TANÚSÍTVÁNY KARBANTARTÁSI és FELÜLVIZSGÁLATI Jegyzőkönyv

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt tanúsító szervezet és mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

Tanúsítvány karbantartás eljárás keretében

a **HUNG-T-029-2006 TANÚSÍTVÁNY állításait**

kiterjeszti

a

polysys ®

által továbbfejlesztett alábbi verzióra:

A2-Polysys CryptoSigno Interop JAVA API 2.4.0-ás verzió /build 142/

a2-api-BIN-2_4_0.jar
SHA256:3E2A3C8EAD99B12870FA65D3CFB477224E1D86BAB4C93E59D14CE09C40D25B46

a fent nevezett tanúsítvány
1. számú mellékletében áttekintett funkcionalitással, valamint
a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vétele mellett.
Felülvizsgálati eljárás során továbbá megállapítja, hogy a tanúsított állapot az alábbi verziókra 2015. február 23-ig fenntartható:
v2.2.0 build 138, v2.2.1 build 140, v2.3.0 build 141, v2.4.0 build 142.

A Karbantartási Jegyzőkönyv regisztrációs száma: **HUNG-FJ-029/3-2012**

Kelt: Budapest, 2012. december 11.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

Az A2-Polysys CryptoSigno Interop JAVA API megfelel az alábbi normatív dokumentumokban meghatározott követelményeknek:

- 2001. évi törvény az elektronikus aláírásról
- Directive 1999/93/EC (on a Community framework for electronic signatures),
- Directive 2006/123/EC (on services in the internal market)
- 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)
- 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)
- 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)

Az A2-Polysys CryptoSigno Interop JAVA API megfelel az alábbi szabványoknak:

- ETSI TS 101 903 v1.4.2 (2010-12), v1.4.1 (2009-06), v1.1.3.2 (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

Az A2-Polysys CryptoSigno Interop JAVA API támogatja:

A Magyar Elektronikus Aláírás Szövetség (MELASZ) 2012. április 24. tájékoztatójában (MELASZ tájékoztatója a biztonsággal használható kriptográfiai algoritmusokról) foglalt álláspontot:

1. 2012. június 30. után mind a fokozott biztonságú, mind a minősített elektronikus aláírások létrehozását csak biztonságos kriptográfiai algoritmussal (SHA256, RSA2048 vagy erősebb) lehessen megvalósítani.
2. A 2012. június 30-a előtt készült, a 2012. június 30-a után már biztonságosnak nem tekintett kriptográfiai algoritmusok használatával készült fokozott biztonságú és minősített elektronikus aláírásokat 2012. december 31-e után is érvényesnek kell tekintetni, amennyiben ezen aláírások 2012. december 31-ig a 2012. június 30-a után is biztonságosnak tekintett kriptográfiai algoritmusok használatával megerősítésre kerültek (pl. felülbélyegzés által).
3. Az aláírás-ellenőrző alkalmazások legkésőbb 2012. december 31-ig legyenek felkészítve arra, hogy a 2012. június 30-át követően biztonságosnak már nem tekintett kriptográfiai algoritmusok felhasználásával készült fokozott biztonságú és minősített elektronikus aláírások ellenőrzése során jelezzék a felhasználónak, hogy az elektronikus aláírás olyan kriptográfiai algoritmus felhasználásával készült, amely már nem feltétlenül tekinthető biztonságosnak.

2. számú melléklet

A2-Polysys CryptoSigno Interop JAVA API -val tesztelt platformok

2.2.0-ás verzió /build 138/ verziótól:

Ssz	Hardver konfiguráció	szoftver konfiguráció
1	IBM eServer xSeries 346 2x3.6 GHz Intel Xeon processzorral, 8x1 GB PC3200 ECC DDR333 ECC memóriával, 2x36 GB 10K U320 SCSI SL HDD merevlemezzel, 2xQLogic FC2-133 Host Bus Adapterrel	Novell/SuSE Linux Enterprise Server 9 SP2 operációs rendszer
2	IBM eServer iSeries 550 4xPower5+ 1.75 GHz processzorral, 25 GB memóriával, 6x73 GB merevlemezzel, 3x Giga Ethernet kártyával	AS400 i5OS 5.3 JAVA Level 7 OS level 5207530 operácós rendszer
3	IBM eSeries pSeries 570 4xPower5+ 1.9 GHz processzorral, 12 GB memóriával, 6x73 GB merevlemezzel, 3x Giga Ethernet kártyával	IBM AIX 5.3.3 és RedHat Enterprise Linux Advanced Server 4 SR1 operációs rendszerek
4	Sun Fire V20z 2xAMD Opteron 244 processzorral, 2 GB DDR1/333 memóriával, 73 GB ULTRA 320 Scsi merevlemezzel	Red Hat Enterprise Linux 3 operációs rendszer
5	Sun Java Workstation W1100z Single AMD Opteron 246 proceszorral, 2 GB PC3200 DDR-400 memóriával, 73 GB ULTRA 320 Scsi merevlemezzel	Solaris 10 x86 with recommended patch cluster operációs rendszer
6	Sun Java Workstation W2100z Dual AMD Opteron 252 proceszorral, 2 GB PC3200 DDR-400 memóriával, 73 GB ULTRA 320 Scsi merevlemezzel	SuSE Linux Enterprise Server 9 AMD 64 operációs rendszer
7	Sun Ultra 20 Workstation „Large” AMD Opteron 152 proceszorral, 2 GB ECC PC3200 memóriával, 250 GB SATA merevlemezzel	Windows XP operációs rendszer
8	Sun Fire V120, one pack 650 Mhz proceszorral, 1 GB memóriával, 2x73 GB ULTRA 320 Scsi merevlemezzel	Solaris 9 SPARC 09/04 operációs rendszer
9	Sun Blade 2500 Workstation modell 1x1.05 GHz UltraSPARC IIIi proceszorral, 1 GB DDR1 memóriával, 73 GB ULTRA 320 Scsi merevlemezzel,	Solaris 10 SPARC First Customer Shipment operációs rendszer
10	Sun Fire V440 Server 4x1.062 GHz UltraSPARC IIIi proceszorral, 2 GB DDR1 memóriával, 2x73 GB ULTRA 320 Scsi merevlemezzel	Solaris 10 SPARC First Customer Shipment operációs rendszer
11	Sun Fire V240 2x1.5 GHz UltraSPARC IIIi proceszorral, 8 GB DDR1 memóriával, 2x73 GB ULTRA 320 Scsi merevlemezzel,	Solaris 10 SPARC First Customer Shipment operációs rendszer
12	Gericom Holywood XXL	Suse 9.3 operációs rendszer
13	HP szerver rx1620 model, 1 db 1300 MHz Itanium2 CPU, 2 GB RAM, 2 db 36 GB UW320 HD, 2 db Gbps LAN	Windows 2003 szerver operációs rendszer
14	Intel Pentium processzor	Novell/SuSE Linux 10 operációs rendszer
15	HP szerver 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 operációs rendszer
16	HP szerver 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 operációs rendszer
17	HP szerver rx1620 model, 1 db 1300 MHz Itanium2 CPU, 2 GB RAM, 2 db 36 GB UW320 HD, 2 db Gbps LAN	RedHat Enterprise és Linux Advanced Server 4 Update 2 JDK 1.4.2.10 operációs rendszerek
18	Apple MacBook, Intel Core 2 Duo 2GHz processzor, 1 GB RAM	Mac OS X Tiger 10.4.9 operációs rendszer, Apple Java 1.5.0_07-164
19	Apple MacBook, Intel Core 2 Duo 2GHz processzor, 756 MB RAM	Windows Vista 6.0 operációs rendszer, 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 memória; 300 GB HDD	Ubuntu Linux 8.12: Java:SUN 1.6.0_12-b04, Java HotSpot(TM) Client VM

2.2.1-ás verzió /build 140/ verziótól:

Ssz	Hardver konfiguráció	szoftver konfiguráció
27	Intel Core 2 CPU, 2 GB RAM	Mac OS X 10.6.2 (Snow Leopard) operációs rendszer, Apple Java 1.5.0_19_b02-304 32 Bit
28	Intel Core 2 CPU, 1 GB RAM	Windows 7 Enterprise 32-bit operációs rendszer, 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 operációs rendszer, Sun Java 1.6.0_18-b07 HotSpot(TM) 64-Bit Server VM

2.4.0-ás verzió /build 142/ verziótól:

Ssz	Hardver konfiguráció	szoftver konfiguráció
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)

3. számú melléklet

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

2.2.0-ás verzió /build 138/ verziótól:

Ssz	eszköz	operációs rendszer	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

2.2.1-ás verzió /build 140/ verziótól:

Ssz	eszköz	operációs rendszer	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

2.3.0-ás verzió /build 141/ verziótól:

Ssz	eszköz	operációs rendszer	chip
10	Gemalto Classic V3 (GemP15-1)	Firmware : 3.01	Hw: 59.125
11	Touch&Sign 2048	T&S DS/2048	ST19WR66I ICC