TANÚSÍTÁSI JELENTÉS

A tanúsított termék megnevezése, jele:	Trident HSM v2.1.3
Tanúsítási terület:	Informatikai termék: Minősített elektronikus aláírást és bélyegzőt létrehozó eszközök
Megbízó:	I4P-informatikai Kft., 1125 Budapest, Fogaskerekű u. 4-6.
Projektazonosító:	E-I4P22-TAN
Dokumentumazonosító:	TJ_E-I4P22-TAN
Tanúsítvány száma, kelte[1]:	---
Tanúsítvány érvényessége:	---
Készítette:	Gyursánszky János
Jóváhagyás dátuma:	2022. 12.09.
Jóváhagyta:	Giday Eörs

[1] Tanúsítvány megújítása esetén.

ÜRES OLDAL

Tartalomjegyzék

1. BEVEZETÉS

Az I4P-Informatikai Kft. (a továbbiakban I4P Kft. Vagy Megrendelő) szerződést kötött a VERITAN Hírközlési és Informatikai Tanúsító Kft.-vel (továbbiakban VERITAN Kft.) az általa fejlesztett, EN 419 221-5 védelmi profilnak CC EAL4+ szintű megfelelését igazoló érvényes OCSI tanúsítvánnyal rendelkező Trident HSM v2.1.3. eszköz un. „local use case" felhasználási módjában minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközként történő alkalmazásához esetleges szükséges megkötések melletti különbözeti tanúsítására.

A különbözeti tanúsítást az tette lehetővé, hogy a Trident HSM v2.1.3 már sikeresen átesett egy EN ISO/IEC 18045:2020 módszertan szerint, AVA_VAN.5-tel megemelt EAL4+ garanciaszinten végrehajtott értékelésen és tanúsításon.

A különbözeti tanúsítást az tette szükségessé, hogy a lokális használati eset keretében is igény mutatkozott minősített elektronikus aláírások és bélyegzők létrehozására, de az erre való alkalmasságát a termék meglévő tanúsítása közvetlenül nem erősíti meg.

A VERITAN Kft. a tanúsítást mint a Nemzeti Akkreditáló Hatóság által akkreditált terméktanúsító szervezet, valamint a Belügyminisztérium által kijelölt minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközök megfelelőségt tanúsító szervezet végezte.

Jelen tanúsítási jelentés az elvégzett vizsgálatok és a tanúsítási döntést megalapozó eredményeinek leírását tartalmazza.

2. A TANÚSÍTÁS JELLEMZŐ ADATAI

2.1 A tanúsítás céljának meghatározása

A tanúsítás célja az I4P-Informatikai Kft. általa fejlesztett Trident HSM v2.1.3. eszköz un. „local use case" felhasználási módjában minősített elektronikus aláírás és minősített elektronikus bélyegző létrehozó eszközként történő alkalmazásához a megfelelőség megállapítása és az esetleges szükséges megkötések melletti különbözeti tanúsítására.

2.2 Az elvégzendő tanúsítási feladat meghatározása

Az elvégzendő tanúsítási feladatot az alábbiak szerint határozzuk meg:

A tanúsítás tárgyát képező eszköz első tanúsítása – különbözeti tanúsítás	☒
A tanúsítás tárgyát képező eszköz megújító tanúsítása	☐

2.3 A tanúsítás típusának meghatározása

Tanúsítás a tanúsító szervezet értékelése alapján	☐
Tanúsítás vizsgálólaboratórium értékelési jelentése alapján	☒

2.4 Tanúsítási séma

A VERITAN Kft. a tanúsítást a Nemzeti Akkreditáló Hatóság által akkreditált, és a Belügyminisztérium által kijelölt minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközök megfelelőségt tanúsító szervezet végezte, az alábbi tanúsítási séma szerint:

[FL-09] Folyamatleírás. A tanúsítás eljárási szabályai minősített elektronikus aláírást létrehozó eszközök tanúsítása során (a 910/2014/EU Rendelet II. mellékletében lefektetett biztonsági követelmények szerint), 2022.08.01., verzió 3.0.0

2.5 A vizsgálólaboratórium feladatainak azonosítása

A vizsgálólaboratórium megnevezése	VALILAB IT Biztonsági Vizsgálólaboratórium Kft.
Címe	1067 Budapest, Eötvös u. 49.
Akkreditációs száma	NAH-1-1843/2018
Akkreditáló szervezet	Nemzeti Akkreditáló Hatóság
A vizsgálólaboratórium feladatának leírása	Trident HSM v2.1.3 különbözeti tanúsításához szükséges biztonsági vizsgálatok elvégzése[2]

[2] A VALILAB Kft. a feladat végrehajtását, mint informatikai biztonság értékelést végző, az értékelési módszereket ismerő, hasonló, átfogó értékelésekre akkreditált vizsgálólaboratóriumént, de nem akkreditált státuszban végezte el.

Követelmény előírás	910/2014/EU RENDELET
Vizsgálati módszer azonosítója	MSZ EN ISO/IEC 18045:2020
Vizsgálat típusa	EAL 4 megemelve AVA_VAN.5
A vizsgálólaboratórium értékelési jelentés címe, azonosítója	Értékelési jelentés (Evaluation techical Report) – Trident v2.1.3 (local use case in CC restricted mode); SSCD_Evaluation Technical Report_v06_signed.pdf

3. A TANÚSÍTÁS TÁRGYÁNAK AZONOSÍTÁSA

A tanúsított termék megnevezése:	Trident HSM
Verzió:	v2.1.3
Tanúsítást kérő neve, székhelye:	I4P-Informatikai Kft., 1125 Budapest, Fogaskerekű u. 4-6
Fejlesztő:	I4P-Informatikai Kft.

