

HUNG-MJ-010-2011 számú

**MEGFELELÉS
ÉRTÉKELÉSI JELENTÉS**

a

**XadesMagic
v2.0.0 (build 24)
megfelelése az**

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

Verzió: 1.0
Fájl: HUNG-MJ-010-2011.doc
Minősítés: Nyilvános
Oldalak: 17

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2011.02.20.	A fejlesztőknek egyeztetésre megküldött változat.
v1.0	2011.02.22	A tanúsító szervezetnek átadott végleges változat.

A megfelelés értékelési jelentést készítette:

dr. Balázs István
Hunguard Kft.
értékelési divízió vezető

Tartalomjegyzék

Változáskezelés	2
1. Bevezetés	4
1.1 Előzmények	4
1.2 Cél.....	4
1.3 Azonosító adatok.....	4
1.4 Az értékelés mérföldkövei.....	4
1.5 Az értékelők adatai.....	4
2. A termék leírása	5
2.1 Legfontosabb tulajdonságok	5
2.2 Architektúra	5
3. Az értékelés jellemzése.....	7
3.1 Értékelési módszerek.....	7
3.2 Vizsgált programok.....	7
3.3 Tesztesetek.....	8
3.3.1 Pozitív tesztesetek	8
3.3.2 Negatív tesztesetek.....	9
3.4 Tesztsorozatok.....	10
3.4.1 Páronkénti To_c tesztelés.....	10
3.4.2 Páronkénti To_a tesztelés.....	10
3.4.3 Tesztelés negatív tesztesetekkel.....	10
4. Az értékelés eredményei	11
4.4.1 A páronkénti To_c tesztelés eredményei	11
4.4.2 A páronkénti To_a tesztelés eredményei	14
4.4.3 A negatív tesztelés eredményei	15
5. Következtetések és javaslatok	16
5.1 Az értékelés összefoglaló eredménye	16
5.2 Javaslat	16
6. Hivatkozások és rövidítések	17
6.1 Hivatkozások.....	17
6.2 Rövidítések.....	17

1. Bevezetés

1.1 Előzmények

Az SDA Stúdió Kft. által kifejlesztett „XadesMagic 2.0.0 elektronikus aláírási termék (aláíró alkalmazás-fejlesztő készlet, aláíró motor)” termékre vonatkozó biztonsági értékelésen alapuló tanúsítás megállapította, hogy a termék megfelel a 2001. évi XXXV. törvényben szereplő fokozott biztonságú és minősített elektronikus aláírás létrehozására és ellenőrzésére alkalmazható szabványos és biztonságos alkalmazások fejlesztéséhez (lásd Hung-T-052/2010 és Hung-TJ-052/2010).

1.2 Cél

Jelen értékelési jelentés célja egy interoperabilitás tesztelés eredményeinek bemutatásával megalapozni egy másik tanúsítványt, nevezetesen a MELASZ együttműködő képességet igazoló tanúsítványát.

1.3 Azonosító adatok

A vizsgált termék neve	XadesMagic (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz)
Verziója	2.0.0 (build 24)
A termék rövid neve	XadesMagic
Az értékelő szervezet adatai	Hunguard Kft. 1125 Budapest, Kékgolyó u. 6.
A megbízó adatai	SDA Stúdió Kft., 1111 Budapest, Budafoki út 59
A termék fejlesztő adatai	SDA Stúdió Kft., 1111 Budapest, Budafoki út 59

1.4 Az értékelés mérföldkövei

Az előkészítési szakasz kezdési dátuma	2010.10.11.
Az előkészítési szakasz befejezési dátuma	2010.10.29.
Az interoperabilitási tesztelés kezdés dátuma	2010.10.30.
Az interoperabilitási tesztelés befejezés dátuma	2011.02.19.
Értékelési jelentés tervezet elkészítésének dátuma	2011.02.20.
Értékelési jelentés (végleges) elkészítésének dátuma	2011.02.22.

1.5 Az értékelők adatai

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

2. A termék leírása

2.1 Legfontosabb tulajdonságok

A XadesMagic egy szoftver fejlesztőkészlet (programozói könyvtár), amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.

A fokozott biztonságú és a minősített elektronikus aláírásokat egyaránt támogatja.

