HUNGUARD

CERTIFICATE MAINTENANCE and REVIEW RECORD

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. IKF/19519-2/2012-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

in Certificate Maintenance Process

extends

the claims of the HUNG-T-029-2006 CERTIFICATE
for the following version developed by

polysys®

A2-Polysys CryptoSigno Interop JAVA API version 2.4.1 /build 143/

a2-api-BIN-2_4_1.jar
SHA256: 57569757F027EBD9D6BFF6995D70C818B75C79B8DE4948F44EA1AD59158E1A8F

with the functionality listed in Annex 1 and
with the secure usage conditions contained in Annex 2 of the referenced certificate.

Besides, as a result of the review process the certification authority declares that the certified status can be maintained until 23 February 2018 for the following certified versions:

v2.3.0 build 141, v2.4.0 build 142, v2.4.1 build 143.

Registration number of this Maintenance Record: **HUNG-FJ-029/4-2015**

Budapest, 12 February 2015

PH.

Szabó Bálint Quality assurance director	Csik Balázs Managing director

Annex 1

A2-Polysys CryptoSigno Interop JAVA API conforms to the requirements laid down in the following normative documents:

- Regulation 2014/910/EU (on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC)
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 2014/148/EU (amending Decision 2011/130/EU)
- 2013/662/EU (amending Decision 2009/767/EC)
- 2011/130/EU (establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market)
- 2010/425/EU (amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States)
- 2009/767/EC (setting out measures facilitating the use of procedures by electronic means through the ‘points of single contact’ under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market)
- Directive 2006/123/EC (on services in the internal market)
- Directive 1999/93/EC (on a Community Framework for electronic signatures)

A2-Polysys CryptoSigno Interop JAVA API conforms to the following standards:

- ETSI TS 101 903 v1.4.2 (2010-12), v1.4.1 (2009-06), v1.3.2 (2006-03), v1.2.2 (2004-04) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
- ETSI TS 103 171 v2.1.1 (2012-03) XAdES Baseline Profile
- ETSI TS 119 134-5 v1.1.1 (2012-04) Conformance Testing for XAdES Baseline Profile

A2-Polysys CryptoSigno Interop JAVA API supports the standpoint written in the informative document on the secure cryptographic algorithms, issued on 24th April 2012 by the Hungarian Electronic Signature Association (MELASZ):

1. After 30 June 2012, advanced and qualified electronic signatures should be implemented only by applying secure cryptographic algorithms (SHA256, RSA2048 or stronger).

2. Those advanced and qualified electronic signatures that had been created before 30 June 2012 – by applying cryptographic algorithms which should not be considered secure after 30 June 2012– must be accepted valid after 31 December 2012 if these signatures are strengthened (e.g. with archive validation data) until 31 Dec 2012 by applying such cryptographic algorithms on them that are considered secure after 30 June 2012 as well.

3. Until 31 December 2012 at the latest, signature verification applications should be prepared in such a way that –in case of advanced and qualified electronic signatures created by cryptographic algorithms that cannot be considered secure after 30 June 2012– during the verification process these applications notify the users that the electronic signature under verification has been created by a cryptographic algorithm that may not necessarily be regarded as secure.

Annex 2

Platforms tested with A2-Polysys CryptoSigno Interop JAVA API

From version 2.2.0 /build 138/:

	Hardware configuration	Software configuration
1	IBM eServer xSeries 346 2x3.6 GHz Intel Xeon processor, 8x1 GB PC3200 ECC DDR333 ECC memory, 2x36 GB 10K U320 SCSI SL HDD, 2xQLogic FC2-133 Host Bus adapter	Novell/SuSE Linux Enterprise Server 9 SP2 operating system
2	IBM eServer iSeries 550 4xPower5+ 1.75 GHz processor, 25 GB memory, 6x73 GB HDD, 3x Giga Ethernet card	AS400 i5OS 5.3 JAVA Level 7 OS level 5207530 operating system
3	IBM eSeries pSeries 570 4xPower5+ 1.9 GHz processor, 12 GB memory, 6x73 GB HDD, 3x Giga Ethernet card	IBM AIX 5.3.3 and RedHat Enterprise Linux Advanced Server 4 SR1 operating systems
4	Sun Fire V20z 2xAMD Opteron 244 processor, 2 GB DDR1/333 memory, 73 GB ULTRA 320 Scsi HDD	Red Hat Enterprise Linux 3 operating system
5	Sun Java Workstation W1100z Single AMD Opteron 246 processor, 2 GB PC3200 DDR-400 memory, 73 GB ULTRA 320 Scsi HDD	Solaris 10 x86 with recommended patch cluster operating system
6	Sun Java Workstation W2100z Dual AMD Opteron 252 processor, 2 GB PC3200 DDR-400 memory, 73 GB ULTRA 320 Scsi HDD	SuSE Linux Enterprise Server 9 AMD 64 operating system
7	Sun Ultra 20 Workstation „Large” AMD Opteron 152 processor, 2 GB ECC PC3200 memory, 250 GB SATA HDD	Windows XP operating system
8	Sun Fire V120, one pack 650 Mhz processor, 1 GB memory, 2x73 GB ULTRA 320 Scsi HDD	Solaris 9 SPARC 09/04 operating system
9	Sun Blade 2500 Workstation model 1x1.05 GHz UltraSPARC IIIi processor, 1 GB DDR1 memory, 73 GB ULTRA 320 Scsi HDD,	Solaris 10 SPARC First Customer Shipment operating system
10	Sun Fire V440 Server 4x1.062 GHz UltraSPARC IIIi processor, 2 GB DDR1 memory, 2x73 GB ULTRA 320 Scsi HDD	Solaris 10 SPARC First Customer Shipment operating system
11	Sun Fire V240 2x1.5 GHz UltraSPARC IIIi processor, 8 GB DDR1 memory, 2x73 GB ULTRA 320 Scsi HDD,	Solaris 10 SPARC First Customer Shipment operating system
12	Gericom Holywood XXL	Suse 9.3 operating system
13	HP server rx1620 model, 1 db 1300 MHz Itanium2 CPU, 2 GB RAM, 2 db 36 GB UW320 HD, 2 db Gbps LAN	Windows 2003 server operating system
14	Intel Pentium processor	Novell/SuSE Linux 10 operating system
15	HP server rx1620 model, 1 db 1300 MHz Itanium2 CPU, 2 GB RAM, 2 db 36 GB UW320 HD, 2 db Gbps LAN	Windows 2003 Enterprise Edition JDK 1.4.2.10 operating system
16	HP server rx1620 model, 1 db 1300 MHz Itanium2 CPU, 2 GB RAM, 2 db 36 GB UW320 HD, 2 db Gbps LAN	HP-UX 11.23 May 2005 JDK 1.5.0.02 operating system
17	HP server rx1620 model, 1 db 1300 MHz Itanium2 CPU, 2 GB RAM, 2 db 36 GB UW320 HD, 2 db Gbps LAN	RedHat Enterprise and Linux Advanced Server 4 Update 2 JDK 1.4.2.10 operating system
18	Apple MacBook, Intel Core 2 Duo 2GHz processor, 1 GB RAM	Mac OS X Tiger 10.4.9 operating system, Apple Java 1.5.0_07-164
19	Apple MacBook, Intel Core 2 Duo 2GHz processor, 756 MB RAM	Windows Vista 6.0 operating system, Sun Java 1.6.0_01-b06
20	Apple iMac 24-inch, 2.4 GHz Intel Core 2 Duo, 4 GB RAM	Mac OS Leopard X 10.5.2 Apple Java 1.5.0_13-119