3.1 A tanúsított termék áttekintése

A Trident v2.1.3 olyan többfelhasználós, többkulcsos eszköz, amely különböző követelmény készleteknek való megfelelés érdekében az alábbi két fő összetevő együttműködésén alapszik:

- A kriptográfiai modul (Cryptographic Module, CM) komponens egy általános célú kriptográfiai modul, amely alkalmas a jogosult felhasználói számára szükséges kriptográfiai támogatás megvalósítására (jogosult felhasználók például: lokális vagy távoli elektronikus aláírást és elektronikus bélyegzőt támogató szolgáltatók, tanúsítványok kibocsátását és visszavonását, időbélyegzés műveleteket és hitelesítés szolgáltatást nyújtó szolgáltatók).
- Az aláírás aktiváló modul (Signature Activation Module, SAM) a Trident v2.1.3 fizikai manipulálástól védett határain belüli lokális alkalmazás, ami az aláírás aktiválási protokollt (Signature Activation Protocol, SAP) valósítja meg. Használja a távoli aláíró által megadott aláírás aktiváló adatot (Signature Activation Data, SAD) a megfelelő aláíró kulcs kriptográfiai modulban megvalósuló aktiválásához.

A Trident v2.1.3 alkalmas az [EN 419221-5]-ben megadott lokális és távoli („local" és „remote") használati esetekben való használatra is.

Az eszköz fémházas, rackbe szerelhető kialakítású, amelyet az **1. ábra** mutat be.

1. ábra: az eszköz fizikai kialakítása

A Trident v2.1.3 távoli („remote") használati esetre való alkalmassága az EN 419 221-5 védelmi profilnak CC EAL4+ szinten értékelt és tanúsított, a tanúsító szervezet az OCSI (Organismo di Certificazione delle Sicurezza Informatica), a tanúsítvány száma 5/20, érvényessége 2025. szeptember 2.

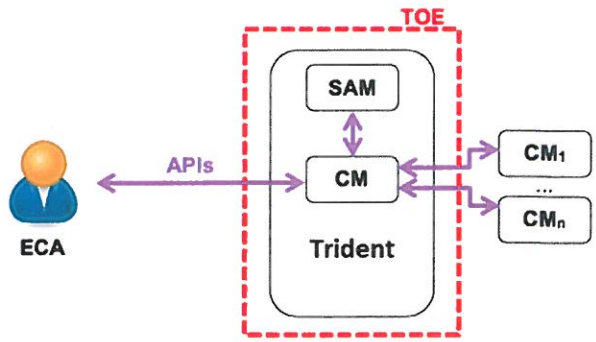
Jelen különbözeti tanúsításnak a távoli („remote") használati eset **nem tárgya**, így a továbbiakban a **lokális („local") használati esetet ismertetjük.**

3.2 A lokális használati eset

Ebben a használati esetben (lásd **2. ábrát**) a helyi kulcstulajdonosok használják a saját elektronikus aláírásukat vagy bélyegzőjüket. Ekkor a TOE-nak csak a kriptográfiai modul (CM) funkcionalitása érvényesül, helyben végrehajtott kriptográfiai műveletekkel, és a kapcsolódó kulcsmenedzsmenttel. Ezeket a műveleteket használhatja egy kliens alkalmazás minősített és nem minősített elektronikus aláírások és elektronikus bélyegzők létrehozására, a természetes vagy jogi személyiséggel rendelkező helyi kulcstulajdonos részére. Vonatkozó példák: tanúsítványokat és időbélyegeket kibocsátó bizalmi szolgáltatók (Trusted Service Providers, TSP), támogató alkalmazás szolgáltatások, mint például e-számlák és regisztrált e-mailek, ahol a szolgáltató saját bélyegzőjét vagy aláírását alkalmazza, illetve gazdasági szereplők, melyek nagy tömegben, automatikus rendszerrel kívánnak minősített aláírásokat vagy bélyegzőt elhelyezni a dokumentumaikra.

Ezen használati esetben a lokális kulcstulajdonos felelős annak a környezetnek a biztonságáért, amelyben a Trident v2.1.3 üzemel (használatban van és menedzselik). Ez esetben a Trident v2.1.3 a belső védelmi mechanizmusokhoz elengedhetetlen infrastrukturális kulcsokon kívül csak olyan kulcsokat generál, tárol és használ, amelyek a lokális végfelhasználókhoz tartoznak, őket/azokat (természetes vagy jogi személyt) reprezentálják.

A Trident v2.1.3 saját fejlesztői API-t szolgáltat (CMAPI néven, alkalmazások széles skálájához biztosítva gördülékeny integrációt), valamint más, gyakran használt API-khoz (például PKCS#11 és OpenSSL API) nyújt csatlakozási felületet.



2. ábra: A Trident v2.1.3 a „lokális" használati esetben

3.3 Biztonsági előirányzat

A Trident HSM v.2.1.3 OCSI (Organismo di Certificazione della Sicurezza Informatica) tanúsított termék Biztonsági előirányzata az alábbi (Security Target):

- Trident, the distributed remote Qualified Signature Creation Device (Trident or drQSCD), Security Target, v2.1 I4P-Informatikai Kft., 28 August 2020. (a továbbiakban: **ST_certified**)

A különbözeti tanúsításra az I4P-Informatikai Kft. az alábbi biztonsági előirányzatot adta át:

- TRIDENT v2.1.3 - local use case in CC restricted mode - Secure Signature Creation Device (SSCD) - Security Target, I4P-Informatikai Kft., 20 July 2022 (a továbbiakban: **ST_SSCD**)

A Biztonsági előirányzat feladata, hogy az adott termék konkrét megvalósításának megfelelő követelményrendszert véglegesítve és pontosítva leírja a termék által megvalósított biztonsági funkcionalitását.

Egy biztonsági előirányzat értékelésének hármas feladata van:

1. annak kimutatása, hogy megfelel a tanúsított védelmi profil(ok)nak, így egy konzisztens, nemzetközileg elfogadott biztonsági normát követ,
2. annak ellenőrzése, hogy a benne szereplő információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó módszertani elvárásoknak,
3. annak megállapítása, hogy teljes, következetes, és belsőleg ellentmondásmentes, így a termék értékelés alapjaként szolgálhat.

