HUNG-MJ-005-2010 számú

MEGFELELÉS ÉRTÉKELÉSI JELENTÉS

az Nlcapi3 v3.3.1 (build 1) /benne az NLxades modul v2.0.4/

megfelelése az

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

Verzió:	1.0
Fájl:	HUNG-MJ-005-2010.pdf
Minősítés:	Nyilvános
Oldalak:	18

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2010.04.05.	A fejlesztőknek egyeztetésre megküldött változat.
v0.2	2010.04.09.	A fejlesztőkkel egyeztetett, tanúsító szervezetnek megküldött változat.
v1.0	2010.04.10.	A tanúsító szervezettel is egyeztetett, 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: 2010.04.22 11:10:08 +02'00'

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
Location: Budapest
Date: 2010.04.22 12:51:02 +02'00'

Tartalomjegyzék

1. Bevezetés

1.1 Előzmények

A Netlock Kft. által kifejlesztett „Nlcapi3 v3.2.0 kriptográfiai modul (elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói függvény könyvtár) v3.2.0" 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, valamint időbélyeg kérelmezésére és ellenőrzésre alkalmazható szabványos és biztonságos alkalmazások fejlesztéséhez (lásd Hung-T-027/2005 és Hung-TJ-027/2005).
A Netlock Kft. által kifejlesztett MMMEAA_NET.exe alkalmazás interoperabilitás tesztelésen alapuló tanúsítványban (MMMEAA 2009/003) a Magyar Elektronikus Aláírás Szövetség tanúsítja, hogy az Nlcapi3 (NLxades modullal) 3.3.0 elektronikus aláírási alkalmazás megfelel az elektronikus aláírásokra kidolgozott egységes MELASZ formátum 2.0 verziójának.
A fenti két tanúsítást követően a fejlesztők több változtatást végeztek a terméken. Az új verzió biztonsági hatásvizsgálatán alapulva, a tanúsítvány karbantartás eljárás keretében kiadott Tanúsítvány karbantartás jegyzőkönyv (HUNG-TK-027/5-2010) kiterjeszti a HUNG-T-027-2005 tanúsítvány állításait a továbbfejlesztett alábbi verzióra: Nlcapi3 3.3.1-es verzió /build 1/.

1.2 Cél

Jelen értékelési jelentés célja kettős, egyrészt egy új interoperabilitás tesztelés eredményeinek bemutatásával megalapozni a MELASZ tanúsítvány állításainak kiterjesztését az MMMEAA_NET.exe alkalmazás új verziójára, másrészt kimutatni, hogy az interoperabilitás teszteléssel vizsgált MMMEAA_NET.exe alkalmazás és az informatika biztonsági szempontból tanúsított Nlcapi3 3.3.1-es verzió /build 1/ termékek együttműködő képessége azonos.

1.3 Azonosító adatok

A vizsgált termék neve Verziója A termék rövid neve	Nlcapi3 kriptográfiai modul (elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói függvény könyvtár) 3.3.1 (build 1) Nlcapi3
Az értékelő szervezet adatai	Hunguard Kft. 1125 Budapest, Kékgolyó u. 6.
A megbízó adatai	NetLock Kft, 1023 Budapest, Zsigmond tér 10.
A termék fejlesztő adatai	NetLock Kft, 1023 Budapest, Zsigmond tér 10.

1.4 Az értékelés mérföldkövei

Az előkészítési szakasz kezdési dátuma	2010.02.05.
Az előkészítési 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	2010.04.05.
Értékelési jelentés (végleges) elkészítésének dátuma	2010.04.09

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 Nlcapi3 egy programozói könyvtár, amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.

