Tanúsítási Jelentés

A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal v2.6.1

mint informatikai biztonsági funkciókat megvalósító szoftver termék

HUNG-TJ-15408-002-2024

Verzió:	1.0
Fájl:	HUNG-TJ-15408-002-2024_v10.docx
Minősítés:	Nyilvános
Oldalak:	19

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2024.12.10.	A szerkezet felállítása
v0.2	2024.12.18.	Belső egyeztetésre kiadott verzió
v0.9	2024.12.18.	Külső egyeztetésre kiadott verzió
v1.0	**2024.12.20.**	**Végleges verzió**

A Tanúsítási Jelentést készítette:

Digitálisan aláírta:
Endrődi Zsolt Attila

Endrődi Zsolt Attila
HUNGUARD Kft.
Tanúsítási divízió

Tartalom

I. Összefoglaló

I.1. A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői

TOE név:	**A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal**
TOE rövid neve:	A2-Polysys CryptoSigno Interop JAVA API
TOE verzió:	v2.6.1
Fejlesztő:	Polysys Kft. 1162 Budapest, Margitháza u. 1.
Értékelő:	HUNGUARD Kft. Értékelési Divízió 1123 Budapest, Kékgolyó u. 6.
Értékelés befejezése:	2024. december 17.
Az értékelés módszere:	MSZ EN ISO/IEC 15408-1/2/3:2020 MSZ EN ISO/IEC 18045:2020
Az értékelés garanciaszintje:	Fokozott (EAL3) kiterjesztve ALC_FLR.2 komponenssel

I.2. A tanúsítás tárgya

Az A2-Polysys CryptoSigno Interop JAVA API (A2API) egy olyan, kizárólag szoftveres megoldás, amely az alábbiakban leírt szolgáltatásokat nyújtja a Java nyelven írt biztonságos alkalmazások számára.

Csomag neve	Funkcionalitás	Függőség
Tanúsítvány lánc validáció (CPV) alap	Az összes X.509 érvényesítési ellenőrzés elvégzése a politika feldolgozás és a névkorlátozások feldolgozása kivételével.	CRL
PKI aláírás generálás	Magánkulcs használata az aláírás létrehozásához Az aláírási információk generálása	Nincs
PKI aláírás hitelesítés	Az aláírási információk feldolgozása Nyilvános kulcs használata az aláírás ellenőrzéséhez	Tanúsítvány lánc validáció (CPV) alap
PKI titkosítás „Key Transfer” algoritmussal	A titkosítási boríték információinak generálása Nyilvános kulcs használata a titkosításhoz	Tanúsítvány lánc validáció (CPV) alap
PKI dekódolás „Key Transfer” algoritmussal	Titkosítási boríték információk feldolgozása Magánkulcs használata a dekódoláshoz	Nincs

Online tanúsítvány státusz protokol kliens	OCSP-kérelem generálása az RFC 6960 vagy 2560 szerint	Tanúsítvány lánc validáció (CPV) alap
Tanúsítvány visszavonási lista ellenőrzés	CRL beszerzése CRL feldolgozása	Nincs
Időbélyeg kliens	Időbélyegző-kérelem generálása az RFC 3161 szabványnak megfelelően Az időbélyegzővel kapcsolatos válasz ellenőrzése az RFC 3161 szerint.	Tanúsítvány lánc validáció (CPV) alap

I.2.1. A TOE szolgáltatásainak összefoglalása

Az A2-API platform független JAVA technológiával készülő, széles skálán mozgó alkalmazások (AHA) számára támogatást nyújt:

- minősített vagy fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére
- titkosításra és visszafejtésre
- tanúsítványok és visszavonási információk ellenőrzésére, a tanúsítási útvonal felépítésére és érvényesítésére
- azonosításra (identification), hitelesítésre (authentication) és jogosultság ellenőrzésre (authorization)

Elektronikus aláírás

Az A2-API az XML-Signature Syntax and Processing (XMLDSIG) szabvány és az XML Advanced Electronic Signature (XAdES) v1.2.2, v1.3.2, v1.4.1, v1.4.2 valamint EN 319 132 szabvány BES, EPES, T, C, X, X-L, A formátumai szerint készít és ellenőriz elektronikus aláírásokat.

Titkosítás és visszafejtés

Az A2-API PKI, hibrid, kulcsátviteli algoritmusokkal történő titkosítást és visszafejtést végez.