A 4.1 pont alatt felsorolt szabványok (Védelmi profilok) alkalmazása a következő kombinációkban lehetséges:

- [EN 419 211-2] alkalmazása alap Védelmi profilként, melyet opcionálisan kiegészíthet [EN 419211-4] és/vagy [EN 419211-5],
- [EN 419211-3] alkalmazása alap Védelmi profilként, melyet opcionálisan kiegészíthet [EN 419211-6].

A különbözeti vizsgálatra átadott Biztonsági előirányzat az alábbi Védelmi profiloknak való szigorú megfelelést vállalta fel:

- [EN 419211-2], kiegészítve [EN 419211-4] és [EN 419211-5]

4. A TANÚSÍTÁS SORÁN ALKALMAZOTT NORMATÍVÁK

4.1 Jogszabályok, szabványok

Jelen fejezet tartalmazza az jelentés elkészítése során felhasznált jogszabályok és szabványok jegyzékét.

[eIDAS]	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
[2016/650]	A BIZOTTSÁG (EU) 2016/650 VÉGREHAJTÁSI HATÁROZATA (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról
[CC]	Common Criteria for Information Technology Security Evaluation, Part 1, Part 2, Part 3 Version 3.1, Revision 5, April 2017,
[CEM]	Common Methodology for Information Technology Security Evaluation
[EN 419211-1]	Protection profiles for secure signature creation device Part 1: Overview (Part1_overview_preview.pdf)
[EN 419211-2]	Protection profiles for secure signature creation device — Part 2: Device with key generation (pp0059b_pdf)
[EN 419211-3]	Protection profiles for secure signature creation device — Part 3: Device with key import (pp0075b_pdf)
[EN 419211-4]	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application (pp0071b_pdf)
[EN 419211-5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application (pp0072b_pdf)
[EN 419211-6]	Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application (pp0076b_pdf)
[EN 419221-5]	Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services
[EN 419241-2]	Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing

1. táblázat: a tanúsítás során alkalmazott normatívák listája

4.2 Funkcionális biztonsági követelmények

Az alábbi táblázat összefoglalja a már tanúsított (ST_certified) és a jelenlegi különbözeti tanúsítás (ST_SSCD) funkcionális biztonsági követelményeit:

ST_certified	ST_SSCD		
EN 419221-5 által elvárt követelmények (SFR)	**MSZ EN 419211-2 által elvárt követelmények (SFR)**	**MSZ EN 419211-4 kiegészítő követelményei (SFR)**	**MSZ EN 419211-5 kiegészítő követelményei (SFR)**
Naplózás (Class FAU: Security audit)			
FAU_GEN.1			
FAU_GEN.2			
FAU_STG.2			
Kriptográfiai támogatás (Class FCS: Cryptographic support)			
FCS_CKM.1	FCS_CKM.1		
FCS_CKM.4	FCS_CKM.4		
FCS_COP.1	FCS_COP.1		
FCS_RNG.1			
Azonosítás és hitelesítés (Class FIA: Identification and authentication)			
FIA_UID.1	FIA_UID.1		
FIA_UAU.1	FIA_UAU.1		
FIA_AFL.1	FIA_AFL.1		
		FIA_API.1	
FIA_UAU.6/AKeyAuth FIA_UAU.6/GenKeyAuth			
A felhasználói adatok védelme (Class FDP: User data protection)			
	FDP_ACC.1/ SCD/SVD_Generation_SFP FDP_AFC.1/ SCD/SVD_Generation_SFP		
	FDP_ACC.1/ SVD_Transfer_SFP FDP_AFC.1/ SVD_Transfer_SFP		

ST_certified	ST_SSCD		
EN 419221-5 által elvárt követelmények (SFR)	**MSZ EN 419211-2 által elvárt követelmények (SFR)**	**MSZ EN 419211-4 kiegészítő követelményei (SFR)**	**MSZ EN 419211-5 kiegészítő követelményei (SFR)**
		FDP_DAU.2/SVD	
			FDP_UIT.1/DTBS
FDP_ACC.1/KeyUsage FDP_ACF.1/KeyUsage	FDP_ACC.1/Signature-creation_SFP FDP_AFC.1/Signature-creation_SFP		
FDP_SDI.2	FDP_SDI.2/Persistent		
FDP_RIP.1	FDP_RIP.1		
	FDP_SDI.2/DTBS		
FDP_IFC.1/KeyBasics FDP_IFF.1/KeyBasics			
FDP_ACC.1/Backup FDP_AFC.1/Backup			
Biztonságkezelés (Class FMT: Security management)			
FMT_SMR.1	FMT_SMR.1		
FMT_SMF.1	FMT_SMF.1		
	FMT_MOF.1		
	FMT_MSA.1/Admin		
	FMT_MSA.1/Signatory		
	FMT_MSA.2		
FMT_MSA.3/Keys	FMT_MSA.3		
	FMT_MSA.4		
	FMT_MTD.1/Admin		
	FMT_MTD.1/Signatory		
FMT_MSA.1/AKeys			
FMT_MSA.1/GenKeys			
FMT_MTD.1/Unblock			

ST_certified	ST_SSCD		
EN 419221-5 által elvárt követelmények (SFR)	**MSZ EN 419211-2 által elvárt követelmények (SFR)**	**MSZ EN 419211-4 kiegészítő követelményei (SFR)**	**MSZ EN 419211-5 kiegészítő követelményei (SFR)**
FMT_MTD.1/AuditLog			
A biztonsági funkciók védelme (Class FPT: Protection of the TSF)			
FPT_FLS.1	FPT_FLS.1		
FPT_PHP.1	FPT_PHP.1		
FPT_PHP.3	FPT_PHP.3		
FPT_TST_EXT.1	FPT_TST.1		
	FPT_EMS.1		
FPT_STM.1			
Megbízható útvonalak és csatornák (Class FTP: Trusted path/channels)			
FTP_TRP.1/External FTP_TRP.1/Admin			FTP_ITC.1/VAD
			FTP_ITC.1/DTBS
		FTP_ITC.1/SVD	
FTP_TRP.1/Local			

2. táblázat: A tanúsított és a különbözeti tanúsítás tárgyát képező funkcionális biztonsági követelmények összefoglalása

4.3 A tanúsítás alapját képező értékelési jelentés

A Trident HSM v2.13 különbözeti értékelését (vizsgálatát) egy akkreditált szervezet, a Valilab IT biztonsági Vizsgálólaboratórium Kft. végezte.

