HUNG-MJ-006-2010 számú

MEGFELELÉS ÉRTÉKELÉSI JELENTÉS

az A2-Polysys CryptoSigno Interop JAVA API v2.2.1 (build 140)

megfelelése az

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

Verzió:	1.0
Fájl:	HUNG-MJ-006-2010.pdf
Minősítés:	Nyilvános
Oldalak:	20

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2010.03.23.	A fejleszt□knek egyeztetésre megküldött változat.
v0.2	2010.04.05.	A fejleszt□kkel egyeztetett, tanúsító szervezetnek megküldött változat.
v0.3	2010.04.10.	A tanúsító szervezet észrevételeit figyelembe vev□változat.
v1.0	2010.04.10.	Végleges változat.

A megfelelés értékelési jelentést készítette:

dr. Balázs István
Hunguard Kft.
értékelési divízió vezet□

Tartalomjegyzék

1. Bevezetés

1.1 Előzmények

A polysys® által kifejlesztett „A2-Polysys CryptoSigno Interop JAVA API min□sített elektronikus aláíráshoz v.2.0.0 build:125” termékre vonatkozó biztonsági értékelésen alapuló tanúsítás megállapította, hogy a termék megfelel a 2001. évi XXXV. törvényben szerepl□ min□sített elektronikus aláírás létrehozása és ellen□rzése céljából történ□ szabványos és biztonságos alkalmazások fejlesztéséhez (lásd Hung-T-029/2006 és Hung-TJ-029/2006).

A polysys® által kifejlesztett MMMEAA_POL.jar alkalmazás interoperabilitás tesztelésen alapuló tanúsítványban (MMMEAA 2009/005) a Magyar Elektronikus Aláírás Szövetség tanúsítja, hogy a CryptoSigno Interop JAVA API 2.2.1 elektronikus aláírási alkalmazás megfelel az elektronikus aláírásokra kidolgozott egységes MELASZ formátum 2.0 verziójának.

A fenti két tanúsítást követ□en a fejleszt□k több változtatást végeztek a terméken.

Az új verzió biztonsági hatásvizsgálatán alapulva, a tanúsítvány karbantartás eljárás keretében kiadott Tanúsítvány karbantartás jegyz□könyv (HUNG-TK-029/5-2010) kiterjeszti a HUNG-T-029-2006 tanúsítvány állításait a továbbfejlesztett alábbi verzióra: A2-Polysys CryptoSigno Interop JAVA API 2.2.1-ás verzió /build 140/.

1.2 Cél

Jelen értékelési jelentés célja kett□s, egyrészt egy új interoperabilitás tesztelés eredményeinek bemutatásával megalapozni a MELASZ tanúsítvány állításainak kiterjesztését az MMMEAA_POL.jar alkalmazás új verziójára, másrészt kimutatni, hogy az interoperabilitás teszteléssel vizsgált MMMEAA_POL.jar alkalmazás és az informatika biztonsági szempontból tanúsított A2-Polysys CryptoSigno Interop JAVA API 2.2.1-ás verzió /build 140/ termékek együttm□köd□képessége azonos.

1.3 Azonosító adatok

A vizsgált termék neve Verziója A termék rövid neve	A2-Polysys CryptoSigno Interop JAVA API min□sített elektronikus aláíráshoz használható fejleszt□készlet 2.2.1 (build 140) A2-Polysys CryptoSigno Interop
Az értékel□szervezet adatai	Hunguard Kft. 1125 Budapest, Kékgolyó u. 6.
A megbízó adatai	Polysys Kft. 1162 Budapest, Margitháza u. 1.
A termék fejleszt□adatai	Polysys Kft. 1162 Budapest, Margitháza u. 1.

1.4 Az értékelés mérföldkövei

Az el□készítési szakasz kezdési dátuma	2010.02.05.
Az el□készítési szakasz befejezési dátuma	2010.02.10.
Az értékelési szakasz kezdés dátuma	2010.02.11.
Az értékelési szakasz befejezési dátuma	2010.03.08
Az interoperabilitási tesztelés kezdés dátuma	2010.02.28.
Az interoperabilitási tesztelés befejezés dátuma	2010.04.06.
Értékelési jelentés tervezet elkészítésének dátuma	2010.03.08.
Értékelési jelentés (végleges) elkészítésének dátuma	2010.04.10

1.5 Az értékelők adatai

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

2. A termék leírása

2.1 Legfontosabb tulajdonságok

Az A2-Polysys CryptoSigno Interop egy olyan platform független fejleszt□ készlet, mely a ráépül□, Java technológiával készül□ alkalmazások számára PKI szolgáltatásokkal kapcsolatos különböz□ támogatást nyújt.

