HUNG-MJ-011-2011 számú

MEGFELELÉS ÉRTÉKELÉSI JELENTÉS

az InfoSigno PKI SDK v3.0.1 (build 9)

megfelelése az

„Egységes MELASZ formátum elektronikus aláírásokra v2.0” dokumentumban megfogalmazott interoperabilitási követelményeknek

Verzió:	1.0
Fájl:	HUNG-MJ-011-2011.doc
Minősítés:	Nyilvános
Oldalak:	19

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2011.02.28.	A fejlesztőknek egyeztetésre megküldött változat.
v0.2	2011.03.02.	Pontosított változat.
v1.0	2011.03.03.	A tanúsító szervezetnek átadott végleges változat.

A megfelelés értékelési jelentést készítette:

Dr. Balázs István

Digitally signed by Dr. Balázs István
DN: CN = Dr. Balázs István, SN = Dr. Balázs, C = HU, L = Budapest, O = HUNGUARD Kft., OU = értékelési divízió, T = értékelési divízió vezető
Reason: I am the author of this document
Date: 2011.03.03 13:36:09 +01'00'

dr. Balázs István

Hunguard Kft.

értékelési divízió vezető

Dr. Szabó István

Digitally signed by Dr. Szabó István
DN: CN = Dr. Szabó István, C = HU, L = Budapest, O = HUNGUARD Kft.
Reason: I am approving this document
Date: 2011.03.03 13:44:08 +01'00'

Tartalomjegyzék

1. Bevezetés

1.1 Előzmények

Az ARGEON Informatikai Szolgáltató Kft. által kifejlesztett „InfoSigno (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz) v1.0.0” termékre vonatkozó biztonsági értékelésen alapuló tanúsítás megállapította, hogy a termék megfelel a 2001. évi XXXV törvényben szereplő minősített elektronikus aláírás létrehozására és ellenőrzésére alkalmazható szabványos és biztonságos alkalmazások fejlesztéséhez. (lásd Hung-T-031/2006 és Hung-TJ-031/2006).

Az ARGEON Informatikai Szolgáltató Kft. által kifejlesztett MMMEAA_ARG.exe alkalmazás interoperabilitás tesztelésen alapuló tanúsítványban a Magyar Elektronikus Aláírás Szövetség tanúsítja, hogy Argeon Informatikai Szolgáltató Kft. által kifejlesztett InfoSigno PKI SDK 3.0.0 elektronikus aláírási alkalmazás megfelel az elektronikus aláírásokra kidolgozott egységes MELASZ formátum (MELASZ Munkacsoport Megállapodás) 2.0 verziójának. (lásd MMMEAA 2009/001).

A fenti két tanúsítást követően a fejlesztők több változtatást végeztek a terméken. Az új verzió biztonsági hatásvizsgálatán alapulva, a tanúsítvány karbantartás eljárás keretében kiadott új tanúsítvány (HUNG-T-055-2011) megerősíti a HUNG-T-031-2006 tanúsítvány állításait a továbbfejlesztett alábbi verzióra: InfoSigno PKI SDK v3.0.1 (build 9).

1.2 Cél

Jelen értékelési jelentés célja kettős, egyrészt egy új interoperabilitás tesztelés eredményeinek bemutatásával megalapozni a MELASZ tanúsítvány állításainak kiterjesztését az MMMEAA_ARG.exe alkalmazás új verziójára, másrészt kimutatni, hogy az interoperabilitás teszteléssel vizsgált MMMEAA_ARG.exe alkalmazás és az informatika biztonsági szempontból tanúsított InfoSigno PKI SDK 3.0.1-es verzió /build 9/ termékek együttműködő képessége azonos.

1.3 Azonosító adatok

A vizsgált termékek neve Verziók	MMMEAA_ARG.exe, mely meghívja az InfoSigno.dll-t MMMEAA_ARG.exe: v3.0.1 (build 4) InfoSigno.dll: v3.0.1 (build 9)
Az értékelő szervezet adatai	Hunguard Kft. 1125 Budapest, Kékgolyó u. 6.
A megbízó adatai	Argeon Informatikai Szolgáltató Kft. 4034 Debrecen, Vágóhíd utca 2.
A termék fejlesztő adatai	ARGEON Informatikai Szolgáltató Kft.

1.4 Az értékelés mérföldkövei

Az előkészítési szakasz kezdési dátuma	2010.10.28.
Az előkészítési szakasz befejezési dátuma	2010.12.04.
Az interoperabilitási tesztelés kezdés dátuma	2010.12.05.
Az interoperabilitási tesztelés befejezés dátuma	2011.02.28.
Értékelési jelentés tervezet elkészítésének dátuma	2011.02.28.
Értékelési jelentés (végleges) elkészítésének dátuma	2011.03.03.

1.5 Az értékelők adatai

Az értékelő munkacsoport tagjai	dr. Balázs István, Farkas Gábor, Staub Klára

2. A termék leírása

2.1 Legfontosabb tulajdonságok

Az InfoSigno PKI SDK egy szoftver fejlesztőkészlet, melyre épülő alkalmazásokkal szabványos formátumú elektronikus aláírások készíthetők, illetve ellenőrizhetők biztonságos módon.