Jelen tanúsítási jelentés alapját a vizsgálólaboratórium által átadott értékelési jelentés képezte.

5. A VIZSGÁLAT EREDMÉNYEI

A vizsgálat eredményei a vizsgálólaboratórium Értékelési Jelentése alapján kerültek meghatározásra. Az eredmények értékelése (határozatai) az alábbiak lehetnek: ***Megfelelt, Nem felelt meg.***

Megfelelt (M) döntési eredmény akkor hozható, ha egy adott követelmény vizsgálata esetén nem merült fel eltérés.

Nem felelt meg (NF) döntési eredményt kell hozni, ha egy adott követelmény vizsgálatakor eltérés merült fel.

5.1 A biztonsági előirányzat értékelésének eredményei

Értékelői akcióelem	Leírás	Eredmény
ASE_INT.1.1E	A bevezető rész tartalmi értékelése	M
ASE_INT.1.2E	A bevezető rész belső ellentmondás mentességének értékelése	M
ASE_CCL.1.1E	A megfelelőségi nyilatkozat értékelése	M
ASE_SPD.1.1E	A biztonsági probléma meghatározás rész értékelése	M
ASE_OBJ.2.1E	A biztonsági célok rész értékelése	M
ASE_ECD.1.1E	A kiterjesztett követelmények rész tartalmi értékelése	M
ASE_ECD.1.2E	A kierjesztett követelmények rész szükségességének értékelése	M
ASE_REQ.2.1E	A biztonsági követelmények értékelése	M
ASE_TSS.1.1E	A TOE összefoglaló előírás rész értékelése	M
ASE_TSS.1.2E	A TOE összefoglaló előírás rész konzisztenciájának értékelése	M

3. táblázat: a Biztonsági előirányzat értékelésének eredményei

A fentiek alapján megállapítható, hogy az ST_SSCD egy konzisztens, nemzetközileg elfogadott biztonsági normát követ. A Vizsgálólaboratórium a tanúsító részére a döntések indoklását tartalmazó részjelentést átadta, amelyet a tanúsító elfogadott.

5.2 A funkcionális követelmények értékelésének eredményei

Az alábbi táblázat tartalmazza a 4.1 pontban szereplő különbségi funkcionális követelmények értékelését. A táblázat a már tanúsított (azaz már teljesített) és a különbözeti tanúsítás vizsgálati szakaszában értékelt (azaz teljesítendő) követelményeket is tartalmazza.

Az értékelés során két szempontot kellett szem előtt tartani:

1. A tanúsított (azaz már teljesítettnek tekinthető) követelményekből következik-e a különbözeti tanúsítás során vizsgált követelmények teljesülése – táblázat „Eredmény" oszlop
2. A tanúsított (azaz a termékben megvalósított) követelményekből nem következik-e olyan felhasználási lehetőség, amely különbözeti tanúsítás során vizsgált minősített aláírás/bélyegző létrehozásának ellentmond – táblázat „Ellentmondás" oszlop

Amennyiben a fenti 1. pontban az eredmény kiegészítő feltétellel teljesül, abban az esetben az „Eredmény" oszlopban a kiegészítő feltétel kerül leírásra. A fenti 2. pontban az értékelők ellentmondást tártak fel, akkor az ellentmondás feloldására vonatkozó kiegészítő feltétel került megfogalmazásra az „Ellentmondás" oszlopban.

A termék így megfogalmazott feltételekkel a teljesíti a különbözeti tanúsítás feltételeit. A vizsgálat eredményeit az alábbi 2. táblázat tartalmazza.

ST_certified tanúsított módon teljesített funkcionális biztonsági követelmények	ST_SSCD teljesítendő funkcionális biztonsági követelmények	Eredmény	Ellentmondás
Naplózás (Class FAU: Security Audit)			
FAU_GEN.1 (Audit data generation)	-	-	nincs
FAU_GEN.2 (User identity association)	-	-	nincs
FAU_STG.2(Guarantees of audit data availability)	-	-	nincs
Kriptográfiai támogatás (Class FCS: Cryptographic support)			
FCS_CKM.1 (Criptographic key generation)	FCS_CKM.1 (Criptographic key generation)	M	-
FCS_CKM.4 (Criptographic key destruction)	FCS_CKM.4 (Criprtographic key destruction)	M	-
FCS_COP.1 (Criptographic operation)	FCS_COP.1 (Criptographic operation)	M	-
FCS_RNG.1 (Generation of random numbers)	-	-	nincs
Azonosítás és hitelesítés (Class FIA: Identification and authentikation)			
FIA_UID.1	FIA_UID.1	M	-
FIA_UAU.1	FIA_UAU.1	M	-
FIA_AFL.1 /CM_authentication	FIA_AFL.1	M	-
-	FIA_APL.1 (+ FDP_DAU.2/SVD) (+FTP_ITC.1_SVD)	Kiegészítő feltételekkel teljesül (OE.CGA, OE.CMS)	-
FIA.UAU.6/AKeyAuth FIA_UAU.6/GenKeyAuth	-	.	nincs
A felhasználói adatok védeleme (Class FDP: User data protection)			
-	FDP_ACC.1/SCD/SVD_Generation_SFP FDP_AFC.1/SCD/SVD_Generation_FSP	M	-
-	FDP_AFC.1/ SVD_Transfer_SFP FDP_ACC.1/ SVD_Transfer_SFP	M	-
-	FDP_DAU.2/SVD	Kiegészítő feltételekkel teljesül (OE.CGA, OE.CMC)	-
-	FDP_UIT.1/DTBS	Kiegészítő feltétellel teljesül (OE.TLS)	-
FDP_ACC.1/KeyUsage FDP_ACF.1/KeyUsage	FDP_ACC.1/Signature-creation_SFP FDP_AFC.1/Signature-creation_SFP	M	nincs
FDP_SDI.2	FDP_SDI.2/Persistent	M	nincs
FDP_RIP.1	FDP_RIP.1	M	-