Az A2-API hibrid típusú (PKI alapú, kulcsátviteli algoritmus és szimmetrikus titkosító algoritmus kombinációjára épülő) titkosítást és visszafejtést végez. A szimmetrikus titkosítás algoritmusa AES/256, amelynek titkos kulcsát aszimmetrikus RSA/2048 bites titkosítás védi.

Tanúsítványok és visszavonási információk ellenőrzése

Az A2-API a PKIX, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280) szerint végzi a tanúsítványok és tanúsítvány visszavonási listák ellenőrzését, a tanúsítási útvonal felépítését és érvényesítését.

Azonosítás, hitelesítés és jogosultság ellenőrzés

Az A2-API PKI alapú azonosítás, hitelesítés és jogosultság ellenőrzés szolgáltatást nyújt, a Java Authentication and Authorization Service (JAAS) architektúrának megfelelően.

Üzemmódok

Az A2-API-nak két használati módja különböztethető meg:

- szigorú üzemmód: - minősített elektronikus aláírás létrehozására alkalmas
- normál üzemmód: - fokozott biztonságú elektronikus aláírás létrehozására alkalmas

Az A2-API a szigorú üzemmódjában egy, az eIDAS II. mellékletének megfelelő QSCD eszközzel és minősített tanúsítvánnyal használva megfelel az eIDAS megfelelő minősített elektronikus aláírásra vonatkozó előírásainak.

Az A2-API a normál üzemmódjában használva megfelel az eIDAS fokozott biztonságú elektronikus aláírásra vonatkozó előírásainak.

I.3. A TOE biztonsági környezete és határai

A TOE működőképességéhez Java futtató környezetre van szükség. A TOE bármely hardver vagy operációs rendszer környezetben képes működni, amennyiben az előírt Java verzió azt támogatja és kielégíti a biztonsági előirányzatban megfogalmazott környezeti biztonsági célokban leírtakat (lásd továbbá jelen dokumentum IV.1 fejezetét). A tanúsítás során tesztelt környezetek a III.1.5 fejezetben azonosítottak.

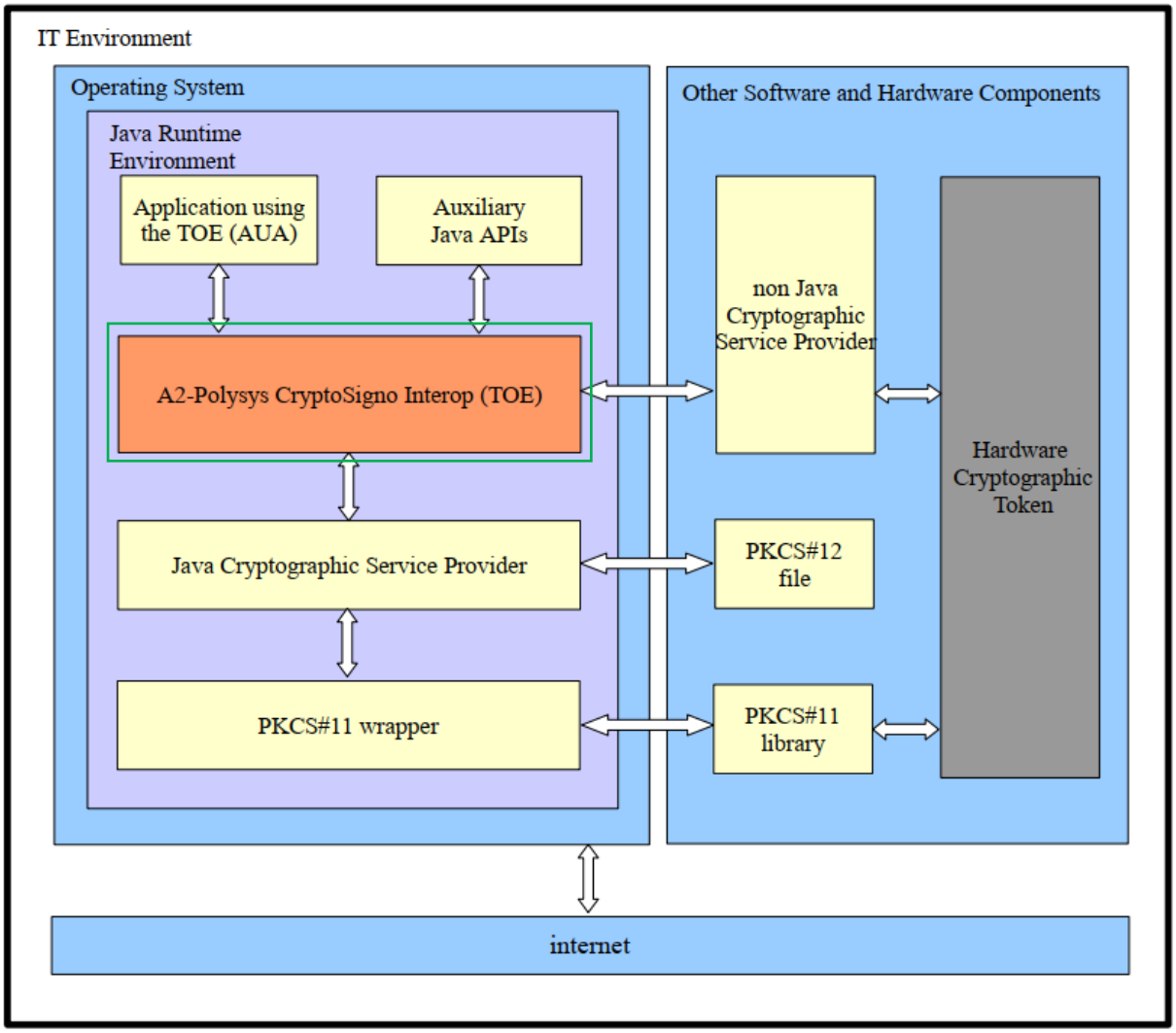
Szigorú üzemmódban a TOE elvárja a működési környezetében megfelelően telepített és konfigurált QSCD jelenlétét. Normál üzemmódban a TOE használható különböző megfelelően telepített és konfigurált hardver alapú aláírás létrehozó eszközzel. Ezen eszközöknek, legyen az intelligens kártya vagy HSM modul PKCS#11 interfésszel kell rendelkezniük. A TOE a kriptográfiai eszközök szolgáltatásait a saját PKCS#11 interfészükön éri el.

