TANÚSÍTÁSI JELENTÉS

TRUST&CA v2.0
megbízható rendszer
hitelesítés-szolgáltatáshoz

HUNG-TJ-36-2007

Verzió:	1.0
Fájl:	HUNG_TJ_36_2007_v10.doc
Minősítés:	Nyilvános
Oldalak:	37

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2007.07.04	A szerkezet felállítása
v0.8	2007.07.17	A tanúsítás eredményeit tartalmazó teljes változat
v0.81	2007.07.18	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v0.9	2007.07.20	Utolsó egyeztetésre kiadott változat
v1.0	**2007.07.24**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz**
Verzió szám:	**v2.0**
Rövid elnevezés:	**TCA v2.0 vagy TCA rendszer**
Az értékelt termék típusa:	Megbízható rendszer hitelesítés-szolgáltatáshoz
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2007. június 28.
Az értékelés módszere:	CEM, Common Evaluation Methodology, v2.3
Az értékelés garanciaszintje:	EAL4
Az értékelt termék funkcionalitása:	A TCA v2.0 (TCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik. Alap (kötelező) szolgáltatások: • Regisztrációs szolgáltatás (a TCA rendszeren kívül valósul meg, eredményét a TCA rendszer használja) • tanúsítvány előállítás szolgáltatás (funkciók: kezdeti tanúsítvány előállítás, tanúsítvány megújítás, tanúsítvány módosítás), mely szabványos X.509 formátumú tanúsítványokat állít elő, • 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). Kiegészítő (opcionális) szolgáltatások: • aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (funkciók: kulcspár generáltatás, nyilvános kulcs import, tanúsítvány export). • titkosító magánkulcs letétbe helyezése szolgáltatás (funkció: letétbe helyezés), • titkosító magánkulcs helyreállítása szolgáltatás (funkció: helyreállítás funkció)
Konfigurációs követelmények:	Szerver szoftver konfiguráció • operációs rendszer: MS Windows 2003 Server Enterprise Edition SP1 • MS SQL Szerver 2005 • OpenLDAP 2.2.29, • Syslog 0.3 • cknfast.dll 1.54.4.0 • .NET 3.0 Kliens szoftver konfiguráció • operációs rendszer: MS Windows XP Professional SP2 • .NET 3.0

2 Azonosítás

Az értékelt termék neve:	**TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz**
Verzió szám:	**v2.0**
Az értékelt termék alkotó elemei:	• TrustCA: 1.0.1.1480 • TrustCASetup: 1.0.3.690 • CertSigner.dll: 1.0.0.216 • ExtConfig.dll: 1.0.1.21 (noreq) / 1.0.1.22 (req) • TrustRA: 1.0.2.949 • Dokumentáció: o Adminisztrátori kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 o RA kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 o Telepítési kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján a TCA v2.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást. Először a TCA v2.0 egy üzemmódját határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

Jelen tanúsítási jelentés a TCA v2.0 azon üzemmódjára korlátozódik amelybe a tanúsítványok elektronikus aláírása HSM modul felhasználásával történik, valamint a magánkulcsok tárolása és visszaállítása tiltott funkció.

3.2 Biztonsági funkciók

A TCA rendszer az alábbi 8 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 üzenetek védelme
- BF7: Tanúsítvány előállítás
- BF8: Tanúsítvány visszavonás

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 a TCA rendszer adott elemét (TrustCASetup.exe, TrustRA.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 elenőrzése. Ez a biztonsági funkció egyaránt visszautasítja az érvényes aláírás nélküli, illetve a jogosulatlanul aláírt állományokat.

A **Kulcskezelés biztonsági funkció** biztonságosan kezeli a TCA rendszer általt 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 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[1].

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 össszeköti a kiváltásukban közreműködő felhasználókkal, valamint digitálisan aláírja a naplóeseményeket. (A generált és aláírt naplóesemények egy Syslog szerverre továbbítódnak, így kikerülnek a TCA rendszerből. Következésképpen a naplórekordok megvédése, áttekintése és kiértékelése a TCA rendszer környezetének a feladata.)