A biztonsági értékelés az A2-Polysys CryptoSigno Interop alábbi biztonsági funkcióit vizsgálta:

- BF1: Alap (SF.BASE): az AHA-k számára biztosítja a modell létrehozásának, valamint a vezérl□ megszerzésének a lehet□ségét, valamint a többi biztonsági funkció számára bels□ támogatást, alapozást biztosít.
- BF2: Inicializálás (SF.INIT): biztosítja az A2-Polysys CryptoSigno Interop hitelességét, annak sértetlenségének és megváltozatlanságának fenntartását.
- BF3: Azonosítás, hitelesítés és jogosultság ellen□rzés (SF.IAA): kikényszeríti, hogy az AHA felhasználója sikeresen azonosítva, majd sikeresen hitelesítve legyen, valamint jogosultsága ellen□rzésre kerüljön, miel□tt engedélyezné az A2-Polysys CryptoSigno Interop valamely szolgáltatásának igénybe vételét.
- BF4: Menedzsment (SF.MAN): kezeli a biztonságot érint□ jellemz□ket.
- BF5: Tanúsítási útvonal érvényesítés (SF.CPV): ellen□rzi a tanúsítványokat, felépíti a tanúsítási útvonalakat, ellen□rzi a tanúsítási útvonalak érvényességét.
- BF6: Visszavonási információ érvényesítés (SF.CRL): ellen□rzi a CRL visszavonási információk érvényességét.
- BF7: Elektronikus aláírás létrehozása és ellen□rzése (SF.SIGSIV): a felhasználó aláíró magánkulcsának felhasználásával elektronikus aláírást és azt kiegészít□ aláírási információkat hoz létre, illetve elektronikus aláírást és azt kiegészít□ aláírási információk érvényességét ellen□rzi.
- BF8: Titkosítás és dekódolás (SF.ENCDEC): titkosítja a címzettnek továbbítandó információkat a címzett nyilvános kulcsát tartalmazó tanúsítvány felhasználásával, illetve dekódolja a titkosított információkat az AHA felhasználó dekódoló magánkulcsának felhasználásával.
- BF9: Id□bélyeg kliens (SF.TSP): id□bélyeget kér az id□bélyegzés-szolgáltatótól, illetve ellen□rzi az id□bélyegzés-szolgáltatótól kapott, vagy az elektronikus aláírásban talált id□bélyeget.
- BF10: Valós idej□ tanúsítvány állapot protokoll kliens (SF.OCSP): OCSP-t kér az OCSP válaszadótól, illetve ellen□rzi az OCSP válaszadótól kapott, vagy az elektronikus aláírásban talált OCSP választ.

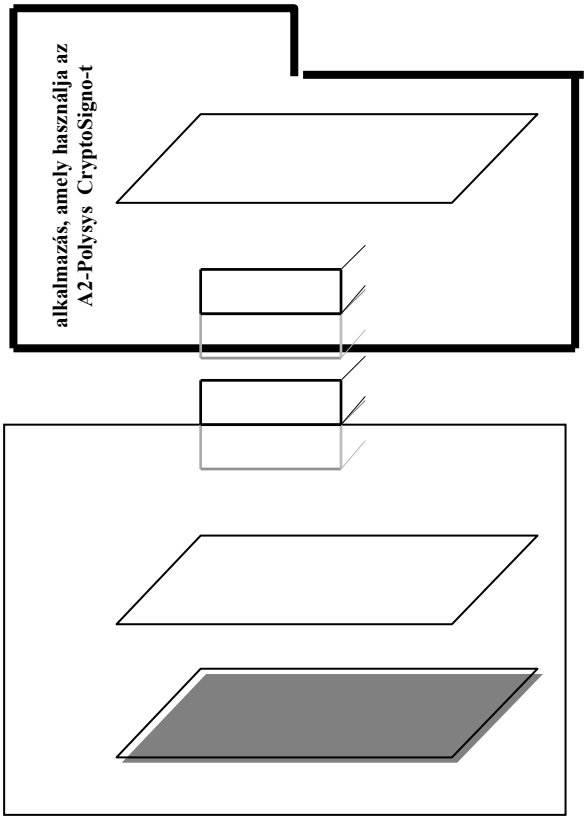
A biztonsági értékelés az A2-Polysys CryptoSigno Interop alábbi szabványos, interoperabilitást biztosító funkcióit vizsgálta:

- 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 id□bélyeg kérés és ellen□rzés,
- a visszavonási listák (CRL) kezelése az RFC 5280 [4] szerint,
- az RFC 2560 [6] szerinti OCSP kérés és az OCSP válasz ellen□rzése,
- együttm□ködés különböz□ PKCS#11-es felületen keresztül elérhet□ BALE-vel.

2.2 Architektúra

Az A2-Polysys CryptoSigno Interop v2.2.1 architektúrája a Model-Controller-View (MCV) paradigmán alapul:

- a modell (model) leírja egy objektum állapotát
- a vezérl□(controller) képes az objektum állapotának megváltoztatására
- a látvány (view) megjeleníti az objektum állapotát



2.3 Alrendszerek

A biztonsági értékelés az A2-Polysys CryptoSigno alábbi alrendszereit vizsgálta:

- AR1: Azonosítás, hitelesítés és jogosultság ellen□rzés alrendszer (SS.IAA)
- AR2: Felhasználói interfész alrendszer (SS.GUI)
- AR3: AHA interfész alrendszer (SS.SERVICE)
- AR4: Kriptográfiai alrendszer (SS.CRYPTO)
- AR5: SCDEV alrendszer (SS.SCDEV)

A jelen értékelési jelentés tárgyát képező interoperabilitási követelményeket az AR4 alrendszer juttatja érvényre.

