HUNGUARD

TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. (1123 Budapest, Kékgolyó u. 6.) mint a NAH által NAH-6-0048/2023 számon akkreditált terméktanúsító szervezet a HUNG_TMK-2-termek_20230109 azonosítójú tanúsítási rendszer szerint

tanúsítja, hogy a

polysys ®

által fejlesztett

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

verziója

mint informatikai biztonsági funkciókat megvalósító szoftver termék

megfelel

a 3. sz. mellékletben meghatározott Biztonsági Előirányzatnak
az MSZ EN ISO/IEC 15408-3:2020 szabványban szereplő az ALC_FLR.2
komponenssel kiterjesztett EAL3 biztonsági szinten.

Jelen Tanúsítvány a **HUNG-TJ-15408-002-2024** számú
Tanúsítási Jelentés alapján került kiadásra.

Készült a Polysys Kft.
(*1162 Budapest, Margitháza u. 1.*) megbízásából.
A Tanúsítvány regisztrációs száma: **HUNG-T-15408-002-2024**
A Tanúsítvány érvényességének kezdete: *2024. december 20.*
A Tanúsítvány érvényességének vége: *2027. december 20.*
A Tanúsítvány terjedelme nyolc oldal az érvényességi feltételeket és egyéb jellemzőket tartalmazó mellékletekkel együtt.

Kelt: Budapest, 2024. december 20.

Digitálisan aláírta:
Endrődi Zsolt Attila

PH.

Digitálisan aláírta:
Szűcs Ákos Balázs

Endrődi Zsolt Attila
Tanúsítási igazgató

Szűcs Ákos Balázs
Ügyvezető igazgató

1. számú melléklet

A Tanúsítvány érvényességi feltételei

Az üzemeltetési környezetre vonatkozó biztonsági célok:

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 környeztetett 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.

2. számú melléklet

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

3. számú melléklet

A tanúsítási eljárás egyéb jellemzői

Jelen Tanúsítvány az alábbi értékelési dokumentum alapján került kiadásra:

- 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

Az értékelés az alábbi biztonsági előirányzatot alkalmazta:

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

Az értékelés garancia szintje: EAL3, kiterjesztve ALC_FLR.2 komponenssel

Figyelembe vett mértékadó 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

4. számú melléklet

A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seallel tesztelt platformok

#	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: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s) Java 23 (BellSoft 23.0.1+13 aarch64)
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:	Ubuntu 24.04.1 LTS (virtualizált) (external SSD ADATA 3000 MB/s)

	MacBook Pro 2021	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)

5. számú melléklet

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

#	Hardver	Típus
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** ST19WR661 mikrochip, Touch & SIGN 2048 V1.00 alkalmazás	QSCD
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