A szolgáltatások által létrehozott üzenetek védelme biztonsági funkció biztosítja a TCA 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 a TCA rendszer belső (az RA kliens és a CA szerver közötti) adatkommunikációját is.

A **Tanúsítvány előállítás biztonsági funkció** biztosítja a TCA 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 a TCA rendszer alap szolgáltatásai közé tartozó, tanúsítvány felfüggesztésre, felfüggesztés megszüntetésre és tanúsítvány visszavonásra irányuló jogosult kérelmek biztonságos végrehajtását, frissíti a tanúsítvány állapot adatbázist, valamint CRL-ek kibocsátásával biztosítja a tanúsítvány állapotok lekérdezhetőségét, megismerhetőségét.

[1] Aláíró magán kulcsok letétbe helyezése, tárolása és visszaállítása a tiltott funkció

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 a TCA v2.0 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 HSM támogatására építő üzemmód

A TCA 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 TrustCAInstaller.exe alkalmazás futtatásakor, a rendszeradminisztrátor választja ki a megfelelő Crypto üzemmódot.

Érvényességi feltétel:

1. A TCA 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

A TCA 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 a TCA rendszer biztosítja (azaz teljes mértékben megfelel a követelménynek), egy másik részét pedig támogatja (azaz részben megfelel a követelménynek).
A követelmények egy harmadik csoportjában a TCA 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:

2. Az IT környezet biztosítsa és kezelje a rendszeradminisztrátor, a rendszerüzemeltető 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.

5. Az IT környezet biztosítsa a tanúsítvány helyességének garantálása céljából a gyökértanúsítvány lenyomatának ellenőrizhetőségét egy megbízható útvonalon biztosított információ megadásával.
6. A TCA rendszer használata során biztosítani kell a megfelelő tanúsítvány profile kizárólagos használatát.
7. Elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén az aláíró tanúsítvány profilokban a kulcsletétbe helyezés funkciót tiltani kell.
8. A TCA rendszer futtatható állományainknak sértetlenségét az IT környezetnek biztosítani kell.
9. Minősített elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén a TCA 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 digitális aláírás ellenőrzését (vagyis a sértetlenség igazolását) az IT környezetnek kell biztosítania.
12. Az RA és CA alrendszerek között cserélt információk bizalmasságát az IT környezet biztosítsa.
13. A megújítandó tanúsítványok érvényességét IT és nem IT eljárásokkal biztosítani kell.
14. 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]; [CG3.1]; [D1.1];
    [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1]; [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 a TCA v2.0 valamennyi biztonsági funkcióját.

5 A TCA v2.0 szerkezeti leírása

A TCA v2.0 (TCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

A TCA rendszer az alábbi hitelesítés-szolgáltatásokat támogatja:

Alap (kötelező) szolgáltatások:

regisztrációs szolgáltatás (a TCA rendszeren kívül valósul meg, eredményét a TCA rendszer használja)
tanúsítvány előállítás szolgáltatás (funkciók: kezdeti tanúsítvány előállítás, tanúsítvány megújítás, tanúsítvány módosítás), mely szabványos X.509 formátumú tanúsítványokat állít elő,

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).