2.4 Az értékelés hatóköre

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

Ez az interoperabilitás vizsgálat els□sorban az alábbi biztonsági funkciókat érinti :

- BF1, BF5, BF6, BF7, BF9, BF10

Az interoperabilitás vizsgálat az architektúra alábbi rétegeit érinti:

- egy speciális AHA (MMMEAA_POL.jar teszprogram)
- a Model és Controller rétegeket megvalósító a1.jar állomány.

Az interoperabilitás vizsgálat els□sorban az alábbi alrendszerre fókuszál:

- AR4.

3. Az értékelés jellemzése

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

3.1 Értékelési módszerek

Az A2-Polysys CryptoSigno Interop 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 A2-Polysys CryptoSigno Interop 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
A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz v2.2.1 (build 140)	**polysys ®**	**MMMEAA_POL.jar**	**POL**

alábbi termékekkel való együttm□köd□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
SDX (Signed Document eXpert) 2.2.1	MMMEAA 2009/006	E-Group ICT Software Zrt.	MMMEAA_EGR.exe	EGR
Nlcapi3 3.3.1 (benne NLxades modul v2.0.4)	MMMEAA 2010/001	NetLock Kft.	MMMEAA_NET.exe	NET
Noreg eSign Toolkit 2.2.1	MMMEAA 2009/004	Noreg Kft.	MMMEAA_NOR.exe	NOR
e-Szignó 3.1	MMMEAA 2009/002	Microsec Kft.	MMMEAA_MIC.exe	MIC

3.3 Tesztesetek

3.3.1 Pozitív tesztesetek

A programok párokat az alábbi pozitív tesztesetekkel vizsgáltuk:

Teszteset azonosító	Teszteset leíró (és kiegészít□)	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	ellenjegyz□	ellenjegyz□aláírás létrehozás
epes08	párhuzamos	párhuzamos aláírás létrehozás
epes09	AllDataObjects TimeStamp	aláírás létrehozás adott id□pontú eredet bizonyítással (AllDataObjects TimeStamp)
epes10	IndividualData ObjectsTimeStamp	aláírás létrehozás adott id□pontú eredet bizonyítással (IndividualData ObjectsTime Stamp)
epes2t	SignatureTimeStamp	a bemenetként megadott XAdES-EPES formátumú aláírás ellen□rzése, egyúttal XAdES-T formátumú aláírás létrehozása
t2c1	CRLRefs	a bemenetként megadott XAdES-T formátumú aláírás ellen□rzése, egyúttal XAdES-C formátumú aláírás létrehozása CRL visszavonási információ befoglalásával
t2c2	OCSPRefs	a bemenetként megadott XAdES-T formátumú aláírás ellen□rzése, 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 ellen□rzése, egyúttal XAdES-A formátumú aláírás létrehozása
c2a2	Archive TimeStamp OCSPRefs	a bemenetként megadott (OCSP visszavonási információt tartalmazó) XAdES-C formátumú aláírás ellen□rzése, egyúttal XAdES-A formátumú aláírás létrehozása
x2a1	Archive TimeStamp RefsOnly TimeStamp	a bemenetként megadott (CRL-t felül id□bélyegz□) XAdES-XL formátumú aláírás ellen□rzése, egyúttal XAdES-A formátumú aláírás létrehozása
x2a2	Archive TimeStamp SigAndRefs TimeStamp	a bemenetként megadott (OCSP választ felül id□bélyegz□) XAdES-XL formátumú aláírás ellen□rzése, egyúttal XAdES-A formátumú aláírás létrehozása
a2a	2 darab Archive TimeStamp	a bemenetként megadott XAdES-A formátumú aláírás ellen□rzése, egyúttal egy új XAdES-A formátumú aláírás létrehozása egy másik archív id□bélyegzés létrehozásával

Az epes07–epes10 teszteseteket csak annak a programnak kell létrehoznia, amely az érintett opcionális elemet támogatja. Ellen□rizni 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.

POL az epes07–epes10 tesztesetekben érintett valamennyi opcionális elemet támogatja.

