TANÚSÍTÁSI JELENTÉS

InfoCA v2.5
megbízható rendszer
hitelesítés-szolgáltatáshoz

HUNG-TJ-48-2009

Verzió:	1.0
Fájl:	HUNG-TJ-48-2009v10.pdf
Minősítés:	Nyilvános
Oldalak:	38

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2009.07.30	A szerkezet felállítása
v0.8	2009.08.04	A tanúsítás eredményeit tartalmazó teljes változat
v0.9	2009.08.**0**6	Belső egyeztetésen átesett változat
v1.0	**2009.08.19**	**Külső egyeztetésen átesett végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
Hunguard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

Az INFOCA v2.5 a 2007-ben Hung-T-36/2007 számon tanúsított TRUST&CA v2.0 hitelesítés-szolgáltatáshoz alkalmazható megbízható rendszer továbbfejlesztése.

A jelen tanúsítási eljárás alapját szolgáló értékelés a TRUST&CA v2.0 rendszer garancia folyamatosságának biztosítására létrejött szerződés keretein belül került sor.

Az INFOCA v2.5 verzióban a fejlesztők különböző piaci igények alapján több változtatást végeztek a terméken:

- felkészítették a rendszert (a korábbi SHA1 mellett) az SHA256, SHA348 és SHA512 hash függvények támogatására,
- időbélyegzés és OCSP szolgáltatásokkal bővítették a rendszert,
- új nevet adtak rendszerüknek (InfoCA).

Az értékelők megállapították, hogy a fenti változtatásoknak jelentős a kihatása, ezért a garancia folyamatosság fenntartására szolgáló rövidített karbantartási eljárás nem lehetséges ezért, újraértékelés és új tanúsítás szükséges.

A fejlesztők aktualizálták és az értékelő szervezet számára átadták fejlesztői bizonyítékaikat.

Az értékelők az újraértékelést a korábbi értékeléshez viszonyítva hajtották végre, felhasználva a korábbi értékelésből származó minden olyan eredményt, ami még érvényes.

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz**
Verzió szám:	**v2.5**
Rövid elnevezés:	**InfoCA v2.5 vagy InfoCA rendszer**
Az értékelt termék típusa:	Megbízható rendszer hitelesítés-szolgáltatáshoz
Értékelő szervezet:	Hunguard Kft.
Értékelés befejezése:	2009. július 30.
Az értékelés módszere:	CEM, Common Evaluation Methodology, v2.3
Az értékelés garanciaszintje:	EAL4+ (ALC_FLR.2 hibajelentési eljárásokkal kibővítve)

Az értékelt termék funkcionalitása:

Az InfoCA v2.5 (InfoCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Alap (kötelező) szolgáltatások:

- Regisztrációs szolgáltatás (az InfoCA rendszeren kívül valósul meg, de eredményét az InfoCA rendszer használja)
- Tanúsítvány előállítás szolgáltatás,
- Tanúsítvány szétosztás szolgáltatás,
- Visszavonás kezelés szolgáltatás,
- Visszavonás állapot szolgáltatás (CRL, OCSP).

Kiegészítő (opcionális) szolgáltatások:

- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás,
- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (az InfoCA rendszeren kívül valósul meg),
- időbélyegzés szolgáltatás.

Konfigurációs követelmények:

Szerver szoftver konfiguráció

- Windows 2003 Szerver, Enterprise edition, SP1
- MS SQL Szerver 2005
- OpenLDAP 2.2.29
- Syslog-win32-0.3
- nShield F3 500 PCI kriptográfiai hardver modul (egyik HSM)
- SafeNet Luna® PCICryptographic Module v2.2 (másik HSM)
- .NET 3.0

Kliens szoftver konfiguráció

- Windows XP, Professional, SP2
- .NET 3.0
- Omnikey CardMan 3121
- Oberthur CosmopolIC SmartCard
- Giesecke, SPK 2.3 Standard V7.0 T=1, SmartCard (StarCert)
- Giesecke, StarSign

Webszerver (TS, OCSP) környezet elemei:

- nShield F3 500 PCI kriptográfiai hardver modul (egyik HSM)
- SafeNet SafeNet Luna® PCICryptographic Module v2.2 (másik HSM)
- Microsoft Internet Information Server 6.0

2 Azonosítás

Az értékelt termék neve:	**InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz**
Verzió szám:	**v2.5**
Az értékelt termék alkotó elemei:	CA: • InfoCA.exe (2.0.0.31) • InfoCASetup.exe (2.0.4.2) • InfoCAKeySetup.exe (2.0.0.3) • Setup_InfoCA.exe (2.0.0.31) • CertSigner.dll (2.0.0.14) • CertSigner_NShield.dll (2.0.0.9) • ExtConfig.dll (1.0.1.21/1.0.1.22, norec/rec) RA: • InfoRA.exe (2.0.4.3) • Setup_InfoRA.exe (2.0.4.3) OCSP • OCSPResponder.dll (2.0.1.1) • OCSPResponderIsapi.dll (2.0.0.16) TSP • TSSResponder.dll (2.0.1.14) • TSSResponderIsapi.dll (2.0.0.67) • TimeServer.exe (2.0.0.3) Dokumentáció: • Adminisztrátori kézikönyv-v1.11 – InfoCA hitelesítés-szolgáltatás szoftver v2.5 • RA kézikönyv-v1.0 – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 *(nem változott az előző értékeléshez képest)* • Telepítési kézikönyv-v1.8 – InfoCA hitelesítés-szolgáltatás szoftver v2.5

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az InfoCA v2.5 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást. Először az InfoCA v2.5 egy üzemmódját határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

Jelen tanúsítási jelentés az InfoCA v2.5 azon üzemmódjára korlátozódik, amelybe a tanúsítványok elektronikus aláírása HSM modul felhasználásával történik, valamint a magánkulcsok tárolása és visszaállítása tiltott funkció.

3.2 Biztonsági funkciók

Az InfoCA rendszer az alábbi 10 biztonsági funkciót (BF) valósítja meg:

- BF1: Bizalmi munkakörök kezelése
- BF2: Azonosítás és hitelesítés
- BF3: Hozzáférés ellenőrzés
- BF4: Kulcskezelés
- BF5: Biztonsági naplózás
- BF6: A szolgáltatások által létrehozott és fogadott üzenetek védelme
- BF7: Tanúsítvány előállítás
- BF8: Tanúsítvány visszavonás
- BF9: Visszavonás állapot (CRL, OCSP)
- BF10: Időbélyegzés

A **Bizalmi munkakörök kezelése biztonsági funkció** megkülönbözteti az alábbi munkaköröket: rendszer biztonsági tisztviselő (SSO, System Security Officer), biztonsági tisztviselő (SO, Security Officer), regisztrációs tisztviselő (RO, Registration Officer). A felhasználókat összekapcsolja a fenti munkakörökkel, a különböző munkakörökhöz tartozó jogosultságokat pedig egységesen és biztonságosan kezeli.

Az **Azonosítás és hitelesítés biztonsági funkció** egyértelműen és hitelesen azonosítja a jogosult felhasználókat. Sikeres hitelesítés esetén a hitelesített felhasználó biztonsági tulajdonságait (szerepkör, s az ebből adódó jogosultságok) összekapcsolja az adott felhasználó nevében tevékenykedő szubjektumokkal. Sikertelen hitelesítés esetén az InfoCA rendszer adott elemét (InfoCaSetup.exe, InfoRA.exe) leállítja.

