TANÚSÍTÁSI JELENTÉS

NCA TWS v2.6.0
NCA megbízható rendszer hitelesítés-szolgáltatáshoz

HUNG-TJ-37-2007

Verzió:	1.0
Fájl:	HUNG_TJ_36_2007_v10.doc
Minősítés:	Nyilvános
Oldalak:	41

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2007.08.06	A szerkezet felállítása
v0.8	2007.08.14	A tanúsítás eredményeit tartalmazó teljes változat
v0.81	2007.08.16	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v0.9	2007.08.24	Utolsó egyeztetésre kiadott változat
v1.0	**2007.08.27**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 ÖSSZEFOGLALÓ 4
1.1 AZ ÉRTÉKELÉS JELLEMZŐI 4
2 AZONOSÍTÁS 6
3 BIZTONSÁGI SZABÁLYZAT 7
3.1 ÜZEMMÓDOK 7
3.2 BIZTONSÁGI FUNKCIÓK 7
4 FELTÉTELEZÉSEK ÉS HATÓKÖR 10
4.1 FELTÉTELEZÉSEK AZ NCA V2.6.0 INFORMATIKAI KÖRNYEZETÉRE 10
4.1.1 Személyi feltételek 10
4.1.2 Kapcsolódási feltételek 10
4.1.3 Fizikai feltételek 11
4.2 A BIZTONSÁGOS FELHASZNÁLÁS EGYÉB FELTÉTELEI 11
4.2.1 MSZ CWA 14167-1 követelményeknek való megfelelés 11
4.3 AZ ÉRTÉKELÉS HATÓKÖRE 12
5 AZ NCA V2.6.0 SZERKEZETI LEÍRÁSA 13
5.1 ARCHITEKTÚRA 14
5.2 ALRENDSZEREK 16
6 DOKUMENTÁCIÓ 17
7 TESZTELÉS 18
7.1 A FEJLESZTŐK TESZTELÉSE 18
7.2 AZ ÉRTÉKELŐK TESZTELÉSE 18
8 AZ ÉRTÉKELT KONFIGURÁCIÓ 19
8.1 SZERVER 19
8.2 KLIENS 19
9 AZ ÉRTÉKELÉS EREDMÉNYEI 20
10 ÉRTÉKELŐI MEGJEGYZÉSEK ÉS JAVASLATOK 23
11 MELLÉKLETEK 24
11.1 AZ NCA V2.6.0 MEGFELELÉSE AZ MSZ CWA-14167-1:2006 KÖVETELMÉNYEINEK 24
11.2 A PROTECT SERVER ORANGE (CSA8000) HASZNÁLATA AZ NCA RENDSZERREL 33
11.3 A TANÚSÍTOTT TERMÉKEK LISTÁJÁBA JAVASOLT SZÖVEG 35
12 BIZTONSÁGI ELŐIRÁNYZAT 36
13 FOGALMAK ÉS RÖVIDÍTÉSEK 37
13.1 FOGALMAK 37
13.2 RÖVIDÍTÉSEK 39
14 FELHASZNÁLT DOKUMENTUMOK 40
14.1 A TANÚSÍTÁSHOZ FELHASZNÁLT KIINDULÓ DOKUMENTUMOK 40
14.2 AZ ÉRTÉKELÉSHEZ FELHASZNÁLT FEJLESZTŐI BIZONYÍTÉKOK 40
14.3 AZ ÉRTÉKELÉSHEZ FELHASZNÁLT MÓDSZERTANI ANYAGOK 41
14.4 AZ ÉRTÉKELÉSHEZ FELHASZNÁLT EGYÉB DOKUMENTUMOK 41

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**NCA TWS megbízható rendszer hitelesítés-szolgáltatáshoz v2.6.0**
Verzió szám:	**v2.6.0**
Rövid elnevezés:	**NCA v2.6.0 vagy NCA rendszer**
Az értékelt termék típusa:	Megbízható rendszer hitelesítés-szolgáltatáshoz
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2007. augusztus 06.
Az értékelés módszere:	CEM, Common Evaluation Methodology, v2.3
Az értékelés garanciaszintje:	EAL4 (ALC_FLR.2, Hibajavítási eljárások garanciaosztállyal kibővítve)
Az értékelt termék funkcionalitása:	Az NCA rendszer v2.6.0 a meghívó alkalmazásoktól szolgáltatási üzeneteket, parancsokat fogad, azokat (amennyiben erre szükség van) jogosultságellenőrzés alá veti, majd végrehajtja. Az alábbi hitelesítés-szolgáltatásokat támogatja: Alap szolgáltatások (minden üzemmód része): • Regisztráció szolgáltatás, • Tanúsítvány előállítás szolgáltatás, • Tanúsítvány szétosztás szolgáltatás, • Visszavonás kezelés szolgáltatás (CRL, OCSP), • Visszavonás állapot szolgáltatás. Kiegészítő szolgáltatások (egyes üzemmódok része): • időbélyegzés szolgáltatás, • általános aláírás szolgáltatás (GSU), • titkosító magánkulcs letétbe helyezése szolgáltatás, • titkosító magánkulcs helyreállítása szolgáltatás.
Konfigurációs követelmények:	**Szerver** szoftver konfigurációk: Operációs rendszer: Solaris 9 Adatbázis kezelő: mysql 4.0.27 with innodb HSM middleware: Cprov 3.10 Operációs rendszer: Slackware 10.1 Adatbázis kezelő: mysql 4.0.27 with innodb HSM middleware: Cprov 3.10 Slackware Ntpd 4.2.0a@1.11.96-r Operációs rendszer: Windows XP Sp2 Adatbázis kezelő: MSACCES 2003 HSM middleware: Cprov 3.10 NTPd: 4.2.0.a@mbg-fluxcap-v2-beta-o ProtectServer Orange (Eracom CSA 8000) (Hardware 71.00 (G))

Kliens szoftver konfigurációk:

Operációs rendszer: Windows XP SP2;
perl 5.8.x; IIS 5.1

Operációs rendszer: Solaris 9;
myodbc: 3.51.11; unixodbc 2.2.12; perl 5.8.x
apache 1.3.29

Operációs rendszer: Slackware 10.1
myodbc: 3.51.11; unixodbc 2.2.12; perl 5.8.x
apache 1.3.29

2 Azonosítás

Az értékelt termék neve:	**NCA TWS megbízható rendszer hitelesítés-szolgáltatáshoz v2.6.0**
Verzió szám:	**v2.6.0**
Az értékelt termék alkotó elemei:	• ncaadm 2.6.0 build 1985 • ncatools: 2.6.0 build 129 • ncacllib.so 2.6.0 std build 321 • ncacllib.so 2.6.0 full build 321 • Dokumentáció: o NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – KLIENS OLDALI FÜGGVÉNYEK ÉS KONZOLPARANCSOK v1.0 o NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz –A KONFIGURÁCIÓS ÁLLOMÁNYOK SZERKEZETE v1.0

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az NCA v2.6.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást. Először az NCA v2.6.0 két tanúsított üzemmódját határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmódok

Jelen tanúsítási jelentés az NCA v2.6.0 két üzemmódjára korlátozódik:
CWA üzemmód: az nca.lic konfigurációs állományban a `CWAMode` paraméter 1 értéket vesz fel. Így az NCA v2.6.0 üzemeltetése során az MSZ CWA 14167-1:2006 követelményrendszer szerinti üzemmódban működik.
Minősített üzemmód: az nca.lic konfigurációs állományban a `CWAMode` és `QualifiedMode` paraméterek 1 értéket vesznek fel. Így az NCA v2.6.0 üzemeltetése során az MSZ CWA 14167-1:2006 követelményrendszerben szereplő minősített hitelesítés-szolgáltatók szerinti üzemmódban működik.

3.2 Biztonsági funkciók

Az NCA v2.6.0 rendszer az alábbi 13 biztonsági funkciót (BF) valósítja meg:

Általános (szolgáltatásoktól független) biztonsági funkciók:
- BF1: Bizalmi munkakörök kezelése
- BF2: Időszinkronizálás
- BF3: Azonosítás és hitelesítés
- BF4: Hozzáférés ellenőrzés
- BF5: Kulcskezelés és kriptográfiai műveletek
- BF6: Biztonsági naplózás
- BF7: Mentés és helyreállítás
- BF8: Archiválás

Az egyes szolgáltatásokra vonatkozó biztonsági funkciók
- BF9: Távoli adatbevitel és export
- BF10: Tanúsítvány előállítás
- BF11: Visszavonás kezelés
- BF12: Visszavonás állapot
- BF13: Időbélyegzés

A **BF1** (**Bizalmi munkakörök kezelése) biztonsági funkció** az alábbi munkaköröket különbözteti meg: biztonsági adminisztrátor (ncasa), rendszeradminisztrátor (ncaroot), rendszerüzemeltető (ncaop), rendszervizsgáló (ncaau), tisztviselők (ncara, ncaca, ncakr), általános aláíró (gsu), ügyfél (ncauser), érintett fél (anonymous). Összekapcsolja a felhasználókat a fenti munkakörökkel, valamint egységesen és biztonságosan kezeli a különböző munkakörökhöz tartozó jogosultságokat.

A **BF2** (**Időszinkronizálás) biztonsági funkció** üzembiztos és pontos időt garantál az NCA rendszer időkritikus szolgáltatásaihoz. Az informatikai környezet szinkronizált független időforrásaira ellenőrzi, hogy annak az UTC-től való maximális eltérése a konfigurálható határon belül van-e. Ha igen, akkor ezt a rendszeridőt elfogadja, ha nem, akkor leállít minden időkritikus hitelesítés-szolgáltatást.

