TANÚSÍTÁSI JELENTÉS

Attribútum-szolgáltató szoftver (Info&AA) v1.0

HUNG-TJ-50-2010

Verzió:	1.0
Fájl:	HUNG-TJ-50-2010_v10.pdf
Minősítés:	Nyilvános
Oldalak:	38

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2009.08.13.	A szerkezet felállítása
v0.8	2010.08.15.	A tanúsítás eredményeit tartalmazó teljes változat
v0.9	2010.08.19.	Belső egyeztetésre kiadott változat
v0.91	2010.08.23.	Belső egyeztetésen átesett változat
v1.0	**2009.08.27**	**Külső egyeztetésen átesett végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
Hunguard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**Attribútum szolgáltató szoftver**
Verzió szám:	**v1.0**
Rövid elnevezés:	**Info&AA**
Az értékelt termék típusa:	Megbízható rendszer hitelesítés-szolgáltatáshoz
Értékelő szervezet:	Hunguard Kft.
Értékelés befejezése:	2010. augusztus 06.
Az értékelés módszere:	MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma)
Az értékelés garanciaszintje:	MIBÉTS szerinti kiemelt értékelési garanciaszint (EAL4)
Az értékelt termék funkcionalitása:	Az Info&AA v1.0 az alábbi attribútum-szolgáltatásokat támogatja: a.) attribútum regisztráció szolgáltatás, b.) attribútum tanúsítvány igénylés szolgáltatás, c.) attribútum tanúsítvány előállítás szolgáltatás, d.) attribútum tanúsítvány szétosztás szolgáltatás, e.) attribútum tanúsítvány visszavonás kezelés szolgáltatás, f.) attribútum tanúsítvány visszavonás állapot szolgáltatás. A támogatott szolgáltatásokon belül az alábbiakat valósítja meg: - attribútum tanúsítvány előállítás (már kiadott PKI tanúsítványokhoz kapcsolódó, X.509 és RFC 3281 szabványoknak megfelelő attribútum tanúsítványok generálása), - attribútum tanúsítvány visszavonás kezelés (már kiadott attribútum tanúsítványok visszavonása, felfüggesztése, újra aktiválása), - attribútum tanúsítvány visszavonás állapot szolgáltatás (a visszavont és felfüggesztett attribútum tanúsítványokat tartalmazó, X.509 és RFC 5280 szabványoknak megfelelő ACRL-ek előállítása és LDAP-ba publikálása)
Konfigurációs követelmények:	Az Info&AA v1.0 valamennyi futtatható alkalmazása (InfoAA, InfoAA Setup, InfoAA Policy Manager és InfoAA RA) Windows-os, .Net 3.5-ös környezetben működik a következő minimális szoftver környezetben: • Windows XP Professional SP3 (további támogatott operációs rendszerek: Vista, Win7, 2003Server, 2008Server) • .Net 3.5 futtató környezet (.NET Framework 3.5) • Microsoft Message Queue Az Info&AA alkalmazása a következő környezeti szoftver elemeket is megköveteli: • adatbázis kezelő (támogatott adatbázis kezelők: tetszőleges szabványos SQL szerver

alkalmazható, amelyik támogatja a tranzakciókat, valamint rendelkezik OLDEDB provider-rel, például: MSSQL Desktop Edition, MSSQL 2000, MSSQL 2005, MSSQL 2008)

- Syslog szerver (támogatott napló szerverek: tetszőleges szabványos syslog megoldás.)
- LDAP szerver (támogatott címtárak: tetszőleges szabványos LDAP szerver)
- HSM modul és a hozzá tartozó middleware (támogatott kriptográfiai hardver modul: nCipher nShield + CertSigner.dll v2.0.0.9)
- hardver token és a hozzátartozó middleware (támogatott eszközök: tetszőleges olyan intelligens kártya vagy token, amely szabványos, Microsoft-os CSP driverrel rendelkezik.)

