szint

A MATRIX Kft. igazolja, hogy a Docler Solutions Kft. által fejlesztett 2. pontban azonosított MALE megfelel a MATRIX Kft. által értékelt normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben.

A tanúsítás során meghatározott Biztonsági Garanciaszint: ISO/IEC 15408 EAL 4+ AVA_VAN.5.

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

5 RÖVIDÍTÉSEK

Rövidítés	Tartalom
ALA	Aláírás Létrehozó Alkalmazás
MALE (QSCD)	Minősített Elektronikus Aláírást Létrehozó Eszköz (Qualified Signature Creation Device)
TOE	Target of Evaluation – az ÉT eredeti, angol nyelvű megfelelője
CC	Common Criteria
CEM	Common Evaluation Methodology
HSM	Hardware Security Module
PP	Protection Profile – Védelmi Profil
ÉT	Értékelés Tárgya
BSZ /TSP	Bizalmi szolgáltató / Trust Service Provider
ST	Security Target – Biztonsági Előirányzat
SAM	Signature Activation Module (Aláírás aktiváló modul)
SAP	Signature Activation Protocol (Aláírás aktíváló protokoll)
SAD	Signature Activation Data (Aláírás aktiváló adat)
SVD	Signature Verification Data (Aláírás verefikáló adat)
DTBS/R	Data To Be Signed / Representation (Aláírandó adat)
CA	Certification Authority (Tanúsítvány kiadó)
CM	Cryptographic Module (Kriptográfiai modul)
CSR	Certification Signing Request (Tanúsítvány aláírási kérés)
SSA	Server Signing Application (Szerver oldali aláíró alkalmazás)
EMC	Electromagnetic Compatibility (Elektromágneses kompatibilitás)
SHA	Secure Hash Algorithm (Biztonságos Hash Algoritmus)
RSA	Rivest–Shamir–Adleman cryptosystem (RSA titkosítási eljárás)
ECC	Elliptic Curve Cryptography (Elliptikus görbe kriptográfia)

Dokumentum vége.