A szoftverkomponenseket az alábbi táblázat mutatja be

TOE vagy környezeti elem	Komponens	Leírás
TOE	A2-Polysys CryptoSigno Interop JAVA API	JAVA programozói könyvtár, aláírt Java archív file formátumban.
Környezeti elem	Operációs rendszer	Bármely operációs rendszer, ahol a JRE elérhető
Környezeti elem	Java Runtime Enviroment	Java futtató környezet
Környezeti elem	FIPS 140 kompatibilis kriptográfiai szolgáltatás	Egy vagy több FIPS 140-2 Level 1 szintű kriptográfiai szolgáltatás a Java Kriptográfiai kiegészítéshez telepítve.
Környezeti elem	PKCS#11 API	Operációs rendszer függő TOE által alkalmazni kívánt kriptográfiai eszköz natív programozói könyvtára.
Környezeti elemek	Kiegészítő Java API-k	Xerces XML parser 2.7.2 vagy magasabb Xalan XSLT támogató and XPath feldolgozó 2.11.0 vagy magasabb

		PolysysGUI GUI komponens könyvtár 2.0.0 vagy magasabb Log4j naplózó könyvtár 1.2.17 vagy magasabb

A TOE és környezetét az 1. számú ábra mutatja be.



1. számú ábra A TOE és környezete

I.4. A rendszer főbb komponenseinek azonosítása

Értékelt TOE verzió:

Fájlnév	Verzió
a2-api-BIN-2_6_1.jar	2.6.1
SHA256: 18922E23F2629C2902ACC91B6D20F6D7C71D3C5B2B0E4F9FC632EE5E9735477A	

Az értékelt konfiguráció elemei:

Operációs rendszerek:

- OS X Sonoma 14.51
- OS X Sequoia 15.1
- Windows 11
- Ubuntu 24.04.1 LTS
- RHEL 9.5 ARM
- RHEL 9.5 AMD

JAVA platformok:

- Java 21 LTS
- Java 17 LTS
- Java 22
- Java 23
- Java 8 LTS

Hardver aláírás-létrehozó eszközök:

1. SafeNet IDPrime 940, illetve SafeNet IDPrime 3940 típusú intelligens kártya, IAS Classic v4.4.2, MOC v1.1 szerverrel, Java Card MultiApp V4.0.1 platformon, Infineon M7892 G12 chipkártyán