2 Azonosítás

Az értékelt termék neve:	**Attribútum szolgáltató szoftver (Info&AA)**
Verzió szám:	**v1.0**
Az értékelt termék alkotó elemei:	Szoftver: • infoaa_installer.exe (1.0.0.1)- (az InfoAA.exe telepítő alkalmazása) • infoaara_installer.exe (1.0.0.0) - (az InfoAARA.exe telepítő alkalmazása) • infoaapm_installer.exe (1.0.0.0) - (az InfoAAPolicyManager.exe telepítő alkalmazása) • InfoAASsoSetup.exe (2.0.0.3) – (a 3 SSO kezdeti meghatározását, fiókjuk beállítását végző alkalmazás) • InfoAASetup.exe (1.0.0.0) - az InfoAA.exe beállítását végző alkalmazás • InfoAARA.exe (1.0.0.0) - regisztrációs alkalmazás • InfoAA.exe (1.0.0.401) – attribútum tanúsítványokat kezelő szerver oldali alkalmazás • InfoAAPolicyManager.exe (1.0.0.0) – attribútum kollekciók szerkesztését biztosító alkalmazás • BusinessEntities.dll (1.0.0.0) - attribútum tanúsítványokhoz kapcsolódó általános segédkönyvtár • CertSigner.dll (2.0.0.14) - szoftveres aláíró könyvtár (teszt üzemmódhoz) • PkiMiddleware.dll (1.0.0.0) - a konfigurációs állományok és a szolgáltatói kérések aláírását, valamint a különböző tisztviselők (SSO, SO, RO, PO) beléptetését végző segédkönyvtár • Repository.dll (1.0.0.0) - a konfigurációs állományok mentését és betöltését támogató segédkönyvtár • aa.sql - adatbázis generáló script Dokumentáció: • Telepítési kézikönyv (a teljes Info&AA rendszerre és informatikai környezetére) • InfoAA Policy Manager kézikönyv • InfoAA RA kézikönyv • InfoAA Setup kézikönyv

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az Info&AA v1.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást. Először az Info&AA v1.0 egy üzemmódját határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

Jelen tanúsítási jelentés az Info&AA v1.0 azon üzemmódjára korlátozódik, amelybe az attribútum tanúsítványok elektronikus aláírása HSM modul felhasználásával történik, valamint a magánkulcsok tárolása és visszaállítása tiltott funkció.

3.2 Felhasználók

Az Info&AA által kezelt felhasználótípusok:

Rendszer biztonsági tisztviselő (**SSO**) A biztonsági tisztviselők (SO) felhasználói fiókjainak kezelésére feljogosított bizalmi munkakört betöltő személy.

Biztonsági tisztviselő (**SO**) A regisztrációs tisztviselők (RO) és attribútum-szabályzó tisztviselők (PO) felhasználói fiókjai, az InfoAA.config és az InfoAA.raconfig konfigurációs állományok, valamint az attribútum tanúsítvány és ACRL profilok kezelésére feljogosított bizalmi munkakört betöltő személy.

Regisztrációs tisztviselő (**RO**) Attribútum tanúsítványokra vonatkozó különböző szolgáltatási kérések (kibocsátás, visszavonás, felfüggesztés, újra aktiválás) kiadásának, valamint az ezekre kapott válaszok lekérdezésére feljogosított bizalmi munkakört betöltő személy.

Attribútum-szabályzó tisztviselő (**PO**) Az egyes attribútum tanúsítványokon belüli attribútum kollekciók kezelésére feljogosított bizalmi munkakört betöltő személy.

Az Info&AA üzemeltetési környezetétől elvárt felhasználótípusok:

Rendszergazda (ADM) Az Info&AA rendszer telepítését végző, valamint az ehhez szükséges szoftver környezetet (operációs rendszer, Microsoft Message Queue, .Net 3.5 futtató környezet, LDAP szerver, Syslog szerver, Syslog szerver) biztosító, a működő TOE-hez közvetlenül hozzá nem férő, bizalmi munkakört betöltő személy.

Rendszer auditor (SA) Az Info&AA rendszerben keletkezett, majd részben a syslog szerverre továbbított naplóadatok kezelését (megtekintés, szűrés, átvizsgálás, mentés, törlés) végző, közvetlenül a TOE-hez hozzá nem férő, bizalmi munkakört betöltő személy.