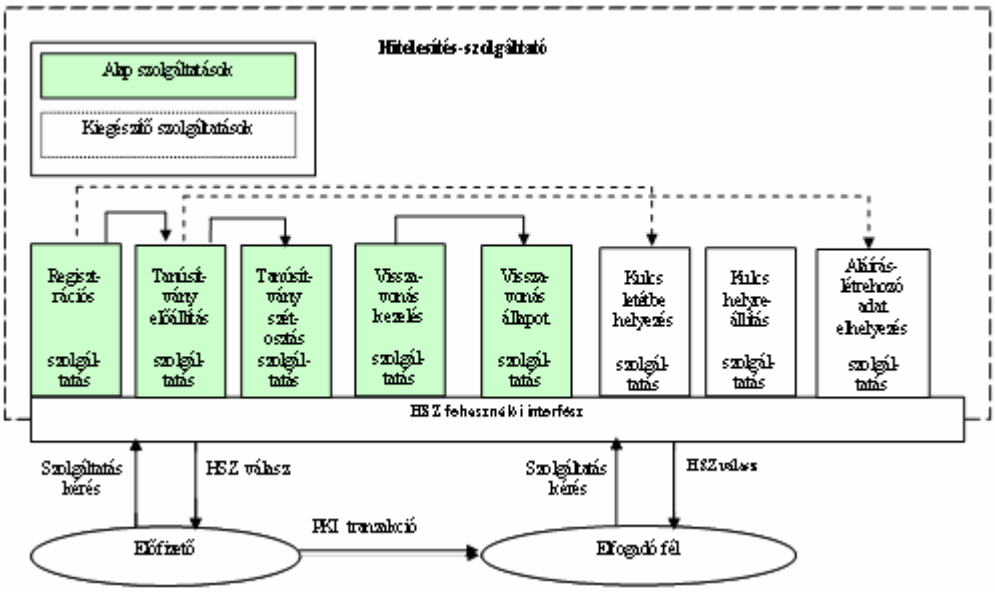
Kiegészítő (opcionális) szolgáltatások:

aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (funkciók: kulcspár generáltatás, nyilvános kulcs import, tanúsítvány export).

titkosító magánkulcs letétbe helyezése szolgáltatás (funkció: letétbe helyezés),

titkosító magánkulcs helyreállítása szolgáltatás (funkció: helyreállítás funkció)

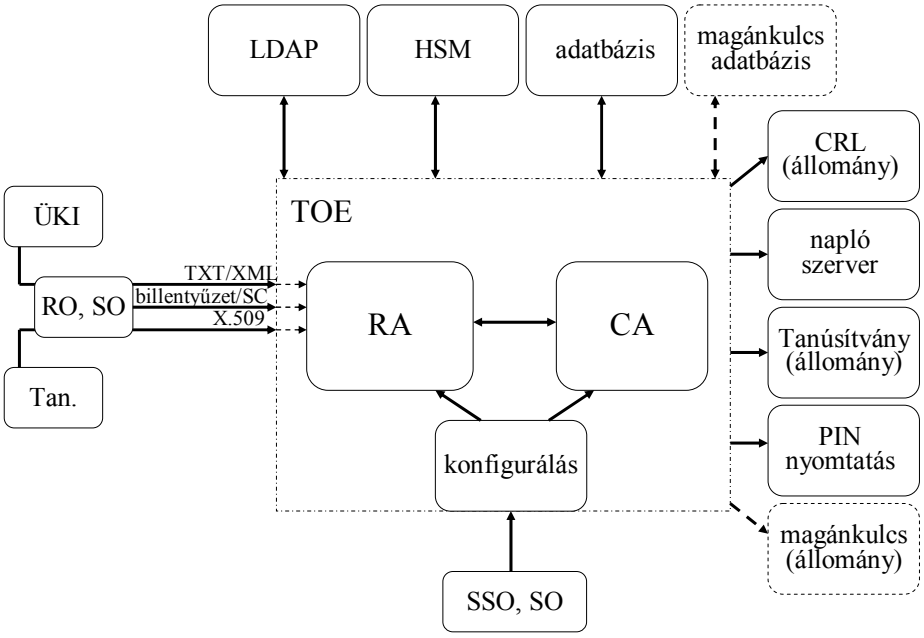
A TCA rendszer alapvetően egy hitesítés-szolgáltató megbízható rendszerének lett tervezve, mely a hitesítés-szolgáltató által nyújtott (alap és kiegészítő) szolgáltatásokat valósítja meg, vagy nyújt a megvalósításhoz műszaki támogatást, ahogyan azt az 1. ábra szemlélteti. /Az ábrán jelzett regisztrációs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



1. ábra A TCA v2.0 általános felépítése

5.1 Architektúra

A 2. ábra a TCA v2.0 struktúráját és az IT környezetbe való beágyazódását mutatja be.



2 ábra A TCA v2.0 és környezete

A TCA rendszer (a 2. ábrán TOE) szerverből (a 2. ábrán CA) és hozzá kapcsolódó kliensből (a 2. ábrán RA) áll. 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 a TCA 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.