A biztonsági értékelés az InfoSigno PKI SDK alábbi biztonsági funkcióit vizsgálta:

Aláírás létrehozáskor:

- SF1: Dokumentum stabilitás ellenőrzése
- SF2: Aláírási tulajdonságok
- SF3: Aláíró tanúsítványa
- SF4: Aláíró tanúsítványa
- SF5: Az aláírási folyamat megszakíthatósága
- SF6: Kriptográfiai műveletek
- SF7: Az aláírás létrehozása
- SF8: Az aláírás exportálása
- SF9: Biztonsági szerepkörök
- SF10: Adminisztrálás

Aláírás ellenőrzéskor:

- SF11: Ellenőrzés a dokumentum importálása során
- SF12: Az aláírt dokumentum megjelenítése
- SF13: Aláírási szabályzatok
- SF14: Az elektronikus aláírás és az aláírási tulajdonságok importálása
- SF15: Egy érvényes idő hivatkozás importálása
- SF16: Egy érvényes tanúsítványlánc importálása
- SF17: Az importált adatok értelmezésének képessége
- SF18: Az ellenőrzés állapotának visszaadása
- SF19: Kriptográfiai műveletek
- SF20: Biztonsági szerepkörök

A biztonsági értékelés az InfoSigno PKI SDK alábbi interoperabilitást biztosító funkcióit vizsgálta:

- szabványos XAdES formátumok teljes skálájának - köztük az [1]-ben meghatározott egységes MELASZ formátum - támogatása,
- az X.509 v3 tanúsítványok kezelése, tanúsítási útvonal felépítése és érvényesítése az RFC 5280 [4] alapján,
- az RFC 3161 [5] szerinti időbélyeg kérés és ellenőrzés,
- a visszavonási listák (CRL) kezelése az RFC 5280 [4] szerint,
- az RFC 2560 [6] szerinti OCSP kérés és az OCSP válasz ellenőrzése.

2.2 Architektúra

Az InfoSigno PKI SDK egy programozói könyvtár (dll), amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.

A jelen megfelelés értékelési jelentés tárgyát képező MMMEAA_ARG.exe tesztprogram egy olyan alkalmazás, amely az InfoSigno dll-re épül.

2.3 Modulok

A biztonsági értékelés az InfoSigno PKI SDK alábbi moduljait (döntően osztályait) vizsgálta:
Biztonsági követelményt (SFR-t) érvényre juttató modulok:

- Container
- ContainerInfoSigno
- ContainerMELASZ
- ContainerMicrosec
- ContainerXML
- CryptoDataStore
- CryptoDataStoreFile
- CryptoDataStoreRegistry
- CryptoDataStoreXML
- DataUser
- DataUserEnveloped
- DataUserInfoSigno
- DataUserInfoSignoLinked
- DataUserMicrosecDocument
- DataUserMicrosecDocumentProfile
- DataUserMicrosecDocuments
- DataUserMicrosecDossierProfile
- DataUserMicrosecSignatureProfile
- DataUserObject
- DataUserURI
- DataUserXML
- Certificate
- Revocation
- RevocationCRL
- RevocationOCSP
- Signature
- SignatureMELASZ
- SignatureMELASZCounter
- TimeStamp
- TimeStampAllDataObject
- TimeStampArchive
- TimeStampData
- TimeStampEasy
- TimeStampIndividualDataObject
- TimeStampRefsOnly

- TimeStampSigAndRefs
- TimeStampSignatureMELASZ
- HashValue
- Biztonsági követelményt (SFR-t) támogató modulok:
- Infosigno
- ContainerFactoryBase
- ContainerFactoryDefault
- ContainerFactoryMELASZ
- ContainerFactoryMicrosec
- ContainerFactoryXML
- ConfigHandler
- XmlSchemaFactory

2.4 Az értékelés hatóköre

Jelen értékelési jelentés az [1]-ben meghatározott egységes MELASZ formátum (mely egy speciális XAdES formátumnak tekinthető) támogatásának vizsgálatára szorítkozik.

Az interoperabilitás vizsgálat elsősorban az alábbi biztonsági funkciókat érinti:

- SF7: Az aláírás létrehozása
- SF11: Ellenőrzés a dokumentum importálása során
- SF13: Aláírási szabályzatok
- SF14: Az elektronikus aláírás és az aláírási tulajdonságok importálása
- SF15: Egy érvényes idő hivatkozás importálása
- SF16: Egy érvényes tanúsítványlánc importálása
- SF17: Az importált adatok értelmezésének képessége
- SF18: Az ellenőrzés állapotának visszaadása

Az interoperabilitás vizsgálat elsősorban az alábbi modulokra fókuszál:

- ContainerMELASZ,
- SignatureMELASZ,
- SignatureMELASZCounter,
- TimeStampSignatureMELASZ,
- ContainerFactoryMELASZ.

3. Az értékelés jellemzése

Az alábbiakban az értékelés során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

3.1 Értékelési módszerek

Az InfoSigno PKI SDK biztonsági értékelése során az informatikai termékek technológia szempontú biztonsági értékelésére szolgáló nemzeti séma, a MIBÉTS módszertanát követtük. A MIBÉTS módszertan szerinti értékelés eredményét egy különálló értékelési jelentés tartalmazza.

Az InfoSigno PKI SDK interoperabilitás tesztelése során a MELASZ által kidolgozott módszertant alkalmaztuk.

A módszertant az alábbi dokumentumok határozzák meg:

- Egységes MELASZ formátum elektronikus aláírásokra v2.0 [1],
- Egységes MELASZ aláírási formátumok (v2.0) interoperabilitás tesztelésének módszere [2],
- Egységes MELASZ aláírási formátumok (v2.0) interoperabilitás tesztelésének módszere csatlakozás és garancia karbantartás esetén [3].