21	IBM System x3850M2, 4 x Intel Xeon Processor x7350 - 2.93GHz 8MB L2 Quad Core , 16 x 1GB DIMM PC2-5300 CL5 ECC DDR2 SDRAM LP RDIMM 4 x 73GB 2.5 15K RPM SAS Hot-Swap HDD	Windows 2008 Enterprise Java:SUN 1.6.0_12-b04, Java HotSpot(TM) 64-Bit Server VM
22	IBM System x3650, 2 x Quad-Core Intel Xeon Processor X5470 (3.33GHz 1333MHz 12MB L2 Cache 120W) 12 x 4GB kit Quad Rank PC2-5300 CL5 ECC Low Power 6 x 450 15K SAS 3.5-inch HS HDD QLogic 8Gb FC Dual-port HBA IBM ServeRAID-MR10is VAULT SAS/SATA Controller Remote Supervisor Adapter II Slimline 2 x 835 Watt Hot-swap Power Supply	Redhat Enterprise 5.3 Java: J2RE 1.6.0 IBM J9 2.4 Linux amd64-64 jvmxa6460-20081105_25433
23	IBM HS21 BladeServer, 2 x Quad-Core Intel Xeon Processor X5470 (3.33GHz 1333MHz 12MB L2 Cache 120W) 12 x 4GB kit Quad Rank PC2-5300 CL5 ECC Low Power 6 x 450 15K SAS 3.5-inch HS HDD QLogic 8Gb FC Dual-port HBA IBM ServeRAID-MR10is VAULT SAS/SATA Controller Remote Supervisor Adapter II Slimline 2 x 835 Watt Hot-swap Power Supply	Suse Enterprise 10.2, SP2 Java: J2RE 1.6.0 IBM J9 2.4 Linux amd64-64 jvmxa6460-20081105_25433
24	IBM POWER Systems 570 (9406-MMA), 2 x Dual-Core POWER6 Processor (4,7GHz) 8 x 4GB DDR2, 667, CL5, ECC 6 x 146 GB 15K SAS HDD Partition: 2 core 7GB memory	IBMi 6.1 (OS/400 V6R1) Java:IBM 1.5.0_13-b05, PowerPC, OS/400
25	IBM POWER Systems 570 (9117-MMA) ,2 x Dual-Core POWER6 Processor (4,7GHz) 24 x 1GB DDR2, 667, CL5, ECC 6 x 146 GB 15K SAS HDD Partition: 2 core 4GB memory	AIX 6.1 Java:J2RE 1.6.0 IBM J9 2.4 AIX ppc64-64 jvmap6460-20081105_25433
26	Apple iMac 24 inch, 2 x Dual-Core Intel Processor 2,4GHz ,4 GB memory; 300 GB HDD	Ubuntu Linux 8.12: Java:SUN 1.6.0_12-b04, Java HotSpot(TM) Client VM

From version 2.2.1 /build 140/:

	Hardware configuration	Software configuration
27	Intel Core 2 CPU, 2 GB RAM	Mac OS X 10.6.2 (Snow Leopard) operating system, Apple Java 1.5.0_19_b02-304 32 Bit
28	Intel Core 2 CPU, 1 GB RAM	Windows 7 Enterprise 32-bit operating system, Sun Java 1.6.0_18-b07 HotSpot(TM) Client VM 32 bit
29	Intel Core 2 CPU, 1 GB RAM	Windows 7 Enterprise 64-bit operating system, Sun Java 1.6.0_18-b07 HotSpot(TM) 64-Bit Server VM

From version 2.4.0 /build 142/:

	Hardware configuration	Software configuration
30	Intel Core i7 2,4 GHz 2 GB RAM arch: amd64, processor: 2	Windows 8 Enterprise 64 bit Oracle Java 1.7.0_09-b05 Java HotSpot(TM) 64-Bit Server VM (OS: Windows 8 6.2, arch: amd64, processor: 2)
31	Intel Core i7 2,4 GHz 2 GB RAM arch: x86, processor: 2	Windows 8 Enterprise 32 bit Oracle Java 1.7.0_09-b05 Java HotSpot(TM) 64-Bit Server VM (OS: Windows 8 6.2, arch: x86, processor: 2)
32	Intel Core i7 2,4 GHz 1 GB RAM arch: amd64, processor: 2	Windows 7 Home Premium 64 bit Oracle Java 1.7.0_05-b06 Java HotSpot(TM) 64-Bit Server VM (OS: Windows 7 6.1, arch: amd64, processor: 2)
33	Apple MacBook Pro Intel Core i7 2,4 GHz 8 GB RAM arch: x86_64, processor: 8	Mac OS X Mountain Lion 10.8.2 Oracle Java 1.7.0_04-b21 Java HotSpot(TM) 64-Bit Server VM (OS: Mac OS X 10.8.2, arch: x86_64, processor: 8)
34	Apple MacBook Pro Intel Core i7 2,4 GHz 8 GB RAM arch: x86_64, processor: 8	Mac OS X Mountain Lion 10.8.2 Apple Java 1.6.0_37-b06-434-11M3909 Java HotSpot(TM) 64-Bit Server VM (OS: Mac OS X 10.8.2, arch: x86_64, processor: 8)
35	IBM Flex System(TM) X240 Compute Node, KVM virtualization hypervisor, Intel Xeon Processor E5-2600 3,3 GHz, 64 GB RAM arch: amd64, processor: 8	Redhat Enterprise Linux 6.2 64 bit Oracle Java 1.7.0_09-b05 Java HotSpot(TM) 64-Bit Server VM (OS: Linux 2.6.32-220.el6.x86_64, arch: amd64, processor: 8)