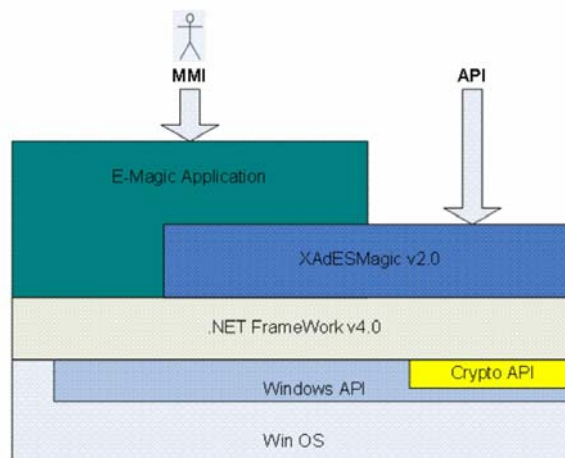
A XadesMagic számos más aláíró alkalmazásnak is alapja lehet.

A XadesMagic az alábbi szabványoknak, illetve ajánlásoknak megfelelő működést biztosít:

- [RFC 2560] (OCSP kérés előállítás, valamint OCSP és OCSP válasz ellenőrzés)
- [RFC 3161] (Időbélyeg kérés, valamint az időbélyeg és időbélyeg válasz ellenőrzés)
- [RFC 5280] (Tanúsítványok és CRL-ek ellenőrzése, tanúsítási útvonal felépítése és érvényesítése. A tanúsítványlánc felépítésénél az alábbi kiterjesztéseket támogatja:
 - ExtendedKeyUsage
 - KeyUsage
 - BasicConstraints
 - CRLDistributionPoints
 - SubjectAlternativeName
 - IssuerAlternativeName

2.2 Architektúra

A XadesMagic környezetét szemlélteti az 1. ábra.



1. ábra A XadesMagic és környezete

A XadesMagic önállóan is meghívható fejlesztő készlet (az ábrán jelzett API-n keresztül), de beépülhet egy aláíró alkalmazásba is (az ábrán az E-Magic alkalmazás).

A XadesMagic az alábbi informatikai elemekből álló környezetben működőképes:

- Windows operációs rendszerek (XP, Windows7, Vista),
- Windows API (benne CryptoAPI),
- fejlesztő környezet (.NET Framework 4.0)
- minősített elektronikus aláírás létrehozásához: biztonságos aláírás-létrehozó eszköz, a hozzátartozó middleware-rel
- fokozott biztonságú elektronikus aláírás létrehozásához: aláírás-létrehozó eszköz a hozzátartozó middleware-rel, vagy Microsoft CryptoAPI (külön hardver eszköz nélkül).

A XadesMagic (v2.0.0.24) az alábbi dll-ekből áll:

- SDA.XadesMagic.dll (v2.0.0.24)
- SDA.Cryptography.dll (v2.0.0.8)
- SDA.Cryptography.Framework.dll (v2.0.0.2)
- SDA.TimestampProtocol.dll (v2.0.0.2)

A jelen értékelési jelentés tárgyát képező MMMEAA_SDA.exe tesztprogram egy a XadesMagic fejlesztő készletre épülő speciális alkalmazás.

3. Az értékelés jellemzése

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

3.1 Értékelési módszerek

A XadesMagic 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.

A XadesMagic 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
XadesMagic v2.0.0 (build 24)	SDA Stúdió Kft.	MMMEAA_SDA.exe	SDA

alábbi termékekkel való együttműködő képességét vizsgáltuk:

termék neve és verziója	MELASZ tanúsítvány azonosító	fejlesztő	tesztprogram	rövidítés
InfoSigno PKI SDK 3.0.0	MMMEAA 2009/001	Argeon Informatikai Szolgáltató Kft.	MMMEAA_ARG.exe	ARG
DSS.SDS.dll v2.0.0.0	MMMEAA 2010/003	DSS Consulting Kft.	MMMEAA_DSS.exe	DSS
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
Nlcap3 v3.3.3 (build 2) /benne: az nlxades 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 archiv 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.