ST_certified tanúsított módon teljesített funkcionális biztonsági követelmények	ST_SSCD teljesítendő funkcionális biztonsági követelmények	Eredmény	Ellentmondás
FDP_IFC.1/KeyBasics FDP_IFF.1/KeyBasics	-	-	van /kiegészítő feltétellel feloldható: (OE.KGen)/
FDP_ACC.1/Backup FDP_ACF.1/Backup	-	-	nincs
Biztonságkezelés (Class FMT: Security Management)			
FMT_SMR.1	FMT_SMR.1	M	-
FMT_SMF.1 kivéve (5) Key import function (6) Key export function (8) Configuration Management	FMT_SMF.1 (9) Key import function (10) Key export funkction (12) Configuration management	M	nincs van /kiegészítő feltétellel feloldható OE.KGen/ van /kiegészítő feltétellel feloldható OE.KGen/ van /kiegészítő feltétellel feloldható OE.CCmode OE.TLS/
-	FMT_MOF.1	M	nincs
-	FMT_MSA.1/Admin	M	nincs
-	FMT_MSA.1/Signatory	M	nincs
-	FMT_MSA.2	M	nincs
FMT_MSA.3/Keys	FMT_MSA.3	M	nincs
-	FMT_MSA.4	M	nincs
-	FMT_MTD.1/Admin	M	nincs
-	FMT_MTD.1/Signatory	M	nincs
FMT_MSA.1/AKeys	-	-	nincs
FMT_MSA.1/GenKeys	-	-	nincs
FMT_MTD.1/Unblock	-	-	nincs
FMT_MTD.1/AuditLog	-	-	nincs
A biztonsági funkciók védelme (Class FPT: Protection of the TSF			
FPT_PHP.1	FPT_PHP.1	M	-
FPT_PHP.3	FPT_PHP.3	M	-
FPT_FLS.1	FPT_FLS.1	M	-
FPT_TST_EXT.1	FPT_TST.1	M	-

ST_certified tanúsított módon teljesített funkcionális biztonsági követelmények	ST_SSCD teljesítendő funkcionális biztonsági követelmények	Eredmény	Ellentmondás
-	FPT_EMS.1	M	-
FPT_STM.1	-	M	nincs
Megbízható útvonalak/csatornák (Class FTP: Trusted path/channels)			
FTP_TRP.1/External FTP_TRP.1/Admin	FTP_ITC.1/VAD	Kiegészítő feltétellel teljesül (OE.TLS)	nincs
	FTP_ITC.1/DTBS	Kiegészítő feltétellel teljesül (OE.TLS)	
	FTP_ITC.1/SVD	Kiegészítő feltétellel teljesül (OE.TLS, OE.CGA)	
FTP_TRP.1/Local	-	-	nincs

4. táblázat: A funkcionális vizsgálatok eredményei

A Vizsgálólaboratórium a tanúsító részére a fenti táblázatban szereplő döntéseket az átadott Értékelési jelentésben részletesen indokolta, amelyet a tanúsító elfogadott.

A fentiek alapján a vizsgált termék a különbözeti követelményeknek a megfogalmazott kiegészítő feltételekkel megfelel.

5.3 A garanciális biztonsági követelmények értékelésének eredményei

A garanciális biztonsági követelmények teljesülésének különbözeti értékelését nagyban megkönnyíti az a tény, hogy az ST_certified és az ST_SSCD által megcélzott védelmi profilok (szigorú megfeleléssel) ugyanazokat a garanciális biztonsági követelményeket várják el, nevezetesen az AVA_VAN.5-tel megemelt EAL4 garanciaszintet. Az ST_certified ezt emeli még meg az ALC_FLR.3-al, ami az összehasonlíthatóságon nem változtat.

Ebből következően csak azoknak a garanciális követelményeknek a teljesülését kell külön megerősíteni, melyek valamilyen funkcionális biztonsági követelménnyel is kapcsolatba hozhatók. A funkcionalitástól független (pl. a fejlesztés körülményeire vonatkozó) garanciális követelmények automatikusan teljesültnek tekinthetők.

A Biztonsági előirányzat értékelésére vonatkozó értékelést az 5.1 fejezet tartalmazza.

A lenti táblázat tartalmazza a garanciális biztonsági követelmények értékelésének eredményeit. Az egyes garancia osztályokban szereplő összetevők értékelése során felmerülő kiegészítő feltételek a táblázat utolsó, „Felhasználásra vonatkozó kiegészítő feltételek" oszlopában szerepelnek.

A vizsgálat eredményeit az alábbi 3. táblázat tartalmazza.