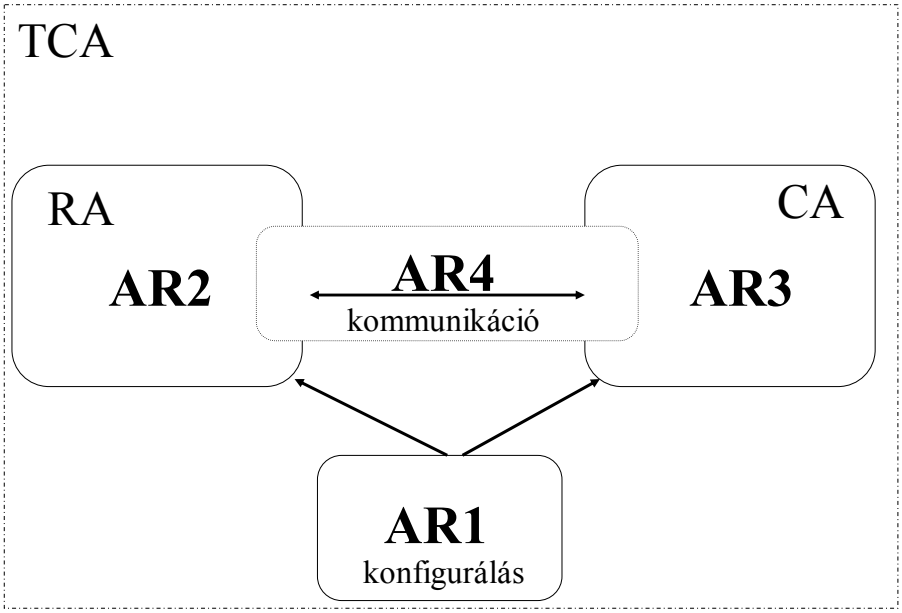
A TCA rendszer biztonságot növelő szerkezeti különlegessége, hogy a biztonság-kritikus CA alrendszernek ügyfelekkel nincs közvetlenül kommunikációs kapcsolata:

- az ügyfelektől származó kérések helyességét és jogosultságát a TCA 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 a TCA 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.

5.2 Alrendszerek

A TCA rendszer logikailag az alábbi 4 fő alrendszerre osztható, ahogyan azt a 3. ábra szemlélteti:

- AR1: konfigurálás (RA-t és CA-t konfiguráló alrendszer)
- AR2: RA (kliens oldali alrendszer)
- AR3: CA (szerver oldali alrendszer)
- AR4: kommunikáció (RA és CA közötti kommunikációt megvalósító alrendszer)



3. ábra: A TCA v2.0 alrendszerei

6 Dokumentáció

Az értékelt termék alkotó elemei az alábbiak:

- TrustCA.exe, mely a szervel oldal (CA) funkcionalitását automatikusan megvalósító alkalmazás,
- TrustCAInstaller.exe, mely a TrustCA.exe telepítését végző alkalmazás,
- TrustKeySetup.exe, mely a telepített TrustCA.exe konfigurálásának első lépését teszi végrehajthatóvá,
- TrustCASetup.exe, mely a telepített TrustCA.exe (s ezen keresztül a TrustRA.exe) konfigurálásának további lépéseit teszi végrehajthatóvá,
- TrustRA.exe, mely a kliens (RA) funkcionalitását megvalósító alkalmazás,
- TrustRAInstaller.exe, mely a TrustRA,exe telepítését végző alkalmazás.
- Adminisztrátori kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0
- RA kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0
- Telepítési kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0

7 Tesztelés

7.1 A fejlesztők tesztelése

A fejlesztő tesztelése nagyon alapos, dokumentálása kellően részletes.

A tesztelési dokumentáció 299 különböző tesztesetet ír le, 7 csoportba kategorizálva.

Tesztelési stratégiaként a funkcionális és biztonsági funkciók minden elemének egyedi leteszteléséét, a hiba ágak megfelelő kezelésének megalapítását lehetővé tevő, nagy munkaidő ráfordítást igénylő, de teljeségre törekedő irányt választották.