A biztonsági értékelés az Nlcapi3 alábbi biztonsági funkcióit vizsgálta:

- BF1 (Elektronikus aláírás létrehozás előkészítés): Hash számítás, majd az elektronikus aláírás létrehozás létrehozása folyamatának inicializálása, végül a megfelelő formátumú elektronikus aláírás összeállítása.
- BF2 (Elektronikus aláírás ellenőrzés): A hash értékek és az elektronikus aláírások ellenőrzése CRL (kötelező), OCSP válasz (opcionális) és időbélyeg (opcionális, ha nincs, akkor az aláírásba foglalt állított idő) felhasználásával.
- BF3 (Tanúsítványlánc ellenőrzése): Tanúsítványláncok ellenőrzése RFC 5280 szerint.
- BF4 (Időbélyeg kezelés): Az időbélyeg kérése és a megszerzett időbélyeg csatolás előtti ellenőrzése RFC 3161-nek megfelelően.
- BF5 (OCSP kezelés): Az OCSP kérése és a megszerzett időbélyeg csatolás előtti ellenőrzése RFC 2560-nak megfelelően.
- BF6 (Megjelenítés): Az aláírandó adatok egyértelmű megjelenítése.
- BF7 (Integritás ellenőrzés): A program manipulálás észlelése.

A biztonsági értékelés az Nlcapi3 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 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 Nlcapi3 egy programozói könyvtár, amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.

Az Nlcapi3 teljes mértékben a Windows operációs rendszer Crypto API-jára támaszkodik, annak használatát leegyszerűsíti. A Crypto API-n keresztül a Microsoft vagy más gyártók CSP-jét használja az aláírás-létrehozó eszköz funkcionalitásának elérésére.

A lenyomatoló eljárások szintén a Crypto API függvényei.

A tanúsítványlánc ellenőrzésére az OpenSSL (v0.9.8i) függvényeit használja.

A jelen értékelési jelentés tárgyát képező MMMEAA_NET.exe tesztprogram egy az Nlcapi3 programozói könyvtárra épülő speciális alkalmazás.

2.3 Alrendszerek

A biztonsági értékelés az Nlcapi3 alábbi alrendszereit vizsgálta:

- AR1: Aláírás készítő alrendszer
- AR2: Aláírás ellenőrző alrendszer
- AR3: Tanúsítvány kezelő alrendszer
- AR4: Megjelenítő alrendszer
- AR5: Tanúsítványlánc ellenőrző alrendszer
- AR6: Titkosító alrendszer
- AR7: Időbélyeg kezelő alrendszer
- AR8: Kulcskezelő alrendszer
- AR9: NLCAPI specifikus alrendszer
- AR10: Hibakezelő alrendszer

A jelen értékelési jelentés tárgyát képező interoperabilitási követelményeket alapvetően az AR1 és AR2 alrendszer juttatja érvényre.

2.4 Az értékelés hatóköre

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

Ez az interoperabilitás vizsgálat elsősorban az alábbi biztonsági funkciókat érinti :

- BF1 és BF2.

Az interoperabilitás vizsgálat elsősorban az alábbi alrendszerre fókuszál:

- AR1 és AR2.

3. Az értékelés jellemzése

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

3.1 Értékelési módszerek

Az Nlcapi3 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 Nlcapi3 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
Nlcapi3 v3.3.1 (build 1) /benne a NLxades modul v2.0.4/	**NetLock Kft.**	**MMMEAA_NET.exe**	**NET**

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
SDX (Signed Document eXpert) 2.2.1	MMMEAA 2009/006	E-Group ICT Software Zrt.	MMMEAA_EGR.exe	EGR
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
A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz v2.2.1	MMMEAA 2009/005	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	a bemenetként megadott XAdES-A formátumú aláírás ellenőrzése,

Teszteset azonosító	Teszteset leíró (és kiegészítő)	megjegyzés
	Archive TimeStamp	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.

NET 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_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.

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 (NET-ARG, NET-EGR, NET-NOR, NET-MIC, NET-POL) 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 (NET-ARG, NET-EGR, NET-NOR, NET-MIC, NET-POL) 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 (NET) teszteltük a Teszt_N1 - Teszt_N13 negatív tesztesetekkel.