SDA az epes07–epes10 tesztesetekben érintett opcionális elemeket nem 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 (ARG-SDA, DSS-SDA, EGR-SDA, MIC-SDA, NET-SDA, NOR-SDA, POL-SDA) 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 (ARG-SDA, DSS-SDA, EGR-SDA, MIC-SDA, NET-SDA, NOR-SDA, POL-SDA) 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 (SDA) 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 találhatóak: sca_sda\2010\MELASZ_Ready\Results_110220

A Results_110220 alkönyvtár szerkezete az alábbi:

- ARG_SDA (az ARG – SDA programpár tesztelési eredményei)
- DSS_SDA (a DSS – SDA programpár tesztelési eredményei)
- EGR_SDA (az EGR – SDA programpár tesztelési eredményei)
- MIC_SDA (a MIC – SDA programpár tesztelési eredményei)
- NET_SDA (a NET – SDA programpár tesztelési eredményei)
- NOR_SDA (a NOR – SDA programpár tesztelési eredményei)
- POL_SDA (a POL – NOR programpár tesztelési eredményei)
- SDA_SDA (a negatív tesztesetek eredményei)

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

- ARG (az ARG tesztprogram és futtatási környezete)
- SDA (az SDA 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:

2011-02-16_08:30:47 ARG_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_ARG_a2a_1, ahol:

- 2011-02-16_08:30:47 a teszt lefutásának dátuma és időpontja
- ARG_epes01_: 1. lépés: ARG meghívásával epes01 aláírás létrehozása
- SDA_epes2t_: 2. lépés: SDA meghívásával az 1. lépés eredményének ellenőrzése, majd ebből epes2t létrehozása
- SDA_t2c1_: 3. lépés: SDA meghívásával a 2. lépés eredményének ellenőrzése, majd ebből t2c1 létrehozása
- ARG_c2a1_: 4. lépés: ARG meghívásával a 3. lépés eredményének ellenőrzése, majd ebből c2a1 létrehozása
- ARG_a2a_: 5. lépés: ARG 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 programmal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt. Példaképp az ARG-SDA eredménye az alábbi:

```
2010-12-19_17:07:42 ARG_epes01_1
2010-12-19_17:07:43 ARG_epes02_1
2010-12-19_17:07:45 ARG_epes03_1
2010-12-19_17:07:46 ARG_epes04_1
2010-12-19_17:07:48 ARG_epes05_1
2010-12-19_17:07:50 ARG_epes06_1
2010-12-19_17:07:53 ARG_epes09_1
2010-12-19_17:07:56 ARG_epes10_1
```