A tesztelt konfiguráció megfelel a biztonsági előirányzatban foglaltaknak.

7.2 Az értékelők tesztelése

Az értékelő független tesztelését a fejlesztői tesztelés helyszínén végezte.

A tesztelt konfiguráció megegyezett a fejlesztői tesztelés konfigurációjával, így ez megfelelt a biztonsági előirányzatban foglaltaknak is.

A független tesztelés (egy teszttől eltekintve) a fejlesztői tesztekből vett mintára szorítkozott, mivel a fejlesztői tesztelést az értékelők nagyon részletesnek és kielégítőnek ítélték meg.

A független tesztelés során az értékelők alkalmaztak a fejlesztői tesztekben lévő paramétereket, illetve új input adatokat is. Összesen 57 fejlesztői tesztesetet ismételtek meg, mely az összes fejlesztői tesztesetek 20 %-a volt.

Az egyetlen új tesztesetet az RA és CA közötti üzenetek sértetlenségének ellenőrzése jelentette. Ennek keretében egy visszavonáskérés üzenet meghamisítására került sor. (A CA az elvárásoknak megfelelően a kérést elutasította.)

A független tesztelés során hiba nem lépett fel.

8 Az értékelt konfiguráció

8.1 Szerver

Windows 2003 Szerver, Enterprise edition, SP1
Intel P4 Cel, 3,2 GHz
256 MB RAM
MS SQL Szerver 2005 Express edition
OpenLDAP 2.2.29
Syslog 0.3
IBM 4758 PCI és nCipher nShield 500 F3 HSM modulok
.NET 3.0
TrustCA: 1.0.1.1480
TrustCASetup: 1.0.3.690
CertSigner.dll: 1.0.0.216
ExtConfig.dll: 1.0.1.21 (noreq)
1.0.1.22 (req)
NShieldServer.exe 1.0.0.1
cknfast.dll 1.54.4.0

8.2 Kliens

- 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)
- TrustRA: 1.0.2.949
- Giesecke, StarSign
- Axalto, Cyberflex Access 64K v2

9 Az értékelés eredményei

A TCA v2.0 a CEM (Common Evaluation Methodology) v2.3 módszertana szerint független értékelésre és tanúsításra került, EAL4 értékelési garanciaszinten.

Az értékelés fő következtetése az alábbi:

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy a TCA v2.0 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:

A TCA v2.0 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[2] /és a fejlesztői bizonyíték/
Biztonsági előirányzat	ASE_DES.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_ENV.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_INT.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_OBJ.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_PPC.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_REQ.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_SRE.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**
	ASE_TSS.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Biztonsági előirányzat**