3.3.2 Negatív tesztesetek

A programot az alábbi negatív tesztesetekkel vizsgáltuk:

Teszteset azonosító	Teszteset leíró	megjegyzés
Teszt_N1	A kivárási id□helyes kezelésének vizsgálata	A bemenetként megadott XAdES-T formátumú aláírás ellen□rzése, közvetlenül az id□bélyegzés után, tehát a kivárási id□letelte el□tt.
Teszt_N2	Aláírás visszavont tanúsítvánnyal	A bemenetben lév□aláírás egy visszavont tanúsítványhoz tartozó magánkulccsal készült.
Teszt_N3	Az explicit módon meghatározott szabályzat ellen□rzésének vizsgálata	Az epes06 tesztesetet egy olyan aláírással futtatják, amelyben a SignaturePolicyId által meghatározott szabályzat sérült.
Teszt_N4	Ellenjegyz□aláírás ellen□rzésének vizsgálata	Az epes07 tesztesetet egy olyan aláírással futtatják, amelyben az egyik ellenjegyz□aláírás sérült.
Teszt_N5	Párhuzamos aláírás ellen□rzésének vizsgálata	Az epes08 tesztesetet egy olyan aláírással futtatják, amelyben az egyik párhuzamos aláírás sérült.
Teszt_N6	Adott id□pontú eredet bizonyítás (AllDataObjects TimeStamp) ellen□rzésének vizsgálata	Az epes09 tesztesetet egy olyan aláírással futtatják, amelyben az AllDataObjectsTimeStamp sérült
Teszt_N7	Adott id□pontú eredet bizonyítás (IndividualObjectsTimeStamp) ellen□rzésének vizsgálata	Az epes10 tesztesetet egy olyan aláírással futtatják, amelyben az IndividualObjectsTimeStamp sérült.
Teszt_N8	A RefsOnlyTimeStamp ellen□rzésének vizsgálata	A c2a1 tesztesetet egy olyan aláírással futtatják, amelyben a RefsOnlyTimeStamp sérült.
Teszt_N9	A SigAndRefsTimeStamp ellen□rzésének vizsgálata	A c2a2 tesztesetet egy olyan aláírással futtatják, amelyben a SigAndRefsTimeStamp sérült.
Teszt_N10	Az ArchiveTimeStamp ellen□rzésének 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.

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 (POL-ARG, POL-EGR, POL-NET, POL-NOR, POL-MIC) 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 id□ 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 ellen□rzés).

3.4.2 Páronkénti To_a tesztelés

Valamennyi vizsgált tesztprogram-párra (POL-ARG, POL-EGR, POL-NET, POL-NOR, POL-MIC) 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 id□ 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 ellen□rzés).

3.4.3 Tesztelés negatív tesztesetekkel

A vizsgált programot (POL) teszteltük a Teszt_N1 - Teszt_N13 negatív tesztesetekkel.

Mind a tizenhárom tesztesetben az elvárt eredmény: 2 (sikertelen ellen□rzés).

4. Az értékelés eredményei

Az eredmények és a tesztelés megismételhetőségéhez szükséges környezeti elemek az alábbi könyvtárban találhatók:
Polysys\Assurance_Continuity\A2v221\Maintenance\MR2\IOP_test_final

Az IOP_test_final alkönyvtár szerkezete az alábbi:

- ARG_POL (az ARG – POL programpár tesztelési eredményei)
- EGR_POL (az EGR – POL programpár tesztelési eredményei)
- MIC_POL (a MIC – POL programpár tesztelési eredményei)
- NET_POL (a NET – POL programpár tesztelési eredményei)
- NOR_POL (a NOR – POL programpár tesztelési eredményei)
- POL_POL (a negatív tesztesetek eredményei)
- Signer.cer (aláíró tanúsítványa)

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

- ARG (az ARG tesztprogram és futtatási környezete)
- POL (az új POL 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:
2010-03-08_20:24:23 POL_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_POL_a2a_ 1, ahol:

- 2010-03-08_20:24:23 a teszt lefutásának dátuma és időpontja
- POL_epes01_: 1. lépés: POL meghívásával epes01 aláírás létrehozása
- ARG_epes2t_: 2. lépés: ARG 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
- ARG_c2a2_: 4. lépés: ARG meghívásával a 3. lépés eredményének ellenőrzése, majd ebből c2a2 létrehozása
- POL_a2a_: 5. lépés: POL 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 az 5 tesztprogrammal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt. Példaképp az ARG-POL eredménye az alábbi:

2010-03-01_12:38:14 ARG_epes01_ 1
2010-03-01_12:38:20 ARG_epes02_ 1
2010-03-01_12:38:23 ARG_epes03_ 1
2010-03-01_12:38:27 ARG_epes04_ 1
2010-03-01_12:38:31 ARG_epes05_ 1
2010-03-01_12:38:37 ARG_epes06_ 1
2010-03-01_12:38:43 ARG_epes09_ 1
2010-03-01_12:38:49 ARG_epes10_ 1