A **Hozzáférés ellenőrzés biztonsági funkció** ellenőriz minden hozzáférést a rendszer-, illetve felhasználói objektumokhoz. Az azonosított és hitelesített felhasználóknak az általuk betöltött szerepkör alapján engedélyezett hozzáféréseket teszi csak lehetővé. A jogosultság ellenőrzés két lépésben történik: első lépés a fiókok, konfigurációs állományok, profilok, regisztrációs kérelmek aláírásának az ellenőrzése, második lépés (érvényes aláírás esetén) az aláíró jogosultságának ellenőrzése. Ez a biztonsági funkció egyaránt visszautasítja az érvényes aláírás nélküli, illetve a jogosulatlanul aláírt állományokat.

A **Kulcskezelés biztonsági funkció** biztonságosan kezeli az InfoCA rendszer által használt különböző (tanúsítvány és CRL aláíró, infrastrukturális, rendszervezérlési és végfelhasználói) kulcsokat. A kriptográfiai szempontból biztonságkritikus kulcskezelési funkciók döntő többségét az IT környezet részét képező kriptográfiai hardver eszközök (HSM) végzik. Ez a biztonsági funkció a HSM modul aktivizálásával vezérli a kulcskezelési feladatokat. Ezek magukban foglalják a kulcsok generálását és törlését, a titkosító magánkulcsok exportálását, a

felhasználói titkos kulcsok kezelését, a titkosító magánkulcsok letétbe helyezését, tárolását és visszaállítását, valamint a nyilvános kulcsok védelmét.

A **Biztonsági naplózás biztonsági funkció** biztosítja a biztonsági szempontból fontos tevékenységek egyértelmű nyomon követhetőségét, megteremtve a teljes körű ellenőrzés lehetőségét. Ez a biztonsági funkció megfelelő adatokkal napló adatokat generál, az eseményeket összeköti a kiváltásukban közreműködő felhasználókkal, valamint digitálisan aláírja a naplóeseményeket. (A generált és aláírt naplóesemények egy Syslog szerverre továbbítódnak, így kikerülnek az InfoCA rendszerből. Következésképpen a naplórekordok megvédése, áttekintése és kiértékelése az InfoCA rendszer környezetének a feladata.)

A szolgáltatások által létrehozott üzenetek védelme biztonsági funkció biztosítja az InfoCA rendszernek beküldött adatok, valamint a rendszerből kikerülő adatok sértetlenségét és hitelességét. Ellenőrzi a hitelesség szempontjából kritikus bejövő üzenetek eredetét, illetve (digitális aláírással) biztosítja az ilyen kimenő üzenetek eredet bizonyításának a lehetőségét, valamint védi az InfoCA rendszer belső (az RA kliens és a CA szerver közötti) adatkommunikációját is.

A **Tanúsítvány előállítás biztonsági funkció** biztosítja az InfoCA 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 biztosítja, hogy a kiadott tanúsítványok megfelelnek valamelyik profilnak.

A **Tanúsítvány visszavonás biztonsági funkció** biztosítja az InfoCA rendszer alap szolgáltatásai közé tartozó, tanúsítvány felfüggesztésre, felfüggesztés megszüntetésre és tanúsítvány visszavonásra irányuló jogosult kérelmek biztonságos végrehajtását, valamint frissíti a tanúsítvány állapot adatbázist.

A **Visszavonás állapot funkció** biztosítja az InfoCA rendszer visszavonás állapot alap szolgáltatását, CRL-ek rendszeres időközönkénti kibocsátásával, valamint OCSP kérések azonnali megválaszolásával biztosítja a tanúsítvány állapotok lekérdezhetőségét, megismerhetőségét.

Az **Időbélyegzés funkció** biztosítja az InfoCA rendszer időbélyegzés kiegészítő szolgáltatását, szabványos időbélyeg kérésekre szabványos időbélyeg válaszok biztosításával (beleértve az ehhez szükséges pontos idő garantálását is, időszinkronizálás útján).

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 InfoCA v2.5 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. Az InfoCA 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 az InfoCA 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 az InfoCA-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. Az InfoCA 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 az InfoCA 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 az InfoCA 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 az InfoCA által elvárt azon funkciókkal, melyek a biztonsági előirányzat 3.3 alfejezetében meghatározott fenyegetések kivédéséhez szükségesek. (A.Operating System)

4.1.3 Fizikai feltételek

11. Az InfoCA rendszer megfelelő fizikai védelemmel van ellátva a kommunikáció elvesztésével, azaz a kommunikáció rendelkezésre állásának elvesztésével szemben. (A.Communication Protection)
12. Az InfoCA 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 HSM támogatására építő üzemmód

Az InfoCA rendszer a kriptográfiai algoritmusok megvalósítása szempontjából két Crypto üzemmódot is támogat: HSM modulra épülőt, illetve szoftveres megvalósítást.
A CertSigner.dll könyvtárnak két változata van, az egyik egy hardver kriptográfiai modul (HSM) szolgáltatásait aktivizálja a különböző kriptográfiai algoritmusok megvalósításához, a másik szoftveresen valósítja meg ezeket. A telepítés során, a Setup_InfoCA.exe alkalmazás futtatásakor, a rendszeradminisztrátor választja ki a megfelelő Crypto üzemmódot.

Érvényességi feltétel:

1. Az InfoCA rendszer éles használata kizárólag a HSM modul támogatására építő üzemmódra szorítkozhat, a szoftveres üzemmód csak tesztelési célokat szolgál.

4.2.2 MSZ CWA 14167-1 követelményeknek való megfelelés

Az InfoCA rendszerre (mint „megbízható rendszer hitelesítés-szolgáltatáshoz” elektronikus aláírási termék) az alábbi nemzetközi követelményrendszer is vonatkozik, mely egyúttal magyar szabvány is:

- CEN Workshop Agreement 14167-1:2003 Security Requirements for Trustworsthy 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 InfoCA rendszer biztosítja (azaz teljes mértékben megfelel a követelménynek), egy másik részét pedig támogatja (azaz részben megfelel a követelménynek).
A követelmények egy harmadik csoportjában az InfoCA 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 10.1 fejezet részletezi.

Érvényességi feltételek:

2. Az IT környezet biztosítsa és kezelje a rendszeradminisztrátor (SSO, SO), a rendszerüzemeltető (RO) és rendszervizsgáló szerepköröket.
3. Az IT környezet (operációs rendszer) biztosítsa a saját és külső felhasználóknak kinyomtatott PIN kódok, mint érzékeny maradvány információk védelmét.
4. Az IT környezet biztosítsa a megfelelő HSM modul használatát, illetve a HSM modul tanúsításakor meghatározott felhasználási feltételek betartását.