A **BF3 (Azonosítás és hitelesítés) biztonsági funkció** egyértelműen és hitelesen azonosítja a jogosult felhasználókat, majd összekapcsolja velük biztonsági jellemzőiket (pl. munkakörök, jogosultságok). Ezenkívül kezeli a hitelesítési hibákat, megnehezítve a további hitelesítési kísérleteket, ha a sikertelen hitelesítési kísérletek száma elér egy maximumként meghatározott értéket. Végül ellenőrzi, hogy a jelszó alapú hitelesítésben használt titkok (jelszavak) megfelelnek-e az erre meghatározott követelményeknek.

A **BF4 (Hozzáférés ellenőrzés) biztonsági funkció** ellenőrzi és korlátozza a védendő értékekhez való hozzáféréseket. A rendszer-, illetve felhasználói objektumokhoz való minden hozzáférést ellenőriz, s az előzetesen azonosított és hitelesített felhasználóknak kizárólag az általuk betöltött munkakörnek megfelelő hozzáféréseket engedélyezi.

A **BF5 (Kulcskezelés és kriptográfiai műveletek) biztonsági funkció** biztonságosan kezeli az NCA rendszer által használt különböző (tanúsítvány és CRL aláíró, infrastrukturális, rendszervezérlési és végfelhasználói) kulcsokat. Ez magában foglalja a magánkulcsok HSM-ből való exportálását, illetve helyreállítását, a kulcsok aktivizálását (kriptográfiai műveletek végzése), valamint a nyilvános kulcsok védelmét.

A **BF6 (Biztonsági naplózás) biztonsági funkció** biztosítja a biztonsági szempontból fontos tevékenységek egyértelmű nyomon követhetőségét, megteremtve a teljes körű ellenőrzés lehetőségét. E biztonsági funkció megfelelő adatokkal napló adatokat generál, biztosítja a napló adatok rendelkezésre állását és sértetlenségét, a naplózandó adatok kiválasztását és a napló jogosult áttekintését, valamint a biztonság potenciális megsértésének észlelése esetén a rendszeradminisztrátor számára riasztást generál.

A **BF7 (Mentés és helyreállítás) biztonsági funkció** biztosítja az üzemmenet folytonosságát és az adatvesztés elkerülését, a rendszeres mentések elvégezhetőségével, a mentési információ sértetlenségének és bizalmasságának megőrzésével, valamint az informatikai rendszer szükség esetén megvalósítható helyreállításával.

A **BF8 (Archiválás) biztonsági funkció** biztosítja a hosszú távon megőrzendő, de a napi működéshez nem szükséges információk rendszer felügyelet alól való kivételét, szükség esetén visszatöltését, egyúttal megvédi az archivált állományok sértetlenségét és (ahol ez szükséges) bizalmasságát, valamint lehetővé teszi az egyes adatok visszakereshetőségét.

A **BF9 (Távoli adatbevitel és export) biztonsági funkció** biztosítja az NCA rendszernek távolról beküldött adatok, valamint a rendszerből kikerülő adatok sértetlenségét, hitelességét és bizalmasságát. Ellenőrzi a hitelesség szempontjából kritikus bejövő üzenetek eredetét, illetve biztosítja az ilyen kimenő üzenetek eredet bizonyításának a lehetőségét, valamint védi az NCA rendszer belső (a szerver és kliens közötti) adatkommunikációját is.

A **BF10 (Tanúsítvány előállítás) biztonsági funkció** biztosítja az NCA rendszer alap szolgáltatásai közé tartozó, kezdeti tanúsítvány előállításra, megújításra és felülhitelesítésre irányuló jogosult kérelmek biztonságos végrehajtását. A tanúsítvány előállítás mindhárom esete tanúsítvány profilokon alapul, s e biztonsági funkció garantálja, hogy a kiadott tanúsítványok megfelelnek valamelyik profilnak.

A **BF11 (Visszavonás kezelés) biztonsági funkció** biztosítja az NCA rendszer alap szolgáltatásai közé tartozó, tanúsítvány felfüggesztésre, felfüggesztés megszüntetésre és tanúsítvány visszavonásra irányuló jogosult kérelmek biztonságos végrehajtását. E biztonsági funkció frissíti a tanúsítvány állapot adatbázist, mely más szolgáltatás (OCSP, CRL) számára is elérhető.

A **BF12 (Visszavonás állapot) biztonsági funkció** biztosítja a Visszavonás kezelés biztonsági funkció által módosított tanúsítvány állapotok lekérdezhetőségét, megismerhetőségét. E biztonsági funkció támogatja mind a CRL alapú, mind az OCSP alapú visszavonás állapot szolgáltatást. Mindkét szolgáltatás közvetlenül az éles tanúsítvány állapot adatbázis alapján működik.

A **BF13 (Időbélyegzés) biztonsági funkció** az RFC 3161 szabványnak megfelelő időbélyegzést biztosít, az alábbi paraméterekkel: az időbélyeg kérésekben csak az SHA1 algoritmust fogadja el, a kibocsátott időbélyeg válaszok tartalmaznak egy egyedi sorszámot, a használt időforrás pontosságát és az alkalmazott időbélyegzési szabályzat (rend) azonosítóját.

4 Feltételezések és hatókör

A tanúsítás pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

- a biztonsági előirányzat feltételezései (az informatikai környezetre vonatkozó feltételek),
- a biztonságos felhasználás egyéb feltételei.

4.1 Feltételezések az NCA v2.6.0 informatikai környezetére

Az alábbi (a biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

4.1.1 Személyi feltételek

1. A biztonság-kritikus eseményekről naplóbejegyzés készül, s ezeket a rendszervizsgáló átvizsgálja. (A.Auditors Review Audit Logs)
2. A TOE működési környezetében érvényben van egy olyan hitelesítési adat (jelszó és PIN kód) kezelésre vonatkozó szabályzat, melynek betartásával a felhasználók hitelesítési adataikat megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtatják. (A.Authentication Data Management)
3. Szakértő rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók vannak kijelölve a TOE és az általa tartalmazott információk biztonságának kezelésére. (A.Competent Administrators, Operators, Officers and Auditors)
4. Minden rendszeradminisztrátor, rendszerüzemeltető, tisztviselő és rendszervizsgáló jól ismeri azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. (A.CPS)
5. A hitelesítési adatokat és az ezekhez tartozó jogosultságokat eltávolítják, miután a hozzáférési jogosultság megszűnt (pl. munkahely vagy munkakör változás következtében). (A.Disposal of Authentication Data)
6. A TOE számára küldött rosszindulatú futtatható kódot nem írja alá egy megbízható entitás. (A.Malicious Code Not Signed)
7. A rendszeradminisztrátoroknak, a rendszerüzemeltetőknek, a tisztviselőknek, a rendszervizsgálóknak és az egyéb felhasználóknak értesíteniük kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében. (A.Notify Authorities of Security Issues)
8. Az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók képzettek a "social engineering" típusú támadások megakadályozási technikáiban. (A.Social Engineering Training)
9. A felhasználóknak néhány olyan feladatot vagy feladatcsoportot is végre kell hajtani, amelyek biztonságos IT környezetet igényelnek. A felhasználóknak a TOE által kezelt információk közül legalább néhányhoz hozzá kell férniük, egyúttal feltételezzük, hogy a felhasználók együttműködő módon tevékenykednek. (A.Cooperative Users)

4.1.2 Kapcsolódási feltételek

10. Az operációs rendszer úgy kerül kiválasztásra, hogy az rendelkezik a TOE által elvárt azon funkciókkal, melyek a biztonsági előirányzat 3.3 alfejezetében meghatározott fenyegetések kivédéséhez szükségesek. (A.Operating System)

4.1.3 Fizikai feltételek

11. A rendszer megfelelő fizikai védelemmel van ellátva a kommunikáció elvesztésével, azaz a kommunikáció rendelkezésre állásának elvesztésével szemben. (A.Communication Protection)
12. A TOE azon hardver, szoftver és förmver elemei, amelyek létfontosságúak a TOE biztonsági politikája (TSP) érvényre juttatásához, védve vannak a jogosulatlan fizikai módosításokkal szemben. (A.Physical Protection)

4.2 A biztonságos felhasználás egyéb feltételei

4.2.1 MSZ CWA 14167-1 követelményeknek való megfelelés

Az NCA v2.6.0 rendszerre (mint „megbízható rendszer hitelesítés-szolgáltatáshoz" elektronikus aláírási termékre) az alábbi nemzetközi követelményrendszer is vonatkozik, mely egyúttal magyar szabvány is:

- CEN Workshop Agreement 14167-1:2003 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements /June 2003/,
- MSZ CWA 14167-1:2006 - Elektronikus aláírások tanúsítványait kezelő megbízható rendszerek biztonsági követelményei - 1. rész: Rendszerbiztonsági követelmények

A fenti dokumentumban megfogalmazott funkcionális és biztonsági követelmények egy részét az NCA v2.6.0 rendszer biztosítja (azaz teljes mértékben megfelel a követelménynek), egy másik részét pedig támogatja (azaz részben megfelel a követelménynek).

A követelmények egy harmadik csoportjában az NCA v2.6.0 rendszer a megvalósítást az IT és nem IT környezettől várja el (azaz nem vállalja fel a követelmény teljesítését).

Az MSZ CWA 14167-1 követelményeknek való megfelelést a 11.1 fejezet részletezi.

