TANÚSÍTVÁNY (I-NLSAM21T1_TAN) MELLÉKLETE

Dokumentumazonosító	**TAN.ME-01**	
Projektazonosító	**I-NLSAM21T**	**Netlock Kft. NLSAM 1.3 tanúsítás 2021**
MATRIX tanúsítási igazgató	**Molnár Ádám**	
Kelt	**Budaörs, 2021. május 20.**	

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

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 Akkreditáló Hatóság által megfelel az elektronikus aláírási szoftverek tanúsítására, mint kijelölt független tanúsító szervezet.

A Netlock Kft. (továbbiakban: NETLOCK KFT.) elektronikus aláírási termékek fejlesztésével, forgalmazásával foglalkozó, valamint bizalmi szolgáltató vállalat.

A NETLOCK KFT. a következő termék/rendszer – NLSAM 1.3 ST és szoftver - tanúsításával bízta meg a MATRIX-ot.

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

1.1 Érintett Felek

Tanúsító szervezet	**MATRIX Kft.**, 2040 Budaörs, Szabadság út 290.
Termék fejlesztője	**Netlock Kft.**, 1101 Budapest, Expo tér 5-7.
Vizsgáló laboratórium	**SPLAB Kft.,** 2040 Budaörs, Szabadság út 290.

2 AZ ÉRTÉKELÉS TÁRGYA

Értékelés Tárgya	A Netlock Kft. által fejlesztett: **NLSAM V1.3 és az Utimaco SecurityServer Gen2 Se52**
Tanúsító	MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.
Fejlesztő	Netlock Kft.
Értékelő	SPLAB 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
Biztonsági osztály	▪ EAL 4 +, AVA.VAN_5 kiterjesztéssel a CC alapján
ÉT leírása	A TOE egy szoftver komponens, ami megvalósít egy Signature ctivation Protokollt, (SAP) és amely dedikált tamper védett környezettel rendelkezik és trusted channellel kommunikál a tanúsított kriptográfiai modullal. Az aláírás aktiváló adatot (SAD) használja az aláírótól, hogy aktiválja a kulcsot a kriptográfiai modulban az aláíráshoz.
TOE azonosító	▪ **NLSAM V1.3**
Biztonsági Előirányzat	▪ NLSAM CEN 419241-2 szabványnak megfelelő SAM modul biztonsági előirányzata (Security Target): **NLSAM V1.3**
PP megfelelés	▪ EN 419241-2:2019 A PP csomag megfelelése: EAL4 augmented with assurance component AVA_VAN.5 Advanced methodical vulnerability analysis

2.1 Az értékelés tárgyát képező eszközök és dokumentációk

Hivatkozás	Dokumentum	Verzió	Dátum	Kiterjesztés
[ST]	Security Target NLSAM 419241-2 v1.3.pdf	1.3	2021-04-22	PDF
[CMC-LCD]	Szoftverfejlesztési_szabályzat_20190228_applicable.pdf	1.3.6.1.4.1.3555. 2.9.2019022	2019-03-01	PDF
[CMS]	ALC_CMS_NLSign_Framework.pdf	v1.0	2021-04-19	PDF
[OPE]	NLSAM architecture and install v1.1.pdf	1.1	2021-04-19	PDF
[DVS]	ALC_DVS NETLOCK DVS v1.0.pdf	2020-01-13	2020-01-13	PDF
[FSP](1. fejezet) **[TDS](2. fejezet)** **[IMP](3. fejezet)**	NLSAM-audit Functional specification (ADV_FSP), Basic modular design (ADV_TDS) and Implementation representation (ADV_IMP)-20210512.pdf	2021-05-12	2021-05-12	PDF

[COV]	NLSAM_Test_Coverage.pdf	1.0	2021-04-13	PDF
[DPT]	NLSAM_Test_Deepness.pdf	1.0	2020-08-13	PDF
[FUN]	NLSAM-TJK	1.0	2020-08-13	.XLSX
[TJK]	NLSAM-TJK	1.0	2020-08-13	.XLSX
[SV]	Site Visit bizonyíték elemek			

A TOE a deklarált PP megfelelését a tanúsított NETLOCK Sign 1.36 felhő alapú szerver oldali elektronikus aláírás létrehozó és ellenőrző modullal (Tanúsítvány száma: I-NL20T2_TAN-SW és I-NL20T2_TAN-ST) együttesen valósítja meg.

A TOE fizikai környezete:

- Gyártó: Utimaco

- Típus: SecurityServer Gen2 Se52,

- Sorozatszám: CS700121

A TOE fizikai környezete rendelkezik FIPS 140-2 biztonsági tanúsítással, melyet a NIST tanúsított,

a tanúsítvány megtekinthető az alábbi linken:

FIPS 140-2 : https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2814

3 FUNKCIONÁLIS LEÍRÁS

A TOE egy szoftver komponens, ami megvalósít egy Signature ctivation Protokollt, (SAP) és amely dedikált tamper védett környezettel rendelkezik és trusted channellel kommunikál a tanúsított kriptográfiai modullal. Az aláírás aktiváló adatot (SAD) használja az aláírótól, hogy aktiválja a kulcsot a kriptográfiai modulban az aláíráshoz.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

Az ÉT megfelel az alábbi követelményeknek:

- 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

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 HSM hardver elem.
- A 2.1 fejezetben hivatkozott Security Target NLSAM 419241-2 v1.3 dokumentumban foglalt működési környezetre (8 Security Objectives) vonatkozó követelmények betartása mellett.