5. Az IT környezet biztosítsa a tanúsítvány helyességének garantálása céljából a gyökértanúsítvány lenyomatának ellenőrizhetőségét egy megbízható útvonalon biztosított információ megadásával.
6. Az InfoCA rendszer használata során biztosítani kell a megfelelő tanúsítvány profilok kizárólagos használatát.
7. Elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén az aláíró tanúsítvány profilokban a kulcsletétbe helyezés funkciót tiltani kell.
8. Az IT környezet biztosítsa az InfoCA rendszer futtatható állományainak sértetlenségét.
9. Minősített elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén az InfoCA rendszert az ExitConfig.dll (noreq) verziójával kell telepíteni.
10. A naplózás tárolási hibája miatt végzett tevékenységek naplózása érdekében IT és nem IT eljárásokat kell foganatosítani.
11. A napló események digitális aláírásának az ellenőrzését (vagyis a napló sértetlenségének igazolását) az IT környezetnek kell biztosítania
12. Az IT környezet biztosítsa az RA és CA alrendszerek között cserélt információk bizalmasságát.
13. A megújítandó tanúsítványok érvényességét IT és nem IT eljárásokkal biztosítani kell.
14. Az IT környezet biztosítson az OCSP alrendszer és a CA alrendszer között megbízható csatornát és garantálja, hogy az OCSP alrendszer az adott tanúsítvány aktuális állapotával válaszol.
15. Időszakonként az InfoCA rendszerben alkalmazott algoritmusokról ellenőrizni kell, hogy azok megfelelnek-e a "Biztonságos algoritmusok[1]" című dokumentumban meghatározott követelményeknek.
16. IT és nem IT eljárásokat kell foganatosítani az alábbi követelmények teljesüléséhez:
    [M1.4] QCA ;[SO2.1]; [SO2.2]; [SO2.3] ;[SO3.1] QCA; [SO3.1] NQCA;
    [IA2.2] QCA; [SA1.2]; [KM1.2]; [KM1.3]; [KM1.4]; [KM1.7]; [KM2.4]; [KM2.6];
    [KM3.1]; [KM3.2] QCA; [KM4.1]; [KM4.2]; [KM5.1; [KM5.2]; [KM5.3]; [KM5.4];
    [KM6.1]; [KM6.2]; [KM6.3]; [KM6.4]; [KM6.5]; [KM6.6]; [AA2.1]; [AA2.2];
    [AA4.1]; [AA4.2]; [AA5.1]; [AA6.1]; [AA8.1]; [AR1.1]; [AR1.2]; [AR1.3]; [AR1.4];
    [AR2.1]; [AR3.1]; [BK1.1]; [BK1.2]; [BK1.3]; [BK2.1] NQCA; [BK2.1] QCA;
    [BK2.2]; [BK3.1]; [BK3.2]; [R1.1]; [R1.2]; [R1.3] QCA; [R1.4]; [R1.5] QCA; [R1.6];
    [R2.1]; [R3.1]; [CG1.2]; [CG1.3]; [CG2.1]; [CG2.2]; [CG2.3]; [CG2.4]; [CG3.1];
    [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1]; [RS2.2], [TS1.1],
    [TS2.1], [TS2.2], [TS4.2], [TS4.3], [TS4.4], [TS4.6], [TS6.1], [SP1.1]; [SP1.3];
    [SP1.4]; [SP1.5]; [SP1.6]; [SP1.7]; [SP2.1]; [SP3.1]; [SP3.2]

4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az InfoCA v2.5 valamennyi biztonsági funkcióját.

[1] Lásd 13.4: ETSI SR 002 176-1 v2.0.0

5 Az InfoCA v2.5 szerkezeti leírása

Az InfoCA v2.5 (InfoCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Az InfoCA rendszer az alábbi hitelesítés-szolgáltatásokat támogatja:

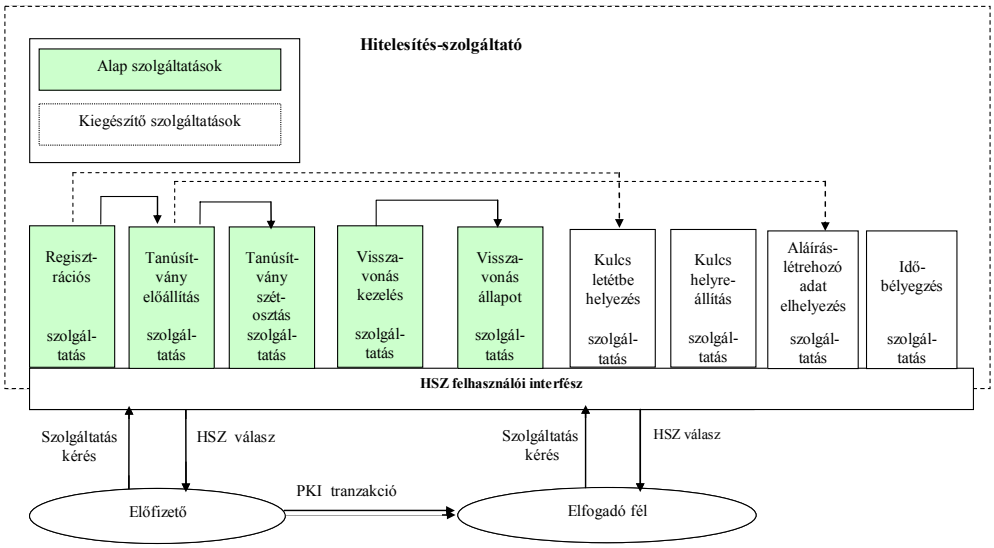
Alap (kötelező) szolgáltatások:

- Regisztrációs szolgáltatás (az InfoCA rendszeren kívül valósul meg, de eredményét az InfoCA rendszer használja)
- Tanúsítvány előállítás szolgáltatás,
- Tanúsítvány szétosztás szolgáltatás,
- Visszavonás kezelés szolgáltatás,
- Visszavonás állapot szolgáltatás (CRL, OCSP).

Kiegészítő (opcionális) szolgáltatások:

- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás,
- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (az InfoCA rendszeren kívül valósul meg),
- időbélyegzés szolgáltatás.

Az InfoCA rendszer alapvetően egy hitesítés-szolgáltató megbízható rendszerének lett tervezve, mely a hitesítés-szolgáltató által nyújtott (alap és kiegészítő) szolgáltatásokat valósítja meg, vagy nyújt a megvalósításhoz műszaki támogatást, ahogyan azt az 1. ábra szemlélteti. /Az ábrán jelzett regisztrációs, valamint az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást az InfoCA rendszer környezete valósítja meg./



1. ábra Az InfoCA v2.5 általános felépítése

5.1 Architektúra

Egy szerverhez elvileg kapcsolódhat több kliens is, egy kliens pedig több szerverrel is képes kommunikálni, biztosítva ezzel a rendelkezésre állás növelésének, illetve a terhelésmegosztásnak a lehetőségét. A szerver és kliensek közötti belső kommunikáció hitelesített.

Az RA kliens felelős a különböző szolgáltatási kérések kiadásáért. (Az előfizetőktől beérkező szolgáltatási kérések fogadása, hitelesség ellenőrzése és megválaszolása nem az InfoCA rendszer feladata.).

A CA szerver végzi a különböző szolgáltatási kérések automatikus feldolgozását, teljesítését. A CA szerver a kérések teljesítése előtt elvégzi a kérést kezdeményező (RO) hitelesítésének és jogosultságának az ellenőrzését is.

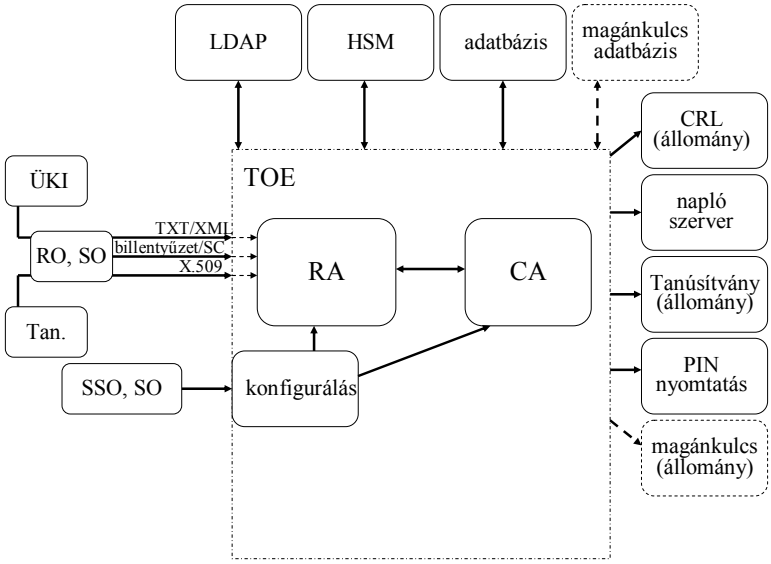
Az InfoCA rendszer biztonságot növelő szerkezeti különlegessége, hogy a biztonság-kritikus CA alrendszernek ügyfelekkel nincs közvetlenül kommunikációs kapcsolata:

- az ügyfelektől származó kérések helyességét és jogosultságát az InfoCA rendszer környezete végzi el, s a helyes és jogosult kéréseket az RO-k továbbítják az RA-ból a CA-nak,
- a CA-hoz beérkező kérésekre születő egyik lehetséges választípus (kibocsátott tanúsítvány, generált kulcspár, kinyomtatott PIN boríték, visszaállított titkosított magánkulcs) az RA közvetítésével, de szintén az InfoCA rendszer környezete által megvalósítva jut el az ügyfelekhez,
- a CA-hoz beérkező kérésekre születő másik választípus a kibocsátott visszavonási lista, melyet a CA LDAP-okba publikál, az ügyfelek azokat onnan érhetik el.