2010-03-01_12:39:04 POL_epes01_ 1
2010-03-01_12:39:23 POL_epes02_ 1
2010-03-01_12:39:38 POL_epes03_ 1
2010-03-01_12:39:54 POL_epes04_ 1
2010-03-01_12:40:09 POL_epes05_ 1
2010-03-01_12:40:30 POL_epes06_ 1
2010-03-01_12:40:48 POL_epes07_ 1
2010-03-01_12:41:06 POL_epes08_ 1
2010-03-01_12:41:22 POL_epes09_ 1
2010-03-01_12:41:37 POL_epes10_ 1
2010-03-01_13:08:56 ARG_epes01_ARG_epes2t_ 1
2010-03-01_13:09:03 ARG_epes02_ARG_epes2t_ 1
2010-03-01_13:09:09 ARG_epes03_ARG_epes2t_ 1
2010-03-01_13:09:16 ARG_epes04_ARG_epes2t_ 1
2010-03-01_13:09:22 ARG_epes05_ARG_epes2t_ 1
2010-03-01_13:09:31 ARG_epes06_ARG_epes2t_ 1
2010-03-01_13:09:38 ARG_epes09_ARG_epes2t_ 1
2010-03-01_13:09:44 ARG_epes10_ARG_epes2t_ 1
2010-03-01_13:09:51 POL_epes01_ARG_epes2t_ 1
2010-03-01_13:09:57 POL_epes02_ARG_epes2t_ 1
2010-03-01_13:10:03 POL_epes03_ARG_epes2t_ 1
2010-03-01_13:10:09 POL_epes04_ARG_epes2t_ 1
2010-03-01_13:10:16 POL_epes05_ARG_epes2t_ 1
2010-03-01_13:10:27 POL_epes06_ARG_epes2t_ 1
2010-03-01_13:10:37 POL_epes07_ARG_epes2t_ 1
2010-03-01_13:10:47 POL_epes08_ARG_epes2t_ 1
2010-03-01_13:10:53 POL_epes09_ARG_epes2t_ 1
2010-03-01_13:11:00 POL_epes10_ARG_epes2t_ 1
2010-03-01_13:11:12 ARG_epes01_POL_epes2t_ 1
2010-03-01_13:11:23 ARG_epes02_POL_epes2t_ 1
2010-03-01_13:11:34 ARG_epes03_POL_epes2t_ 1
2010-03-01_13:11:45 ARG_epes04_POL_epes2t_ 1
2010-03-01_13:11:56 ARG_epes05_POL_epes2t_ 1
2010-03-01_13:12:08 ARG_epes06_POL_epes2t_ 1
2010-03-01_13:12:19 ARG_epes09_POL_epes2t_ 1
2010-03-01_13:12:31 ARG_epes10_POL_epes2t_ 1
2010-03-01_13:12:43 POL_epes01_POL_epes2t_ 1
2010-03-01_13:12:54 POL_epes02_POL_epes2t_ 1
2010-03-01_13:13:05 POL_epes03_POL_epes2t_ 1
2010-03-01_13:13:16 POL_epes04_POL_epes2t_ 1
2010-03-01_13:13:27 POL_epes05_POL_epes2t_ 1
2010-03-01_13:13:39 POL_epes06_POL_epes2t_ 1
2010-03-01_13:13:53 POL_epes07_POL_epes2t_ 1
2010-03-01_13:14:07 POL_epes08_POL_epes2t_ 1
2010-03-01_13:14:18 POL_epes09_POL_epes2t_ 1
2010-03-01_13:14:29 POL_epes10_POL_epes2t_ 1
2010-03-01_13:16:46 ARG_epes01_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:16:55 ARG_epes02_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:17:03 ARG_epes03_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:17:12 ARG_epes04_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:17:21 ARG_epes05_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:17:36 ARG_epes06_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:17:44 ARG_epes09_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:17:53 ARG_epes10_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:18:02 POL_epes01_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:18:11 POL_epes02_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:18:20 POL_epes03_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:18:29 POL_epes04_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:18:38 POL_epes05_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:18:52 POL_epes06_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:19:12 POL_epes07_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:19:31 POL_epes08_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:19:40 POL_epes09_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:19:49 POL_epes10_ARG_epes2t_ARG_t2c2_ 1
2010-03-01_13:19:58 ARG_epes01_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:20:07 ARG_epes02_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:20:15 ARG_epes03_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:20:24 ARG_epes04_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:20:33 ARG_epes05_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:20:49 ARG_epes06_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:20:58 ARG_epes09_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:21:07 ARG_epes10_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:21:16 POL_epes01_POL_epes2t_ARG_t2c2_ 1