Érvényességi feltételek:

1. Minősített hitelesítés-szolgáltatás esetén csak az alábbi üzemmódok lehetnek bekonfigurálva: CWAmode=1, QualifiedMode=1 és CertificateMode= sign.
2. Nem minősített, de az elektronikus törvény hatálya alá tartozó szolgáltatás esetén csak az alábbi üzemmódok lehetnek bekonfigurálva: CWAmode=1, QualifiedMode=0 és CertificateMode= sign.
3. Az IT környezetnek (a független időforrások és szinkronizáló program biztosításával) támogatnia kell a megbízható időpont előállítását.
4. Minősített hitelesítés-szolgáltatás és időbélyeg szolgáltatás esetén az IT környezetnek a megbízható időpontot szinkronizálnia kell a Co-ordinated Universal Time (UTC) egy másodperces időtartamán belüli értékhez.
5. Az IT környezet biztosítsa a megfelelő HSM modul (pl. ProtectServer Orange) használatát, illetve a HSM modul tanúsításakor meghatározott felhasználási feltételek betartását.
6. Az IT környezetnek megbízható csatornát kell biztosítania a távoli felhasználók és az NCA rendszer között (pl. a távoli felhasználók számára elérhető webszervernek SSL kapcsolat kiépítését kell kikényszerítenie).
7. Az IT környezet biztosítsa a hitelesítés-szolgáltató által kiadott tanúsítvány helyességének garantálása céljából a gyökértanúsítvány lenyomatának ellenőrizhetőségét, egy megbízható útvonalon biztosított információ megadásával.

8. Az infrastrukturális és rendszervezérlési kulcsok éves cseréjét IT és nem IT eljárásokkal ellenőrizni kell.
9. A hitelesítés-szolgáltatóhoz eljuttatott tanúsítvány kérelmekben megadott adatok megbízható ellenőrzéséhez IT és nem IT eljárásokat kell foganatosítani.
10. Az NCA rendszerben alkalmazott státuszváltásoknak összhangban kell lenniük a hitelesítés-szolgáltató szabályrendszerével.
11. Az NCA rendszer használata során biztosítani kell a megfelelő tanúsítvány profilok kizárólagos használatát.
12. Minősített hitelesítés-szolgáltatás esetén a szolgáltató tanúsítványának Tulajdonos mezőjében szerepelni kell országkódnak.
13. A hitelesítés-szolgáltatatónak gondoskodnia kell arról, hogy a visszavonásra és/vagy felfüggesztésre vonatkozó kérelmeket és jelentéseket úgy dolgozza fel, hogy a tanúsítvány állapot információban bekövetkező változás között eltelt maximális idő ne lépje túl a 24 órát.
14. Időszakonként az NCA rendszerben alkalmazott algoritmusokról ellenőrizni kell, hogy azok megfelelnek-e az ETSI TS 102 176-1 dokumentumban meghatározott követelményeknek.
15. IT és nem IT eljárásokat kell foganatosítani az alábbi követelmények teljesüléséhez: [SO2.1]; [SO2.2]; [SO2.3]; [KM1.3]; [KM2.4]; [KM3.1]; [KM5.1]; [KM5.2]; [KM5.3]; [KM6.3]; [KM6.6]; [CG2.3]; [RM1.4]; [RM2.1]; [TS2.2]; [TS4.2]

4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az NCA v2.6.0 valamennyi biztonsági funkcióját.

5 Az NCA v2.6.0 szerkezeti leírása

Az NCA v2.6.0 (NCA rendszer) olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Az NCA rendszer v2.6.0 a meghívó alkalmazásoktól szolgáltatási üzeneteket, parancsokat fogad, azokat (amennyiben erre szükség van) jogosultságellenőrzés alá veti, majd végrehajtja. Az alábbi hitelesítés-szolgáltatásokat támogatja:

Alap szolgáltatások (minden üzemmód része):

- Regisztráció szolgáltatás,
- Tanúsítvány előállítás szolgáltatás,
- Tanúsítvány szétosztás szolgáltatás,
- Visszavonás kezelés szolgáltatás (CRL, OCSP),
- Visszavonás állapot szolgáltatás.

Kiegészítő szolgáltatások (egyes üzemmódok része):

- időbélyegzés szolgáltatás,
- általános aláírás szolgáltatás (GSU),
- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás.

Az NCA rendszer képes a tanúsítvány kibocsátásra vonatkozó kérelmeket a konfigurációjában meghatározott ellenőrzések és folyamatvezérlési utasítások alapján emberi beavatkozás segítségével vagy anélkül végrehajtani. Képes kezelni a kérelmek, majd később tanúsítványok teljes életciklusát, a kérelem bejelentésétől (előkérelem), a kulcsgeneráláson, az ellenőrzött tanúsítványban szereplő adatok összeállításán (előtanúsítvány) keresztül a tanúsítvány kiadásáig, valamint a tanúsítvány felfüggesztéséig, visszavonásáig. Képes pontos információkat adni (pl. statisztikák, egyedi státuszok és információk) az életciklus különböző szakaszaiban a kezelőknek, vizsgálóknak, valamint a külvilágnak, ember által (HTML lapok, elektronikus levelek), valamint gépek által értelmezhető formákban (pl. CRL, OCSP vagy akár egyedi protokollok).

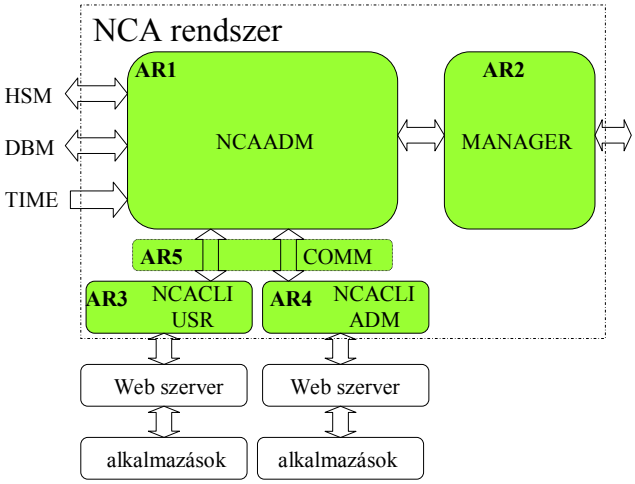
Az NCA rendszer napló állományai biztosítják a teljes körű ellenőrzést, a tevékenységek nyomon követhetőségét.

Az NCA rendszer széleskörűen konfigurálható és biztosítja a futó szolgáltatások monitorozhatóságát.

Alkalmas különböző PKCS#11-es interfészen keresztül elérhető HSM modulok aktivizálására, s ezen keresztül a kriptográfiai funkciók végrehajttatására. A tanúsított konfigurációkban a HSM kizárólag az alábbi hardver kriptográfiai modul: ProtectServer Orange (korábbi nevén Eracom CSA 8000).

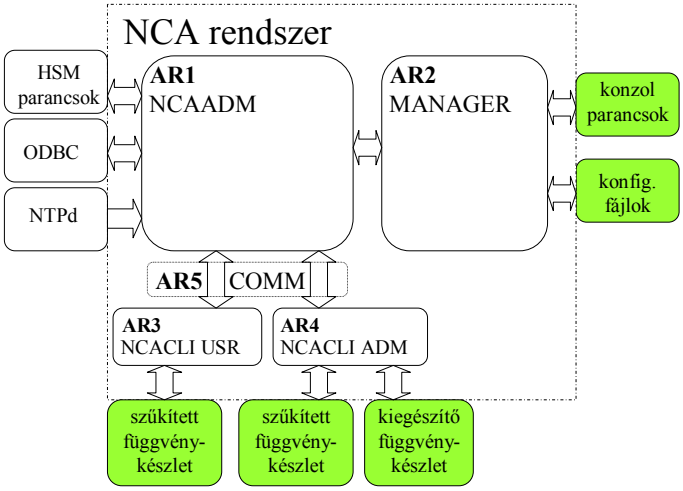
5.1 Architektúra

Az NCA rendszer logikai felépítését, alrendszereit és interfészeit, egyúttal az értékelés tárgya és az informatikai környezet határát mutatja be az 1. ábra. Az ábrán szaggatott vonal jelzi az értékelés hatókörébe eső komponenseket.



1 ábra Az NCA v2.6.0 és környezete

A 2. ábra a (kívülről is látható) külső interfészeket azonosítja, szemlélteti:



2. ábra: Az NCA rendszer külső interfészei

Az **NCACLI USR** felhasználói kliens **szűkített függvénykészlet**ének meghívásán keresztül az érintett felek és az ügyfelek szabadon elérhetik az NCA rendszer alábbi szolgáltatásait:

- keresés a tanúsítványtárban,
- időbélyeg kérés,
- OCSP kérés,
- CRL letöltés,

azonosítás és hitelesítés után pedig az NCA rendszer alábbi szolgáltatásait is elérik:

- regisztrációs adatok felvétele, módosítása,
- tanúsítvány igénylés,
- visszavonás kezelés szolgáltatás (tanúsítvány felfüggesztés és visszavonás).

Az **NCACLI ADM** adminisztrátori kliens **szűkített függvénykészlet**ének meghívásán keresztül a belső felhasználók szabadon elérhetik az NCA rendszer alábbi szolgáltatásait:

- keresés a tanúsítványtárban,
- időbélyeg kérés,
- OCSP kérés,
- CRL letöltés,

azonosítás és hitelesítés után az NCA rendszer alábbi szolgáltatásait is elérik:

- regisztrációs adatok felvétele, módosítása,
- tanúsítvány igénylés,
- visszavonás kezelés szolgáltatás (tanúsítvány felfüggesztés és visszavonás).