2011-02-09_21:23:47 SDA_epes01_1
2011-02-09_21:24:12 SDA_epes02_1
2011-02-09_21:25:04 SDA_epes03_1
2011-02-09_21:25:25 SDA_epes04_1
2011-02-09_21:25:37 SDA_epes05_1
2011-02-09_21:25:49 SDA_epes06_1
2011-02-15_21:33:31 ARG_epes01_ARG_epes2t_1
2011-02-15_21:33:48 ARG_epes02_ARG_epes2t_1
2011-02-15_21:34:03 ARG_epes03_ARG_epes2t_1
2011-02-15_21:34:19 ARG_epes04_ARG_epes2t_1
2011-02-15_21:34:36 ARG_epes05_ARG_epes2t_1
2011-02-15_21:34:54 ARG_epes06_ARG_epes2t_1
2011-02-15_21:35:11 ARG_epes09_ARG_epes2t_1
2011-02-15_21:35:29 ARG_epes10_ARG_epes2t_1
2011-02-15_21:35:43 SDA_epes01_ARG_epes2t_1
2011-02-15_21:35:55 SDA_epes02_ARG_epes2t_1
2011-02-15_21:36:05 SDA_epes03_ARG_epes2t_1
2011-02-15_21:36:21 SDA_epes04_ARG_epes2t_1
2011-02-15_21:36:47 SDA_epes05_ARG_epes2t_1
2011-02-15_21:37:03 SDA_epes06_ARG_epes2t_1
2011-02-15_21:42:27 ARG_epes01_SDA_epes2t_1
2011-02-15_21:42:48 ARG_epes02_SDA_epes2t_1
2011-02-15_21:43:09 ARG_epes03_SDA_epes2t_1
2011-02-15_21:43:30 ARG_epes04_SDA_epes2t_1
2011-02-15_21:43:51 ARG_epes05_SDA_epes2t_1
2011-02-15_21:44:12 ARG_epes06_SDA_epes2t_1
2011-02-15_21:44:34 ARG_epes09_SDA_epes2t_1
2011-02-15_21:44:57 ARG_epes10_SDA_epes2t_1
2011-02-15_21:45:20 SDA_epes01_SDA_epes2t_1
2011-02-15_21:45:42 SDA_epes02_SDA_epes2t_1
2011-02-15_21:46:03 SDA_epes03_SDA_epes2t_1
2011-02-15_21:46:24 SDA_epes04_SDA_epes2t_1
2011-02-15_21:46:44 SDA_epes05_SDA_epes2t_1
2011-02-09_22:07:13 SDA_epes06_SDA_epes2t_1
2011-02-16_07:10:07 ARG_epes01_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:10:19 ARG_epes02_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:10:31 ARG_epes03_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:10:44 ARG_epes04_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:10:56 ARG_epes05_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:11:14 ARG_epes06_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:11:26 ARG_epes09_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:11:39 ARG_epes10_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:11:50 SDA_epes01_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:12:01 SDA_epes02_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:12:13 SDA_epes03_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:12:25 SDA_epes04_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:12:36 SDA_epes05_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:12:52 SDA_epes06_ARG_epes2t_ARG_t2c1_1
2011-02-16_07:13:03 ARG_epes01_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:13:15 ARG_epes02_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:13:29 ARG_epes03_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:13:40 ARG_epes04_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:13:52 ARG_epes05_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:14:08 ARG_epes06_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:14:22 ARG_epes09_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:14:34 ARG_epes10_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:14:46 SDA_epes01_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:14:58 SDA_epes02_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:15:09 SDA_epes03_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:15:23 SDA_epes04_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:15:35 SDA_epes05_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:15:51 SDA_epes06_SDA_epes2t_ARG_t2c1_1
2011-02-16_07:16:18 ARG_epes01_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:16:45 ARG_epes02_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:17:25 ARG_epes03_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:17:54 ARG_epes04_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:18:21 ARG_epes05_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:18:48 ARG_epes06_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:19:16 ARG_epes09_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:19:45 ARG_epes10_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:20:13 SDA_epes01_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:20:41 SDA_epes02_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:21:09 SDA_epes03_ARG_epes2t_SDA_t2c1_1

2011-02-16_07:21:38 SDA_epes04_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:22:05 SDA_epes05_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:22:33 SDA_epes06_ARG_epes2t_SDA_t2c1_1
2011-02-16_07:23:03 ARG_epes01_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:23:30 ARG_epes02_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:23:57 ARG_epes03_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:24:25 ARG_epes04_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:24:52 ARG_epes05_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:25:20 ARG_epes06_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:25:49 ARG_epes09_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:26:17 ARG_epes10_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:26:44 SDA_epes01_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:27:11 SDA_epes02_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:27:39 SDA_epes03_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:28:06 SDA_epes04_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:28:33 SDA_epes05_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:29:00 SDA_epes06_SDA_epes2t_SDA_t2c1_1
2011-02-16_07:30:50 ARG_epes01_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:31:05 ARG_epes02_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:31:19 ARG_epes03_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:32:30 ARG_epes04_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:32:45 ARG_epes05_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:33:05 ARG_epes06_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:33:20 ARG_epes09_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:33:35 ARG_epes10_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:33:51 SDA_epes01_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:34:09 SDA_epes02_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:34:26 SDA_epes03_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:34:41 SDA_epes04_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:34:57 SDA_epes05_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:35:16 SDA_epes06_ARG_epes2t_ARG_t2c2_1
2011-02-16_07:35:37 ARG_epes01_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:35:53 ARG_epes02_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:36:08 ARG_epes03_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:36:24 ARG_epes04_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:36:40 ARG_epes05_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:37:01 ARG_epes06_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:37:18 ARG_epes09_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:37:39 ARG_epes10_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:37:54 SDA_epes01_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:38:09 SDA_epes02_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:38:28 SDA_epes03_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:38:43 SDA_epes04_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:39:00 SDA_epes05_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:39:20 SDA_epes06_SDA_epes2t_ARG_t2c2_1
2011-02-16_07:39:50 ARG_epes01_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:40:21 ARG_epes02_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:40:51 ARG_epes03_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:41:28 ARG_epes04_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:41:59 ARG_epes05_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:42:30 ARG_epes06_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:43:04 ARG_epes09_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:43:36 ARG_epes10_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:44:07 SDA_epes01_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:44:38 SDA_epes02_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:45:09 SDA_epes03_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:45:39 SDA_epes04_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:46:11 SDA_epes05_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:46:42 SDA_epes06_ARG_epes2t_SDA_t2c2_1
2011-02-16_07:47:26 ARG_epes01_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:47:57 ARG_epes02_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:48:28 ARG_epes03_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:49:00 ARG_epes04_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:49:36 ARG_epes05_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:50:07 ARG_epes06_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:50:40 ARG_epes09_SDA_epes2t_SDA_t2c2_1
2011-02-16_08:26:27 ARG_epes10_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:51:49 SDA_epes01_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:52:19 SDA_epes02_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:52:50 SDA_epes03_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:53:21 SDA_epes04_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:53:53 SDA_epes05_SDA_epes2t_SDA_t2c2_1
2011-02-16_07:54:32 SDA_epes06_SDA_epes2t_SDA_t2c2_1