Mind a tizenhárom tesztesetben az elvárt eredmény: 2 (sikertelen ellenőrzés).

4. Az értékelés eredményei

Az eredmények és a tesztelés megismételhetőségéhez szükséges környezeti elemek az alábbi könyvtárban találhatók:
NLCAPI\v3.3.1_MIBETS\MR2_IOP\IOP_test_final

Az IOP_test_final alkönyvtár szerkezete az alábbi:

- ARG_NET (az ARG – NET programpár tesztelési eredményei)
- EGR_NET (az EGR – NET programpár tesztelési eredményei)
- MIC_NET (a MIC – NET programpár tesztelési eredményei)
- NOR_NET (a NOR – NET programpár tesztelési eredményei)
- POL_NET (a POL – NET programpár tesztelési eredményei)
- NET_NET (a negatív tesztesetek eredményei)
- Signer.cer (aláíró tanúsítványa)

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

- ARG (az ARG tesztprogram és futtatási környezete)
- NET (az új NET tesztprogram és futtatási környezete)
- log (napló állományok közös könyvtára)
- bemenet.txt, bemenet.xml (a minden tesztesetben közös aláírandó állomány két formátumban)
- out (a tesztelés során előállított állományok könyvtára)
- result.txt (az egyes tesztesetek eredményeit ábrázoló sorok összessége)

A konkrét futási eredményeket tartalmazó result.txt állomány sorainak jelentését az alábbi példa szemlélteti:
2010-03-21_11:39:49 NET_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_ARG_a2a_ 1, ahol:

- 2010-03-21_11:39:49 a teszt lefutásának dátuma és időpontja
- NET_epes01_: 1. lépés: NET meghívásával epes01 aláírás létrehozása
- NET_epes2t_: 2. lépés: NET meghívásával az 1. lépés eredményének ellenőrzése, majd ebből epes2t létrehozása
- NET_t2c1_: 3. lépés: NET 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 az 5 tesztprogrammal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt. Példaképp az ARG-NET eredménye az alábbi:

2010-03-20_20:17:37 ARG_epes01_ 1
2010-03-20_20:17:39 ARG_epes02_ 1
2010-03-20_20:17:40 ARG_epes03_ 1
2010-03-20_20:17:42 ARG_epes04_ 1
2010-03-20_20:17:43 ARG_epes05_ 1
2010-03-20_20:17:47 ARG_epes06_ 1
2010-03-20_20:17:50 ARG_epes09_ 1