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)

4.2 Működési környezet

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

Ez a szakasz azonosítja és definiálja a biztonsági célokat az ÉT-vel és a működései környezetet.

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-nak biztosítania kell, hogy az, amit az R.Signer-rel asszociált, védett integritás és ha szükséges konfidentalitás szempontjából.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

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

OT.SIGNER_KEY_PAIR_GENERATION

A TOE-na tudnia kell biztonságosan használni a CM-ez, hogy aláíró kulcspárokat genráloi, és hozzárendelje R.Signing_Key_Id-t és R.SVD-t R.Signer-hez.

OT.SVD

A TOE-nak biztosítania kell, hogy az R.SVD ami az R.Signer kötött nem módosul tanúsítványa kiadása előtt.

Felhasználó kezelés

OT.PRIVILEGED_USER_MANAGEMENT

A TOE-nak biztosítania kell, hogy bármely módosítása az R.Privileged_User és az R.Reference_Privileged_User_Authentication_Data-nak Privilegizált User által történik.

OT.PRIVILEGED_USER_AUTHENTICATION

A TOE-nak biztosítania kell, hogy az Privilegizal Usernek autentikálnia kell, mielőtt bármilyen admin műveletet a TOE végrehajtana.

Ez alól kivétel lehet az az eset, amikor egy kezdeti set Priviligizal User a telepítés során létrejön

OT.PRIVILEGED_USER_PROTECTION

A TOE-nak biztosítania kell, hogy R.Privileged_User asszociált adata védett integritásra és ha szükséges konfidentalitásra.

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 User által történjék.

Használat

OT.SAD_VERIFICATION

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

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

OT.SAP

A TOE-nak kell implementálni a szerver oldali végpontját a Signature Activation Protocol (SAP)-na, ami a következőket biztosítja:

- Aláíró authentikációja

- Az átvitt SAD integritás.

- Legalább azon SAD elem konfidentalitása, amit érzékeny adatot tartalmaz.

- Védekezés valamely lépées 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:

- Direkt, Közvetlenül a SAM által, ahol a SAM ellenőrzi az aláíró autentikációs faktora(i)t

- Indirekt a SAM által. Ebben az esetben a külső autentikációs szolgáltatás, mint a TW4S része vagy egy delegált fél ellenőrzi az aláíró autentikációs faktorait és bocsát ki egy igazolást. A SAM ellenőrzi ezt az igazolást.

- Kombinált, Amikor a fenti két séma együtt van, az azonosítás egy része direkt, a másik indirekt.

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.

OT.DTBSR_INTEGRITY

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

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 integritás és konfidentalitás védelme a TOE asseteknek,

Rendszer

OT.RANDOM

A TOE számára generált véletlen számoknak, amit az kulcsokhoz, protokollokhoz és seed adathoz másik randomhoz 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 autorizált 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 TSP aki üzemelteti e rendszer minősített legyen, és megfeleljen az eIDAS rá vonatkozó követelményeinek.

A működtető olyan folyamatot kell használnia, 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 ellenőriznie 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 a TSP-nek be kell tartania az EN 419241-1 SRA_SAP.1.1 követelményeket.

Továbbá a TPS-nek biztosítania kell, hogy:

- a delegált fél megfelel az összes releváns követelmények és standardnak 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 TSP-nek biztosítania kell, hogy a titkos kulcs anyag, 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 TSP 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, 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 interaktálásra 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, aki telepíti az SSA-t és a TOE-t minősített TSP a 910/2014 [eIDAS] 3. cikk (20) szerint és auditált, hogy 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 usereknek 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 assetje 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 kisugárzása ellen (pl. elektromágneses kisugárzás) t

• 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 ha okokból több mint egy példányban található meg a TOE-ban)

OE.CRYPTOMODULE_CERTIFIED

A TOE külön implementált az aláírásra szolgáló Kriptográfiai modultól, így a TOE külön tanúsított. A fizikai határok a TOE belső Kriptográfiai modulja segítségével konformok az FPT_PHP.1 és FPT_PHP.3 követelményekkel az EN 419221-5 szerint.

OE.TW4S_CONFORMANT

A TOE-t egy minősített TSP-nek kell egy a 419241-1-nek megfelelő környezetben 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 és tárolja, 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 alábbi kriptográfiai algoritmuskészletek:

- 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 elemzése 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

4.5 Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a Docler Solutions Kft. által fejlesztett 2. pontban azonosított Értékelés Tárgya megfelel a MATRIX 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
TOE	Target of Evaluation – az ÉT eredeti, angol nyelvű megfelelője
ÉT	Értékelés Tárgya
BSZ	Bizalmi szolgáltató

Dokumentum vége.