2. Thales Solo XC F3

HW verzió: nC3025E/nC4035E/nC4335N

SW verzió: 12.50.11

3. eSzemélyi

IDentity Applet Suite Version 3.2 alkalmazás, NXP J2E120_M65 / J3E120_M65 / J2E082_M65 / J3E082_M65 v2.4.2 R3 Secure Smart Card Controllerekből álló intelligens kártya

4. Gemalto IDClassic 340

MultiApp ID v2.1 Java Card platform, P5CC081V1A mikrochip, MPH117 V2.2 szűrővel

5. Bit4Id Touch & Sign 2048

ST19WR661 mikrochip, Touch & SIGN 2048 V1.00 alkalmazás

6. Gemalto IDPrime 840

MultiApp v3 Java Card platform, M7820 A12 mikrochip, IAS v.4 alkalmazás

7. SafeNet eToken

9.1-es verzió, Athena IDProtect/OS755 Java Card kártya, Atmel AT90SC25672RCT-USB Microcontrolleren, IDSign applet beágyazással

8. ThaleS nShield F3 500e+ PCI Express

NC4433E-500

9. Thales nShield Connect 1500+ F3

NH2061

II. A tanúsítás jellemzése

Jelen tanúsítás a termék biztonsági előirányzatában lefektetetett követelmények teljesülését vizsgálja.

- A2-Polysys CryptoSigno Interop JAVA API for Qualified Electronic Signature and Seal Security Target ST V4.0 (2024. szeptember 16.)

II.1. Az alkalmazott értékelési módszer

Az A2-Polysys CryptoSigno Interop JAVA API modul értékelésére az MSZ EN ISO/IEC 18045:2020 /Informatika. Biztonságtechnika. Az informatikai biztonságértékelés módszertana/ értékelési módszertant alkalmazták.

Az értékelés garanciaszintje MSZ EN ISO/IEC 15408-3:2020 szerinti EAL3-as kiterjesztve ALC_FLR.2 komponenssel.

II.2. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Értékelési Jelentés:

A2-Polysys CryptoSigno Interop JAVA API v2.6.1 ÉRTÉKELÉSI JELENTÉS az MSZ EN ISO/IEC 15408-3:2020 szerinti EAL3-as szintnek kiterjesztve ALC_FLR.2 komponenssel való megfeleltetésről C077-02/P/E/ETR

II.3. Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

fejlesztői bizonyíték	Cím	verzió
Biztonsági előirányzat	A2-Polysys_ST_Security_Target v4.0.pdf	v4.0
Az előkészítő eljárások leírása	A2-Polysys_SG_Support_Guide-signed.pdf	v4.0
Üzemeltetési felhasználói útmutató	A2-Polysys_SG_Support_Guide-signed.pdf	v4.0
Biztonsági szerkezet leírás	A2-Polysys_HLD_HighLevel_Design.docx	v4.0
Funkcionális specifikáció	A2-Polysys_FS_Functional_Specification.docx	v4.0
TOE terv	A2-Polysys_HLD_HighLevel_Design.docx	v4.0
Konfiguráció lista	a2-api-BIN-2_6_1.jar	v2.6.1
A konfiguráció kezelés dokumentációja	A2-Polysys_CM_Configuration_Management.docx	v4.0
A fejlesztés biztonság dokumentációja	A2-Polysys_CM_Configuration_Management.docx	v4.0
Az életciklus meghatározás dokumentációja	A2-Polysys_CM_Configuration_Management.docx	v4.0
A szállítási eljárások leírása	A2-Polysys_DO_Delivery_and_Operation.docx	v4.0
A tesztelésre alkalmas TOE	a2-api-BIN-2_6_1.jar	v2.6.1
Tesztelési terv/Tesztelési dokumentáció	A2-Polysys_TG_Test_Guide.docx	v4.0
Teszt lefedettség elemzés	A2-Polysys_TCD_Test_Coverage_Depth_Analysis.pdf	v4.0
Teszt mélység elemzés	A2-Polysys_TCD_Test_Coverage_Depth_Analysis.pdf	v4.0

II.4. Az értékelési folyamat tanúsítási szempontú ellenőrzése

A Tanúsítási Jelentés készítői a teljes értékelési folyamatot figyelemmel kísérték, ellenőrizték:

- az értékelési folyamatok módszertani szempontú ellenőrzésével;
- különböző szakértői megbeszéléseken való részvétellel.