Az **NCACLI ADM** adminisztrátori kliens **kiegészítő függvénykészlet**ének meghívásán keresztül a belső felhasználók (azonosításuk és betöltött munkakörüket is érintő hitelesítésük után) az NCA rendszer alábbi szolgáltatásait érhetik el (munkakörüktől függően):

- regisztráció szolgáltatás,
- tanúsítvány előállítás szolgáltatás,
- tanúsítvány szétosztás szolgáltatás,
- visszavonás kezelés szolgáltatás (felfüggesztés, visszavonás),
- visszavonás állapot szolgáltatás (CRL, OCSP),
- az NCA rendszer adminisztrálása.

Konzol parancsokon keresztül a belső felhasználók (azonosításuk és betöltött munkakörüket is érintő hitelesítésük után) az NCA rendszer telepítésére, üzemeltetésére, karbantartására és ellenőrzésére vonatkozó funkciókat érhetnek el.

Konfigurációs állományokon keresztül (a 2. ábrán konfig fájlok) az NCA rendszer működése szabályozható, vezérelhető (az erre feljogosított belső felhasználók által).

5.2 Alrendszerek

Az NCA rendszer logikailag az alábbi 5 alrendszerre osztható:

- AR1: NCA ADM (szerver oldali alrendszer)
- AR2: MANAGER (kezelő alrendszer)
- AR3: NCA CLI USR (külső és belső felhasználók által elérhető kliens oldali alrendszer)
- AR4: NCA CLI ADM (belső felhasználók által elérhető kliens oldali alrendszer)
- AR5: COMM (belső kommunikációs alrendszer)

Az **NCA ADM alrendszer (AR1)** valósítja meg az NCA rendszer alap szolgáltatásait (tanúsítvány előállítás, tanúsítvány szétosztás, visszavonás kezelés, visszavonás állapot) és kiegészítő szolgáltatásait (titkosító magánkulcs letétbe helyezése, titkosító magánkulcs helyreállítása, aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése). A szolgáltatások megvalósítása során használja a kriptográfia hardver modul szolgáltatásait, kezeli saját adatbázisát, illetve megbízható időforrásokból időértéket kap.

A **MANAGER alrendszer (AR2)** a konfigurációs állományokon, illetve konzol parancsokon keresztül elérhető külső interfészt kezeli. Segítségével az AR1 (NCA ADM) alrendszer működése szabályozható, vezérelhető. Ennek keretében végezhető el a rendszer mentése, valamint a naplóállományok exportálása is.

Az **NCACLI USR alrendszer (AR3)** a külső felhasználók számára elérhető külső interfészének (pl. webszerver) kezelése. Ezen keresztül az NCA rendszer nem privilegizált felhasználói az AR1 alrendszer szűkített szolgáltatását érhetik el. /Az alrendszert elérő webszerver és az ezeket elérő alkalmazások nem az NCA rendszer, hanem az informatikai környezet részét képezik./

Az **NCACLI ADM alrendszer (AR4)** a belső felhasználók számára elérhető külső interfészének (pl. webszerver) kezelése. Ezen keresztül az NCA rendszer privilegizált felhasználói az AR1 alrendszer bővített szolgáltatását érhetik el. /Az alrendszert elérő webszerver és az ezeket elérő alkalmazások nem az NCA rendszer, hanem az informatikai környezet részét képezik./

A **COMM alrendszer (AR5)** a szerver és kliensek közötti kommunikáció bizalmasságát, sértetlenségét és hitelességét garantálja.

6 Dokumentáció

Az értékelt termék alkotóelemei az alábbiak:

- ncaadm 2.6.0 build 1985
- ncatools: 2.6.0 build 129
- ncacllib.so 2.6.0 std build 321
- ncacllib.so 2.6.0 full build 321
- Dokumentáció:
  - NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz –KLIENS OLDALI FÜGGVÉNYEK ÉS KONZOLPARANCSOK v1.0
  - NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz –A KONFIGURÁCIÓS ÁLLOMÁNYOK SZERKEZETE v1.0

7 Tesztelés

7.1 A fejlesztők tesztelése

A fejlesztői tesztelés két csoportra bontható: egyik a biztonsági funkciók általános tesztelése.

A másik nagy csoport a rendszer függvényeinek automatizált tesztelése. Ennek során minden létező kombinációban részletesen ellenőrizve lett a hozzáférés ellenőrzés (BF4), azaz hogy egy adott funkcióhoz tartozó függvényt csak a dokumentációban meghatározott jogosultsági szinttel rendelkező felhasználó hívhat meg. Ellenőrizve lett továbbá, hogy a teljes függvénykészlet képes a hibás paraméterek hatására megfelelően, azaz hibaüzenet generálása mellett megfelelő visszatérési értéket adni.

7.2 Az értékelők tesztelése

Az értékelői tesztelés tesztelési stratégiaként a biztonsági előirányzatban leírt biztonsági funkciók specifikus részleteit vagy teljes folyamatának tesztelését irányozta elő. A BF4 kivételével (mivel az automata teszt ezt teljesen lefedi) mindegyik biztonsági funkcióra készült egy átfogó vagy több részletet kielemző teszteset.

A fentieken túl a fejlesztő által kidolgozott automata tesztestek eredményei is részletes elemzésre kerültek.

A független tesztelés során hiba nem lépett fel.

8 Az értékelt konfiguráció

8.1 Szerver

Szerver szoftver konfigurációk:

Operációs rendszer: Solaris 9
Adatbázis kezelő: mysql 4.0.27 with innodb
HSM middleware: Cprov 3.10

Operációs rendszer: Slackware 10.1
Adatbázis kezelő: mysql 4.0.27 with innodb
HSM middleware: Cprov 3.10
Slackware Ntpd 4.2.0a@1.11.96-r

Operációs rendszer: Windows XP Sp2
Adatbázis kezelő: MSACCES 2003
HSM middleware: Cprov 3.10
NTPd: 4.2.0.a@mbg-fluxcap-v2-beta-o

ProtectServer Orange (Eracom CSA 8000) (Hardware 71.00 (G))

ncaadm 2.6.0 build 1985
ncatools: 2.6.0 build 129

8.2 Kliens

Kliens szoftver konfigurációk:

Operációs rendszer: Windows XP SP2;
perl 5.8.x; IIS 5.1

Operációs rendszer: Solaris 9;
myodbc: 3.51.11; unixodbc 2.2.12; perl 5.8.x
apache 1.3.29

Operációs rendszer: Slackware 10.1
myodbc: 3.51.11; unixodbc 2.2.12; perl 5.8.x
apache 1.3.29

ncacllib.so 2.6.0 std build 321
ncacllib.so 2.6.0 full build 321

9 Az értékelés eredményei

Az NCA v2.6.0 a CEM (Common Evaluation Methodology) v2.3 módszertana szerint független értékelésre és tanúsításra került, (kibővített) EAL4 értékelési garanciaszinten.

Az értékelés fő következtetése az alábbi:

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy az NCA v2.6.0 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket. A biztonsági előirányzat megfelel a következő védelmi profilnak: Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0 /Security Level 3, 3-as biztonsági szint/.

A fenti megállapítás az EAL4 követelményeinek teljesítésén alapul.

Az értékelés másik következtetése az alábbi:

Az NCA v2.6.0 a 4.2 fejezetben megfogalmazott informatikai és nem informatikai környezetére vonatkozó feltételek teljesülése esetén megfelel az MSZ CWA 14167-1:2006 által a hitelesítés-szolgáltatók megbízható rendszereivel szemben támasztott biztonsági követelményeknek.

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye[1] /és a fejlesztői bizonyíték/
Biztonsági előirányzat	ASE_DES.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_ENV.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_INT.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_OBJ.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_PPC.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_REQ.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_SRE.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**
	ASE_TSS.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**

[1] Az értékelés részletes eredményei üzleti titkot képeznek.

Konfiguráció menedzselés	ACM_CAP.4	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **A konfiguráció menedzselés dokumentációja**
	ACM_SCP.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **A konfiguráció menedzselés dokumentációja**
	ACM_AUT.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **A konfiguráció menedzselés dokumentációja**
Kiszállítás és működtetés	ADO_DEL.2	A követelményeknek **megfelelt**. **Nincs (a fejlesztők szállítják a terméket)**
	ADO_IGS.1	A követelményeknek **megfelelt**. **Nincs (a fejlesztők telepítik a terméket)**
Fejlesztés	ADV_FSP.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Funkcionális specifikáció** NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Kliens oldali függvények és konzolparancsok** NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfigurációs állományok szerkezete**
	ADV_HLD.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Magas szintű terv**
	ADV_IMP.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz **Forráskód**
	ADV_LLD.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Alacsony szintű terv**
	ADV_RCR.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Megfelelés elemzések**
	ADV_SPM.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Biztonsági szabályzat modell**
Útmutató dokumentumok	AGD_ADM.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Kliens oldali függvények és konzolparancsok** NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfigurációs állományok szerkezete**
	AGD_USR.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Kliens oldali függvények és konzolparancsok** NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfigurációs állományok szerkezete**

Az életciklus támogatása	ALC_DVS.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A fejlesztési biztonság dokumentációja**
	ALC_LCD.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Az életciklust meghatározó dokumentáció**
	ALC_TAT.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A fejlesztő eszközök dokumentációja**
	ALC_FLR.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A hibajelentési eljárások**
Tesztelés	ATE_FUN.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **A fejlesztői tesztelés eredményei**
	ATE_COV.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Teszt lefedettség elemzés**
	ATE_DPT.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Teszt mélység elemzés**
	ATE_IND.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz **Telepített rendszer**
A sebezhetőség felmérése	AVA_MSU.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Az útmutatók elemzése**
	AVA_SOF.1	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Biztonsági funkcióerősség elemzés**
	AVA_VLA.2	A követelményeknek **megfelelt**. NCA TWS 2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz – **Sebezhetőség elemzés**

10 Értékelői megjegyzések és javaslatok

Az értékelő nem adott a tanúsítási jelentésben megjelenítendő megjegyzést, illetve javaslatot.