A TS és OCSP alrendszerek elvileg futhatnak két különböző szerveren is, de ezek mindenképpen különböznek a CA szervertől.

Az InfoCA rendszer valamennyi alrendszere (RA, CA, TS, OCSP) különböző módon konfigurálható egy külső interfészen keresztül.

Az InfoCA rendszernek számos külső interfésze van, a 2. és 3. ábrák ezekről adnak egy áttekintést.



2. ábra: Az InfoCA rendszer határai (RA, CA)

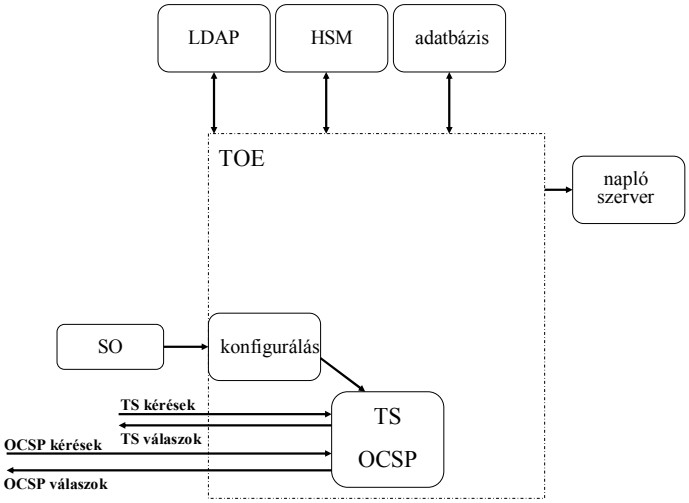
Az InfoCA rendszer (annak RA és CA alrendszerei) különböző helyekről és formákban kaphatja meg a funkcióihoz szükséges adatokat:

- az Ügyfél Kapcsolati Irodától (**ÜKI**) kapott TXT vagy XML formátumú állomány (RO általi) beolvasásával,
- az RA-t kezelő regisztrációs tisztviselő (**RO**) által **billentyűzet**ről történő beütéssel, illetve intelligens kártyáról (**SC**) történő beolvasással.
- X509-es szerkezetű **tanúsítvány**(oka)t tartalmazó állomány (RO általi) beolvasásával,
- a címtárban (**LDAP**) tárolt adatszerkezet lekérdezésével,
- a kriptográfiai hardver modultól **(HSM)** kapott válaszok fogadásával,
- saját **adatbázis**ából,
- **magánkulcs adatbázis**ából (az opcionális „titkosító magánkulcs letétbe helyezés” és „titkosító magánkulcs helyreállítás” szolgáltatások támogatása esetén).

Az InfoCA rendszer (annak RA és CA alrendszerei) különböző helyekre továbbítja az általa elkészített objektumokat:

- az előállított tanúsítványokat és az aktuális CRL-eket címtárba publikálják (**LDAP**),
- különböző kulcsműveletek végrehajtása érdekében parancsokat küld a kriptográfiai hardver modulnak **(HSM)**,
- különböző adatokat küld saját **adatbázis**ába,
- letétbe helyezett kulcsokat küld **magánkulcs adatbázis**ába (amennyiben támogatja a „titkosító magánkulcs letétbe helyezés” és „titkosító magánkulcs helyreállítás” szolgáltatásokat).
- archiválás céljából **CRL állomány**ba menti az aktuális CRL-t,
- a működés jellemzőit rögzítő naplóeseményeket egy **naplószerver**hez továbbítja,
- ügyfélhez való továbbítás céljából **tanúsítvány állomány**ba menti az aktuálisan előállított tanúsítványokat,
- a PKCS#12-es formátumban kibocsátott tanúsítványokhoz, illetve az opcionálisan kezelt aláírás-létrehozó eszközökhöz (intelligens kártyákhoz) tartozó PIN kódokra védett módon elvégezteti a **PIN nyomtatás**t,
- PKCS#12-es formátumban kiadja a **magánkulcs állomány**t (amennyiben támogatja a „titkosító magánkulcs letétbe helyezés” és „titkosító magánkulcs helyreállítás” szolgáltatásokat).

A 3. ábra a TS és OCSP alrendszerek határait tekinti át.



3. ábra: Az InfoCA rendszer határai (TS, OCSP)

A biztonsági tisztviselők (SO) által konfigurálható TS (időbélyegzés) alrendszer:

- az RFC 3161 szabvány előírásainak megfelelő szabványos időbélyeg kérésekre szabványos időbélyeg válaszokat hoz létre,
- az időbélyeg tokeneket a HSM-ben generált és tárolt magánkulccsal aláírattatja,
- a naplószerverre továbbít (archiválási célból) minden időbélyeg tokent.

A biztonsági tisztviselők (SO) által konfigurálható OCSP alrendszer:

- az RFC 2560 szabvány előírásainak megfelelő szabványos OCSP kérésekre szabványos OCSP válaszokat hoz létre,
- a konfigurált üzemmódtól függően az OCSP válaszokat az LDAP vagy az adatbázis információi alapján állítja össze,
- az OCSP válaszokat a HSM-ben generált és tárolt magánkulccsal aláírattatja,
- a naplószerverre továbbít (archiválási célból) minden OCSP kérést és OCSP választ.

5.2 Alrendszerek

Az InfoCA rendszer logikailag az alábbi 6 fő alrendszerre osztható.

- AR1: konfigurálás (RA-t, CA-t, TS-t és OCSP-t konfiguráló alrendszer)
- AR2: RA (kliens oldali alrendszer)
- AR3: CA (szerver oldali alrendszer)
- AR4: kommunikáció (RA és CA közötti kommunikációt megvalósító alrendszer)
- AR5: OCSP (OCSP alrendszer)
- AR6: TS (időbélyeg alrendszer)

6 Tesztelés

Az InfoCA rendszer tesztelésének megközelítése a következő volt:

- Az InfoCA v2.5 a korábban már értékelt TCA v2.0 olyan bővítésével keletkezett, hogy a régi rendszer mellé (a CA és RA alrendszerek), lényegében független módon, egy másik szerveren megvalósították a két új alrendszert (TS és OCSP).
- Az InfoCA v.2.5 korábbi alrendszerei (CA, RA, az ezek közötti kommunikáció, valamint ezek konfigurálása) lényegében változatlanok maradtak, ezek ismételt tesztelése ezért nem szükséges, a korábbi teszteléséi eredmények elfogadhatók.
- Az InfoCA v.2.5 új alrendszerei (TS és OCSP, beleértve ezek konfigurálását is) új fejlesztés, melyet alaposan tesztelni kell.
- Az új alrendszerek tesztelését (a fejlesztők aktív támogatásával) az értékelők végezték el.

6.1 A fejlesztők tesztelése

A fejlesztő tesztelése nagyon alapos, dokumentálása kellően részletes. A korábbi értékelés során végzett tesztelési eredményeket az értékelő elfogadta. Ezért tesztelési stratégiaként az új funkcionális és biztonsági funkciók minden elemének egyedi letesztelését, azoknak a hiba ágainak megfelelő kezelését bemutató irányt választották.