2010-03-01_13:21:24 POL_epes02_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:21:33 POL_epes03_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:21:42 POL_epes04_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:21:53 POL_epes05_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:22:07 POL_epes06_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:22:28 POL_epes07_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:22:48 POL_epes08_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:22:57 POL_epes09_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:23:06 POL_epes10_POL_epes2t_ARG_t2c2_ 1
2010-03-01_13:23:20 ARG_epes01_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:23:33 ARG_epes02_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:23:46 ARG_epes03_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:23:59 ARG_epes04_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:24:12 ARG_epes05_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:24:26 ARG_epes06_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:24:39 ARG_epes09_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:24:52 ARG_epes10_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:25:05 POL_epes01_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:25:18 POL_epes02_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:25:31 POL_epes03_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:25:44 POL_epes04_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:25:57 POL_epes05_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:26:10 POL_epes06_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:26:31 POL_epes07_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:26:51 POL_epes08_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:27:05 POL_epes09_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:27:18 POL_epes10_ARG_epes2t_POL_t2c2_ 1
2010-03-01_13:27:31 ARG_epes01_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:27:44 ARG_epes02_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:27:57 ARG_epes03_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:28:09 ARG_epes04_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:28:22 ARG_epes05_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:28:36 ARG_epes06_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:28:49 ARG_epes09_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:29:02 ARG_epes10_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:29:16 POL_epes01_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:29:29 POL_epes02_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:29:42 POL_epes03_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:29:55 POL_epes04_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:30:07 POL_epes05_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:30:21 POL_epes06_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:30:41 POL_epes07_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:31:01 POL_epes08_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:31:15 POL_epes09_POL_epes2t_POL_t2c2_ 1
2010-03-01_13:31:28 POL_epes10_POL_epes2t_POL_t2c2_ 1
2010-03-02_19:32:56 ARG_epes01_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:03 ARG_epes02_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:10 ARG_epes03_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:16 ARG_epes04_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:24 ARG_epes05_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:41 ARG_epes06_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:49 ARG_epes09_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:33:56 ARG_epes10_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:34:04 POL_epes01_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:34:10 POL_epes02_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:34:17 POL_epes03_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:34:25 POL_epes04_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:34:32 POL_epes05_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:34:50 POL_epes06_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:00 POL_epes07_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:11 POL_epes08_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:19 POL_epes09_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:27 POL_epes10_ARG_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:34 ARG_epes01_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:41 ARG_epes02_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:50 ARG_epes03_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:35:58 ARG_epes04_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:36:06 ARG_epes05_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:36:24 ARG_epes06_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:36:32 ARG_epes09_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:36:42 ARG_epes10_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:36:49 POL_epes01_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:36:56 POL_epes02_POL_epes2t_ARG_t2c1_ 1

2010-03-02_19:37:04 POL_epes03_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:37:11 POL_epes04_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:37:18 POL_epes05_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:37:34 POL_epes06_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:37:44 POL_epes07_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:37:54 POL_epes08_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:38:01 POL_epes09_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:38:08 POL_epes10_POL_epes2t_ARG_t2c1_ 1
2010-03-02_19:38:29 ARG_epes01_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:38:47 ARG_epes02_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:39:03 ARG_epes03_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:39:19 ARG_epes04_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:39:35 ARG_epes05_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:39:54 ARG_epes06_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:40:13 ARG_epes09_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:40:31 ARG_epes10_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:40:48 POL_epes01_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:41:06 POL_epes02_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:41:22 POL_epes03_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:41:37 POL_epes04_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:41:53 POL_epes05_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:42:13 POL_epes06_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:42:33 POL_epes07_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:42:54 POL_epes08_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:43:10 POL_epes09_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:43:26 POL_epes10_ARG_epes2t_POL_t2c1_ 1
2010-03-02_19:43:41 ARG_epes01_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:43:57 ARG_epes02_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:44:13 ARG_epes03_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:44:28 ARG_epes04_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:44:44 ARG_epes05_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:45:02 ARG_epes06_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:45:19 ARG_epes09_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:45:36 ARG_epes10_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:45:52 POL_epes01_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:46:07 POL_epes02_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:46:23 POL_epes03_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:46:39 POL_epes04_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:46:54 POL_epes05_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:47:11 POL_epes06_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:47:31 POL_epes07_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:47:52 POL_epes08_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:48:08 POL_epes09_POL_epes2t_POL_t2c1_ 1
2010-03-02_19:48:24 POL_epes10_POL_epes2t_POL_t2c1_ 1

4.4.2 A páronkénti To_a tesztelés eredményei

Mind az 5 tesztprogrammal az összes eredmény az elvárt 1-es (sikeres ellen□rzés) volt. Példaképp az ARG-POL eredménye az alábbi:

2010-03-08_20:09:41 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-08_20:09:46 POL_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-08_20:09:51 ARG_epes01_POL_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-08_20:09:56 POL_epes01_POL_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-08_20:10:01 ARG_epes01_ARG_epes2t_POL_t2c1_ARG_c2a1_ 1
2010-03-08_20:10:06 POL_epes01_ARG_epes2t_POL_t2c1_ARG_c2a1_ 1
2010-03-08_20:10:11 ARG_epes01_POL_epes2t_POL_t2c1_ARG_c2a1_ 1
2010-03-08_20:10:15 POL_epes01_POL_epes2t_POL_t2c1_ARG_c2a1_ 1
2010-03-08_20:10:28 ARG_epes01_ARG_epes2t_ARG_t2c1_POL_c2a1_ 1
2010-03-08_20:10:35 POL_epes01_ARG_epes2t_ARG_t2c1_POL_c2a1_ 1
2010-03-08_20:10:43 ARG_epes01_POL_epes2t_ARG_t2c1_POL_c2a1_ 1
2010-03-08_20:10:51 POL_epes01_POL_epes2t_ARG_t2c1_POL_c2a1_ 1
2010-03-08_20:10:59 ARG_epes01_ARG_epes2t_POL_t2c1_POL_c2a1_ 1
2010-03-08_20:11:07 POL_epes01_ARG_epes2t_POL_t2c1_POL_c2a1_ 1
2010-03-08_20:11:14 ARG_epes01_POL_epes2t_POL_t2c1_POL_c2a1_ 1
2010-03-08_20:11:25 POL_epes01_POL_epes2t_POL_t2c1_POL_c2a1_ 1
2010-03-08_20:17:04 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:10 POL_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:16 ARG_epes01_POL_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:22 POL_epes01_POL_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:28 ARG_epes01_ARG_epes2t_POL_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:35 POL_epes01_ARG_epes2t_POL_t2c2_ARG_c2a2_ 1