11 Mellékletek

11.1 Az NCA v2.6.0 megfelelése az MSZ CWA-14167-1:2006 követelményeinek

Az alábbi táblázat az MSZ CWA-14167-1 követelményeknek való megfelelésre vonatkozó vizsgálat eredményét foglalja össze.

Az értékelés az egyes követelményekre külön-külön határozatot hozott, hogy az alábbiakból melyik vonatkozik az adott követelményre:

- **Az NCA rendszer teljesíti** (azaz teljes mértékben megfelel a követelménynek)
- **Az NCA rendszer támogatja** (azaz részben megfelel a követelménynek, de a környezetnek is támogatást kell nyújtania),
- **A környezetnek kell biztosítania** (azaz az NCA rendszer nem vállalja fel a követelmény teljesítését, a megvalósítást az IT és nem IT környezettől várja el),

A megállapítások a rendszer CWA módban történő üzemeltetése esetén érvényesek. Azon feltételek esetén, amelyek csak minősített hitelesítés szolgáltatókra vonatkoznak, a rendszer minősített üzemmódját vesszük alapul.

A követelményekre külön-külön meghozott határozatok az alábbiak valamelyike (vagy ezek valamely kombinációja) alapján születtek:

- interjú: a fejlesztőkkel való személyes konzultációk során kapott információk alapján,
- dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- tapasztalat: a program felhasználói felületének működtetése, illetve a tesztelés során szerzett „felhasználói” tapasztalatokból leszűrt következtetések alapján,
- teszt: az értékelők által végzett tesztelés eredményei alapján,
- forrás kód: a fejlesztők által átadott forráskód értékelők általi elemzése alapján.

Általános funkcionális és biztonsági követelmények			
Menedzselés (M)			
M1 Rendszer- és biztonságkezelés			
1	[M1.1]	Különböző jogokkal bíró munkaköröket kell biztosítani.	**Az NCA rendszer teljesíti**.
2	[M1.2]	Legalább a következő munkakörök szükségesek:	**Az NCA rendszer teljesíti**.
3	[M1.3]	Felhasználók és munkakörök összekapcsolási képessége.	**Az NCA rendszer teljesíti**.
4	[M1.4] QCA	Összeférhetetlen munkakörök	**Az NCA rendszer teljesíti**.
Rendszerek és működésük (SO)			
SO1 Üzemeltetés menedzselése			
5	[SO1.1]	Útmutatók biztosítása (helyes és biztonságos működtetés).	**Az NCA rendszer teljesíti**.
SO2 A folyamatos szolgáltatás biztosítása			
6	[SO2.1]	99.9%-os rendelkezésre állás (tanúsítvány szétosztás, visszavonás kezelés, visszavonás állapot szolgáltatás).	**Az NCA rendszer a megvalósítást az IT és nem IT környezettől várja el.**
7	[SO2.2]	Katasztrófahelyzetben is a működés	**Az NCA rendszer**

		(alternatív TWS)	**támogatja.**
8	[SO2.3]	Biztonságos áttérés a katasztrófa-helyreállító rendszerre.	**Az NCA rendszer a megvalósítást az IT és nem IT környezettől várja el.**
SO3 Időszinkronizáció			
9	[SO3.1] QCA	UTC –hez szinkronizált óra, (1sec), 2 független forrás.	**Az NCA rendszer támogatja.**
10	[SO3.1] NQCA	Állítást kell megfogalmazni az idő pontosságára.	**Az NCA rendszer támogatja.**
Azonosítás és hitelesítés (IA)			
IA1 A felhasználó hitelesítése			
11	[IA1.1]	Kötelező felhasználói azonosítás és hitelesítés.	**Az NCA rendszer teljesíti**.
12	[IA1.2]	A felhasználó kijelentkezése után kötelező az újrahitelesítés.	**Az NCA rendszer teljesíti**.
13	[IA1.3]	Egyedi hitelesítő adatok.	**Az NCA rendszer teljesíti**.
IA2 Hitelesítési hiba			
14	[IA2.1]	A sikertelen hitelesítési kísérletek korlátozása.	**Az NCA rendszer teljesíti**.
15	[IA2.2] QCA	Riasztás max. sikertelen hitelesítési kísérlet elérésekor.	**Az NCA rendszer teljesíti**.
IA3 A titok ellenőrzése			
16	[IA3.1]	Mechanizmus a titkok ellenőrzésére.	**Az NCA rendszer teljesíti**.
Rendszer-hozzáférés ellenőrzés (SA)			
SA1 Rendszer-hozzáférés ellenőrzés			
17	[SA1.1]	Azonosított egyének hozzáférésének ellenőrzése, korlátozása.	**Az NCA rendszer teljesíti**.
18	[SA1.2]	Hozzáférés védelem az érzékeny maradvány információkra.	**Az NCA rendszer teljesíti**.
Kulcs kezelés (KM)			
KM1 Kulcs generálás			
19	[KM1.1]	A tanúsítvány aláíró kulcsokat biztonságos kriptográfiai modulban (HSM) kell generálni.	**Az NCA rendszer támogatja**.
20	[KM1.2]	A HSM-et értékelni és tanúsítani kell.	**A környezetnek kell biztosítania.**
21	[KM1.3]	Kettős személyi ellenőrzés a szolgáltatói kulcsgenerálásnál.	**A környezetnek kell biztosítania.**
22	[KM1.4]	Az infrastrukturális és rendszervezérlési kulcsokat egy hardver kriptográfiai eszközben kell generálni.	**Az NCA rendszer támogatja**.
-	[KM1.5] QCA	törölve	-
-	[KM1.6] NQCA	törölve	-
23	[KM1.7]	A kulcs generálás algoritmusa biztonságos legyen.	**Az NCA rendszer teljesíti**.

KM2 Kulcs elosztás			
24	[KM2.1]	A magán/titkos kulcsokat tilos nyílt formában szétosztani.	**Az NCA rendszer támogatja**.
25	[KM2.2]	A még tanúsítványba nem foglalt nyilvános kulcsokat biztonságos környezetben kell tartani.	**Az NCA rendszer teljesíti**.
26	[KM2.3]	Szabványos kriptográfiai kulcselosztó módszer használata.	**Az NCA rendszer teljesíti**.
27	[KM2.4]	A szolgáltatói nyilvános kulcsok szétosztásánál fenn kell tartani a sértetlenséget és hitelességét.	**A környezetnek kell biztosítania.**
28	[KM2.5]	Az önaláírt tanúsítvány jellemzői:	**Az NCA rendszer támogatja**.
29	[KM2.6]	Önaláírt tanúsítványra biztonságos lenyomat készítése.	**Az NCA rendszer teljesíti**.
KM3 Kulcs használat			
30	[KM3.1]	A HSM-hez hozzáférés ellenőrzést kell alkalmazni.	**A környezetnek kell biztosítania.**
31	[KM3.2] QCA	Kettős személyi ellenőrzés rendszervezérlési kulcsokhoz.	**Az NCA rendszer teljesíti**.
32	[KM3.3] QCA	Funkciónként különböző infrastrukturális kulcsok.	**Az NCA rendszer teljesíti**.
33	[KM3.4]	El kell különíteni az aláíró kulcsokat.	**Az NCA rendszer teljesíti**.
34	[KM3.5]	Jogosult kulcshasználat csak életcikluson belül történhet.	**Az NCA rendszer teljesíti**.
35	[KM3.6]	Kulcshasználat előtt tanúsítvány érvényesség ellenőrzés.	**Az NCA rendszer teljesíti**.
KM4 Kulcs csere			
36	[KM4.1]	I és RV kulcsokat rendszeresen (pl. évente) cserélni kell.	**Az NCA rendszer támogatja**.
37	[KM4.2]	A kulcs cserét biztonságosan kell végrehajtani.	**Az NCA rendszer támogatja**.
KM5 Kulcs megsemmisítés			
38	[KM5.1	Tanúsítvány aláíró kulcsok végleges megsemmisítése.	**A környezetnek kell biztosítania.**
39	[KM5.2]	Kivont rendszerek kulcsait meg kell semmisíteni.	**A környezetnek kell biztosítania.**
40	[KM5.3]	Kulcs kinullázás képessége.	**A környezetnek kell biztosítania.**
41	[KM5.4]	Biztonságos SW kulcstörlési folyamatok alkalmazása.	**Az NCA rendszer teljesíti**.
KM6 Kulcs tárolása, mentése és helyreállítása			
42	[KM6.1]	Minden magán/titkos kulcsot biztonságosan kell tárolni.	**Az NCA rendszer támogatja**.
43	[KM6.2]	A TA kulcsokat HSM-ben kell tárolni.	**Az NCA rendszer támogatja**.
44	[KM6.3]	Az I és RV kulcsokat hardver kriptográfiai eszközben kell tárolni.	**A környezetnek kell biztosítania.**