3.2 Vizsgált programok

Az interoperabilitás tesztelés során az alábbi termék:

termék neve és verziója	fejlesztő	tesztprogram	rövidítés
InfoSigno PKI SDK v3.0.1 (build 9)	**Argeon Kft.**	**MMMEAA_ARG.exe**	**ARG**

alábbi termékekkel való együttműködő képességét vizsgáltuk:

termék neve és verziója	MELASZ tanúsítvány azonosító	fejlesztő	tesztprogram	rövidítés
DSS.SDS.dll v2.0.0.0	MMMEAA 2010/003	DSS Consulting Kft.	MMMEAA_DSS.exe	DSS
XadesMagic v2.0.0 (build 24)	MMMEAA 2011/003	SDA Stúdió Kft.	MMMEAA_SDA.exe	SDA
SDX (Signed Document eXpert) 2.2.1	MMMEAA 2009/006	E-Group ICT Software Zrt.	MMMEAA_EGR.exe	EGR
e-Szignó 3.1	MMMEAA 2009/002	Microsec Kft.	MMMEAA_MIC.exe	MIC
Nlcapi3 v3.3.3 (build 2) /benne: az nlsxades modul v2.6.9 (build 2)/	MMMEAA 2011/001	Netlock Kft.	MMMEAA_NET.exe	NET
eSign Toolkit v2.2.2 (build 0)	MMMEAA 2011/002	Noreg Kft.	MMMEAA_NOR.exe	NOR
A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz v2.2.1 (build 140)	MMMEAA 2010/002	polysys ®	MMMEAA_POL.jar	POL

3.3 Tesztesetek

3.3.1 Pozitív tesztesetek

A programok párokat az alábbi pozitív tesztesetekkel vizsgáltuk:

Teszteset azonosító	Teszteset leíró (és kiegészítő)	megjegyzés
epes01	SignatureMethod (rsa-sha1)	aláírás létrehozás SHA-1 hash függvénnyel SignatureMethod: rsa-sha1, DigestMethod: sha1
epes02	SignatureMethod (rsa-sha256)	aláírás létrehozás SHA-256 hash függvénnyel SignatureMethod: rsa-sha256, DigestMethod: sha256
epes03	Reference, Transform (“#valami”)	aláírás létrehozás, Transform: BASE64
epes04	Reference, Transform (“” (üres))	aláírás létrehozás, Transform: enveloped
epes05	Reference, Transform (file:///valami)	aláírás létrehozás,Transform: üres vagy c14n
epes06	SignaturePolicyId	aláírás létrehozás explicit módon meghatározott szabályzat (SignaturePolicyId) mellett
epes07	ellenjegyző	ellenjegyző aláírás létrehozás
epes08	párhuzamos	párhuzamos aláírás létrehozás
epes09	AllDataObjects TimeStamp	aláírás létrehozás adott időpontú eredet bizonyítással (AllDataObjects TimeStamp)
epes10	IndividualData ObjectsTimeStamp	aláírás létrehozás adott időpontú eredet bizonyítással (IndividualData ObjectsTime Stamp)
epes2t	SignatureTimeStamp	a bemenetként megadott XAdES-EPES formátumú aláírás ellenőrzése, egyúttal XAdES-T formátumú aláírás létrehozása
t2c1	CRLRefs	a bemenetként megadott XAdES-T formátumú aláírás ellenőrzése, egyúttal XAdES-C formátumú aláírás létrehozása CRL visszavonási információ befoglalásával
t2c2	OCSPRefs	a bemenetként megadott XAdES-T formátumú aláírás ellenőrzése, egyúttal XAdES-C formátumú aláírás létrehozása OCSP visszavonási információ befoglalásával
c2a1	Archive TimeStamp CRLRefs	a bemenetként megadott (CRL visszavonási információt tartalmazó) XAdES-C formátumú aláírás ellenőrzése, egyúttal XAdES-A formátumú aláírás létrehozása
c2a2	Archive TimeStamp OCSPRefs	a bemenetként megadott (OCSP visszavonási információt tartalmazó) XAdES-C formátumú aláírás ellenőrzése, egyúttal XAdES-A formátumú aláírás létrehozása
x2a1	Archive TimeStamp RefsOnly TimeStamp	a bemenetként megadott (CRL-t felül időbélyegző) XAdES-XL formátumú aláírás ellenőrzése, egyúttal XAdES-A formátumú aláírás létrehozása
x2a2	Archive TimeStamp SigAndRefs TimeStamp	a bemenetként megadott (OCSP választ felül időbélyegző) XAdES-XL formátumú aláírás ellenőrzése, egyúttal XAdES-A formátumú aláírás létrehozása
a2a	2 darab Archive TimeStamp	a bemenetként megadott XAdES-A formátumú aláírás ellenőrzése, egyúttal egy új XAdES-A formátumú aláírás létrehozása egy másik archív időbélyegzés létrehozásával

Az epes07–epes10 teszteseteket csak annak a programnak kell létrehoznia, amely az érintett opcionális elemet támogatja. Ellenőrizni viszont minden programnak tudnia kell a mások által írt epes07 – epes10 formátumokat is.

Az x2a1 és x2a2 tesztesetek csak a Teszt_N7 és Teszt_N8 negatív teszteléshez kellenek.

ARG az epes07–epes8 tesztesetekben érintett opcionális elemeket nem támogatja.

ARG az epes09–epes10 tesztesetekben érintett opcionális elemeket támogatja.

3.3.2 Negatív tesztesetek

A programot az alábbi negatív tesztesetekkel vizsgáltuk:

Teszteset azonosító	Teszteset leíró	megjegyzés
Teszt_N1	A kivárási idő helyes kezelésének vizsgálata	A bemenetként megadott XAdES-T formátumú aláírás ellenőrzése, közvetlenül az időbélyegzés után, tehát a kivárási idő letelte előtt.
Teszt_N2	Aláírás visszavont tanúsítvánnyal	A bemenetben lévő aláírás egy visszavont tanúsítványhoz tartozó magánkulccsal készült.
Teszt_N3	Az explicit módon meghatározott szabályzat ellenőrzésének vizsgálata	Az epes06 tesztesetet egy olyan aláírással futtatják, amelyben a SignaturePolicyId által meghatározott szabályzat sérült.
Teszt_N4	Ellenjegyző aláírás ellenőrzésének vizsgálata	Az epes07 tesztesetet egy olyan aláírással futtatják, amelyben az egyik ellenjegyző aláírás sérült.
Teszt_N5	Párhuzamos aláírás ellenőrzésének vizsgálata	Az epes08 tesztesetet egy olyan aláírással futtatják, amelyben az egyik párhuzamos aláírás sérült.
Teszt_N6	Adott időpontú eredet bizonyítás (AllDataObjects TimeStamp) ellenőrzésének vizsgálata	Az epes09 tesztesetet egy olyan aláírással futtatják, amelyben az AllDataObjectsTimeStamp sérült
Teszt_N7	Adott időpontú eredet bizonyítás (IndividualObjectsTimeStamp) ellenőrzésének vizsgálata	Az epes10 tesztesetet egy olyan aláírással futtatják, amelyben az IndividualObjectsTimeStamp sérült.
Teszt_N8	A RefsOnlyTimeStamp ellenőrzésének vizsgálata	A c2a1 tesztesetet egy olyan aláírással futtatják, amelyben a RefsOnlyTimeStamp sérült.
Teszt_N9	A SigAndRefsTimeStamp ellenőrzésének vizsgálata	A c2a2 tesztesetet egy olyan aláírással futtatják, amelyben a SigAndRefsTimeStamp sérült.
Teszt_N10	Az ArchiveTimeStamp ellenőrzésének vizsgálata	Az a2a tesztesetet egy olyan aláírással futtatják, amelyben az ArchiveTimeStamp sérült.
Teszt_N11	A hivatkozás helyes kezelésének vizsgálata	Az epes2t tesztesetet egy olyan epes03 bemenetre futtatják, melyben a hivatkozás hibás (Type of Reference to SignedProperties nem az alábbi értéket veszi fel: http://uri.etsi.org/01903#SignedProperties).
Teszt_N12	Hibás névtér kezelés_1	A bemenetben a xades:QualifyingProperties / xades:UnsignedProperties / xades:UnsignedSignatureProperties / xades:RevocationValues alatti CRLValues elemnek nincs xades prefixe.
Teszt_N13	Hibás névtér kezelés_2	A bemenetben a xades:QualifyingProperties / xades:UnsignedProperties / xades:UnsignedSignatureProperties / xades:RevocationValues alatti OCSPValues elemnek nincs xades prefixe.
Teszt_N14	Hibás verzió kezelése	A bemenetben egy XAdES v.1.2.2 aláírási csomag szerepel (nem v1.3.2).

3.4 Tesztsorozatok

Az interoperabilitás tesztelés keretében az alábbi három tesztsorozatot végeztük el:

- páronkénti To_c tesztelés,
- páronkénti To_a tesztelés,
- tesztelés negatív tesztesetekkel.

3.4.1 Páronkénti To_c tesztelés

Valamennyi vizsgált tesztprogram-párra (DSS-ARG, EGR-ARG, MIC-ARG, NET-ARG, POL-ARG, SDA-ARG) külön-külön elvégeztük az alábbiakat:

1. Mindkét tesztprogrammal elkészítettük az összes XAdES-EPES aláírást (az epes01–epes06 tesztesetek meghívásával, kiegészítve a támogatott opcionális epes07-epes10 tesztesetek meghívásával).
2. Az 1. lépésben készült összes (12-20 db) aláírást mindkét tesztprogrammal folytattuk XAdES-T-ig (az epes2t teszteset meghívásával).
3. A kivárási idő letelte után a 2. lépés összes (24-40 db) kimenetét futtattuk mindkét tesztprogrammal XAdES-C-ig (a t2c1 és t2c2 tesztesetek meghívásával).

Mindhárom lépés összes tesztesetében az elvárt eredmény: 1 (sikeres létrehozás, illetve sikeres ellenőrzés).

3.4.2 Páronkénti To_a tesztelés

Valamennyi vizsgált tesztprogram-párra (DSS-ARG, EGR-ARG, MIC-ARG, NET-ARG, POL-ARG, SDA-ARG) külön-külön elvégeztük az alábbiakat:

1. Mindkét tesztprogrammal elkészítettünk egy kiinduló XAdES-EPES aláírást (az epes01 teszteset meghívásával).
2. Az 1. lépésben készült 2 aláírást mindkét tesztprogrammal folytattuk XAdES-T-ig (az epes2t teszteset meghívásával).
3. A kivárási idő letelte után a 2. lépés 4 kimenetét futtattuk mindkét tesztprogrammal XAdES-C-ig (a t2c1 és t2c2 tesztesetek meghívásával).
4. A 3. lépés 16 kimenetét futtattuk mindkét tesztprogrammal XAdES-A-ig (a t2c1 ágon készültekre a c2a1, a t2c2 ágon készültekre pedig a c2a2 tesztesetek meghívásával).
5. A 4. lépés 32 kimenetét futtattuk mindkét tesztprogrammal XAdES-A-ig (az a2a teszteset meghívásával).

Mind az öt lépés összes (2+4+16+32+64) tesztesetében az elvárt eredmény: 1 (sikeres létrehozás, illetve sikeres ellenőrzés).

3.4.3 Tesztelés negatív tesztesetekkel

A vizsgált programot (ARG) teszteltük a Teszt_N1 - Teszt_N14 negatív tesztesetekkel.

Valamennyi negatív tesztesetben az elvárt eredmény: 2 (sikertelen ellenőrzés).