2010-03-08_20:17:41 ARG_epes01_POL_epes2t_POL_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:48 POL_epes01_POL_epes2t_POL_t2c2_ARG_c2a2_ 1
2010-03-08_20:17:56 ARG_epes01_ARG_epes2t_ARG_t2c2_POL_c2a2_ 1
2010-03-08_20:18:04 POL_epes01_ARG_epes2t_ARG_t2c2_POL_c2a2_ 1
2010-03-08_20:18:13 ARG_epes01_POL_epes2t_ARG_t2c2_POL_c2a2_ 1
2010-03-08_20:18:21 POL_epes01_POL_epes2t_ARG_t2c2_POL_c2a2_ 1
2010-03-08_20:18:29 ARG_epes01_ARG_epes2t_POL_t2c2_POL_c2a2_ 1
2010-03-08_20:18:37 POL_epes01_ARG_epes2t_POL_t2c2_POL_c2a2_ 1
2010-03-08_20:18:45 ARG_epes01_POL_epes2t_POL_t2c2_POL_c2a2_ 1
2010-03-08_20:18:54 POL_epes01_POL_epes2t_POL_t2c2_POL_c2a2_ 1
2010-03-08_20:20:55 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:21:01 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:21:06 POL_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:21:11 POL_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:21:15 ARG_epes01_POL_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:21:21 ARG_epes01_POL_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:21:26 POL_epes01_POL_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:21:31 POL_epes01_POL_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:21:36 ARG_epes01_ARG_epes2t_POL_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:21:43 ARG_epes01_ARG_epes2t_POL_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:21:49 POL_epes01_ARG_epes2t_POL_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:21:57 POL_epes01_ARG_epes2t_POL_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:22:03 ARG_epes01_POL_epes2t_POL_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:22:09 ARG_epes01_POL_epes2t_POL_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:22:14 POL_epes01_POL_epes2t_POL_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-08_20:22:20 POL_epes01_POL_epes2t_POL_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-08_20:22:25 ARG_epes01_ARG_epes2t_ARG_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:22:32 ARG_epes01_ARG_epes2t_ARG_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:22:37 POL_epes01_ARG_epes2t_ARG_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:22:43 POL_epes01_ARG_epes2t_ARG_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:22:48 ARG_epes01_POL_epes2t_ARG_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:22:54 ARG_epes01_POL_epes2t_ARG_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:22:59 POL_epes01_POL_epes2t_ARG_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:23:04 POL_epes01_POL_epes2t_ARG_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:23:09 ARG_epes01_ARG_epes2t_POL_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:23:15 ARG_epes01_ARG_epes2t_POL_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:23:20 POL_epes01_ARG_epes2t_POL_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:23:26 POL_epes01_ARG_epes2t_POL_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:23:31 ARG_epes01_POL_epes2t_POL_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:23:36 ARG_epes01_POL_epes2t_POL_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:23:40 POL_epes01_POL_epes2t_POL_t2c1_POL_c2a1_ARG_a2a_ 1
2010-03-08_20:23:46 POL_epes01_POL_epes2t_POL_t2c2_POL_c2a2_ARG_a2a_ 1
2010-03-08_20:23:58 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:24:06 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:24:14 POL_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:24:23 POL_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:24:33 ARG_epes01_POL_epes2t_ARG_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:24:42 ARG_epes01_POL_epes2t_ARG_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:24:51 POL_epes01_POL_epes2t_ARG_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:25:00 POL_epes01_POL_epes2t_ARG_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:25:08 ARG_epes01_ARG_epes2t_POL_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:25:21 ARG_epes01_ARG_epes2t_POL_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:25:32 POL_epes01_ARG_epes2t_POL_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:25:43 POL_epes01_ARG_epes2t_POL_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:25:52 ARG_epes01_POL_epes2t_POL_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:26:01 ARG_epes01_POL_epes2t_POL_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:26:10 POL_epes01_POL_epes2t_POL_t2c1_ARG_c2a1_POL_a2a_ 1
2010-03-08_20:26:20 POL_epes01_POL_epes2t_POL_t2c2_ARG_c2a2_POL_a2a_ 1
2010-03-08_20:26:29 ARG_epes01_ARG_epes2t_ARG_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:26:40 ARG_epes01_ARG_epes2t_ARG_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:26:52 POL_epes01_ARG_epes2t_ARG_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:27:02 POL_epes01_ARG_epes2t_ARG_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:27:11 ARG_epes01_POL_epes2t_ARG_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:27:22 ARG_epes01_POL_epes2t_ARG_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:27:34 POL_epes01_POL_epes2t_ARG_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:27:44 POL_epes01_POL_epes2t_ARG_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:27:54 ARG_epes01_ARG_epes2t_POL_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:28:04 ARG_epes01_ARG_epes2t_POL_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:28:13 POL_epes01_ARG_epes2t_POL_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:28:23 POL_epes01_ARG_epes2t_POL_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:28:32 ARG_epes01_POL_epes2t_POL_t2c1_POL_c2a1_POL_a2a_ 1
2010-03-08_20:28:41 ARG_epes01_POL_epes2t_POL_t2c2_POL_c2a2_POL_a2a_ 1
2010-03-08_20:28:50 POL_epes01_POL_epes2t_POL_t2c1_POL_c2a1_POL_a2a_ 1

