HUNGUARD

CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. (6 Kékgolyó str. Budapest 1123 Hungary) as a certification authority accredited by the accreditation document No. NAH-6-0048/2023 of NAH as described in the applied certification system HUNG_TMK-2-termek_20230109

certifies, that

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

developed by

polysys ®

as software product providing IT security functions

conforms

to the security target described in Annex 3 at EAL3, augmented by the ALC_FLR.2 component of ISO/IEC 15408-3:2020

This certificate has been issued on the basis of the Certification report
HUNG-TJ-15408-002-2024

Produced on commission for
Polysys Kft. (1 Margitháza street Budapest 1162 Hungary).

Certificate registration number: **HUNG-T-15408-002-2024**
Validity start date of the certificate: 20 December, 2024
Validity end date of the certificate: 20 December, 2027

This Certificate has eight pages including the Annexes containing validity terms and other attributes.

Budapest, 20 December, 2024

Digitally signed:
Endrődi Zsolt Attila

PH.

Digitally signed:
Szűcs Ákos Balázs

Endrődi Zsolt Attila
Certification director

Szűcs Ákos Balázs
Managing director

Annex 1

Validity terms of the certificate

Security objectives for the IT environment:

The conclusions of the evaluation relies on the environmental assumptions listed in the Security Target.

The following objectives are not handled by A2-Polysys CryptoSigno Interop JAVA API but are expected from the IT environment:

OE.AUDIT_GENERATION The IT Environment will provide the capability to detect and create records of security-relevant events associated with users.

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.AUDIT_REVIEW The IT Environment will provide the capability to selectively view audit information.

OE.Configuration The TOE will be installed and configured properly for starting up the TOE in a secure state.

OE.CORRECT_TSF_OPERATION The IT Environment will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.

OE.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-2 compliant cryptographic services provided by the IT Environment. In addition, the TOE shall use the cryptographic services of a QSCD for QES generation and random number generation during the QES creation.

OE.DISPLAY_BANNER The IT Environment will display an advisory warning regarding use of the TOE.

OE.Basic The TOE will be designed and implemented for a minimum attack potential of "Basic" as validated by the vulnerability analysis.

OE.NO_EVIL Sites using the TOE will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.

OE.PHYSICAL The non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis.

OE.RESIDUAL_INFORMATION The IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

OE.SELF_PROTECTION The IT Environment will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

OE.TIME_STAMPS The IT Environment will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.

OE.TIME_TOE The IT Environment will provide reliable time for the TOE use.

OE.TOE_ACCESS The IT Environment will provide mechanisms that control a user's logical access to the TOE.

OE.TOE_PROTECTION The IT Environment will protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification.

Annex 2

Document containing the requirements

MSZ EN ISO/IEC 15408-1:2020 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

MSZ EN ISO/IEC 15408-2:2020 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

MSZ EN ISO/IEC 15408-3:2020 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

Annex 3

Further features of the certification

This Certificate is issued on the basis of the following evaluation document

- 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

The evaluation has applied the following security target:

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

Evaluation level: EAL3, augmented by the ALC_FLR.2

Considered document about methodology

MSZ EN ISO/IEC 18045:2020 Information technology — Security techniques — Methodology for IT security evaluation

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

Annex 4

Platforms tested with A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal

#	Hardware	Operation system + JAVA version
1.	Apple Silicon M1 Max ARM64 CPU 10 core, GPU 32 core 64 GB RAM Physical 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 Physical host: MacBook Pro 2021	Windows 11 (virtualised) 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 Physical host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualised) (external SSD ADATA 3000 MB/s) Java 22 (BellSoft 22+37 aarch64)
4.	Apple Silicon M1 Max ARM64 CPU 2 core 8 GB RAM Physical host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualised) (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 Physical host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualised) (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 Physical host:	Ubuntu 24.04.1 LTS (virtualised) (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 Physical host: MacBook Pro 2021	Ubuntu 24.04.1 LTS (virtualised) (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 Physical host: MacBook Pro 2021	Red Hat Enterprise Linux 9.5 ARM (virtualised) (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 Physical host: iMac”27 2019	Red Hat Enterprise Linux 9.5 AMD (virtualised) (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 Physical host: MacBook Pro 2021	OS X Sequoia 15.1 Java 23 (BellSoft 23.0.1+13 aarch64)

5. számú melléklet

PKCS#11 hardware signature creation devices tested with A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal

#	Hardver	Típus
1.	**SafeNet IDPrime 940,** or SafeNet IDPrime 3940 smart card type IAS Classic v4.4.2, with MOC v1.1 server, Java Card MultiApp V4.0.1 on Infineon M7892 G12 chipcard	QSCD
2.	**Thales Solo XC F3** HW version: nC3025E/nC4035E/nC4335N SW version: 12.50.11	HSM modul
3.	**eSzemélyi** IDentity Applet Suite Version 3.2 app, smart card consisting of NXP J2E120_M65 / J3E120_M65 / J2E082_M65 / J3E082_M65 v2.4.2 R3 Secure Smart Card Controllers	QSCD
4.	**Gemalto IDClassic 340** MultiApp ID v2.1 Java Card platform, P5CC081V1A microchip, with MPH117 V2.2 filter	QSCD
5.	**Bit4Id Touch & Sign 2048** ST19WR661 microchip, Touch & SIGN 2048 V1.00 app	QSCD
6.	**Gemalto IDPrime 840** MultiApp v3 Java Card platform, M7820 A12 microchip, IAS v.4 app	QSCD
7.	**SafeNet eToken** Version 9.1, Athena IDProtect/OS755 Java Card card, Atmel AT90SC25672RCT-USB on microcontroller, IDSign applet embedded	QSCD
8.	**ThaleS nShield F3 500e+ PCI Express** NC4433E-500	HSM modul
9.	**Thales nShield Connect 1500+ F3** NH2061	HSM modul