Értékelői akcióelem	Leírás	Eredmény	Felhasználásra vonatkozó kiegészítő feltételek
Fejlesztés (Class ADV: Development)			
ADV_FSP.4.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*funkcionális specifikációra és ennek SFR-ekre való visszavezetésére vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek	M	OE.CCmode, OE.extCM, OE.TLS, OE.CMC, OE.KGen, OE.Sign
ADV_FSP.4.2E	Annak megállapítása, hogy a funkcionális specifikáció a TOE funkcionális biztonsági követelményeinek pontos és teljes megvalósulása/	M	
ADV_TDS.3.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*TOE tervre, valamint a biztonságkritikus interfészek és a modulok közötti megfeleltetésre vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	
ADV_TDS.3.2E	Annak megállapítása, hogy a TOE terv a TOE funkcionális biztonsági követelményeinek pontos és teljes megvalósulása.	M	
ADV_IMP.1.1E	/Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a biztonságkritikus forráskód részekre vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	
Útmutató dokumentumok (Class AGD: Guidance Documents)			
AGD_PRE.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*telepítési eljárásokra vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
AGD_PRE.1.2E	Annak megerősítése, hogy a telepítés biztonságos működést alapoz meg.	M	nincs
AGD_OPE.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*felhasználói útmutatóra vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
Életciklus támogatás (Class ALC: Life Cycle support)			
ALC_CMC.4.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott *(TOE hivatkozásra, konfigurációkezelés dokumentációra és konfigurációkezelő rendszer használatára vonatkozó)* információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs

Értékelői akcióelem	Leírás	Eredmény	Felhasználásra vonatkozó kiegészítő feltételek
ALC_CMS.4.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott *(konfiguráció listára vonatkozó)* információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
ALC_DEL.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a szállítási eljárások és ezek használatára vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
ALC_DEL.1.2E	ALC_DEL.1.2E Annak megerősítése, hogy a fejlesztő alkalmazza a szállítási eljárásokat.	M	nincs
ALC_DVS.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a fejlesztés biztonsági dokumentációra vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
ALC_DVS.1.2E	Annak megerősítése, hogy a fejlesztő alkalmazza a biztonsági eljárásokat	M	nincs
ALC_LCD.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a Trident fejlesztésére és karbantartására használt életciklus modellre és ennek dokumentációjára vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
ALC_TAT.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a Trident fejlesztéséhez használt fejlesztő eszközök és ezek kiválasztott, megvalósítás-függő opcióinak dokumentálására vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
Tesztelés (Class ATE: Test)			
ATE_FUN.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*A TOE biztonsági funkcióinak tesztelésére és ennek dokumentálására vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
ATE_COV.2.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a teszt lefedettség vizsgálatára vonatkozó*) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.	M	nincs
ATE_DPT.1.1E	Annak megerősítése, hogy az értékelés rendelkezésére bocsátott (*a teszt mélység*	M	nincs

Értékelői akcióelem	Leírás	Eredmény	Felhasználásra vonatkozó kiegészítő feltételek
	vizsgálatára vonatkozó) információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó követelménynek.		
ATE_IND.2.1E	Annak megerősítése, hogy a TOE-t a független teszteléshez rendelkezésére bocsátották.	M	nincs
ATE_IND.2.2E	Az értékelő a teszt dokumentáció egy mintaként kiválasztott részhalmazának megismétlésével igazolta a fejlesztő tesztelési eredményeit	M	nincs
ATE_IND.2.3E	Az értékelő tesztelte a biztonsági funkciók egy részét annak megerősítése érdekében, hogy az a specifikáltaknak megfelelően működik.	M	nincs
Sérülékenység elemzés (Class AVA: Vulnerability assessment)			
AVA_VAN.5.1E	Annak megerősítése, hogy a tesztelhető TOE-t a sérülékenység elemzéshez rendelkezésére bocsátották.	M	nincs
AVA_VAN.5.2E	Az értékelő lehetséges sérülékenységeket keresett nyilvános adatbázisokban.	M	nincs
AVA_VAN.5.3E	Az értékelő lehetséges sérülékenységeket keresett a fejlesztői bizonyítékok (útmutatók, funkcionális specifikáció, TOE terv, biztonsági szerkezet leírás, forráskód) független, módszeres sérülékenység elemzésével.	M	nincs
AVA_VAN.5.4E	Az értékelő az azonosított lehetséges sérülékenységekre behatolás tesztelést végzett, annak megállapítása érdekében, hogy a TOE ellenáll magas támadó képességgel rendelkező támadók által végrehajtott támadásoknak	M	nincs

5. táblázat: A garanciális vizsgálatok eredményei

A Vizsgálólaboratórium a tanúsító részére a döntések indoklását tartalmazó részjelentést átadta, amelyet a tanúsító elfogadott.

6. ÖSSZEFOGLALÓ ÉRTÉKELÉS

6.1 A döntések összegzése

Az alábbi táblázat összefoglalja az egyes funkcionális és garanciális biztonsági osztályokban meghozott döntéseket:

Funkció/Garancia osztály	Döntés	Kiegészítő feltétel
Biztonsági előirányzat (ASE: Security Target Evaluation)	megfelelt	-
Naplózás (FAU: Security audit)	megfelelt	-
Kriptográfiai támogatás (FCS: Cryptographic support)	megfelelt	-
Azonosítás és hitelesítés (FIA: Identification and authentication)	megfelelt	OE.CGA OE.CMS
A felhasználói adatok védelme (FDP: User data protection)	megfelelt	OE.CGA OE.CMS OE.TLS OE.KGen
Biztonságkezelés (FMT: Security management)	megfelelt	OE.KGen OE.CCmode OE.TLS
A biztonsági funkciók védelme (FPT: Protection of the TSF)	megfelelt	-
Megbízható útvonalak/csatornák (FTP: Trusted path/channels)	megfelelt	OE.TLS OE.CGA
Fejlesztés (ADV: Development)	megfelelt	OE.CCmode, OE.extCM, OE.TLS, OE.CMC, OE.KGen, OE.Sign
Útmutató dokumentáció (AGD: Guidance Documents)	megfelelt	-
Életciklus támogatás (ALC: Life cycle support)	megfelelt	-
Tesztelés (ATE: Test)	megfelelt	-
Sérülékenység elemzés (AVA: Vulnerability assessment)	megfelelt	-

6. táblázat: A funkcionális és garanciális követelmény vizsgálatok eredményeinek összefoglaló táblázata

6.2 A tanúsítás megadására vonatkozó összefoglaló értékelés

A vizsgált termék a biztonsági előirányzatában (*TRIDENT v2.1.3 - local use case in CC restricted mode - Secure Signature Creation Device (SSCD) - Security Target, I4P-Informatikai Kft., 20 July 2022*) szereplő **valamennyi funkcionális és garanciális követelménynek megfelel**, a felhasználásra vonatkozó, 7. pontban megfogalmazott feltételek érvényre jutása esetén.