2010-03-20_20:17:53 ARG_epes10_ 1
2010-03-20_20:17:54 NET_epes01_ 1
2010-03-20_20:17:55 NET_epes02_ 1
2010-03-20_20:17:56 NET_epes03_ 1
2010-03-20_20:17:56 NET_epes04_ 1
2010-03-20_20:17:57 NET_epes05_ 1
2010-03-20_20:17:58 NET_epes06_ 1
2010-03-20_20:30:37 ARG_epes01_ARG_epes2t_ 1
2010-03-20_20:30:40 ARG_epes02_ARG_epes2t_ 1
2010-03-20_20:30:44 ARG_epes03_ARG_epes2t_ 1
2010-03-20_20:30:48 ARG_epes04_ARG_epes2t_ 1
2010-03-20_20:30:53 ARG_epes05_ARG_epes2t_ 1
2010-03-20_20:31:09 ARG_epes06_ARG_epes2t_ 1
2010-03-20_20:31:13 ARG_epes09_ARG_epes2t_ 1
2010-03-20_20:31:17 ARG_epes10_ARG_epes2t_ 1
2010-03-20_20:31:21 NET_epes01_ARG_epes2t_ 1
2010-03-20_20:31:25 NET_epes02_ARG_epes2t_ 1
2010-03-20_20:31:30 NET_epes03_ARG_epes2t_ 1
2010-03-20_20:31:33 NET_epes04_ARG_epes2t_ 1
2010-03-20_20:31:41 NET_epes05_ARG_epes2t_ 1
2010-03-20_20:31:44 NET_epes06_ARG_epes2t_ 1
2010-03-20_20:31:46 ARG_epes01_NET_epes2t_ 1
2010-03-20_20:31:49 ARG_epes02_NET_epes2t_ 1
2010-03-20_20:31:51 ARG_epes03_NET_epes2t_ 1
2010-03-20_20:31:53 ARG_epes04_NET_epes2t_ 1
2010-03-20_20:31:55 ARG_epes05_NET_epes2t_ 1
2010-03-20_20:32:04 ARG_epes06_NET_epes2t_ 1
2010-03-20_20:32:06 ARG_epes09_NET_epes2t_ 1
2010-03-20_20:32:08 ARG_epes10_NET_epes2t_ 1
2010-03-20_20:32:10 NET_epes01_NET_epes2t_ 1
2010-03-20_20:32:16 NET_epes02_NET_epes2t_ 1
2010-03-20_20:32:18 NET_epes03_NET_epes2t_ 1
2010-03-20_20:32:20 NET_epes04_NET_epes2t_ 1
2010-03-20_20:32:22 NET_epes05_NET_epes2t_ 1
2010-03-20_20:32:24 NET_epes06_NET_epes2t_ 1
2010-03-21_05:23:45 ARG_epes01_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:23:48 ARG_epes02_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:23:51 ARG_epes03_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:23:54 ARG_epes04_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:19 ARG_epes05_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:27 ARG_epes06_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:31 ARG_epes09_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:34 ARG_epes10_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:38 NET_epes01_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:41 NET_epes02_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:44 NET_epes03_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:48 NET_epes04_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:51 NET_epes05_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:55 NET_epes06_ARG_epes2t_ARG_t2c1_ 1
2010-03-21_05:24:59 ARG_epes01_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:04 ARG_epes02_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:08 ARG_epes03_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:12 ARG_epes04_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:16 ARG_epes05_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:28 ARG_epes06_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:33 ARG_epes09_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:40 ARG_epes10_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:47 NET_epes01_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:53 NET_epes02_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:25:57 NET_epes03_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:26:05 NET_epes04_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:26:10 NET_epes05_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:26:16 NET_epes06_NET_epes2t_ARG_t2c1_ 1
2010-03-21_05:34:17 ARG_epes01_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:34:22 ARG_epes02_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:34:28 ARG_epes03_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:34:33 ARG_epes04_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:34:37 ARG_epes05_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:34:51 ARG_epes06_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:34:56 ARG_epes09_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:00 ARG_epes10_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:05 NET_epes01_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:10 NET_epes02_ARG_epes2t_ARG_t2c2_ 1