[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	Az követelményeknek **megfelelt**. **A konfiguráció menedzselés dokumentációja** -Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	ACM_SCP.2	Az követelményeknek **megfelelt**. **A konfiguráció menedzselés dokumentációja** -Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	ACM_AUT.1	Az követelményeknek **megfelelt**. **A konfiguráció menedzselés dokumentációja** -Trust&CA hitelesítés-szolgáltatás szoftver v2.0
Kiszállítás és működtetés	ADO_DEL.2	Az követelményeknek **megfelelt**. Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	ADO_IGS.1	Az követelményeknek **megfelelt**. **Telepítési kézikönyv** Trust&CA hitelesítés-szolgáltatás szoftver v2.0
Fejlesztés	ADV_FSP.2	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Funkcionális specifikáció (FS)**
	ADV_HLD.2	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Magas szintű terv (HLD)**
	ADV_IMP.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **Forráskód**
	ADV_LLD.1	Az követelményeknek **megfelelt**. TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz **- Alacsony szintű terv (LLD)**
	ADV_RCR.1	Az követelményeknek **megfelelt**. **Megfelelés elemzések** Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	ADV_SPM.1	Az követelményeknek **megfelelt**. **Biztonsági szabályzat modell** Trust&CA hitelesítés-szolgáltatás szoftver v2.0
Útmutató dokumentumok	AGD_ADM.1	Az követelményeknek **megfelelt**. **Adminisztrátori kézikönyv** – Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	AGD_USR.1	Az követelményeknek **megfelelt**. **RA kézikönyv** – 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	Az követelményeknek **megfelelt**. **A fejlesztési biztonság dokumentációja** - Trust&CA hitelesítés-szolgáltatás szoftver v2.
	ALC_LCD.1	Az követelményeknek **megfelelt**. **Az életciklust meghatározó dokumentáció** –Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	ALC_TAT.1	Az követelményeknek **megfelelt**. **A fejlesztő eszközök dokumentációja** -Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	ALC_FLR.2	Az követelményeknek **megfelelt**. **A hibajelentési eljárások leírása** –Trust&CA hitelesítés-szolgáltatás szoftver v2.0
Tesztelés	ATE_FUN.1	Az követelményeknek **megfelelt**. **Trust&CA teszt jegyzőkönyv**
	ATE_COV.2	Az követelményeknek **megfelelt**. **Teszt lefedettség elemzés** TCA_ATE_COV_v10.doc
	ATE_DPT.1	Az követelményeknek **megfelelt**. **Teszt mélység elemzés** v1.0, TCA_ATE_DPT_v10.doc
	ATE_IND.2	Az követelményeknek **megfelelt**. **Független tesztelés** - TCA_ATE_IND_v10.doc
A sebezhetőség felmérése	AVA_MSU.2	Az követelményeknek **megfelelt**. **Az útmutatók elemzése** –Trust&CA hitelesítés-szolgáltatás szoftver v2.0
	AVA_SOF.1	Az követelményeknek **megfelelt**.
	AVA_VLA.2	Az követelményeknek **megfelelt**. **Sebezhetőség elemzés** –Trust&CA hitelesítés-szolgáltatás