7. A FELHASZNÁLÁSRA VONATKOZÓ FELTÉTELEK

7.1 Az OCSI tanúsítás során a lokális használati esetre megfogalmazott feltételek

Az OCSI (Organismo di Certificazione della Sicurezza Informatica) által tanúsított Biztonsági előirányzatban (Trident, the distributed remote Qualified Signature Creation Device (Trident or drQSCD), Security Target, v2.1 I4P-Informatikai Kft., 28 August 2020) szereplő, a lokális használati esetre vonatkozó biztonsági feltételek:

- OE.Env (ST_certified 4.2.1 pontja)
- OE.ExternalData (ST_certified 4.2.2 pontja)
- OE.DataContext (ST_certified 4.2.2 pontja)
- OE.Uauth (ST_certified 4.2.2 pontja)
- OE.AuditSupport (ST_certified 4.2.2 pontja)
- OE.AppSupport (ST_certified 4.2.2 pontja)

7.2 A különbözeti tanúsításkor vizsgált biztonsági előirányzat használati feltételei

A különbözeti tanúsításra benyújtott Biztonsági előirányzatból (TRIDENT v2.1.3 - local use case in CC restricted mode - Secure Signature Creation Device (SSCD) - Security Target, I4P-Informatikai Kft., 20 July 2022) következő felhasználásra vonatkozó feltételek az alábbiak (ST_SSCD 4.2 pontja):

- OE.SVD_Auth *(Az aláírás ellenőrző adat (SVD) hitelessége)*
- OE.CGA_QCert (*Minősített tanúsítványok generálása*)
- OE.Dev_Prov_Service (*BALE-szolgáltató által biztosított hiteles BALE*)
- OE.HID_TC_VAD_Exp (*VAD exportáláshoz HID megbízható csatorna*)
- OE.DTBS_Intend *(SCA továbbítja az aláírandó adatot)*
- OE.SCA_TC_DTBS_Exp (*SCA-hoz megbízható csatorna az aláírandó adat (DTBS) exportálási művelet során)*
- OE.Signatory (*Az aláíró biztonsági kötelezettségei*)
- OE.CGA_SSCD_Auth (*A TOE előkészítése SSCD hitelesítéshez*)
- OE.CGA_TC_SVD_Imp (*CGA megbízható csatorna az SVD importálásához*)

7.3 A jelen különbözeti tanúsítás kiegészítő feltételei

A jelenkülönbözeti tanúsítás eredményeiből következő, a minősített elektronikus aláírást/bélyegzőt létrehozó eszközként alkalmazásra vonatkozó kiegészítő feltételek, környezeti biztonsági célok az alábbiak:

OE.CCmode *CC értékelt üzemmód*
A TOE-t (értékelés tárgyát) CC-értekelt módban kell működtetni, amelyben a Trident a Common Criteria védelmi profiloknak való megfelelés szerint működik; ezen túlmenően, bizonyos konfigurációs paraméterek értékét szigorúan korlátozni kell.

(Ezáltal a Trident v2.1.3 Common Criteria tanúsítvánnyal igazolt eredményei érvényesek a most vizsgált esetre is.)

OE.extCM *Külső kriptográfiai modul (external CM) használatának kizárása*
Az ***mpcm_keydev<name_1>.. mpcm_keydev<name_n>*** konfigurációs paramétert nem szabad szerepeltetni a konfigurációs fájlban, ezzel kizárva külső kriptográfiai modulok használatát.

OE.TLS *Megbízható csatorna az aláírás létrehozó alkalmazáshoz*
Az ***mpcm_svcssl*** konfigurációs paraméternek szerepelnie kell a konfigurációs fájlban a megengedett értékek egyikével.
(Ebben az esetben a Trident kikényszeríti, hogy csak TLS 1.2 védett csatornán lehet számára aláírandó adatot beküldeni.)

OE.CGA *Megbízható csatorna a tanúsítvány generáló alkalmazáshoz*
A Trident üzemeltetőjének előzetesen, egy megbízható csatornán keresztül:

- elérhetővé kell tennie a tanúsítványkibocsátó számára a Trident v2.1.3 egyedi csisk_mpcm infrastrukturális RSA2048 magánkulcsának nyilvános párját,
- jeleznie kell a tanúsítványkibocsátónak, hogy az ezzel aláírt PKCS#7 fájlba foglalt tanúsítványkérelem minősített tanúsítványt kér.

(Így a tanúsítványkibocsátó ellenőrizni tudja, hogy a tanúsítványkérelem a TOE-ból származik, és minősített tanúsítvány kérelmet tartalmaz.)

OE.CMC *Szabványos tanúsítvány kérelmet tartalmazó hitelesített adat*
Az aláírónak vagy az adminisztrátornak 'CMC' típusú tanúsítványkérelmet kell generáltatnia.
(A ***getkey*** CMAPI parancs *reqt* bemeneti paraméterének 'CMC' értéket adva.)

OE.KGen *Kulcsgenerálás*
A kulcsgenerálás során biztosítani kell, hogy kizárólag aláírás/bélyegző létrehozására szolgáló, egyetlen aláíróhoz tartozó, nem exportálható, nem módosítható kulcspár generálódjon a TOE-ban.