45	[KM6.4]	Kulcs exportálás csak védett módon.	**Az NCA rendszer teljesíti**.
46	[KM6.5]	Kulcsokat csak jogosult személy (pl. SO) kezelheti.	**Az NCA rendszer teljesíti**.
47	[KM6.6]	TA magánkulcsok kezelése kettős személyi ellenőrzés alatt.	**Az NCA rendszer támogatja**.
48	[KM6.7]	Tilos aláíró magánkulcsot menteni, letétbe helyezni.	**Az NCA rendszer teljesíti**.
KM7 Kulcs archiválás			
53	[KM7.1]	Tilos az aláíró magánkulcsok archiválása.	**Az NCA rendszer teljesíti**.
Naplózás (AA)			
AA1 Napló adatok generálása			
54	[AA1.1]	A következő események naplózása feltétlenül szükséges:	**Az NCA rendszer teljesíti**.
AA2 Napló adatok garantált rendelkezésre állása			
55	[AA2.1]	Karban kell tartani a naplózási adatokat.	**Az NCA rendszer teljesíti**.
56	[AA2.2]	A naplóbejegyzéseket nem szabad automatikusan felülírni.	**Az NCA rendszer teljesíti**.
AA3 Naplózási paraméterek			
57	[AA3.1]	Minden naplórekordnak tartalmaznia kell a következőket:…	**Az NCA rendszer teljesíti**.
AA4 A napló választható áttekintése			
58	[AA4.1]	Gondoskodni kell a naplóesemények közötti keresésről.	**Az NCA rendszer teljesíti**.
59	[AA4.2]	A naplórekordot ember által olvashatóan kell megjeleníteni.	**Az NCA rendszer teljesíti**.
AA5 Korlátozott naplómegtekintés			
60	[AA5.1]	A naplót csak jogosultsággal lehessen olvasni.	**Az NCA rendszer teljesíti**.
61	[AA5.2]	Meg kell akadályozni a naplózási rekordok módosítását.	**Az NCA rendszer teljesíti**.
AA6 Riasztás generálása			
62	[AA6.1]	Riasztás kell a biztonság potenciális megsértése esetén.	**Az NCA rendszer teljesíti**.
AA7 A napló adatok sértetlenségének garantálása			
63	[AA7.1] NQCA	Biztosítani kell a napló adatok sértetlenségét.	**Az NCA rendszer teljesíti**.
64	[AA7.1] QCA	Biztosítani kell a napló sértetlenségét: (DS, HMAC, auth)	**Az NCA rendszer teljesíti**.
AA8 A napló időbejegyzéseinek garantálása			
65	[AA8.1]	Megbízható időforrást kell alkalmazni a naplóhoz.	**Az NCA rendszer támogatja**.
Archiválás (AR)			
AR1 Archív adatok generálása			
66	[AR1.1]	Képesnek kell lenni archívum létrehozására.	**Az NCA rendszer teljesíti**.
67	[AR1.2]	Archiválni kell: (tanúsítványok, CRL-ek, naplók)	**Az NCA rendszer teljesíti**.

68	[AR1.3]	Minden bejegyzésnek tartalmaznia kell az időpontot.	**Az NCA rendszer teljesíti**.
69	[AR1.4]	Archívumban kritikus biztonsági paraméter csak védetten.	**Az NCA rendszer teljesíti**.
	AR2 Szelektálható keresés		
70	[AR2.1]	Az archívumra biztosítani kell egy keresési lehetőséget.	**Az NCA rendszer teljesíti**.
	AR3 Az archivált adatok sértetlensége		
71	[AR3.1]	Az archívum bejegyzéseit védeni kell a módosítástól.	**Az NCA rendszer teljesíti**.
Mentés és helyreállítás (BK)			
	BK1 Mentés generálása		
72	[BK1.1]	Léteznie kell egy mentési funkciónak.	**Az NCA rendszer teljesíti**.
73	[BK1.2]	A mentett adatokból a rendszer visszaállítható legyen.	**Az NCA rendszer teljesíti**.
74	[BK1.3]	A mentési funkció meghívható legyen (jogosultan).	**Az NCA rendszer teljesíti**.
	BK2 A mentési információ sértetlensége és bizalmassága		
75	[BK2.1] NQCA	A mentést védeni kell a módosítás ellen.	**Az NCA rendszer teljesíti**.
76	[BK2.1] QCA	A mentést védeni kell a módosítás ellen: (DS, HMAC, auth).	**Az NCA rendszer teljesíti**.
77	[BK2.2]	Kritikus bizt. par-k csak titkosított formában tárolhatók.	**Az NCA rendszer teljesíti**.
	BK3 Helyreállítás		
78	[BK3.1]	Biztosítani kell egy helyreállítási funkciót.	**Az NCA rendszer teljesíti**.
79	[BK3.2]	A helyreállítási funkció meghívható legyen (jogosultan).	**Az NCA rendszer teljesíti**.
Az egyes szolgáltatásokra vonatkozó funkcionális és biztonsági követelmények			
Általános követelmények (GE)			
	GE1 szolgáltatások által létrehozott üzenetek védelme		
80	[GE1.1]	A szolgáltatások által létrehozott üzenetre biztosítani kell: (üzenet és visszajátszás elleni védelem, létrehozási időpont)	**Az NCA rendszer teljesíti**.
Regisztráció szolgáltatás (R)			
	R1 Tanúsítvány kérelem		
81	[R1.1]	A tanúsítvány kérést szükség esetén védeni kell.	**Az NCA rendszer teljesíti**.
82	[R1.2]	Megfelelő mechanizmus szükséges a birtoklás bizonyítására.	**Az NCA rendszer teljesíti**.
83	[R1.3] QCA	A regisztráció tegye lehetővé az aláíró adatai összegyűjtését.	**Az NCA rendszer támogatja**.
84	[R1.4]	Mechanizmus kell a tanúsítvány kérelmek jóváhagyására.	**Az NCA rendszer teljesíti**.
85	[R1.5] QCA	A kérelmeket el kell látni a következő jellemzőkkel:	**Az NCA rendszer teljesíti**.

86	[R1.6]	A regisztráció üzeneteit alá kell írni.	**Az NCA rendszer teljesíti**.
	R2 Tanúsítvány kérelem		
87	[R2.1]	Az alanyra vonatkozó információ bizalmasságát védeni kell.	**Az NCA rendszer teljesíti**.
	R3 Regisztráció szolgáltatás naplózása		
88	[R3.1]	A regisztráció alábbi eseményeit kötelező naplózni:	**Az NCA rendszer teljesíti**.
Tanúsítvány előállítás szolgáltatás (CG)			
	CG1 Tanúsítvány előállítás		
89	[CG1.1]	Biztosítani kell a tanúsítvány kérelem üzenet védelmét.	**Az NCA rendszer teljesíti**.
90	[CG1.2]	A tanúsítvány kérelmet biztonságosan kell feldolgozni.	**Az NCA rendszer támogatja**.
91	[CG1.3]	Biztosítani kell a birtoklás bizonyításának az ellenőrzését.	**Az NCA rendszer teljesíti**.
92	[CG1.4] - QCA	A TA csak erre (és a CRL aláírására) használható fel.	**Az NCA rendszer teljesíti**.
93	[CG1.5]	Meg kell felelni a meghatározott profiloknak.	**Az NCA rendszer teljesíti**.
94	[CG1.6] NQCA	A tanúsítványoknak meg kell felelniük az alábbiaknak:	**Az NCA rendszer támogatja.**
95	[CG1.6] QCA	A tanúsítványoknak meg kell felelniük: ETSI TS 101 862	**Az NCA rendszer támogatja.**
	CG2 Tanúsítvány megújítás		
96	[CG2.1]	A tanúsítvány megújítás során védekezni kell a tanúsítvány helyettesítés támadás ellen.	**Az NCA rendszer teljesíti**.
97	[CG2.2]	I és RV kulcsokra a tanúsítvány megújításnak teljesítenie kell a KM.4 (kulcs csere) feltételeit is.	**Az NCA rendszer támogatja.**
98	[CG2.3]	Biztosítani kell a TA tanúsítványok időbeli megújítását.	**A környezetnek kell biztosítania.**
99	[CG2.4]	Biztonságos mechanizmus kell az alany kulcsainak újra hitelesítésére és/vagy kulcs megújítására.	**Az NCA rendszer teljesíti**.
	CG3 Felülhitelesítés		
100	[CG3.1]	Felülhitelesítés alkalmazása esetén biztosítania kell:…	**Az NCA rendszer teljesíti**.
	CG4 A tanúsítvány előállítás szolgáltatás naplózása		
101	[CG4.1]	A tanúsítvány előállítás alábbi eseményeit kell naplózni:	**Az NCA rendszer teljesíti**.
Tanúsítvány szétosztás szolgáltatás (D)			
	D1 Szétosztás kezelés		
102	[D1.1]	A tanúsítvány szétosztás csak alanyoknak és az engedélyezett érintett feleknek.	**Az NCA rendszer teljesíti**.
103	[D1.2]	A szétosztás folyamata [D1.1]-nek megfelelő legyen.	**Az NCA rendszer teljesíti**.