4. Az értékelés eredményei

Az eredmények és a tesztelés megismételhetőségéhez szükséges környezeti elemek az alábbi könyvtárban találhatók: ARGEON\InfoSigno\2010\MR2\Results_110227

A Results_110227 alkönyvtár szerkezete az alábbi:

- DSS_ARG (a DSS – ARG programpár tesztelési eredményei)
- EGR_ARG (az EGR – ARG programpár tesztelési eredményei)
- MIC_ARG (a MIC – ARG programpár tesztelési eredményei)
- NET_ARG (a NET – ARG programpár tesztelési eredményei)
- NOR_ARG (a NOR – ARG programpár tesztelési eredményei)
- POL_ARG (a POL – ARG programpár tesztelési eredményei)
- SDA_ARG (az SDA – ARG programpár tesztelési eredményei)
- ARG_ARG (a negatív tesztesetek eredményei)

Az egyes programpárok alkönyvtárai hasonló szerkezetűek, pl. a NOR_ARG-é az alábbi:

- NOR (a NOR tesztprogram és futtatási környezete)
- ARG (az új ARG tesztprogram és futtatási környezete)
- log (napló állományok közös könyvtára)
- out (a tesztelés során előállított állományok könyvtára)
- bemenet.txt, bemenet.xml (a minden tesztesetben közös aláírandó állomány két formátumban)
- result.txt (az egyes tesztesetek eredményeit ábrázoló sorok összessége)

A konkrét futási eredményeket tartalmazó result.txt állomány sorainak jelentését az alábbi példa szemlélteti:

2011-02-27_18:00:55 ARG_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_NOR_a2a_ 1, ahol

- 2011-02-27_18:00:55 a teszt lefutásának dátuma és időpontja
- ARG_epes01_: 1. lépés: ARG meghívásával epes01 aláírás létrehozása
- NOR_epes2t_: 2. lépés: NOR meghívásával az 1. lépés eredményének ellenőrzése, majd ebből epes2t létrehozása
- ARG_t2c2_: 3. lépés: ARG meghívásával a 2. lépés eredményének ellenőrzése, majd ebből t2c2 létrehozása
- NOR_c2a2_: 4. lépés: NOR meghívásával a 3. lépés eredményének ellenőrzése, majd ebből c2a2 létrehozása
- NOR_a2a_: 5. lépés: NOR meghívásával a 4. lépés eredményének ellenőrzése, majd ebből a2a létrehozása
- 1: a futás visszaadott eredménye (sikeres ellenőrzés, mely értelemszerűen mind az 5 lépésre vonatkozik)

4.4.1 A páronkénti To_c tesztelés eredményei

Mind a 7 másik tesztprogrammal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt. Példaképp a NOR-ARG eredménye az alábbi:

2011-02-26_20:05:25 NOR_epes01_ 1
2011-02-26_20:06:02 NOR_epes02_ 1
2011-02-26_20:06:47 NOR_epes03_ 1
2011-02-26_20:07:26 NOR_epes04_ 1
2011-02-26_20:08:04 NOR_epes05_ 1
2011-02-26_20:08:37 NOR_epes06_ 1
2011-02-26_20:09:13 NOR_epes09_ 1
2011-02-26_20:09:52 NOR_epes10_ 1

2011-02-26_20:09:58 ARG_epes01_ 1
2011-02-26_20:10:05 ARG_epes02_ 1
2011-02-26_20:10:11 ARG_epes03_ 1
2011-02-26_20:10:17 ARG_epes04_ 1
2011-02-26_20:10:25 ARG_epes05_ 1
2011-02-26_20:10:34 ARG_epes06_ 1
2011-02-26_20:10:42 ARG_epes09_ 1
2011-02-26_20:10:50 ARG_epes10_ 1
2011-02-26_21:30:07 NOR_epes01_NOR_epes2t_ 1
2011-02-26_21:30:46 NOR_epes02_NOR_epes2t_ 1
2011-02-26_21:31:23 NOR_epes03_NOR_epes2t_ 1
2011-02-26_21:32:00 NOR_epes04_NOR_epes2t_ 1
2011-02-26_21:32:37 NOR_epes05_NOR_epes2t_ 1
2011-02-26_21:33:14 NOR_epes06_NOR_epes2t_ 1
2011-02-26_21:33:57 NOR_epes09_NOR_epes2t_ 1
2011-02-26_21:34:36 NOR_epes10_NOR_epes2t_ 1
2011-02-26_21:35:13 ARG_epes01_NOR_epes2t_ 1
2011-02-26_21:35:50 ARG_epes02_NOR_epes2t_ 1
2011-02-26_21:36:26 ARG_epes03_NOR_epes2t_ 1
2011-02-26_21:37:03 ARG_epes04_NOR_epes2t_ 1
2011-02-26_21:37:40 ARG_epes05_NOR_epes2t_ 1
2011-02-26_21:38:18 ARG_epes06_NOR_epes2t_ 1
2011-02-26_21:38:56 ARG_epes09_NOR_epes2t_ 1
2011-02-26_21:39:35 ARG_epes10_NOR_epes2t_ 1
2011-02-26_21:39:48 NOR_epes01_ARG_epes2t_ 1
2011-02-26_21:40:07 NOR_epes02_ARG_epes2t_ 1
2011-02-26_21:40:24 NOR_epes03_ARG_epes2t_ 1
2011-02-26_21:40:41 NOR_epes04_ARG_epes2t_ 1
2011-02-26_21:41:00 NOR_epes05_ARG_epes2t_ 1
2011-02-26_21:41:19 NOR_epes06_ARG_epes2t_ 1
2011-02-26_21:41:37 NOR_epes09_ARG_epes2t_ 1
2011-02-26_21:41:54 NOR_epes10_ARG_epes2t_ 1
2011-02-26_21:42:10 ARG_epes01_ARG_epes2t_ 1
2011-02-26_21:42:26 ARG_epes02_ARG_epes2t_ 1
2011-02-26_21:42:41 ARG_epes03_ARG_epes2t_ 1
2011-02-26_21:42:56 ARG_epes04_ARG_epes2t_ 1
2011-02-26_21:43:12 ARG_epes05_ARG_epes2t_ 1
2011-02-26_21:43:28 ARG_epes06_ARG_epes2t_ 1
2011-02-26_21:43:44 ARG_epes09_ARG_epes2t_ 1
2011-02-26_21:44:00 ARG_epes10_ARG_epes2t_ 1
2011-02-27_08:17:00 NOR_epes01_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:17:39 NOR_epes02_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:18:18 NOR_epes03_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:18:59 NOR_epes04_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:19:35 NOR_epes05_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:20:12 NOR_epes06_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:20:51 NOR_epes09_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:21:30 NOR_epes10_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:22:07 ARG_epes01_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:22:44 ARG_epes02_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:23:21 ARG_epes03_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:23:58 ARG_epes04_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:24:35 ARG_epes05_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:25:12 ARG_epes06_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:25:51 ARG_epes09_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:26:28 ARG_epes10_NOR_epes2t_NOR_t2c1_ 1
2011-02-27_08:27:06 NOR_epes01_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:27:46 NOR_epes02_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:28:25 NOR_epes03_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:29:04 NOR_epes04_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:29:43 NOR_epes05_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:30:23 NOR_epes06_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:31:02 NOR_epes09_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:31:40 NOR_epes10_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:32:18 ARG_epes01_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:32:56 ARG_epes02_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:33:33 ARG_epes03_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:34:11 ARG_epes04_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:34:48 ARG_epes05_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:35:26 ARG_epes06_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:36:04 ARG_epes09_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:36:44 ARG_epes10_ARG_epes2t_NOR_t2c1_ 1
2011-02-27_08:36:56 NOR_epes01_NOR_epes2t_ARG_t2c1_ 1