Olyan kulcs igénylése esetén, melyet tulajdonosa minősített aláírás/bélyegző létrehozására kívánja használni:
A ***keyreq*** CMAPI parancsban:

- a keydev bemeneti paraméterben az 'mpcm' (default) értéket kell megadni (hogy a kulcs a TOE-ban generálódjék, ne lehessen sem külső HSM-ben generáltatni, sem importálni)
  - a *mosk* bemeneti paraméterben üres sztring (nincs megadva) kell legyen (hogy a kulcsnak egyetlen tulajdonosa a kérelmező legyen),
- a keyusage bemeneti paraméterben az 's' (signing) értéket kell megadni (hogy a kulcsot aláírás/bélyegző létrehozására lehessen használni),
- a keyattr bemeneti paraméterben az alábbi értékválasztásokat kell megadni:
  - SIGN:0/**1** (is the key usable for signing? no/**yes**),
  - VERIFY:0/**1** (is the key usable for signature verification? no/**yes**),
  - ENCRYPT:**0**/1 (is the key usable for encryption? **no**/yes),

- DECRYPT:**0**/1 (is the key usable for decryption? **no**/yes),
- WRAP:**0**/1 (is the key usable for key wrapping? **no**/yes),
- UNWRAP:**0**/1 (is the key usable for key unwrapping? **no**/yes),
- EXPORTABLE:**0**/1 (is the key exportable? **no**/yes),
- SENSITIVE:0/**1** (is the key protected with password? no/**yes**),
- MODIFIABLE:**0**/1 (is the key modifiable? **no**/yes)
- DERIVEKEY:**0**/1 (is the key usable for key derivation? **no**/yes),
- CMAC:**0**/1 (is the key usable for CMAC generation? **no**/yes)
- KUC: 0/1 (key usage counter is enabled by default? no/yes), szabadon választható
- PROTECTED: 0/1 (is the key protected by key password? no/yes), szabadon választható

(hogy a kulcsot kizárólag aláírás/bélyegző létrehozására lehessen használni, ne lehessen exportálni és módosítani),

- a keytec bemeneti paraméterben pedig csak az 1,4,5 értékek egyikét lehet megadni (kizárva ezzel a külső HSM-ekben történő generáltatás és az egyéb kívülről történő importálás lehetőségét).

Olyan kulcsra, melyet tulajdonosa minősített elektronikus aláírás/bélyegző létrehozására kíván használni, tilos kiadni az alábbi CMAPI parancsot:

- keyimpop (amivel kívülről lehetne a kulcsot importálni).

OE.Sign *Szabványos feltöltés aláírás során*
Az aláírás/bélyegző létrehozása során az aláíró kulcs algoritmusának megfelelő szabványos feltöltést kell kérni.

(Minősített aláírás/bélyegző létrehozása esetén:
A ***sign*** CMAPI parancsban:

- a padding bemeneti paraméterben:
  - RSA kulcs esetén a 'pkcs1-1.5' vagy a 'pkcs1-pss',
  - EC kulcs esetén az 'ecdsa'

értéket kell megadni.)

8. RÖVIDÍTÉSEK ÉS SZAKKIFEJEZÉSEK

CM	Cryptographic Module (kriptográfiai modul)
CSP	Certification Service Provider (tanúsítvány-kibocsátási szolgáltató)
CSR	Certificate Singing Request (tanúsítvány kérelem)
DTBS	Data To Be Signed (aláírandó adat)
EAL	Evaluation Assurance Level (értékelési garanciaszint)
ECA	External Client Application
ETR	Evaluation Technical Report (értékelési jelentés)
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
HID	Human Interface Device
HSM	Hardware Security Module (hardver biztonsági modul)
OR	Observation Report (észrevételezési jelentés)
RAD	Reference Authentication Data (hitelesítő adat tárolt képe)
SAM	Signature Activation Module (aláíró aktivizáló modul)
SAR	Security Assurance Requirement (garanciális biztonsági követelmény)
SF	Security Function (biztonsági funkció)
SFR	Security Functional Requirement (funkcionális biztonsági követelmény)
SCD	Signature Creation Data (aláírás létrehozó adat, magánkulcs)
SSCD	Secure Signature Creation Device (biztonságos aláírás létrehozó eszköz)
SVD	Signature Verification Data (aláírás ellenőrző adat, nyilvános kulcs)
TOE	Target of Evaluation (a vizsgálat tárgya, a vizsgált termék)
TSFI	TOE Security Functionality Interface (biztonságkritikus interfész)
TSP	Trust Service Provider (megbízható szolgáltató)
VAD	Verification Authentication Data (ellenőrzésre beküldött hitelesítő adat)

9. TANÚSÍTVÁNY KIADÁSA

I. A jelen Tanúsítási Jelentésben foglaltak alapján a VERITAN **Kft. megállapítja,** hogy az

I4P-Informatikai Kft.
(1125 Budapest, Fogaskerekű u. 4-6.)
által fejlesztett

Trident HSM v2.1.3 verziója

mint minősített elektronikus aláírást és bélyegzőt létrehozó
„CC üzemmód, lokális használati eset"
felhasználási módjában

MEGFELEL

AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.)
II. mellékletében meghatározott
minősített elektronikus aláírást és bélyegzőt létrehozó eszközökre vonatkozó követelményeknek

II. A VERITAN tanúsítói javasolják a VERITAN Tanúsítási igazgatójának a fenti megállapítást igazoló

Tanúsítvány kiadását feltétel nélkül	☐
Tanúsítvány kiadását jelen tanúsítási jelentés 7. fejezetében leírt feltételekkel	☒
Hibajegyzék kiadását	☐

A Tanúsítási igazgató a javaslat elfogadását a kiállított Tanúsítvány aláírásával igazolja.

III. A Tanúsítvány érvényességi ideje:

a kiadás dátumától 2025.09.02.-ig

- Dokumentum vége -