Korábbi értékelés tesztelése (most nem került megismétlésre):

BF	pozitív	negatív	összesen
1	3	0	3
2	2	2	4
3	6	6	12
4	16	6	22
5	65	28	93
6	5	0	5
7	112	22	134
8	14	12	26
	223	76	299

Újraértékelés tesztelése:

BF	pozitív	negatív	összesen
9	11	9	20
10	10	10	20
	21	19	40

A tesztelt konfiguráció megfelel a biztonsági előirányzatban foglaltaknak.

6.2 Az értékelők tesztelése

A független tesztelés stratégiája az alábbi volt: A fejlesztői teszt megismétlése az új biztonsági funkciókra (BF9, BF10).

A független tesztelés során hiba nem lépett fel.

7 Az értékelt konfiguráció

7.1 CA szerver

CA szerver (CA) TOE elemei:

- InfoCA.exe (2.0.0.31)
- InfoCASetup.exe (2.0.4.1)
- Setup_InfoCA.exe (2.0.4.2)
- CertSigner.dll (2.0.0.14)
- CertSigner_NShield.dll (2.0.0.9)
- ExtConfig.dll (1.0.1.21/1.0.1.22, norec/rec)

CA szerver (CA) környezet elemei:

- Windows 2003 Szerver, Enterprise edition, SP1
- Intel P4, 1,8 GHz
- 256 MB RAM
- MS SQL Szerver 2005
- OpenLDAP 2.2.29
- Syslog-win32-0.3
- nShield F3 500 PCI kriptográfiai hardver modul (egyik HSM)
- SafeNet Luna® PCICryptographic Module v2.2 (másik HSM)
- .NET 3.0

7.2 RA kliens

Kliens (RA) TOE elemei:

- InfoRA.exe (2.0.4.3)
- Setup_InfoRA.exe (2.0.4.3)

Kliens (RA) környezet elemei:

- Windows XP, Professional, SP2
- Intel P4 Cel., 2,4 GHz
- 768 MB RAM
- .NET 3.0
- Omnikey CardMan 3121
- Oberthur CosmopolIC SmartCard
- Giesecke, SPK 2.3 Standard V7.0 T=1, SmartCard (StarCert)
- Giesecke, StarSign

7.3 TS, OCSP alrendszerek

TS, OCSP TOE elemei:

- TSSResponder.dll (2.0.1.14)
- TSSResponderIsapi.dll (2.0.0.67)
- TimeServer.exe (2.0.0.3)
- OCSPResponder.dll (2.0.1.1)
- OCSPResponderIsapi.dll (2.0.0.16)

TS, OCSP környezet elemei:

- nShield F3 500 PCI kriptográfiai hardver modul (egyik HSM)
- SafeNet SafeNet Luna® PCICryptographic Module v2.2 (másik HSM)
- Microsoft Internet Information Server 6.0

8 Az értékelés eredményei

Az InfoCA v2.5 a CEM (Common Evaluation Methodology) v2.3 módszertana szerint független értékelésre és tanúsításra került, (Hibajelentési eljárásokkal, ALC_FLR.2) kibővített EAL4+ értékelési garanciaszinten.

Az értékelés fő következtetése az alábbi:

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy az InfoCA v2.5 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

A fenti megállapítás az EAL4+ követelményeinek teljesítésén alapul.

Az értékelés másik következtetése az alábbi:

Az InfoCA v2.5 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[2] /és a fejlesztői bizonyíték/
Biztonsági előirányzat	ASE_DES.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_ENV.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_INT.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_OBJ.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_PPC.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_REQ.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_SRE.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1
	ASE_TSS.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Biztonsági előirányzat** v1.1

[2] Az értékelés részletes eredményei üzleti tikot képez

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye[2] /és a fejlesztői bizonyíték/
Konfiguráció menedzselés	ACM_CAP.4	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfiguráció menedzselés dokumentációja** v1.2
	ACM_SCP.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfiguráció menedzselés dokumentációja** v1.2
	ACM_AUT.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfiguráció menedzselés dokumentációja** v1.2
Kiszállítás és működtetés	ADO_DEL.2	A követelményeknek **megfelelt**. InfoCA v2.5 hitelesítés-szolgáltatás szoftver **Telepítési kézikönyv** v1.8
	ADO_IGS.1	A követelményeknek **megfelelt**. InfoCA v2.5 hitelesítés-szolgáltatás szoftver **Telepítési kézikönyv** v1.8
Fejlesztés	ADV_FSP.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Funkcionális specifikáció (FS) v1.1**
	ADV_HLD.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **Magas szintű terv (HLD) v1.1**
	ADV_IMP.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **Forráskód**
	ADV_LLD.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **Alacsony szintű terv (LLD)** v1.1
	ADV_RCR.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **Megfelelés elemzés** v1.1
	ADV_SPM.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz **–** **Biztonsági szabályzat modell** v1.1
Útmutató dokumentumok	AGD_ADM.1	A követelményeknek **megfelelt**. **Adminisztrátori kézikönyv** v1.11 – InfoCA v2.5 hitelesítés-szolgáltatás szoftver
	AGD_USR.1	A követelményeknek **megfelelt**. **RA kézikönyv** v1.0 – Trust&CA hitelesítés-szolgáltatás szoftver v2.0

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye[2] /és a fejlesztői bizonyíték/
Az életciklus támogatása	ALC_DVS.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **A fejlesztési biztonság dokumentációja** v1.1
	ALC_LCD.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Az életciklust meghatározó dokumentáció** v1.1
	ALC_TAT.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **A fejlesztő eszközök dokumentációja** v1.1
	ALC_FLR.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **A hibajelentési eljárások** v1.1
Tesztelés	ATE_FUN.1	A követelményeknek **megfelelt**. **Tesztelési dokumentáció (tesztelési jegyzőkönyvek)**
	ATE_COV.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **Teszt lefedettség elemzés** v1.1
	ATE_DPT.1	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **Teszt mélység elemzés** v1.1
	ATE_IND.2	A követelményeknek **megfelelt**. **A tesztelésre alkalmas InfoCA v2.5**
A sebezhetőség felmérése	AVA_MSU.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **Az útmutatók elemzése** v1.1
	AVA_SOF.1	A követelményeknek **megfelelt**. **Biztonsági funkcióerősség elemzés v1.0** – Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	AVA_VLA.2	A követelményeknek **megfelelt**. InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Sebezhetőség elemzés** v1.1

9 Értékelői megjegyzések és javaslatok

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

10 Mellékletek

10.1 Az InfoCA v2.5 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 InfoCA v2.5 rendszer teljesíti** (azaz teljes mértékben megfelel a követelménynek)
- **Az InfoCA v2.5 rendszer támogatja** (azaz részben megfelel a követelménynek, de a környezetnek is támogatást kell nyújtania),
- **A környezetnek kell biztosítania** (azaz az InfoCA v2.5 rendszer nem vállalja fel a követelmény teljesítését, a megvalósítást az IT és nem IT környezettől várja el),
- **Az InfoCA v2.5 rendszerre nem vonatkozik a követelmény.**

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 InfoCA rendszer teljesíti**
2	[M1.2]	Legalább a következő munkakörök szükségesek:	**az InfoCA rendszer támogatja**
3	[M1.3]	Felhasználók és munkakörök összekapcsolási képessége.	**az InfoCA rendszer támogatja**
4	[M1.4] QCA	Összeférhetetlen munkakörök	**a környezetnek kell biztosítania**
Rendszerek és működésük (SO)			
SO1 Üzemeltetés menedzselése			
5	[SO1.1]	Útmutatók biztosítása (helyes és biztonságos működtetés).	**az InfoCA rendszer teljesíti**
SO2 A folyamatos szolgáltatás biztosítása			
6	[SO2.1]	99.9%-os rendelkezésre állás (tanúsítvány szétosztás, visszavonás kezelés, visszavonás állapot szolgáltatás).	**a környezetnek kell biztosítania**
7	[SO2.2]	Katasztrófahelyzetben is a működés (alternatív TWS)	**a környezetnek kell biztosítania**
8	[SO2.3]	Biztonságos áttérés a katasztrófa-helyreállító rendszerre.	**a környezetnek kell biztosítania**