2011-02-27_08:37:04 NOR_epes02_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:37:12 NOR_epes03_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:37:19 NOR_epes04_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:37:27 NOR_epes05_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:37:39 NOR_epes06_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:37:51 NOR_epes09_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:00 NOR_epes10_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:08 ARG_epes01_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:17 ARG_epes02_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:24 ARG_epes03_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:30 ARG_epes04_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:38 ARG_epes05_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:48 ARG_epes06_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:38:56 ARG_epes09_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:04 ARG_epes10_NOR_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:14 NOR_epes01_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:21 NOR_epes02_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:29 NOR_epes03_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:37 NOR_epes04_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:44 NOR_epes05_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:39:54 NOR_epes06_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:02 NOR_epes09_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:11 NOR_epes10_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:19 ARG_epes01_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:27 ARG_epes02_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:36 ARG_epes03_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:43 ARG_epes04_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:40:50 ARG_epes05_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:41:01 ARG_epes06_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:41:09 ARG_epes09_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:41:18 ARG_epes10_ARG_epes2t_ARG_t2c1_ 1
2011-02-27_08:42:04 NOR_epes01_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:42:53 NOR_epes02_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:43:40 NOR_epes03_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:44:24 NOR_epes04_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:45:10 NOR_epes05_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:45:57 NOR_epes06_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:46:43 NOR_epes09_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:47:29 NOR_epes10_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:48:12 ARG_epes01_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:48:55 ARG_epes02_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:49:54 ARG_epes03_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:51:04 ARG_epes04_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:52:16 ARG_epes05_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:53:21 ARG_epes06_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:54:12 ARG_epes09_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:55:00 ARG_epes10_NOR_epes2t_NOR_t2c2_ 1
2011-02-27_08:55:46 NOR_epes01_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_08:56:32 NOR_epes02_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_08:57:17 NOR_epes03_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_08:58:00 NOR_epes04_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_08:58:47 NOR_epes05_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_08:59:58 NOR_epes06_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:01:10 NOR_epes09_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:02:05 NOR_epes10_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:02:51 ARG_epes01_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:03:38 ARG_epes02_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:04:24 ARG_epes03_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:05:11 ARG_epes04_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:06:26 ARG_epes05_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:07:28 ARG_epes06_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:08:14 ARG_epes09_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_09:08:59 ARG_epes10_ARG_epes2t_NOR_t2c2_ 1
2011-02-27_11:46:36 NOR_epes01_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:47:03 NOR_epes02_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:47:19 NOR_epes03_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:47:40 NOR_epes04_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:48:01 NOR_epes05_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:48:26 NOR_epes06_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:48:44 NOR_epes09_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:48:59 NOR_epes10_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:49:14 ARG_epes01_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:49:29 ARG_epes02_NOR_epes2t_ARG_t2c2_ 1

2011-02-27_11:50:03 ARG_epes03_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:50:19 ARG_epes04_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:50:33 ARG_epes05_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:50:54 ARG_epes06_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:51:12 ARG_epes09_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:51:25 ARG_epes10_NOR_epes2t_ARG_t2c2_ 1
2011-02-27_11:51:43 NOR_epes01_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:51:56 NOR_epes02_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:52:13 NOR_epes03_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:52:25 NOR_epes04_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:52:40 NOR_epes05_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:52:59 NOR_epes06_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:53:18 NOR_epes09_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:53:31 NOR_epes10_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:53:53 ARG_epes01_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:54:25 ARG_epes02_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:54:53 ARG_epes03_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:55:19 ARG_epes04_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:55:56 ARG_epes05_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:56:43 ARG_epes06_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:57:17 ARG_epes09_ARG_epes2t_ARG_t2c2_ 1
2011-02-27_11:57:58 ARG_epes10_ARG_epes2t_ARG_t2c2_ 1

4.4.2 A páronkénti To_a tesztelés eredményei

Mind a 7 másik tesztprogrammal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt. Példaképp az ARG-NET eredménye az alábbi:

2011-02-27_13:19:01 NOR_epes01_NOR_epes2t_NOR_t2c1_NOR_c2a1_ 1
2011-02-27_13:19:50 ARG_epes01_NOR_epes2t_NOR_t2c1_NOR_c2a1_ 1
2011-02-27_13:20:35 NOR_epes01_ARG_epes2t_NOR_t2c1_NOR_c2a1_ 1
2011-02-27_13:21:22 ARG_epes01_ARG_epes2t_NOR_t2c1_NOR_c2a1_ 1
2011-02-27_13:22:07 NOR_epes01_NOR_epes2t_ARG_t2c1_NOR_c2a1_ 1
2011-02-27_13:22:55 ARG_epes01_NOR_epes2t_ARG_t2c1_NOR_c2a1_ 1
2011-02-27_13:23:43 NOR_epes01_ARG_epes2t_ARG_t2c1_NOR_c2a1_ 1
2011-02-27_13:24:26 ARG_epes01_ARG_epes2t_ARG_t2c1_NOR_c2a1_ 1
2011-02-27_13:24:49 NOR_epes01_NOR_epes2t_NOR_t2c1_ARG_c2a1_ 1
2011-02-27_13:24:59 ARG_epes01_NOR_epes2t_NOR_t2c1_ARG_c2a1_ 1
2011-02-27_13:25:11 NOR_epes01_ARG_epes2t_NOR_t2c1_ARG_c2a1_ 1
2011-02-27_13:25:27 ARG_epes01_ARG_epes2t_NOR_t2c1_ARG_c2a1_ 1
2011-02-27_13:25:37 NOR_epes01_NOR_epes2t_ARG_t2c1_ARG_c2a1_ 1
2011-02-27_13:25:53 ARG_epes01_NOR_epes2t_ARG_t2c1_ARG_c2a1_ 1
2011-02-27_13:26:10 NOR_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ 1
2011-02-27_13:26:25 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ 1
2011-02-27_13:27:13 NOR_epes01_NOR_epes2t_NOR_t2c2_NOR_c2a2_ 1
2011-02-27_13:28:00 ARG_epes01_NOR_epes2t_NOR_t2c2_NOR_c2a2_ 1
2011-02-27_13:28:50 NOR_epes01_ARG_epes2t_NOR_t2c2_NOR_c2a2_ 1
2011-02-27_13:29:37 ARG_epes01_ARG_epes2t_NOR_t2c2_NOR_c2a2_ 1
2011-02-27_13:30:26 NOR_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_ 1
2011-02-27_13:31:14 ARG_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_ 1
2011-02-27_13:31:59 NOR_epes01_ARG_epes2t_ARG_t2c2_NOR_c2a2_ 1
2011-02-27_13:32:48 ARG_epes01_ARG_epes2t_ARG_t2c2_NOR_c2a2_ 1
2011-02-27_13:33:08 NOR_epes01_NOR_epes2t_NOR_t2c2_ARG_c2a2_ 1
2011-02-27_13:33:26 ARG_epes01_NOR_epes2t_NOR_t2c2_ARG_c2a2_ 1
2011-02-27_13:33:41 NOR_epes01_ARG_epes2t_NOR_t2c2_ARG_c2a2_ 1
2011-02-27_13:33:59 ARG_epes01_ARG_epes2t_NOR_t2c2_ARG_c2a2_ 1
2011-02-27_13:34:15 NOR_epes01_NOR_epes2t_ARG_t2c2_ARG_c2a2_ 1
2011-02-27_13:34:34 ARG_epes01_NOR_epes2t_ARG_t2c2_ARG_c2a2_ 1
2011-02-27_13:34:50 NOR_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ 1
2011-02-27_13:35:07 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ 1
2011-02-27_17:50:15 NOR_epes01_NOR_epes2t_NOR_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_17:51:16 NOR_epes01_NOR_epes2t_NOR_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_17:52:15 ARG_epes01_NOR_epes2t_NOR_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_17:53:15 ARG_epes01_NOR_epes2t_NOR_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_17:54:11 NOR_epes01_ARG_epes2t_NOR_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_17:55:07 NOR_epes01_ARG_epes2t_NOR_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_17:56:08 ARG_epes01_ARG_epes2t_NOR_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_17:57:07 ARG_epes01_ARG_epes2t_NOR_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_17:58:02 NOR_epes01_NOR_epes2t_ARG_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_17:58:59 NOR_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_17:59:57 ARG_epes01_NOR_epes2t_ARG_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_18:00:55 ARG_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_18:01:51 NOR_epes01_ARG_epes2t_ARG_t2c1_NOR_c2a1_NOR_a2a_ 1

2011-02-27_18:02:48 NOR_epes01_ARG_epes2t_ARG_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_18:03:43 ARG_epes01_ARG_epes2t_ARG_t2c1_NOR_c2a1_NOR_a2a_ 1
2011-02-27_18:04:39 ARG_epes01_ARG_epes2t_ARG_t2c2_NOR_c2a2_NOR_a2a_ 1
2011-02-27_18:05:38 NOR_epes01_NOR_epes2t_NOR_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:06:44 NOR_epes01_NOR_epes2t_NOR_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:07:49 ARG_epes01_NOR_epes2t_NOR_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:09:00 ARG_epes01_NOR_epes2t_NOR_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:10:01 NOR_epes01_ARG_epes2t_NOR_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:11:06 NOR_epes01_ARG_epes2t_NOR_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:12:12 ARG_epes01_ARG_epes2t_NOR_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:13:13 ARG_epes01_ARG_epes2t_NOR_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:14:13 NOR_epes01_NOR_epes2t_ARG_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:15:14 NOR_epes01_NOR_epes2t_ARG_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:16:18 ARG_epes01_NOR_epes2t_ARG_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:17:21 ARG_epes01_NOR_epes2t_ARG_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:18:21 NOR_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:19:26 NOR_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:20:25 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_NOR_a2a_ 1
2011-02-27_18:21:34 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_NOR_a2a_ 1
2011-02-27_18:21:54 NOR_epes01_NOR_epes2t_NOR_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:22:14 NOR_epes01_NOR_epes2t_NOR_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:22:30 ARG_epes01_NOR_epes2t_NOR_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:22:46 ARG_epes01_NOR_epes2t_NOR_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:23:05 NOR_epes01_ARG_epes2t_NOR_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:23:25 NOR_epes01_ARG_epes2t_NOR_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:23:44 ARG_epes01_ARG_epes2t_NOR_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:24:02 ARG_epes01_ARG_epes2t_NOR_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:24:16 NOR_epes01_NOR_epes2t_ARG_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:24:31 NOR_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:24:41 ARG_epes01_NOR_epes2t_ARG_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:24:54 ARG_epes01_NOR_epes2t_ARG_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:25:04 NOR_epes01_ARG_epes2t_ARG_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:25:19 NOR_epes01_ARG_epes2t_ARG_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:25:30 ARG_epes01_ARG_epes2t_ARG_t2c1_NOR_c2a1_ARG_a2a_ 1
2011-02-27_18:25:44 ARG_epes01_ARG_epes2t_ARG_t2c2_NOR_c2a2_ARG_a2a_ 1
2011-02-27_18:26:01 NOR_epes01_NOR_epes2t_NOR_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:26:22 NOR_epes01_NOR_epes2t_NOR_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:26:41 ARG_epes01_NOR_epes2t_NOR_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:26:57 ARG_epes01_NOR_epes2t_NOR_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:27:11 NOR_epes01_ARG_epes2t_NOR_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:27:34 NOR_epes01_ARG_epes2t_NOR_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:27:50 ARG_epes01_ARG_epes2t_NOR_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:28:14 ARG_epes01_ARG_epes2t_NOR_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:28:26 NOR_epes01_NOR_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:28:47 NOR_epes01_NOR_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:28:59 ARG_epes01_NOR_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:29:15 ARG_epes01_NOR_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:29:30 NOR_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:29:41 NOR_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2011-02-27_18:29:57 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2011-02-27_18:30:11 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1