2010-03-21_05:35:15 NET_epes03_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:19 NET_epes04_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:24 NET_epes05_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:30 NET_epes06_ARG_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:35 ARG_epes01_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:40 ARG_epes02_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:46 ARG_epes03_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:52 ARG_epes04_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:35:57 ARG_epes05_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:09 ARG_epes06_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:16 ARG_epes09_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:23 ARG_epes10_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:29 NET_epes01_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:34 NET_epes02_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:40 NET_epes03_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:46 NET_epes04_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:51 NET_epes05_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:36:59 NET_epes06_NET_epes2t_ARG_t2c2_ 1
2010-03-21_05:41:46 ARG_epes01_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:41:48 ARG_epes02_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:41:49 ARG_epes03_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:41:50 ARG_epes04_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:41:51 ARG_epes05_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:00 ARG_epes06_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:02 ARG_epes09_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:03 ARG_epes10_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:04 NET_epes01_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:05 NET_epes02_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:07 NET_epes03_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:09 NET_epes04_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:10 NET_epes05_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:11 NET_epes06_ARG_epes2t_NET_t2c2_ 1
2010-03-21_05:42:13 ARG_epes01_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:14 ARG_epes02_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:15 ARG_epes03_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:16 ARG_epes04_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:18 ARG_epes05_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:31 ARG_epes06_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:32 ARG_epes09_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:33 ARG_epes10_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:35 NET_epes01_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:36 NET_epes02_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:37 NET_epes03_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:38 NET_epes04_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:40 NET_epes05_NET_epes2t_NET_t2c2_ 1
2010-03-21_05:42:41 NET_epes06_NET_epes2t_NET_t2c2_ 1
2010-03-21_08:31:12 ARG_epes01_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:13 ARG_epes02_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:13 ARG_epes03_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:14 ARG_epes04_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:15 ARG_epes05_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:25 ARG_epes06_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:26 ARG_epes09_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:27 ARG_epes10_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:28 NET_epes01_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:29 NET_epes02_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:29 NET_epes03_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:30 NET_epes04_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:31 NET_epes05_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:32 NET_epes06_ARG_epes2t_NET_t2c1_ 1
2010-03-21_08:31:33 ARG_epes01_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:34 ARG_epes02_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:34 ARG_epes03_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:35 ARG_epes04_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:36 ARG_epes05_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:45 ARG_epes06_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:46 ARG_epes09_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:47 ARG_epes10_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:47 NET_epes01_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:48 NET_epes02_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:49 NET_epes03_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:50 NET_epes04_NET_epes2t_NET_t2c1_ 1
2010-03-21_08:31:51 NET_epes05_NET_epes2t_NET_t2c1_ 1

2010-03-21_08:31:52 NET_epes06_NET_epes2t_NET_t2c1_ 1

4.4.2 A páronkénti To_a tesztelés eredményei

Mind az 5 tesztprogrammal az összes eredmény az elvárt 1-es (sikeres ellenőrzés) volt. Példaképp az ARG-NET eredménye az alábbi:

2010-03-21_08:32:17 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:21 NET_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:25 ARG_epes01_NET_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:29 NET_epes01_NET_epes2t_ARG_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:33 ARG_epes01_ARG_epes2t_NET_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:37 NET_epes01_ARG_epes2t_NET_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:41 ARG_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:44 NET_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_ 1
2010-03-21_08:32:46 ARG_epes01_ARG_epes2t_ARG_t2c1_NET_c2a1_ 1
2010-03-21_08:32:48 NET_epes01_ARG_epes2t_ARG_t2c1_NET_c2a1_ 1
2010-03-21_08:32:50 ARG_epes01_NET_epes2t_ARG_t2c1_NET_c2a1_ 1
2010-03-21_08:32:52 NET_epes01_NET_epes2t_ARG_t2c1_NET_c2a1_ 1
2010-03-21_08:32:53 ARG_epes01_ARG_epes2t_NET_t2c1_NET_c2a1_ 1
2010-03-21_08:32:55 NET_epes01_ARG_epes2t_NET_t2c1_NET_c2a1_ 1
2010-03-21_08:32:57 ARG_epes01_NET_epes2t_NET_t2c1_NET_c2a1_ 1
2010-03-21_08:32:59 NET_epes01_NET_epes2t_NET_t2c1_NET_c2a1_ 1
2010-03-21_08:39:43 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-21_08:39:50 NET_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:01 ARG_epes01_NET_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:08 NET_epes01_NET_epes2t_ARG_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:18 ARG_epes01_ARG_epes2t_NET_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:25 NET_epes01_ARG_epes2t_NET_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:37 ARG_epes01_NET_epes2t_NET_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:44 NET_epes01_NET_epes2t_NET_t2c2_ARG_c2a2_ 1
2010-03-21_08:40:48 ARG_epes01_ARG_epes2t_ARG_t2c2_NET_c2a2_ 1
2010-03-21_08:40:51 NET_epes01_ARG_epes2t_ARG_t2c2_NET_c2a2_ 1
2010-03-21_08:40:56 ARG_epes01_NET_epes2t_ARG_t2c2_NET_c2a2_ 1
2010-03-21_08:41:00 NET_epes01_NET_epes2t_ARG_t2c2_NET_c2a2_ 1
2010-03-21_08:41:04 ARG_epes01_ARG_epes2t_NET_t2c2_NET_c2a2_ 1
2010-03-21_08:41:08 NET_epes01_ARG_epes2t_NET_t2c2_NET_c2a2_ 1
2010-03-21_08:41:12 ARG_epes01_NET_epes2t_NET_t2c2_NET_c2a2_ 1
2010-03-21_08:41:15 NET_epes01_NET_epes2t_NET_t2c2_NET_c2a2_ 1
2010-03-21_11:38:46 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:38:51 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:38:55 NET_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:00 NET_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:04 ARG_epes01_NET_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:11 ARG_epes01_NET_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:15 NET_epes01_NET_epes2t_ARG_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:20 NET_epes01_NET_epes2t_ARG_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:24 ARG_epes01_ARG_epes2t_NET_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:29 ARG_epes01_ARG_epes2t_NET_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:33 NET_epes01_ARG_epes2t_NET_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:37 NET_epes01_ARG_epes2t_NET_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:41 ARG_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:45 ARG_epes01_NET_epes2t_NET_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:49 NET_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_ARG_a2a_ 1
2010-03-21_11:39:53 NET_epes01_NET_epes2t_NET_t2c2_ARG_c2a2_ARG_a2a_ 1
2010-03-21_11:39:57 ARG_epes01_ARG_epes2t_ARG_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:02 ARG_epes01_ARG_epes2t_ARG_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:06 NET_epes01_ARG_epes2t_ARG_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:11 NET_epes01_ARG_epes2t_ARG_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:15 ARG_epes01_NET_epes2t_ARG_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:20 ARG_epes01_NET_epes2t_ARG_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:25 NET_epes01_NET_epes2t_ARG_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:29 NET_epes01_NET_epes2t_ARG_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:33 ARG_epes01_ARG_epes2t_NET_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:37 ARG_epes01_ARG_epes2t_NET_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:41 NET_epes01_ARG_epes2t_NET_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:45 NET_epes01_ARG_epes2t_NET_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:49 ARG_epes01_NET_epes2t_NET_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:40:54 ARG_epes01_NET_epes2t_NET_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:40:58 NET_epes01_NET_epes2t_NET_t2c1_NET_c2a1_ARG_a2a_ 1
2010-03-21_11:41:05 NET_epes01_NET_epes2t_NET_t2c2_NET_c2a2_ARG_a2a_ 1
2010-03-21_11:41:08 ARG_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_NET_a2a_ 1

2010-03-21_11:41:10 ARG_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:12 NET_epes01_ARG_epes2t_ARG_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:14 NET_epes01_ARG_epes2t_ARG_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:16 ARG_epes01_NET_epes2t_ARG_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:19 ARG_epes01_NET_epes2t_ARG_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:21 NET_epes01_NET_epes2t_ARG_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:23 NET_epes01_NET_epes2t_ARG_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:26 ARG_epes01_ARG_epes2t_NET_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:28 ARG_epes01_ARG_epes2t_NET_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:30 NET_epes01_ARG_epes2t_NET_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:32 NET_epes01_ARG_epes2t_NET_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:34 ARG_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:37 ARG_epes01_NET_epes2t_NET_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:39 NET_epes01_NET_epes2t_NET_t2c1_ARG_c2a1_NET_a2a_ 1
2010-03-21_11:41:41 NET_epes01_NET_epes2t_NET_t2c2_ARG_c2a2_NET_a2a_ 1
2010-03-21_11:41:43 ARG_epes01_ARG_epes2t_ARG_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:41:46 ARG_epes01_ARG_epes2t_ARG_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:41:48 NET_epes01_ARG_epes2t_ARG_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:41:50 NET_epes01_ARG_epes2t_ARG_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:41:52 ARG_epes01_NET_epes2t_ARG_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:41:55 ARG_epes01_NET_epes2t_ARG_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:41:57 NET_epes01_NET_epes2t_ARG_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:41:59 NET_epes01_NET_epes2t_ARG_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:42:01 ARG_epes01_ARG_epes2t_NET_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:42:04 ARG_epes01_ARG_epes2t_NET_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:42:06 NET_epes01_ARG_epes2t_NET_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:42:08 NET_epes01_ARG_epes2t_NET_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:42:10 ARG_epes01_NET_epes2t_NET_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:42:13 ARG_epes01_NET_epes2t_NET_t2c2_NET_c2a2_NET_a2a_ 1
2010-03-21_11:42:15 NET_epes01_NET_epes2t_NET_t2c1_NET_c2a1_NET_a2a_ 1
2010-03-21_11:42:17 NET_epes01_NET_epes2t_NET_t2c2_NET_c2a2_NET_a2a_ 1