2010-03-08_20:29:00 POL_epes01_POL_epes2t_POL_t2c2_POL_c2a2_POL_a2a_ 1

4.4.3 A negatív tesztelés eredményei

Valamennyi negatív teszteset az elvárt eredményt (2: sikertelen ellen□rzés) adta:

2010-04-06_19:26:47 POL_epes01_ 1 (ez az N1 negatív teszt el□készítése)
2010-04-06_19:26:55 POL_epes01_POL_epes2t_ 1 (ez az N1 negatív teszt el□készítése)
2010-04-06_19:26:59 NEG_N1_POL_t2c1_ 2
2010-04-06_19:27:05 NEG_N2_POL_t2c2_ 2
2010-04-06_19:27:10 NEG_N3_POL_c2a1_ 2
2010-04-06_19:27:15 NEG_N4_POL_c2a1_ 2
2010-04-06_19:27:23 NEG_N5_POL_c2a1_ 2
2010-04-06_19:27:28 NEG_N6_POL_c2a1_ 2
2010-04-06_19:27:34 NEG_N7_POL_c2a1_ 2
2010-04-06_19:27:40 NEG_N8_POL_x2a1_ 2
2010-04-06_19:27:46 NEG_N9_POL_x2a2_ 2
2010-04-06_19:27:55 NEG_N10_POL_a2a_ 2
2010-04-06_19:28:00 NEG_N11_POL_epes2t_ 2
2010-04-06_19:28:06 NEG_N12_POL_c2a1_ 2
2010-04-06_19:28:11 NEG_N13_POL_c2a2_ 2

4.4.4 A tesztprogram és a termék összehasonlításának eredménye

A vizsgált tesztprogram: MMMEAA_POL.jar

A forgalmazott termék: A2-Polysys CryptoSigno Interop JAVA API v2.2.1 (build 140)

A két program együttm□ködési képessége megegyezik, mert az MMMEAA_POL.jar (mint alkalmazás) a1.jar, a5.jar, a6.jar állományai megegyeznek a biztonsági szempontból értékelt és tanúsított TOE v2.2.1 a2csapi.jar, xalan.jar és xerceslmpl.jar állományaival (ami az a2-api-BIN_2_2_1 állományt teljesen lefedi.

5. Következtetések és javaslatok

5.1 Az értékelés összefoglaló eredménye

Az értékelés f□következtetései az alábbiak:

1. A polysys® által kifejlesztett MMMEAA_POL.jar elektronikus aláírás termék megfelel az [1]-ben az egységes MELASZ formátumokra meghatározott interoperabilitási követelményeknek.
2. A polysys® által kifejlesztett A2-Polysys CryptoSigno Interop JAVA API min□sített elektronikus aláíráshoz v2.2.1 (build140) függvénykészlet, valamint az interoperabilitás tesztelésen bevizsgált MMMEAA_POL.jar alkalmazás együttm□ködési képessége megegyezik.

5.2 Javaslatok

1. A Hunguard kft. (mint értékel□ szervezet) vizsgálati eredményei alapján javasolja a Magyar Elektronikus Aláírás Szövetségnek (mint tanúsító szervezetnek) egy új tanúsítványt (MMMEAA 2010/002 számmal) kibocsátani az alábbi verzióra:
   - A2-Polysys CryptoSigno Interop JAVA API v 2.2.1 (build 140)
2. Javasoljuk továbbá, hogy a jöv□ben az egységes MELASZ formátumra kiadott tanúsítványok, illetve az ezekbe foglalt állítások esetleges kiterjesztései (pl. tanúsítvány karbantartás jegyz□könyvek) a vizsgált termékek pontos verzióit tartalmazzák, beleértve a build számot is.

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, v0.7)

[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

AHA	az **A**2-Polysys CryptoSigno Interop-t **H**asználó **A**lkalmazás
BALE	biztonságos aláírás-létrehozó eszköz
CRL	Certificate Revocation List (tanúsítvány visszavonási lista)
MCV	Model-Controller-View
MELASZ	Magyar Elektronikus Aláírás Szövetség
MIBÉTS	Magyar Informatikai Biztonsági és Értékelési Séma
MMM	MELASZ Munkacsoport Megállapodás
OCSP	Online Certificate Status Protocol (valós idej□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