10 Értékelői megjegyzések és javaslatok

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

11 Mellékletek

11.1 A TCA v2.0 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:

- **A TCA rendszer teljesíti** (azaz teljes mértékben megfelel a követelménynek)
- **A TCA rendszer támogatja** (azaz részben megfelel a követelménynek, de a környezetnek is támogatást kell nyújtania),
- **A környezetnek kell biztosítania** (azaz a TCA rendszer nem vállalja fel a követelmény teljesítését, a megvalósítást az IT és nem IT környezettől várja el),
- **A TCA 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.	**A TCA rendszer támogatja**.
2	[M1.2]	Legalább a következő munkakörök szükségesek:	**a TCA rendszer támogatja**
3	[M1.3]	Felhasználók és munkakörök összekapcsolási képessége.	**a TCA 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).	**a TCA 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.	**a TCA rendszer támogatja**
12	[IA1.2]	A felhasználó kijelentkezése után kötelező az újrahitelesítés.	**a TCA rendszer támogatja**
13	[IA1.3]	Egyedi hitelesítő adatok.	**a TCA rendszer támogatja**
IA2 Hitelesítési hiba			
14	[IA2.1]	A sikertelen hitelesítési kísérletek korlátozása.	**a TCA 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.	**a TCA rendszer támogatja**
Rendszer-hozzáférés ellenőrzés (SA)			
SA1 Rendszer-hozzáférés ellenőrzés			
17	[SA1.1]	Azonosított egyének hozzáférésének ellenőrzése, korlátozása.	**a TCA 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.	**a TCA 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.	**a TCA rendszer támogatja**
25	[KM2.2]	A még tanúsítványba nem foglalt nyilvános kulcsokat biztonságos környezetben kell tartani.	**a TCA rendszer teljesíti**
26	[KM2.3]	Szabványos kriptográfiai kulcselosztó módszer használata.	**a TCA 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:	**a TCA 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.	**a TCA rendszer teljesíti**
33	[KM3.4]	El kell különíteni az aláíró kulcsokat.	**a TCA rendszer támogatja**
34	[KM3.5]	Jogosult kulcshasználat csak életcikluson belül történhet.	**a TCA rendszer teljesíti**
35	[KM3.6]	Kulcshasználat előtt tanúsítvány érvényesség ellenőrzés.	**a TCA 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]	Bztonságos 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, letétbe helyezni.	**a TCA rendszer támogatja**
KM7 Kulcs archiválás			
53	[KM7.1]	Tilos az aláíró magánkulcsok archiválása.	**a TCA rendszer támogatja**
Naplózás (AA)			
AA1 Napló adatok generálása			
54	[AA1.1]	A következő események naplózása feltétlenül szükséges:	**a TCA rendszer támogatja**
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:…	**a TCA 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.	**a TCA 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 sértetlenségét.	**a TCA rendszer támogatja**
64	[AA7.1] QCA	Biztosítani kell a napló sértetlenségét: (DS, HMAC, auth)	**a TCA 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: (tanúsítványok, CRL-ek, naplók)	**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)	**a TCA 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.	**a TCA 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.	**a TCA rendszer teljesíti**
93	[CG1.5]	Meg kell felelni a meghatározott profiloknak.	**a TCA rendszer teljesíti**
94	[CG1.6] NQCA	A tanúsítványoknak meg kell felelniük az alábbiaknak:	**a TCA rendszer támogatja**
95	[CG1.6] QCA	A tanúsítványoknak meg kell felelniük: ETSI TS 101 862	**a TCA 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 TCA rendszer támogatja**
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:	**a TCA 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.	**a TCA rendszer teljesíti**
107	[RM1.3]	Visszavont tanúsítványt nem lehet újra használatba venni.	**a TCA 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.	**a TCA 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:…	**a TCA rendszer teljesíti**
113	[RM2.3]	Valós idejű üzenetek használata esetén:….	**Az TCA rendszerre nem vonatkozik a követelmény**
RM3 A Visszavonás kezelés naplózása			
114	[RM3.1]	A visszavonás kezelés alábbi eseményeit kötelező naplózni:	**a TCA rendszer teljesíti**
Visszavonás állapot szolgáltatás (RS)			
RS1 Visszavonás állapot adatok			
115	[RS1.1]	Csak megbízható tanúsítvány visszavonás kezelő szolgáltatásoktól származó üzenet dolgozható fel.	**a TCA rendszer teljesíti**
116	[RS1.2]	OCSP üzenetek sértetlenségét és hitelességét ellenőrizni kell.	**Az TCA rendszerre nem vonatkozik a követelmény**
117	[RS1.3]	OCSP válaszokra garantálni kell, hogy a tanúsítvány-állapot adatbázisból valóban a kért tanúsítványra vonatkozó választ kapták.	**Az TCA rendszerre nem vonatkozik a követelmény**
RS2 Állapot kérés/válasz			
118	[RS2.1]	Minden választ digitálisan alá kell írni.	**A TCA rendszerre nem vonatkozik a követelmény**
119	[RS2.2]	Aláírni csak biztonságos algoritmussal.	**A TCA rendszerre nem vonatkozik a követelmény**
-	[RS2.3]	törölve	-
120	[RS2.4]	A válasz üzenetnek tartalmaznia kell az aláírás idejét.	**A TCA rendszerre nem vonatkozik a követelmény**
RS3 A tanúsítvány visszavonás állapot naplózása			
121	[RS3.1]	A tanúsítvány visszavonás alábbi eseményeit kell naplózni:…	**A TCA rendszerre nem vonatkozik a követelmény**
Időbélyegzés szolgáltatás (TS)			
TS1 Kérés helyessége			
122	[TS1.1]	A kérések eredete ellenőrizhető.	**A TCA rendszerre nem vonatkozik a követelmény**
123	[TS1.2]	Ellenőriznie kell, hogy az időbélyeg kérés biztonságos lenyomatkészítő algoritmust használ.	**A TCA rendszerre nem vonatkozik a követelmény**