SO3 Időszinkronizáció			
9	[SO3.1] QCA	UTC –hez szinkronizált óra, (1sec), 2 független forrás.	**a környezetnek kell biztosítania**
10	[SO3.1] NQCA	Állítást kell megfogalmazni az idő pontosságára.	**a környezetnek kell biztosítania**
Azonosítás és hitelesítés (IA)			
IA1 A felhasználó hitelesítése			
11	[IA1.1]	Kötelező felhasználói azonosítás és hitelesítés.	**az InfoCA rendszer támogatja**
12	[IA1.2]	A felhasználó kijelentkezése után kötelező az újrahitelesítés.	**az InfoCA rendszer támogatja**
13	[IA1.3]	Egyedi hitelesítő adatok.	**az InfoCA rendszer támogatja**
IA2 Hitelesítési hiba			
14	[IA2.1]	A sikertelen hitelesítési kísérletek korlátozása.	**az InfoCA rendszer támogatja**
15	[IA2.2] QCA	Riasztás max. sikertelen hitelesítési kísérlet elérésekor.	**a környezetnek kell biztosítania**
IA3 A titok ellenőrzése			
16	[IA3.1]	Mechanizmus a titkok ellenőrzésére.	**az InfoCA rendszer támogatja**
Rendszer-hozzáférés ellenőrzés (SA)			
SA1 Rendszer-hozzáférés ellenőrzés			
17	[SA1.1]	Azonosított egyének hozzáférésének ellenőrzése, korlátozása.	**az InfoCA rendszer támogatja**
18	[SA1.2]	Hozzáférés védelem az érzékeny maradvány információkra.	**a környezetnek kell biztosítania**
Kulcs kezelés (KM)			
KM1 Kulcs generálás			
19	[KM1.1]	A tanúsítvány aláíró kulcsokat biztonságos kriptográfiai modulban (HSM) kell generálni.	**az InfoCA 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.	**a környezetnek kell biztosítania**
-	[KM1.5] QCA	törölve	-
-	[KM1.6] NQCA	törölve	-
23	[KM1.7]	A kulcs generálás algoritmusa biztonságos legyen.	**a környezetnek kell biztosítania**
KM2 Kulcs elosztás			
24	[KM2.1]	A magán/titkos kulcsokat tilos nyílt formában szétosztani.	**az InfoCA rendszer támogatja**
25	[KM2.2]	A még tanúsítványba nem foglalt nyilvános kulcsokat biztonságos környezetben kell tartani.	**az InfoCA rendszer teljesíti**
26	[KM2.3]	Szabványos kriptográfiai	**az InfoCA rendszer teljesíti**

		kulcselosztó módszer használata.	
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 InfoCA rendszer támogatja**
29	[KM2.6]	Önaláírt tanúsítványra biztonságos lenyomat készítése.	**a környezetnek kell biztosítania**
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.	**a környezetnek kell biztosítania**
32	[KM3.3] QCA	Funkciónként különböző infrastrukturális kulcsok.	**az InfoCA rendszer teljesíti**
33	[KM3.4]	El kell különíteni az aláíró kulcsokat.	**az InfoCA rendszer teljesíti**
34	[KM3.5]	Jogosult kulcshasználat csak életcikluson belül történhet.	**az InfoCA rendszer teljesíti**
35	[KM3.6]	Kulcshasználat előtt tanúsítvány érvényesség ellenőrzés.	**az InfoCA rendszer támogatja**
KM4 Kulcs csere			
36	[KM4.1]	I. és RV kulcsokat rendszeresen (pl. évente) cserélni kell.	**a környezetnek kell biztosítania**
37	[KM4.2]	A kulcs cserét biztonságosan kell végrehajtani.	**a környezetnek kell biztosítania**
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.	**a környezetnek kell biztosítania**
KM6 Kulcs tárolása, mentése és helyreállítása			
42	[KM6.1]	Minden magán/titkos kulcsot biztonságosan kell tárolni.	**a környezetnek kell biztosítania**
43	[KM6.2]	A TA kulcsokat HSM-ben kell tárolni.	**a környezetnek kell biztosítania**
44	[KM6.3]	Az I és RV kulcsokat HKE-ben kell tárolni.	**a környezetnek kell biztosítania**
45	[KM6.4]	Kulcs exportálás csak védett módon.	**a környezetnek kell biztosítania**
46	[KM6.5]	Kulcsokat csak jogosult személy (pl. SO) kezelheti.	**a környezetnek kell biztosítania**
47	[KM6.6]	TA magánkulcsok kezelése kettős személyi ellenőrzés alatt.	**a környezetnek kell biztosítania**
48	[KM6.7]	Tilos aláíró magánkulcsot menteni,	**az InfoCA rendszer teljesíti**

		letétbe helyezni.	
49	[KM6.8][3]	Biztosítani kell a titkosító magánkulcsok letétbe helyezését lehetővé tévő funkciót.	**az InfoCA rendszer teljesíti**
50	[KM6.9][4]	Biztosítani kell a letétbe helyezett titkosító magánkulcsok sértetlenségét és bizalmasságát.	**az InfoCA rendszer teljesíti**
51	[KM6.10][5]	Biztosítani kell a letétbe helyezett titkosító magánkulcsok helyreállítását lehetővé tévő funkciót.	**az InfoCA rendszer teljesíti**
52	[KM6.11][6]	Biztosítani kell, hogy a titkosító magánkulcsok helyreállítása csak kettős személyi ellenőrzés mellett valósulhasson meg.	**a környezetnek kell biztosítania**
KM7 Kulcs archiválás			
53	[KM7.1]	Tilos az aláíró magánkulcsok archiválása.	**az InfoCA rendszer teljesíti**
Naplózás (AA)			
AA1 Napló adatok generálása			
54	[AA1.1]	A következő események naplózása feltétlenül szükséges: …..	**az InfoCA rendszer teljesíti**
AA2 Napló adatok garantált rendelkezésre állása			
55	[AA2.1]	Karban kell tartani a naplózási adatokat.	**a környezetnek kell biztosítania**
56	[AA2.2]	A naplóbejegyzéseket nem szabad automatikusan felülírni.	**a környezetnek kell biztosítania**
AA3 Naplózási paraméterek			
57	[AA3.1]	Minden naplórekordnak tartalmaznia kell a következőket: …	**az InfoCA rendszer teljesíti**
AA4 A napló választható áttekintése			
58	[AA4.1]	Gondoskodni kell a naplóesemények közötti keresésről.	**a környezetnek kell biztosítania**
59	[AA4.2]	A naplórekordot ember által olvashatóan kell megjeleníteni.	**a környezetnek kell biztosítania**
AA5 Korlátozott naplómegtekintés			
60	[AA5.1]	A naplót csak jogosultsággal lehessen olvasni.	**a környezetnek kell biztosítania**
61	[AA5.2]	Meg kell akadályozni a naplózási rekordok módosítását.	**az InfoCA rendszer támogatja**
AA6 Riasztás generálása			
62	[AA6.1]	Riasztás kell a biztonság potenciális megsértése esetén.	**a környezetnek kell biztosítania**
AA7 A napló adatok sértetlenségének garantálása			
63	[AA7.1] NQCA	Biztosítani kell a napló adatok	**az InfoCA rendszer támogatja**

[3] nincs a CWA-ban, kiegészítés!
[4] nincs a CWA-ban, kiegészítés!
[5] nincs a CWA-ban, kiegészítés!
[6] nincs a CWA-ban, kiegészítés!