4.4.2 A páronkénti To_a tesztelés eredményei

Mind a 7 másik programmal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt.

Példaképp az ARG-SDA eredménye az alábbi:

```
2011-02-16_08:05:35 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_1
2011-02-16_08:06:01 SDA_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_1
2011-02-16_08:06:14 ARG_epes01_SDA_epes2t_ARG_t2c1_ARG_c2a1_1
2011-02-16_08:06:28 SDA_epes01_SDA_epes2t_ARG_t2c1_ARG_c2a1_1
2011-02-16_08:06:41 ARG_epes01_ARG_epes2t_SDA_t2c1_ARG_c2a1_1
2011-02-16_08:06:55 SDA_epes01_ARG_epes2t_SDA_t2c1_ARG_c2a1_1
2011-02-16_08:07:08 ARG_epes01_SDA_epes2t_SDA_t2c1_ARG_c2a1_1
2011-02-16_08:12:29 SDA_epes01_SDA_epes2t_SDA_t2c1_ARG_c2a1_1
2011-02-16_08:09:26 ARG_epes01_ARG_epes2t_ARG_t2c1_SDA_c2a1_1
2011-02-16_08:09:49 SDA_epes01_ARG_epes2t_ARG_t2c1_SDA_c2a1_1
2011-02-16_08:10:13 ARG_epes01_SDA_epes2t_ARG_t2c1_SDA_c2a1_1
2011-02-16_08:10:39 SDA_epes01_SDA_epes2t_ARG_t2c1_SDA_c2a1_1
2011-02-16_08:11:04 ARG_epes01_ARG_epes2t_SDA_t2c1_SDA_c2a1_1
2011-02-16_08:11:27 SDA_epes01_ARG_epes2t_SDA_t2c1_SDA_c2a1_1
2011-02-16_08:11:49 ARG_epes01_SDA_epes2t_SDA_t2c1_SDA_c2a1_1
2011-02-16_08:12:11 SDA_epes01_SDA_epes2t_SDA_t2c1_SDA_c2a1_1
2011-02-16_08:13:33 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_1
2011-02-16_08:13:48 SDA_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_1
2011-02-16_08:14:02 ARG_epes01_SDA_epes2t_ARG_t2c2_ARG_c2a2_1
2011-02-16_08:23:47 SDA_epes01_SDA_epes2t_ARG_t2c2_ARG_c2a2_1
2011-02-16_08:18:31 ARG_epes01_ARG_epes2t_SDA_t2c2_ARG_c2a2_1
2011-02-16_08:18:48 SDA_epes01_ARG_epes2t_SDA_t2c2_ARG_c2a2_1
2011-02-16_08:19:02 ARG_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_1
2011-02-16_08:19:18 SDA_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_1
2011-02-16_08:19:51 ARG_epes01_ARG_epes2t_ARG_t2c2_SDA_c2a2_1
2011-02-16_08:20:22 SDA_epes01_ARG_epes2t_ARG_t2c2_SDA_c2a2_1
2011-02-16_08:20:54 ARG_epes01_SDA_epes2t_ARG_t2c2_SDA_c2a2_1
2011-02-16_08:21:25 SDA_epes01_SDA_epes2t_ARG_t2c2_SDA_c2a2_1
2011-02-16_08:21:55 ARG_epes01_ARG_epes2t_SDA_t2c2_SDA_c2a2_1
2011-02-16_08:22:24 SDA_epes01_ARG_epes2t_SDA_t2c2_SDA_c2a2_1
2011-02-16_08:22:53 ARG_epes01_SDA_epes2t_SDA_t2c2_SDA_c2a2_1
2011-02-16_08:23:22 SDA_epes01_SDA_epes2t_SDA_t2c2_SDA_c2a2_1
2011-02-16_08:28:09 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:28:22 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:28:34 SDA_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:28:47 SDA_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:28:59 ARG_epes01_SDA_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:29:11 ARG_epes01_SDA_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:29:23 SDA_epes01_SDA_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:29:36 SDA_epes01_SDA_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:29:47 ARG_epes01_ARG_epes2t_SDA_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:29:59 ARG_epes01_ARG_epes2t_SDA_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:30:12 SDA_epes01_ARG_epes2t_SDA_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:30:24 SDA_epes01_ARG_epes2t_SDA_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:30:35 ARG_epes01_SDA_epes2t_SDA_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:30:47 ARG_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:30:59 SDA_epes01_SDA_epes2t_SDA_t2c1_ARG_c2a1_ARG_a2a_1
2011-02-16_08:31:11 SDA_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_ARG_a2a_1
2011-02-16_08:31:23 ARG_epes01_ARG_epes2t_ARG_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:31:36 ARG_epes01_ARG_epes2t_ARG_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:31:47 SDA_epes01_ARG_epes2t_ARG_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:32:15 SDA_epes01_ARG_epes2t_ARG_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:32:27 ARG_epes01_SDA_epes2t_ARG_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:32:40 ARG_epes01_SDA_epes2t_ARG_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:32:53 SDA_epes01_SDA_epes2t_ARG_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:33:06 SDA_epes01_SDA_epes2t_ARG_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:33:18 ARG_epes01_ARG_epes2t_SDA_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:33:30 ARG_epes01_ARG_epes2t_SDA_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:33:42 SDA_epes01_ARG_epes2t_SDA_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:33:54 SDA_epes01_ARG_epes2t_SDA_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:34:06 ARG_epes01_SDA_epes2t_SDA_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:34:20 ARG_epes01_SDA_epes2t_SDA_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:34:33 SDA_epes01_SDA_epes2t_SDA_t2c1_SDA_c2a1_ARG_a2a_1
2011-02-16_08:34:45 SDA_epes01_SDA_epes2t_SDA_t2c2_SDA_c2a2_ARG_a2a_1
2011-02-16_08:35:27 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_SDA_a2a_1
2011-02-16_08:36:01 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_SDA_a2a_1
2011-02-16_08:36:24 SDA_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_SDA_a2a_1
```