4.4.3 A negatív tesztelés eredményei

Valamennyi negatív teszteset az elvárt eredményt (2: sikertelen ellenőrzés) adta:

2011-02-26_19:52:45 ARG_epes01_ 1 (ez a sikeres előkészület: EPES01 létrehozása)
2011-02-26_19:52:54 ARG_epes01_ARG_epes2t_ 1 (ez a sikeres előkészület: -T létrehozása)

2011-02-26_19:53:02 NEG_N1_ARG_t2c1_ 2
2011-02-26_19:53:13 NEG_N2_ARG_t2c2_ 2
2011-02-26_19:53:19 NEG_N3_ARG_c2a1_ 2
2011-02-26_19:53:30 NEG_N4_ARG_c2a1_ 2
2011-02-26_19:53:40 NEG_N5_ARG_c2a1_ 2
2011-02-26_19:53:47 NEG_N6_ARG_c2a1_ 2
2011-02-26_19:53:53 NEG_N7_ARG_c2a1_ 2
2011-02-26_19:54:01 NEG_N8_ARG_x2a1_ 2
2011-02-26_19:54:08 NEG_N9_ARG_x2a2_ 2
2011-02-26_19:54:16 NEG_N10_ARG_a2a_ 2
2011-02-26_19:54:20 NEG_N11_ARG_epes2t_ 2
2011-02-26_19:54:24 NEG_N12_ARG_c2a1_ 2
2011-02-26_19:54:29 NEG_N13_ARG_c2a2_ 2
2011-02-26_19:54:33 NEG_N14_ARG_epes2t_ 2

4.4.4 A tesztprogram és a termék összehasonlításának eredménye

A vizsgált tesztprogram: MMMEAA_ARG.exe /benne InfoSigno PKI SDK v3.0.1 (build 9) /

A forgalmazott termék: InfoSigno PKI SDK v3.0.1 (build 9)

A két program együttműködési képessége megegyezik, hiszen az MMMEAA_ARG.exe (mint teszt alkalmazás) a biztonsági szempontból értékelt és tanúsított InfoSigno PKI SDK v3.0.1 (build 9) függvénykészletre épülő speciális alkalmazás.

5. Következtetések és javaslatok

5.1 Az értékelés összefoglaló eredménye

Az értékelés fő következtetései az alábbiak:

1. Az ARGEON Informatikai Szolgáltató Kft. által kifejlesztett MMMEAA_ARG.exe elektronikus aláírás termék megfelel az [1]-ben az egységes MELASZ formátumokra meghatározott interoperabilitási követelményeknek.
2. Az ARGEON Informatikai Szolgáltató Kft. által kifejlesztett InfoSigno PKI SDK v3.0.1 (build 9) programozói függvény könyvtár, valamint az interoperabilitás tesztelésen bevizsgált MMMEAA_ARG.exe alkalmazás együttműködési képessége megegyezik.

5.2 Javaslat

A Hunguard kft. (mint értékelő szervezet) vizsgálati eredményei alapján javasolja a Magyar Elektronikus Aláírás Szövetségnek (mint tanúsító szervezetnek) egy új tanúsítványt (MMMEAA 2011/004 számmal) kibocsátani az alábbi verzióra:

- InfoSigno PKI SDK v3.0.1 (build 9)

6. Hivatkozások és rövidítések

6.1 Hivatkozások

[1] Egységes MELASZ formátum elektronikus aláírásokra v2.0 (MMM-001: 2008, v2.0)

[2] Egységes MELASZ aláírási formátumok (v2.0) interoperabilitás tesztelésének módszere (MMM-001_IopTest: 2009, v1.1)

[3] Egységes MELASZ aláírási formátumok (v2.0) interoperabilitás tesztelésének módszere csatlakozás és garancia karbantartás esetén (MMM-001_IopTest_AC: 2010, v0.9)

[4] RFC 5280 Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008

[5] RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001

[6] RFC 2560 X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999

6.2 Rövidítések

CRL	Certificate Revocation List (tanúsítvány visszavonási lista)
MELASZ	Magyar Elektronikus Aláírás Szövetség
MIBÉTS	Magyar Informatikai Biztonsági és Értékelési Séma
MMM	MELASZ Munkacsoport Megállapodás
OCSP	Online Certificate Status Protocol (valós idejű tanúsítvány állapot protokoll)
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RFC	Request for Comment
XAdES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language