III. Az értékelés eredményei

III.1. A garanciális biztonsági követelményeknek való megfelelés

Az értékelés módszertana a MSZ EN ISO/IEC 18045:2020 szabványt követte, az eredmények leírása is az ott meghatározott jelöléseket alkalmazza.

III.1.1. A biztonsági előirányzat értékelése

Értékelői feladatelem	határozat
ASE_INT.1: Biztonsági előirányzat, Bevezetés	megfelelt
ASE_CCL.1 Biztonsági előirányzat, Megfelelőségi nyilatkozatok	megfelelt
ASE_SPD.1: Biztonsági előirányzat, Biztonsági probléma meghatározás	megfelelt
ASE_OBJ.2: Biztonsági előirányzat, Biztonsági célok	megfelelt
ASE_ECD.1: Biztonsági előirányzat, Kiterjesztett biztonsági követelmények	megfelelt
ASE_REQ.2: Biztonsági előirányzat, Biztonsági követelmények	megfelelt
ASE_TSS.1: Biztonsági előirányzat, Az értékelés tárgya összefoglaló előírása	megfelelt

III.1.2. A fejlesztés értékelése

Értékelői feladatelem	határozat
ADV_ARC.1: Biztonsági szerkezet leírás	megfelelt
ADV_FSP.3: Funkcionális specifikáció teljes összegzéssel	megfelelt
ADV_TDS.2: Szerkezeti terv	megfelelt

III.1.3. Az útmutatók értékelése

Értékelői feladatelem	határozat
AGD_OPE.1: Üzemeltetési felhasználói útmutató	megfelelt
AGD_PRE.1: Előkészítő eljárások	megfelelt

III.1.4. Az életciklus támogatás értékelése

Értékelői feladatelem	határozat
ALC_CMC.3: Engedélyezéssel kapcsolatos intézkedések	megfelelt
ALC_CMS.3: A megvalósítási reprezentáció CM lefedettsége	megfelelt
ALC_DEL.1: Szállítási eljárások	megfelelt
ALC_DVS.1: A biztonsági intézkedések azonosítása	megfelelt
ALC_FLR.2: Hibabejelentési eljárások[1]	megfelelt
ALC_LCD.1: A fejlesztő által meghatározott életciklus modell	megfelelt

III.1.5. A tesztelés értékelése

Értékelői feladatelem	határozat
ATE_FUN.1: Funkcionális tesztelés	megfelelt
ATE_COV.2: A lefedettség vizsgálata	megfelelt
ATE_DPT.1: Az alap terv tesztelése	megfelelt
ATE_IND.2: Független tesztelés - minta	megfelelt

III.1.5.1. A2-Polysys CryptoSigno Interop JAVA API -val tesztelt platformok

A fejlesztői tesztek az alábbi szoftverkörnyezetben zajlottak:

#	Hardver	Operációs rendszer + JAVA verzió
1.	Apple Silicon M1 Max ARM64 CPU 10 core, GPU 32 core 64 GB RAM Fizikai host: MacBook Pro 2021	OS X Sonoma 14.51 Java 21 LTS (BellSoft 21.0.4+9-LTS aarch64)
2.	Apple Silicon M1 Max ARM64 CPU 4 core 16 GB RAM Fizikai host: MacBook Pro 2021	Windows 11 (virtualizált) 21H2 22000.2538 Java 17 LTS (BellSoft 21.0.2+14-LTS aarch64)
3.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Fizikai host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s) Java 22 (BellSoft 22+37 aarch64)
4.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Fizikai host:	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s) Java 23 (BellSoft 23.0.1+13 aarch64)

[1] Kiterjesztés

	MacBook Pro 2021	
5.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Fizikai host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s) Java 21 LTS (BellSoft 21.0.5+11-LTS aarch64)
6.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Fizikai host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s) Java 8 LTS (BellSoft 1.8.0_432-b07 aarch64)
7.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Fizikai host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s) Java 21 LTS (Oracle 21.0.5+9-LTS-239 aarch64)
8.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Fizikai host: MacBook Pro 2021	Red Hat Enterprise Linux 9.5 ARM (virtualizált) (external SSD ADATA 3000 MB/s) Java 23 (BellSoft 23.0.1+13 aarch64)
9.	Apple 3.6 GHz Intel Core i9 CPU 2 core 8 GB RAM Fizikai host: iMac”27 2019	Red Hat Enterprise Linux 9.5 AMD (virtualizált) (external SSD ADATA 3000 MB/s) Java 21 (Oracle 21.0.5+9-LTS-239 amd64)
10.	Apple Silicon M1 Max ARM64 CPU 10 core, GPU 32 core 64 GB RAM Fizikai host: MacBook Pro 2021	OS X Sequoia 15.1 Java 23 (BellSoft 23.0.1+13 aarch64)