D2 Objektumok exportja/importja			
104	[D2.1]	A tanúsítványtárra hozzáférés-ellenőrzési politika kell.	**Az NCA rendszer teljesíti**.
Visszavonás kezelés szolgáltatás (RM)			
RM1 Tanúsítvány állapotváltozás kérések			
105	[RM1.1]	A visszavonás/felfügg kérelmek végrehajtása 24 órán belül.	**Az NCA rendszer támogatja.**
106	[RM1.2]	Minden kérelmet hitelesíteni és érvényesíteni kell.	**Az NCA rendszer teljesíti**.
107	[RM1.3]	Visszavont tanúsítványt nem lehet újra használatba venni.	**Az NCA rendszer teljesíti**.
108	[RM1.4]	TA kulcs- tanúsítványok visszavonása kettős ellenőrzéssel.	**A környezetnek kell biztosítania.**
109	[RM1.5]	Állapot változtatását csak a következők kezdeményezhetik:	**Az NCA rendszer teljesíti**.
110	[RM1.6]	A tanúsítvány állapot adatbázist azonnal frissíteni kell.	**Az NCA rendszer teljesíti**.
RM2 Tanúsítvány felfüggesztés/visszavonás			
111	[RM2.1]	Tanúsítvány visszavonása, még katasztrófát követően is.	**A környezetnek kell biztosítania.**
112	[RM2.2]	Időszakos frissítő üzenetek használata esetén:…	**Az NCA rendszer teljesíti**.
113	[RM2.3]	Valós idejű üzenetek használata esetén:….	**Az NCA rendszer teljesíti**.
RM3 A Visszavonás kezelés naplózása			
114	[RM3.1]	A visszavonás kezelés alábbi eseményeit kötelező naplózni:	**Az NCA rendszer teljesíti**.
Visszavonás állapot szolgáltatás (RS)			
RS1 Visszavonás állapot adatok			
115	[RS1.1]	Csak megbízható tanúsítvány visszavonás kezelő szolgáltatásoktól származó üzenet dolgozható fel.	**Az NCA rendszer teljesíti**.
116	[RS1.2]	OCSP üzenetek sértetlenségét és hitelességét ellenőrizni kell.	**Az NCA rendszer teljesíti**.
117	[RS1.3]	OCSP válaszokra garantálni kell, hogy a tanúsítvány-állapot adatbázisból valóban a kért tanúsítványra vonatkozó választ kapták.	**Az NCA rendszer teljesíti**.
RS2 Állapot kérés/válasz			
118	[RS2.1]	Minden választ digitálisan alá kell írni.	**Az NCA rendszer teljesíti**.
119	[RS2.2]	Aláírni csak biztonságos algoritmussal.	**Az NCA rendszer támogatja**.
-	[RS2.3]	törölve	-
120	[RS2.4]	A válasz üzenetnek tartalmaznia kell az aláírás idejét.	**Az NCA rendszer teljesíti**.

RS3 A tanúsítvány visszavonás állapot naplózása			
121	[RS3.1]	A tanúsítvány visszavonás alábbi eseményeit kell naplózni:…	**Az NCA rendszer teljesíti**.
Időbélyegzés szolgáltatás (TS)			
TS1 Kérés helyessége			
122	[TS1.1]	A kérések eredete ellenőrizhető.	**A környezetnek kell biztosítania.**
123	[TS1.2]	Ellenőriznie kell, hogy az időbélyeg kérés biztonságos lenyomatkészítő algoritmust használ.	**Az NCA rendszer támogatja**.
TS2 Időparaméter generálása			
124	[TS2.1]	Az időforrás(oka)t szinkronizálni kell (UTC, 1 sec).	**Az NCA rendszer támogatja**.
125	[TS2.2]	Megbízható mechanizmussal kell szinkronizálni.	**A környezetnek kell biztosítania.**
TS3 Időbélyeg token (TST) létrehozása			
126	[TS3.1]	A TST-be egyedi sorszámot kell foglalni.	**Az NCA rendszer teljesíti**.
127	[TS3.2]	A TST tartalmazza az időforrás pontosságát is.	**Az NCA rendszer teljesíti**.
128	[TS3.3]	Szerepeltetni kell a szabályzatra való hivatkozást.	**Az NCA rendszer teljesíti**.
TS4 Időbélyeg token (TST) kiszámítása			
129	[TS4.1]	A TSA aláíró kulcsokat HSM-ben kell generálni és tárolni.	**Az NCA rendszer támogatja**.
130	[TS4.2]	Megfelelő HSM-et kell használni.	**A környezetnek kell biztosítania.**
131	[TS4.3]	A TSA rendszervezérlési kulcsokat HSM-ben kell tárolni.	**Az NCA rendszer teljesíti**.
132	[TS4.4]	A TSA aláíró kulcsok csak TST-k aláírására használhatók.	**Az NCA rendszer teljesíti**.
133	[TS4.5]	A TST válasz a kérés adatait tartalmazza.	**Az NCA rendszer teljesíti**.
134	[TS4.6]	Biztonságos aláírási algoritmust kell használni.	**Az NCA rendszer támogatja**.
TS5 Időbélyeg szolgáltatás naplózása			
135	[TS5.1]	Az alábbi időbélyegzési eseményeket naplózni kell:	**Az NCA rendszer teljesíti**.
TS6 Időbélyeg szolgáltatás archiválás			
136	[TS6.1]	Minden időbélyeg tokent archiválni kell.	**Az NCA rendszer teljesíti**.
Aláíró eszköz ellátás szolgáltatás (SP)			
SP1 Kriptográfiai eszköz készítés			
137	[SP1.1]	Idegen gyártmányt előzetesen ellenőrizni kell.	**A környezetnek kell biztosítania.**
-	[SP1.2]	törölve	-
138	[SP1.3]	Inicializáláskor biztonságos konfigurációt kell kialakítani.	**A környezetnek kell biztosítania.**

139	[SP1.4]	BALE-t tanúsíttatni kell.	**A környezetnek kell biztosítania.**
140	[SP1.5]	Tanúsított kriptográfiai modulban lehet csak kulcspárt generálni .	**A környezetnek kell biztosítania.**
141	[SP1.6]	Kívül generált kulcspárt biztonságosan kell feltölteni.	**A környezetnek kell biztosítania.**
142	[SP1.7]	Kívül generált kulcspárt biztonságosan törölni kell.	**A környezetnek kell biztosítania.**
SP2 Aláíró eszköz ellátás			
143	[SP2.1]	Az aláíró eszközt a hitelesített alanyhoz kell eljuttatni.	**A környezetnek kell biztosítania.**
SP3 Aktivizáló adatok létrehozása és szétosztása			
144	[SP3.1]	A kezdeti aktivizáló adatokat biztonságosan kell generálni.	**A környezetnek kell biztosítania.**
145	[SP3.2]	Az alkalmazottak ne élhessenek vissza az aláíró eszközzel.	**A környezetnek kell biztosítania.**
SP4 Az aláíró eszköz ellátás szolgáltatás naplózása			
146	[SP4.1]	Valamennyi biztonságilag fontos eseményt naplózni kell.	**A környezetnek kell biztosítania.**

11.2 A Protect Server Orange (CSA8000) használata az NCA rendszerrel

A jelen tanúsítás tárgya (NCA TWS 2.6.0)az értékelt kiépítésben a ProtectServer Orange korábbi nevén CSA8000 Adapter elektronikus aláírási terméket használja HSM modulként.

A ProtectServer Orange HSM modulra a HUNG-T-28/2005 regisztrációs számú tanúsítvány 19 különböző érvényességi feltételt fogalmazott meg, melyet a HSM modul környezetének kell biztosítania.

Az NCA TWS 2.6.0 (mint a ProtectServer Orange HSM modul informatikai környezete) CWA üzemmódban ezen feltételek egy részét biztosítja, illetve érvényre juttatja. Az alábbiak ezeket a (NCA rendszer használata esetén biztosan teljesített) feltételeket határozzák meg.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 2. feltétele
A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusokra kell korlátozni: DSA, RSA (PKCS #1), SHA-1.

A feltétel teljesítésének indoklása: Az NCA rendszer kizárólag RSA algoritmusra aktivizál digitális aláírással kapcsolatos kriptográfiai funkcionalitást.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 7. feltétele
Minden új slot konfigurálásánál a PIN kód hossza legalább 4 legyen.

A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) a PIN kód számolás alapját képező jelszóra minimum 6 hosszúságot és legalább 36 elemű jelkészletet kényszerít ki, így a választás szabadsági foka több nagyságrenddel nagyobb az elvártnál.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 8. feltétele
RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 1020 bit legyen.

A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) programozott módon, legalább 1024 bit hosszúságot kényszerít ki az RSA aláírási algoritmus modulusára.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 9. feltétele
DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (pMinLen) 1024 bit, a minimális q prímhosszúság (qMinLen) 160 bit legyen.

A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) programozott módon, RSA algoritmus alkalmazását kényszeríti ki digitális aláírások esetén. Így a feltétel egy nem bekövetkező esetre vonatkozik, tehát teljesül.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 10. feltétele
Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet.

A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) mindig 8-cal osztható bithosszúságú blokkot ad át a HSM modulnak digitális aláírásra.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 11. feltétele
A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.
A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) programozott módon érvényre juttatja, hogy a minősített tanúsítványok aláírására használt magánkulcsot kizárólag a minősített tanúsítványok és a rájuk vonatkozó visszavonási listák aláírására használják.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 12. feltétele
Bármilyen, biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a modulnak gondoskodnia kell a kulcs védelméről. Érzékeny kulcsadatok nem védett módon történő tárolása tilos. Minősített tanúsítvány aláíró kulcs csak további biztonsági mechanizmusok alkalmazása esetén tárolható és menthető. Ez megtehető például az alábbiak valamelyikével is:

- az "m az n-ből" technika alkalmazásával (melyet jelenleg a CSA8000 nem támogat, de szabványos felületén keresztül később megvalósítható), ahol m azon komponensek darabszáma a teljes n komponensből, amelynek ismeretében a kulcs inicializálása sikeresen elvégezhető. A hiba esetén alkalmazandó helyreállításra az m = 60% * n érték javasolt (azaz ha n=3, akkor m=2, ha n=4 akkor m=3, ha n=5 akkor m=3,…).
- az alábbi (CSA8000 által támogatott) módszerrel:
  - a mentés intelligens kártyákra (tokenekre) történik,
  - a mentés kódolva van a triple-DES titkosító algoritmus alkalmazásával,
  - a mentés kódolására alkalmazott titkosító kulcs (Key Encryption Key) legalább két véletlen komponensből van előállítva, s ennek megfelelően legalább két erre felhatalmazott személy együttes jelenléte szükséges a magánkulcs helyreállításához.

A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) a HSM modulban tárolt kulcsok exportálásakor programozott módon megvalósítja az „m az n-ből" technikát.