2.4.1 /build 143/ verziótól:

	Hardware configuration	Software configuration
36	Intel Core i7 3,5 GHz 24 GB RAM arch: x86_64, processor: 8	OS X Mavericks 10.9.5 Oracle Java 1.8.0_25-b17 (OS: Mac OS X 10.9.5, arch: x86_64, processor: 8)
37	Intel Core i7 3,5 GHz 16 GB RAM arch: x86_64, processor: 4	OS X Yosemite 10.10.1 Oracle Java 1.8.0_25-b17 (OS: Mac OS X 10.10.1, arch: x86_64, processor: 4)
38	Intel Core i7 3,5 GHz 2 GB RAM arch: amd64, processor: 2	Ubuntu Linux 14.04 Oracle Java 1.8.0_25-b17 (OS: Linux 3.13.0-34-generic, arch: amd64, processor: 2)
39	Intel Core i7 3,5 GHz 4 GB RAM arch: amd64, processor: 4	openSUSE 13.2 Oracle Java 1.8.0_31-b13 (OS: Linux 3.16.6-2-desktop, arch: amd64, processor: 4)
40	Intel Core i7 3,5 GHz 4 GB RAM arch: amd64, processor: 4	Windows 10 Technical Preview 64 bit Oracle Java 1.8.0_31-b13 (OS: Windows 8.1 6.3, arch: amd64, processor: 4)
41	Intel Core i7 3,5 GHz 4 GB RAM arch: amd64, processor: 2	SUSE Linux Enterprise Server 12 Oracle Java 1.8.0_31-b13 (OS: Linux 3.12.28-4-default, arch: amd64, processor: 2)
42	Raspberry PI model B+ ARM11 700 Mhz arch: arm, processor: 1	Raspbian Linux 3.12 Oracle Java 1.7.0_40-b43 (OS: Linux 3.12.22+, arch: arm, processor: 1)

Annex 3

PKCS#11 hardware signature creation devices tested with A2-Polysys CryptoSigno Interop JAVA API

From version 2.2.0 /build 138/:

	device	operating system	chip
1	Aladdin e-Token PRO	CardOS/M4.01	SLE66CX320P
2	Oberthur CosmopolIC intelligens kártya	nyílt Java platform 2.1 V4 verzió	P8WE5033V0G
3	ORGA intelligens kártya	MICARDO v2.1	SLE66CX320P
4	Giesecke & Devrient token	STARCOS SPK 2.3 v7.0	P8WE5032v0G
5	SUN Crypto Accelerator	Solaris 10 SPARC	
6	Axalto Cyberflex Access 64K v2a	Global Platform – Open Platform v2.0.1	SLE66CX640P
7	nCipher netHSM 2000		
8	eToken PRO Java Card 72K	OS755, eToken Java Applet 1.0.37	AT90SC25672RCT-USB

From version 2.2.1 /build 140/:

	device	operating system	chip
9	IDOneClassIC Card: (ID-One Cosmo 64 RSA v5.4 + applet IDOneClassIC v1.0)	JavaCard Operating System: ID-One Cosmo 64 RSA v5.4 (GOP ID MX64)	P5CT072VOP

From version 2.3.0 /build 141/:

	device	operating system	chip
10	Gemalto Classic V3 (GemP15-1)	Firmware : 3.01	Hw: 59.125
11	Touch&Sign 2048	T&S DS/2048	ST19WR66I ICC