III.1.5.2. A2-Polysys CryptoSigno Interop JAVA API-val tesztelt PKCS#11-es hardver aláírás-létrehozó eszközök

A TOE az alábbi aláírás létrehozó eszközökkel tesztelték.

1.	**SafeNet IDPrime 940,** illetve SafeNet IDPrime 3940 típusú intelligens kártya, IAS Classic v4.4.2, MOC v1.1 szerverrel, Java Card MultiApp V4.0.1 platformon, Infineon M7892 G12 chipkártyán	QSCD
2.	**Thales Solo XC F3** HW verzió: nC3025E/nC4035E/nC4335N SW verzió: 12.50.11	HSM modul
3.	**eSzemélyi** IDentity Applet Suite Version 3.2 alkalmazás, NXP J2E120_M65 / J3E120_M65 / J2E082_M65 / J3E082_M65 v2.4.2 R3 Secure Smart Card Controllerekből álló intelligens kártya	QSCD
4.	**Gemalto IDClassic 340** MultiApp ID v2.1 Java Card platform, P5CC081V1A mikrochip, MPH117 V2.2 szűrővel	QSCD
5.	**Bit4Id Touch & Sign 2048**	QSCD

	ST19WR661 mikrochip, Touch & SIGN 2048 V1.00 alkalmazás	
6.	**Gemalto IDPrime 840** MultiApp v3 Java Card platform, M7820 A12 mikrochip, IAS v.4 alkalmazás	QSCD
7.	**SafeNet eToken** 9.1-es verzió, Athena IDProtect/OS755 Java Card kártya, Atmel AT90SC25672RCT-USB Microcontrolleren, IDSign applet beágyazással	QSCD
8.	**ThaleS nShield F3 500e+ PCI Express** NC4433E-500	HSM modul
9.	**Thales nShield Connect 1500+ F3** NH2061	HSM modul

III.1.6. A sebezhetőség értékelése

Az értékelő áttekintette a tesztelési dokumentációt, jegyzőkönyveket, valamint a fejlesztői Sebezhetőség elemzés Developer Vulnerability Analysis VU dokumentációt, annak érdekében, hogy meghatározza a TOE-ban esetlegesen előforduló lehetséges sebezhetőségeket. A TOE üzemeltetési környezetében nem érzékeny a nyilvános forrásokban az értékelés időpontjáig megjelent kereséssel azonosított lehetséges sebezhetőségekre.

Az értékelő tanulmányozta a nyilvános adatbázisokat, információ forrásokat a TOE lehetséges sebezhetőségeinek meghatározása céljából. Ellenőrzésre kerültek a TOE által használt harmadik feles alkalmazások a nyílt sérülékenység adatbázisok által.

A fenti vizsgálatok nem tártak fel kockázatokat, így az értékelés eredménye alapján a TOE üzemeltetési környezetében ellenáll egy alap támadó képességgel rendelkező támadónak.

Értékelői feladatelem	határozat
AVA_VAN.2: Sebezhetőség vizsgálat	megfelelt

IV. Következtetés

A rendszer értékelés fő következtetése az alábbi:

Az A2-Polysys CryptoSigno Interop JAVA API megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés eredménye alapján a Tanúsító megállapítja, hogy az A2-Polysys CryptoSigno Interop JAVA API, mint informatikai biztonsági funkciókat megvalósító szoftver termék megfelel a II.3 fejezetben meghatározott Biztonsági Előirányzatnak az MSZ EN ISO/IEC 15408-3:2020 szabvány EAL 3-as garancia szinten kiterjesztve ALC_FLR.2 komponenssel.

Az eljárás megfelelt a HUNG_TMK-2-termek_20230109 azonosító számú, a terméktanúsító szervezet által működtetett, akkreditált tanúsítási rendszernek.