4.4.3 A negatív tesztelés eredményei

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

2010-04-06_19:29:59 NEG_N2_NET_t2c2_ 2
2010-04-06_19:29:59 NEG_N3_NET_c2a1_ 2
2010-04-06_19:30:00 NEG_N4_NET_c2a1_ 2
2010-04-06_19:30:04 NEG_N5_NET_c2a1_ 2
2010-04-06_19:30:04 NEG_N6_NET_c2a1_ 2
2010-04-06_19:30:05 NEG_N7_NET_c2a1_ 2
2010-04-06_19:30:05 NEG_N8_NET_x2a1_ 2
2010-04-06_19:30:06 NEG_N9_NET_x2a2_ 2
2010-04-06_19:30:07 NEG_N10_NET_a2a_ 2

4.4.4 A tesztprogram és a termék összehasonlításának eredménye

A vizsgált tesztprogram: MMMEAA_NET.exe (v0.7.37a - NLSXades v2.6.6 (w/ NetLock Xades modul v2.0.4)

A forgalmazott termék: Nlcapi3 v3.3.1 (build 1) /benne az NLxades modul v2.0.4/

A két program együttműködési képessége megegyezik, mert az MMMEAA_NET.exe (mint alkalmazás) NLxades modulja megegyezik a biztonsági szempontból értékelt és tanúsított Nlcapi3 v3.3.1 (build 1) NLxades moduljával (v2.0.4), s a biztonsági értékelés keretében elvégzett forráskód elemzés megerősítette, hogy a XAdES formátumok kezelésében kizárólag az NLxades modul függvényei vesznek részt.

5. Következtetések és javaslatok

5.1 Az értékelés összefoglaló eredménye

Az értékelés fő következtetései az alábbiak:

1. A Netlock Kft. által kifejlesztett MMMEAA_NET.exe elektronikus aláírás termék megfelel az [1]-ben az egységes MELASZ formátumokra meghatározott interoperabilitási követelményeknek.
2. A Netlock Kft.által kifejlesztett Nlcapi3 v3.3.1 (build 1) programozói függvény könyvtár), valamint az interoperabilitás tesztelésen bevizsgált MMMEAA_NET.exe (v0.7.37a - NLSXades v2.6.6 (w/ NetLock Xades modul v2.0.4) alkalmazás együttműködési képessége megegyezik.

5.2 Javaslatok

1. A Hunguard kft. (mint értékelő szervezet) vizsgálati eredményei alapján javasolja a Magyar Elektronikus Aláírás Szövetségnek (mint tanúsító szervezetnek) egy új tanúsítványt (MMMEAA 2010/001 számmal) kibocsátani az alábbi verzióra:
   - Nlcapi3 v3.3.1 (build 1) (benne az NLxades modul v2.0.4)
2. Javasoljuk továbbá, hogy a jövőben az egységes MELASZ formátumra kiadott tanúsítványok 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, v0.6)

[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