TS2 Időparaméter generálása			
124	[TS2.1]	Az időforrás(oka)t szinkronizálni kell (UTC, 1 sec).	**A TCA rendszerre nem vonatkozik a követelmény**
125	[TS2.2]	Megbízható mechanizmussal kell szinkronizálni.	**A TCA rendszerre nem vonatkozik a követelmény**
TS3 Időbélyeg token (TST) létrehozása			
126	[TS3.1]	A TST-be egyedi sorszámot kell foglalni.	**A TCA rendszerre nem vonatkozik a követelmény**
127	[TS3.2]	A TST tartalmazza az időforrás pontosságát is.	**A TCA rendszerre nem vonatkozik a követelmény**
128	[TS3.3]	Szerepeltetni kell a szabályzatra való hivatkozást.	**A TCA rendszerre nem vonatkozik a követelmény**
TS4 Időbélyeg token (TST) kiszámítása			
129	[TS4.1]	A TSA aláíró kulcsokat HSM-ben kell generálni és tárolni.	**A TCA rendszerre nem vonatkozik a követelmény**
130	[TS4.2]	Megfelelő HSM-et kell használni.	**A TCA rendszerre nem vonatkozik a követelmény**
131	[TS4.3]	A TSA rendszervezérlési kulcsokat HSM-ben kell tárolni.	**A TCA rendszerre nem vonatkozik a követelmény**
132	[TS4.4]	A TSA aláíró kulcsok csak TST-k aláírására használhatók.	**A TCA rendszerre nem vonatkozik a követelmény**
133	[TS4.5]	A TST válasz a kérés adatait tartalmazza.	**A TCA rendszerre nem vonatkozik a követelmény**
134	[TS4.6]	Biztonságos aláírási algoritmust kell használni.	**A TCA rendszerre nem vonatkozik a követelmény**
TS5 Időbélyeg szolgáltatás naplózása			
135	[TS5.1]	Az alábbi időbélyegzési eseményeket naplózni kell:	**A TCA rendszerre nem vonatkozik a követelmény**
TS6 Időbélyeg szolgáltatás archiválás			
136	[TS6.1]	Minden időbélyeg tokent archiválni kell.	**A TCA rendszerre nem vonatkozik a követelmény**

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]	Ha kívül generálják a kulcspárt, az előállító kriptográfiai modult tanúsíttatni kell.	**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 TCA rendszer támogatja**

11.2 A tanúsított termékek listájába javasolt szöveg

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

" A TCA v2.0 (TCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

A TCA rendszer az alábbi hitelesítés-szolgáltatásokat támogatja:

Alap (kötelező) szolgáltatások:
- *regisztrációs szolgáltatás (a TCA rendszeren kívül valósul meg, eredményét a TCA rendszer használja)*
- *tanúsítvány előállítás szolgáltatás (funkciók: kezdeti tanúsítvány előállítás, tanúsítvány megújítás, tanúsítvány módosítás), mely szabványos X.509 formátumú tanúsítványokat állít elő,*
- *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).*

Kiegészítő (opcionális) szolgáltatások:
- *aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (funkciók: kulcspár generáltatás, nyilvános kulcs import, tanúsítvány export)*
- *titkosító magánkulcs letétbe helyezése szolgáltatás (funkció: letétbe helyezés),*
- *titkosító magánkulcs helyreállítása szolgáltatás (funkció: helyreállítás funkció)"*

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 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.

13.2 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
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)
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
- TCA v2.0 Biztonsági előirányzat v1.0
- TCA v2.0 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:

A fejlesztői bizonyíték címe	verzió
TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Biztonsági előirányzat**	v1.0
A konfiguráció menedzselés dokumentációja -Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Telepítési kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Funkcionális specifikáció**	v1.0
TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Magas szintű terv**	v1.0
TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - **Alacsony szintű terv**	v1.0
Megfelelés elemzések - Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Adminisztrátori kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
RA kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
A fejlesztési biztonság dokumentációja - Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Az életciklust meghatározó dokumentáció –Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
A hibajelentési eljárások –Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
A fejlesztő eszközök dokumentációja -Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Tesztelési dokumentáció: Trust&CA teszt jegyzőkönyv_fin.doc és Trust&CA teszt jegyzőkönyv_nshield.doc	v1.0
Teszt lefedettség elemzés -Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Teszt mélység elemzés -Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Az útmutatók elemzése –Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Biztonsági funkcióerősség elemzés – Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0
Sebezhetőség elemzés – Trust&CA hitelesítés-szolgáltatás szoftver v2.0	v1.0

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 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 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- 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