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-6-0048/2018 of NAH as described in the applied certification system HUNG_TMK-2-termek_20180629

certifies, that

A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal v2.5.0

developed by

polysys ®

as software product providing IT security functions

complies

with moderate security level specified in MIBÉTS methodology in KIB recommendation No 28.

This certificate has been issued on the basis of the Certification report **HUNG-TJ-MIBÉTS-014-2018**

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

Certificate registration number: **HUNG-T-MIBÉTS-014-2018**
Validity start date of the certificate: 28 December, 2018
Validity end date of the certificate: 28 December, 2021

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

Budapest, 28 December, 2018

PH.

Digitálisan aláírta: HUNGUARD

Endrődi Zsolt
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

MIBÉTS 2009 KIB (Information Technology Committee for Public Services) recommendation No 28. „Evaluation methodology for products” v4 2008.09.19

Annex 3

Further features of the certification

This certificate has been issued according to the following:

- System evaluation report: A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal V2.5.0 ÉRTÉKELÉSI JELENTÉS v1.0, C077-02/P/E

Evaluation level: Moderate security level (MIBÉTS Fokozott)

Considered document about methodology

Common Criteria for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4) – Part 1: Introduction and general model

Common Criteria for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4) – Part 2: Security functional components

Common Criteria for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4) – Part 3: Security assurance components

Common Methodology for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4)

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