		sértetlenségét.	
64	[AA7.1] QCA	Biztosítani kell a napló sértetlenségét: (DS, HMAC, auth)	**az InfoCA rendszer támogatja**
AA8 A napló időbejegyzéseinek garantálása			
65	[AA8.1]	Megbízható időforrást kell alkalmazni a naplóhoz.	**a környezetnek kell biztosítania**
Archiválás (AR)			
AR1 Archív adatok generálása			
66	[AR1.1]	Képesnek kell lenni archívum létrehozására.	**a környezetnek kell biztosítania**
67	[AR1.2]	Archiválni kell az alábbiakat: …..	**a környezetnek kell biztosítania**
68	[AR1.3]	Minden bejegyzésnek tartalmaznia kell az időpontot.	**a környezetnek kell biztosítania**
69	[AR1.4]	Archívumban kritikus biztonsági paraméter csak védetten.	**a környezetnek kell biztosítania**
AR2 Szelektálható keresés			
70	[AR2.1]	Az archívumra biztosítani kell egy keresési lehetőséget.	**a környezetnek kell biztosítania**
AR3 Az archivált adatok sértetlensége			
71	[AR3.1]	Az archívum bejegyzéseit védeni kell a módosítástól.	**a környezetnek kell biztosítania**

Mentés és helyreállítás (BK)			
BK1 Mentés generálása			
72	[BK1.1]	Léteznie kell egy mentési funkciónak.	**a környezetnek kell biztosítania**
73	[BK1.2]	A mentett adatokból a rendszer visszaállítható legyen.	**a környezetnek kell biztosítania**
74	[BK1.3]	A mentési funkció meghívható legyen (jogosultan).	**a környezetnek kell biztosítania**
BK2 A mentési információ sértetlensége és bizalmassága			
75	[BK2.1] NQCA	A mentést védeni kell a módosítás ellen.	**a környezetnek kell biztosítania**
76	[BK2.1] QCA	A mentést védeni kell a módosítás ellen: (DS, HMAC, auth).	**a környezetnek kell biztosítania**
77	[BK2.2]	Kritikus bizt. par-k csak titkosított formában tárolhatók.	**a környezetnek kell biztosítania**
BK3 Helyreállítás			
78	[BK3.1]	Biztosítani kell egy helyreállítási funkciót.	**a környezetnek kell biztosítania**
79	[BK3.2]	A helyreállítási funkció meghívható legyen (jogosultan).	**a környezetnek kell biztosítania**
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 InfoCA rendszer teljesíti**
Regisztráció szolgáltatás (R)			
R1 Tanúsítvány kérelem			
81	[R1.1]	A tanúsítvány kérést szükség esetén védeni kell.	**a környezetnek kell biztosítania**
82	[R1.2]	Megfelelő mechanizmus szükséges a birtoklás bizonyítására.	**a környezetnek kell biztosítania**
83	[R1.3] QCA	A regisztráció tegye lehetővé az aláíró adatai összegyűjtését.	**a környezetnek kell biztosítania**
84	[R1.4]	Mechanizmus kell a tanúsítvány kérelmek jóváhagyására.	**a környezetnek kell biztosítania**
85	[R1.5] QCA	A kérelmeket el kell látni a következő jellemzőkkel:	**a környezetnek kell biztosítania**
86	[R1.6]	A regisztráció üzeneteit alá kell írni.	**a környezetnek kell biztosítania**
R2 Tanúsítvány kérelem			
87	[R2.1]	Az alanyra vonatkozó információ bizalmasságát védeni kell.	**a környezetnek kell biztosítania**
R3 Regisztráció szolgáltatás naplózása			
88	[R3.1]	A regisztráció alábbi eseményeit kötelező naplózni:	**a környezetnek kell biztosítania**

Tanúsítvány előállítás szolgáltatás (CG)			
CG1 Tanúsítvány előállítás			
89	[CG1.1]	Biztosítani kell a tanúsítvány kérelem üzenet védelmét.	**az InfoCA rendszer támogatja**
90	[CG1.2]	A tanúsítvány kérelmet biztonságosan kell feldolgozni.	**a környezetnek kell biztosítania**
91	[CG1.3]	Biztosítani kell a birtoklás bizonyításának az ellenőrzését.	**a környezetnek kell biztosítania**
92	[CG1.4] - QCA	A TA csak erre (és a CRL aláírására) használható fel.	**az InfoCA rendszer teljesíti**
93	[CG1.5]	Meg kell felelni a meghatározott profiloknak.	**az InfoCA rendszer teljesíti**
94	[CG1.6] NQCA	A tanúsítványoknak meg kell felelniük az alábbiaknak:	**az InfoCA rendszer támogatja**
95	[CG1.6] QCA	A tanúsítványoknak meg kell felelniük: ETSI TS 101 862	**az InfoCA rendszer támogatja**
CG2 Tanúsítvány megújítás			
96	[CG2.1]	A tanúsítvány megújítás során védekezni kell a tanúsítvány helyettesítés támadás ellen.	**a környezetnek kell biztosítania**
97	[CG2.2]	I és RV kulcsokra a tanúsítvány megújításnak teljesítenie kell a KM.4 (kulcs csere) feltételeit is.	**a környezetnek kell biztosítania**
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.	**a környezetnek kell biztosítania**
CG3 Felülhitelesítés			
100	[CG3.1]	Felülhitelesítés alkalmazása esetén biztosítania kell:…	**a környezetnek kell biztosítania**
CG4 A tanúsítvány előállítás szolgáltatás naplózása			
101	[CG4.1]	A tanúsítvány előállítás alábbi eseményeit kell naplózni:	**az InfoCA rendszer teljesíti**
Tanúsítvány szétosztás szolgáltatás (D)			
D1 Szétosztás kezelés			
102	[D1.1]	A tanúsítvány szétosztás csak alanyoknak és az engedélyezett érintett feleknek.	**a környezetnek kell biztosítania**
103	[D1.2]	A szétosztás folyamata [D1.1]-nek megfelelő legyen.	**a környezetnek kell biztosítania**
D2 Objektumok exportja/importja			
104	[D2.1]	A tanúsítványtárra hozzáférés-ellenőrzési politika kell.	**a környezetnek kell biztosítania**

Visszavonás kezelés szolgáltatás (RM)			
RM1 Tanúsítvány állapotváltozás kérések			
105	[RM1.1]	A visszavonás/felfügg kérelmek végrehajtása 24 órán belül.	**a környezetnek kell biztosítania**
106	[RM1.2]	Minden kérelmet hitelesíteni és érvényesíteni kell.	**az InfoCA rendszer teljesíti**
107	[RM1.3]	Visszavont tanúsítványt nem lehet újra használatba venni.	**az InfoCA rendszer teljesíti**
108	[RM1.4]	TA kulcs- tanúsítványok visszavonása kettős ellenőrzéssel.	**a környezetnek kell biztosítania**
109	[RM1.5]	Állapot változtatását csak a következők kezdeményezhetik:	**a környezetnek kell biztosítania**
110	[RM1.6]	A tanúsítvány állapot adatbázist azonnal frissíteni kell.	**az InfoCA 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 InfoCA rendszer teljesíti**
113	[RM2.3]	Valós idejű üzenetek használata esetén:….	**az InfoCA rendszer támogatja**
RM3 A Visszavonás kezelés naplózása			
114	[RM3.1]	A visszavonás kezelés alábbi eseményeit kötelező naplózni:	**az InfoCA rendszer teljesíti**
Visszavonás állapot szolgáltatás (RS)			
RS1 Visszavonás állapot adatok			
115	[RS1.1]	Csak megbízható tanúsítvány visszavonás kezelő szolgáltatásoktól származó üzenet dolgozható fel.	**az InfoCA rendszer teljesíti**
116	[RS1.2]	OCSP üzenetek sértetlenségét és hitelességét ellenőrizni kell.	**az InfoCA rendszer teljesíti**
117	[RS1.3]	OCSP válaszokra garantálni kell, hogy a tanúsítvány-állapot adatbázisból valóban a kért tanúsítványra vonatkozó választ kapták.	**az InfoCA rendszer támogatja**
RS2 Állapot kérés/válasz			
118	[RS2.1]	Minden választ digitálisan alá kell írni.	**az InfoCA rendszer teljesíti**
119	[RS2.2]	Aláírni csak biztonságos algoritmussal.	**a környezetnek kell biztosítania**
-	[RS2.3]	törölve	-
120	[RS2.4]	A válasz üzenetnek tartalmaznia kell az aláírás idejét.	**az InfoCA rendszer teljesíti**
RS3 A tanúsítvány visszavonás állapot naplózása			
121	[RS3.1]	A tanúsítvány visszavonás alábbi eseményeit kell naplózni:…	**az InfoCA rendszer teljesíti**