IV.1. Feltételek

Az értékelés következtetései a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket az A2-Polysys CryptoSigno Interop JAVA API nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezet teljesítse) az alábbiak:

OE.AUDIT_GENERATION Az IT környezetnek észlelni és naplózni kell a felhasználóra vonatkozó biztonsági eseményeket.

OE.AUDIT_PROTECTION Az IT környezet biztosítsa a napló információk védelmét.

OE.AUDIT_REVIEW Az IT környezet biztosítson szelektív megjelenítést a napló információk tekintetében.

OE.Configuration A TOE megfelelően telepített és a konfigurált legyen a biztonságos állapotban történő elindításhoz.

OE.CORRECT_TSF_OPERATION Az IT környezet biztosítsa a TOE biztonsági funkcióinak tesztelését biztosítva azok ügyféloldali megfelelő működését.

OE.CRYPTOGRAPHY Az IT környezetnek FIPS 140-2 szabványnak megfelelő kriptográfiai szolgáltatásokat kell nyújtania a TOE számára. Minősített elektronikus aláírás vagy elektronikus bélyegző létrehozása esetén a TOE-nak véletlenszám generátort és QSCD által biztosított kriptográfiai szolgáltatást kell használnia.

OE.DISPLAY_BANNER Az IT környezetnek tájékoztató figyelmeztetést kell adnia a TOE használatával kapcsolatban.

OE.Basic A TOE tervezése és megvalósítása alap támadópotenciál elleni védelmet biztosít, ahogy a sérülékenység elemzés megállapította. (Az IT környezetet nem fenyegetheti ennél nagyobb támadópotenciál.)

OE.NO_EVIL A TOE felhasználási helyein az adminisztrátorok nem lehetnek rosszindulatúak, megfelelően képzettek és követik az adminisztrátori útmutató előírásait.

OE.PHYSICAL A TOE fizikai környezete elfogadható szintű biztonságot nyújtson, így a TOE nem manipulálható, illetve nem lehet alanya különböző típusú (pl. áramfelvétel analízis) side-channel támadásnak.

OE.RESIDUAL_INFORMATION Az IT környezet biztosítsa, hogy a tárgykörbe tartozó védett erőforrások által kezelt információk bizalmassága az erőforrások újra alkalmazása esetén sem sérül.

OE.SELF_PROTECTION Az IT környezet olyan működési környezetetett biztosítson, ami védi önmagát és erőforrásait a külső káros megzavarástól, módosítástól vagy jogosulatlan felfedéstől.

OE.TIME_STAMPS Az IT környezet megbízható időszolgáltatást biztosítson, ahol az adminisztrátor képes az alkalmazandó idő beállítására.

OE.TIME_TOE Az IT környezet megbízható idő jelzést biztosítson a TOE számára

OE.TOE_ACCESS Az IT környezet kontroll mechanizmust biztosítson a felhasználók TOE-hez való logikai hozzáférése tekintetében.

OE.TOE_PROTECTION Az IT környezet védje meg a TOE-t és erőforrásait a külső káros megzavarástól, módosítástól vagy jogosulatlan felfedéstől.

V. Hivatkozások, rövidítések

V.1. A követelményeket tartalmazó dokumentum

MSZ EN ISO/IEC 15408-1:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell

MSZ EN ISO/IEC 15408-2:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei

MSZ EN ISO/IEC 15408-3:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei

V.2. Figyelembe módszertani dokumentumok

MSZ EN ISO/IEC 18045:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés módszertana

ETSI TS 119 101 V1.1.1 (2016-03) Policy and security requirements for applications for signature creation and signature validation

V.3. Rövidítések

ADV (Assurance: Development)	Fejlesztés értékelése
AGD (Assurance: Guidance documents)	Útmutató dokumentumok értékelése
ALC (Assurance: Life cycle support)	Életciklus támogatás értékelése
ASE (Assurance: Security Target)	Biztonsági előirányzat értékelése
ATE (Assurance: Tests)	Tesztelés értékelése
AVA (Assurance: Vulnerability assessment)	Sebezhetőségi elemzés értékelése
CC (Common Criteria)	Közös szempontok
CM (Configuration management)	Konfiguráció kezelés
EAL (Evaluation Assurance Level)	Értékelési garanciaszint
ETR (Evaluation Technical Report)	Értékelési jelentés
ST (Security Target)	Biztonsági előirányzat
TOE (Target of Evaluation)	TOE, Értékelés tárgya
API (Application Interface)	Applikációs interfész