2011-02-16_08:36:57 SDA_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:37:19 ARG_epes01_SDA_epes2t_ARG_t2c1_ARG_c2a1_SDA_a2a_1
 2011-02-16_08:37:56 ARG_epes01_SDA_epes2t_ARG_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:38:24 SDA_epes01_SDA_epes2t_ARG_t2c1_ARG_c2a1_SDA_a2a_1
 2011-02-16_08:39:06 SDA_epes01_SDA_epes2t_ARG_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:39:29 ARG_epes01_ARG_epes2t_SDA_t2c1_ARG_c2a1_SDA_a2a_1
 2011-02-16_08:40:00 ARG_epes01_ARG_epes2t_SDA_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:40:23 SDA_epes01_ARG_epes2t_SDA_t2c1_ARG_c2a1_SDA_a2a_1
 2011-02-16_08:40:58 SDA_epes01_ARG_epes2t_SDA_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:41:57 ARG_epes01_SDA_epes2t_SDA_t2c1_ARG_c2a1_SDA_a2a_1
 2011-02-16_08:42:53 ARG_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:43:25 SDA_epes01_SDA_epes2t_SDA_t2c1_ARG_c2a1_SDA_a2a_1
 2011-02-16_08:44:00 SDA_epes01_SDA_epes2t_SDA_t2c2_ARG_c2a2_SDA_a2a_1
 2011-02-16_08:44:25 ARG_epes01_ARG_epes2t_ARG_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:45:02 ARG_epes01_ARG_epes2t_ARG_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:45:27 SDA_epes01_ARG_epes2t_ARG_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:46:07 SDA_epes01_ARG_epes2t_ARG_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:46:32 ARG_epes01_SDA_epes2t_ARG_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:47:27 ARG_epes01_SDA_epes2t_ARG_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:47:53 SDA_epes01_SDA_epes2t_ARG_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:48:32 SDA_epes01_SDA_epes2t_ARG_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:48:56 ARG_epes01_ARG_epes2t_SDA_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:49:30 ARG_epes01_ARG_epes2t_SDA_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:49:54 SDA_epes01_ARG_epes2t_SDA_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:50:28 SDA_epes01_ARG_epes2t_SDA_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:50:52 ARG_epes01_SDA_epes2t_SDA_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:51:23 ARG_epes01_SDA_epes2t_SDA_t2c2_SDA_c2a2_SDA_a2a_1
 2011-02-16_08:51:51 SDA_epes01_SDA_epes2t_SDA_t2c1_SDA_c2a1_SDA_a2a_1
 2011-02-16_08:52:20 SDA_epes01_SDA_epes2t_SDA_t2c2_SDA_c2a2_SDA_a2a_1