Időbélyegzés szolgáltatás (TS)			
TS1 Kérés helyessége			
122	[TS1.1]	A kérések eredete ellenőrizhető legyen.	**a környezetnek kell biztosítania**
123	[TS1.2]	Ellenőriznie kell, hogy az időbélyeg kérés biztonságos lenyomatkészítő algoritmust használ.	**az InfoCA rendszer támogatja**
TS2 Időparaméter generálása			
124	[TS2.1]	Az időforrás(oka)t szinkronizálni kell (UTC, 1 sec).	**a környezetnek kell biztosítania**
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 InfoCA rendszer teljesíti**
127	[TS3.2]	A TST tartalmazza az időforrás pontosságát is.	**az InfoCA rendszer teljesíti**
128	[TS3.3]	Szerepeltetni kell a szabályzatra való hivatkozást.	**az InfoCA rendszer teljesíti**
TS4 Időbélyeg token (TST) kiszámítása			
129	[TS4.1]	A TSA aláíró kulcsokat HSM-ben kell generálni és tárolni.	**az InfoCA 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.	**a környezetnek kell biztosítania**
132	[TS4.4]	A TSA aláíró kulcsok csak TST-k aláírására használhatók.	**a környezetnek kell biztosítania**
133	[TS4.5]	A TST válasz a kérés adatait tartalmazza.	**az InfoCA rendszer teljesíti**
134	[TS4.6]	Biztonságos aláírási algoritmust kell használni.	**a környezetnek kell biztosítania**
TS5 Időbélyeg szolgáltatás naplózása			
135	[TS5.1]	Az alábbi időbélyegzési eseményeket naplózni kell:	**az InfoCA rendszer teljesíti**
TS6 Időbélyeg szolgáltatás archiválás			
136	[TS6.1]	Minden időbélyeg tokent archiválni kell.	**a környezetnek kell biztosítania**

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.	**az InfoCA rendszer támogatja**

10.2 A tanúsított termékek listájába javasolt szöveg

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

"Az InfoCA hitelesítés szolgáltatás szoftver v2.5 (InfoCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.
Az InfoCA rendszer alap (kötelező) szolgáltatásai az alábbiak:

- *tanúsítvány előállítás szolgáltatás (funkciók: kezdeti tanúsítvány előállítás, tanúsítvány megújítás, tanúsítvány módosítás),*
- *tanúsítvány szétosztás szolgáltatás (funkciók: tanúsítvány exportálás LDAP-ba, LDAP újraépítése adatbázisból),*
- *visszavonás kezelés szolgáltatás (funkciók: tanúsítvány visszavonás, tanúsítvány felfüggesztés, tanúsítvány újra érvényesítés),*
- *visszavonás állapot szolgáltatás (funkciók: CRL publikálása LDAP-ba, CRL exportálása állományba, OCSP kérésre OCSP válasz adása).*

Az InfoCA rendszer (konfigurációtól függően opcionálisan) az alábbi kiegészítő szolgáltatásokat is támogatja:

- *időbélyegzés szolgáltatás (funkció: időbélyegzés),*
- *titkosító magánkulcs letétbe helyezése szolgáltatás (funkció: letétbe helyezés),*
- *titkosító magánkulcs helyreállítása szolgáltatás (funkció: helyreállítás funkció).*

11 Biztonsági előirányzat

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

12 Fogalmak és rövidítések

12.1 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 a annak a 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.

12.2 Rövidítések

Az alábbiakban meghatározzuk a jelen tanúsítási jelentésben használt betűszavak jelentését.

ALE	**A**láírás-**l**étrehozó **e**szköz
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)
CCRA	**C**ommon **C**riteria **R**ecognition **A**rrangement (a Közös szempontok szerint kibocsátott tanúsítványok kölcsönös elismeréséről szóló nemzetközi megállapodás)
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
OCSP	**O**n-line **C**erificate **S**tatus **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**trenght **o**f **F**unction (funkcióerősség)
TA	minősített **T**anúsítvány **A**láírására használt kulcs
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)
TS	**T**ime **S**tamp
TSF	**T**OE **S**ecurity **F**unctions (TOE biztonsági funkciói)
TSP	**T**OE **S**ecurity **P**olicy (TOE biztonsági szabályzata)
TSS	**T**ime **S**tamp **S**erver

13 Felhasznált dokumentumok

13.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérelem a tanúsítás kérelmezéséhez
- InfoCA v2.5 Biztonsági előirányzat v1.1
- InfoCA v2.5 Értékelési jelentés v1.1

13.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

A fejlesztői bizonyíték címe	verzió
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**	v1.1
Telepítési kézikönyv – InfoCA hitelesítés-szolgáltatás szoftver, v2.5	v1.8
Adminisztrátori kézikönyv – InfoCA hitelesítés-szolgáltatás szoftver, v2.5	v1.11
RA kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 *(nem változott az előző értékeléshez képest)*	v1.0
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Funkcionális specifikáció**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Magas szintű terv**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Alacsony szintű terv**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Megfelelés elemzés**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági szabályzat modell**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – **A konfiguráció menedzselés dokumentációja**	v1.2
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **A fejlesztési biztonság dokumentációja**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **A fejlesztő eszközök dokumentációja**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Az életciklust meghatározó dokumentáció**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **A hibajelentési eljárások**	v1.1
Tesztelési dokumentáció (tesztelési jegyzőkönyvek): • TJ_090511_OCSP.rtf (OCSP, szoftveres) • TJ_090609_OCSP.rtf (OCSP, Luna HSM-mel) • TJ_090710_OCSP.rtf (OCSP, nShield HSM-mel) • TJ_090511_TSS.rtf (TimeStamp, szoftveres) • TJ_090526_TSS.rtf (TimeStamp, Luna HSM-mel) • TJ_090710_TSS.rtf (TimeStamp, nShield HSM-mel)	
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Teszt lefedettség elemzés**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Teszt mélység elemzés**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Az útmutatók elemzése**	v1.1
InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - **Sebezhetőség elemzés**	v1.1
Biztonsági funkcióerősség elemzés – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 *(nem változott az előző értékeléshez képest)*	v1.0
A tesztelésre alkalmas InfoCA rendszer (Setup_InfoCA.exe, Setup_InfoRA.exe, InfoCAKeySetup.exe, InfoCA.exe, InfoRA.exe, InfoCA Setup.exe, OCSPResponder.dll, OCSPResponderIsapi.dll, TSSResponder.dll, TSSResponderIsapi.dll, CertSigner.dll)	v2.5

13.3 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

13.4 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 Trusthworthy 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 SR 002 176-1 v2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol
- RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol
- RFC 5280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile
- PKCS #11 v2.11 Cryptographic Token Interface Standard
- PKCS #12 v1.0 Personal Information Exchange Information Standard