A HUNG-T-028/2005. regisztrációs számú tanúsítvány 13. feltétele
Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.
A feltétel teljesítésének indoklása: Az NCA rendszer (CWA üzemmódban) programozott módon érvényre juttatja, hogy az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására használják.

11.3 A tanúsított termékek listájába javasolt szöveg

Jelenleg még nincs tanúsított termékek listája. Amennyiben lenne ilyen lista, abba az alábbi szöveg felvételét javasolnánk:

"Az NCA v2.6.0 (NCA rendszer) olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Az NCA rendszer v2.6.0 a meghívó alkalmazásoktól szolgáltatási üzeneteket, parancsokat fogad, azokat (amennyiben erre szükség van) jogosultságellenőrzés alá veti, majd végrehajtja. Az alábbi hitelesítés-szolgáltatásokat támogatja:

Alap szolgáltatások (minden üzemmód része):

- *Regisztráció szolgáltatás,*
- *Tanúsítvány előállítás szolgáltatás,*
- *Tanúsítvány szétosztás szolgáltatás,*
- *Visszavonás kezelés szolgáltatás (CRL, OCSP),*
- *Visszavonás állapot szolgáltatás.*

Kiegészítő szolgáltatások (egyes üzemmódok része):

- *időbélyegzés szolgáltatás,*
- *általános aláírás szolgáltatás (GSU),*
- *titkosító magánkulcs letétbe helyezése szolgáltatás,*
- *titkosító magánkulcs helyreállítása szolgáltatás.*

Az NCA rendszer biztonsági előirányzata megfelel a következő védelmi profilnak: Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0 /Security Level 3, 3-as biztonsági szint/."

12 Biztonsági előirányzat

A jelen tanúsítási jelentés részét képező végleges biztonsági előirányzatot különálló dokumentumként csatoljuk.

13 Fogalmak és rövidítések

13.1 Fogalmak

Az alábbiakban meghatározzuk a jelen tanúsításban használt (nem nyilvánvaló) fogalmak jelentését.

biztonsági előirányzat
Biztonsági követelmények és előírások olyan összessége, amelyet valamilyen adott tárgy értékelésének alapjaként használnak.

biztonsági funkció
Az értékelés tárgyának olyan része vagy részei, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni.

biztonsági szabályzat
Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán belül.

értékelés
A biztonsági előirányzat, illetve az értékelés tárgyának felmérése meghatározott szempontrendszer (a CC módszertana) alapján.

értékelés tárgya
Az az informatikai termék vagy rendszer, valamint a hozzá kapcsolódó adminisztrátori és használati útmutatók, amelyre az értékelés irányul.

értékelési garanciaszint
A CC. 3 rész olyan garancia összetevőiből álló csomag, amelyek egy-egy pontot képviselnek a CC előre meghatározott garanciális skáláján.

felhasználó
Az a személy, aki az alkalmazást használja, azaz annak szolgáltatásait igénybe kívánja venni.

hitelesítő adat
Az az információ, amely a felhasználó állítólagos személyazonosságát igazolja.

kulcs, aláíró kulcs
Elektronikus aláírás létrehozásához használt magánkulcs.

összetevő
Valamely csomag, védelmi profil vagy biztonsági előirányzat számára választható elemek legkisebb összessége.

tanúsítvány, lejárt
Olyan tanúsítvány, melynek a notAfter értéke korábbi, mint az aktuális időpont. A lejárt tanúsítvány szerepel vagy nem szerepel a tanúsítvány visszavonási listában (CRL).

tanúsítvány, végtanúsítvány
Olyan, általában személyes tanúsítvány, amely a tanúsítvány láncban az utolsó helyen szerepel.

tanúsítvány, visszavont
Olyan tanúsítvány, amely már nem használható vagy nem megbízható. A hitelesítés-szolgáltató, amely a tanúsítvány kibocsátotta, a tanúsítványt különféle okokból vonhatja vissza. Az okok között szerepel a kulcs feltételezett vagy tényleges kompromittálódása,

a tanúsítvány alanynak távozása az adott szervezettől, stb. A tanúsítvány visszavonási lista tartalmazza az összes visszavont és még nem lejárt tanúsítványt. Opcionálisan a tanúsítvány visszavonási lista tartalmazhat visszavont és már lejárt tanúsítványokat is.

tanúsítvány lánc

A tanúsítási útvonal felépítése során keletkező, tanúsítványokból álló sorozat, amelyben az első helyen egy megbízható legfelső szintű tanúsítvány áll, azt opcionális közbenső tanúsítványok követnek, az utolsó helyen egy végtanúsítvány szerepel.

tanúsítvány visszavonási lista (CRL, Certificate Revocation List)

Azoknak a visszavont tanúsítványoknak a felsorolása, amelyeket már nem használhatóak vagy nem megbízhatóak. Általában a hitelesítés szolgáltató, amely a tanúsítványt kibocsátotta, adja ki a CRL-t. A tanúsítvány visszavonási listát a kibocsátó elektronikus aláírással látja el.

termék

Informatikai szoftver, förmver és/vagy hardver által alkotott csomag, amely adott használatra vagy különböző rendszerekbe való beépítésre tervezett funkciókészletet szolgáltat.

védelmi profil

Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak egy kategóriájára, amely adott fogyasztói igényeket elégít ki.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen tanúsítási jelentésben használt betűszavak jelentését.

AR	**Al**rendszer
BALE	**B**iztonságos **a**láírás-**l**étrehozó **e**szköz
BF	**B**iztonsági **f**unkció
CA	**C**ertification **A**uthority (Hitelesítés szolgáltató)
CC	**C**ommon **C**riteria (Közös szempontok)
CEM	**C**ommon **E**valuation **M**ethodology (Közös értékelési módszertan)
CEN	**C**omité **E**uropeen de **N**ormalization (Európai Szabványügyi Bizottság)
CRL	**C**ertificate **R**evocation **L**ist (tanúsítvány visszavonási lista)
CWA	**C**EN **W**ork **A**greement (CEN munka megállapodás)
EAL	**E**valuation **A**ssurance **L**evel (értékelési garanciaszint)
ETSI	**E**uropean **T**elecommunication **S**tandard **I**nstitute
HSM	**H**ardware **S**ecurity **M**odule (hardver kriptográfiai modul)
IT	**I**nformáció **t**echnológia
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
PKCS	**P**ublic **K**ey **C**ryptography **S**tandard
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Information Standard
PKI	**P**ublic **K**ey **I**nfrastructure
PP	**P**rotection **P**rofile (Védelmi profil)
RFC	**R**equest **f**or **C**omment
ST	**S**ecurity **T**arget (biztonsági előirányzat)
SOF	**S**trength **o**f **F**unction (funkcióerősség)
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)
TSF	**T**OE **S**ecurity **F**unctions (TOE biztonsági funkciói)
TSP	**T**OE **S**ecurity **P**olicy (TOE biztonsági szabályzata)

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- NCA v2.6.0 Biztonsági előirányzat v1.0
- NCA v2.6.0 Értékelési jelentés v1.0

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

cím	verzió
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – BIZTONSÁGI ELŐIRÁNYZAT	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz - A KONFIGURÁCIÓ MENEDZSELÉS DOKUMENTÁCIÓJA	1.1
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – A FEJLESZTÉS BIZTONSÁG DOKUMENTÁCIÓJA	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – AZ ÉLETCIKLUST MEGHATÁROZÓ DOKUMENTÁCIÓ	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – A HIBAJELENTÉSI ELJÁRÁSOK	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – BIZTONSÁGI SZABÁLYZAT MODELL	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – FUNKCIONÁLIS SPECIFIKÁCIÓ	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – KLIENS OLDALI FÜGGVÉNYEK ÉS KONZOLPARANCSOK	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – A KONFIGURÁCIÓS ÁLLOMÁNYOK SZERKEZETE	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – MAGAS SZINTŰ TERV	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – ALACSONY SZINTŰ TERV	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – MEGFELELÉS ELEMZÉS	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – A FEJLESZTŐ ESZKÖZÖK DOKUMENTÁCIÓJA	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – A FEJLESZTŐI TESZTELÉS EREDMÉNYEI	---
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – TESZT LEFEDETTSÉG ELEMZÉS	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – TESZT MÉLYSÉG ELEMZÉS	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – AZ ÚTMUTATÓK ELEMZÉSE	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – BIZTONSÁGI FUNKCIÓERŐSSÉG ELEMZÉS	1.0
NCA TWS v2.6.0 - NCA megbízható rendszer hitelesítés-szolgáltatáshoz – SEBEZHETŐSÉG ELEMZÉS	1.0

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- MSZ/ISO/IEC 15408:2003 Informatika – Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai
- Common Criteria for Information Technology Security Evaluation (CC) Part 1: Introduction and general model - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 2: Security functional requirements - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 3: Security assurance requirements - Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM), Version 2.3, August 2005

14.4 Az értékeléshez felhasznált egyéb dokumentumok

Az értékelés figyelembe vette az alábbi mértékadó követelményrendszereket is:

- Az elektronikus aláírásról szóló 2001. évi XXXV. törvény
- CEN CWA 14167-1:2003 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- MSZ CWA 14167-1:2006 - Elektronikus aláírások tanúsítványait kezelő megbízható rendszerek biztonsági követelményei - 1. rész: Rendszerbiztonsági követelmények
- ETSI TS 101 862 v1.3.3 Qualified Certificate profile
- ETSI TS 102 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- RFC 2560 Online Certificate Status Protocol - OCSP
- RFC3161 Time-Stamp Protocol (TSP)
- RFC3280 Certificate and Certificate Revocation List (CRL) Profile
- PKCS #11 v2.11 Cryptographic Token Interface Standard
- PKCS #12 v1.0 Personal Information Exchange Information Standard