4.4.3 A negatív tesztelés eredményei

Mind a 14 negatív tesztet az elvárt eredményt (2: sikertelen ellenőrzés) adta:

2011-02-09_21:16:25 SDA_epes01_1 (ez a sikeres előkészület: EPES01 létrehozása)
 2011-02-09_21:16:51 SDA_epes01_SDA_epes2t_1 (ez a sikeres előkészület: -T létrehozása)

2011-02-09_21:17:10 NEG_N1_SDA_t2c1_2
 2011-02-09_21:17:29 NEG_N2_SDA_t2c2_2
 2011-02-09_21:17:44 NEG_N3_SDA_c2a1_2
 2011-02-09_21:18:16 NEG_N4_SDA_c2a1_2
 2011-02-09_21:18:39 NEG_N5_SDA_c2a1_2
 2011-02-09_21:18:56 NEG_N6_SDA_c2a1_2
 2011-02-09_21:19:13 NEG_N7_SDA_c2a1_2
 2011-02-09_21:19:40 NEG_N8_SDA_x2a1_2
 2011-02-09_21:20:39 NEG_N9_SDA_x2a2_2
 2011-02-09_21:21:08 NEG_N10_SDA_a2a_2
 2011-02-09_21:21:25 NEG_N11_SDA_epes2t_2
 2011-02-09_21:21:50 NEG_N12_SDA_c2a1_2
 2011-02-09_21:22:14 NEG_N13_SDA_c2a2_2
 2011-02-09_21:22:17 NEG_N14_SDA_epes2t_2

4.4.4 A tesztprogram és a termék összehasonlításának eredménye

A vizsgált tesztprogram: MMMEAA_SDA.exe

A forgalmazott termék: XadesMagic szoftver fejlesztőkészlet

A két program együttműködési képessége megegyezik, mivel azt a mindkét termék részét képező alábbi azonos dll-ek biztosítják:

- SDA.XadesMagic.dll (v2.0.0.24)
- SDA.Cryptography.dll (v2.0.0.8)
- SDA.Cryptography.Framework.dll (v2.0.0.2)
- SDA.TimestampProtocol.dll (v2.0.0.2)

5. Következtetések és javaslatok

5.1 Az értékelés összefoglaló eredménye

Az értékelés fő következtetései az alábbiak:

1. Az SDA Stúdió Kft. által kifejlesztett MMMEAA_SDA.exe elektronikus aláírás termék megfelel az [1]-ben az egységes MELASZ formátumokra meghatározott interoperabilitási követelményeknek.
2. Az SDA Stúdió Kft. által kifejlesztett XadesMagic v2.0.0 (build 24) szoftver fejlesztőkészlet, valamint az interoperabilitás tesztelésen bevizsgált MMMEAA_SDA.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 2011/003 számmal) kibocsátani az alábbi verzióra:

- XadesMagic v2.0.0 (build 24)

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