3.3 Biztonsági funkciók

Az Info&AA rendszer az alábbi hét biztonsági funkciót (BF) valósítja meg:

- BF1: Biztonság menedzsment
- BF2: Felhasználó adatokra vonatkozó funkciók (hozzáférés ellenőrzés)
- BF3: Azonosítás és hitelesítés
- BF4: Biztonsági naplózás
- BF5: A külső és belső adatátvitel védelme
- BF6: Az attribútum tanúsítvány előállítása
- BF7: Az attribútum tanúsítványok visszavonás kezelése

A **Biztonsági menedzsment biztonsági funkció** meghatározza a rendszerben megvalósítandó biztonság menedzsment funkciókat, melyek az alábbiak:

- SO fiók kezelés,
- RO fiók kezelés, PO fiók kezelés,
- konfigurációs állományok kezelése (InfoAA.config és InfoAA.raconfig),
- AC profil kezelés, ACRL profil kezelés,
- Attribútum kollekciók kezelése.

A **Felhasználó adatokra vonatkozó funkciók (hozzáférés ellenőrzés) biztonsági funkció** biztosítja, hogy a rendszer által a felhasználói adatokra biztosított két funkció („AC előállítás kérés” és „ACRL előállítás kérés”) végrehajtása az alkalmazott ellenőrzési szabályok betartása mellett történjen.

Az **Azonosítás és hitelesítés biztonsági funkció** végzi a rendszerben lévő szerepkörök betöltőinek rendszer általi elfogadását.

A **Biztonsági naplózás biztonsági funkció** biztosítja, hogy minden elvárt esetben készül napló bejegyzés (szerver esetén syslog-ba kliensek esetén lokális file-ba) és minden naplóesemény összekapcsolható az eseményt kiváltó felhasználó azonosítójával.

A külső és belső adatátvitel védelme biztonsági funkció biztosítja, hogy a szolgáltatói kérések és válaszok módosítás ellen védve legyenek, a felhasználói adatok, illetve a kapcsolódó TSF adatok vonatkozásában illetve a syslog szervernek küldött naplórekordok módosítás ellen védve legyenek (beleértve a kihagyást és beszúrást is).

Az attribútum tanúsítvány előállítása biztonsági funkció állítja elő, az Info&AA rendszerben az attribútum tanúsítványokat, amelyek formátuma megfelel az ITU-T X.509-2000, RFC 3281 és RFC 4476 X.509 szabványok elvárásainak illetve lehetőséget ad tanúsítvány profilok és attribútum kollekciók kezelésére.

Az attribútum tanúsítványok visszavonás kezelése biztonsági funkció gondoskodik arról, hogy az Info&AA rendszer által kibocsátott attribútum tanúsítvány visszavonási listák (ACRL) megfelelnek az X.509 szabványnak, illetve lehetőséget ad attribútum tanúsítvány visszavonási lista profilok kezelésére.

4 Feltételezések és hatókör

A tanúsítás pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

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

4.1 Biztonsági célok az Info&AA v1.0 informatikai környezetére

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

1. Biztosítani kell a TOE megfelelő kezelését a bizalmi munkakörök hozzáértő és feljogosított személyekkel való betöltésével a TOE és az általa tartalmazott információk biztonságának kezelésére. (OE.Competent Administrators, Operators, Officers and Auditors)
2. Meg kell gátolni a bizalmi munkakört betöltő személyek hibáit azáltal, hogy megfelelő dokumentációt kell számukra biztosítani a TOE biztonságos konfigurálásához és üzemeltetéséhez. (OE.Administrators, Operators, Officers and Auditors guidance documentation)
3. Biztosítani kell, hogy a felhasználók együttműködők legyenek néhány olyan feladat vagy feladatcsoport végrehajtásában, amelyek biztonságos IT környezetet, s a TOE által kezelt információkat igényelnek. (OE.Cooperative Users)
4. Minden bizalmi munkakört betöltő személynek jól kell ismernie azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. (OE.CPS)
5. Értesíteni kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, az adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében. (OE.Notify Authorities of Security Issues)
6. A bizalmi munkakört betöltő személyek számára képzést kell biztosítani a „social engineering” típusú támadások megakadályozási technikáira. (OE.Social Engineering Training)
7. A hitelesítési adat kezelésre vonatkozó szabályzat érvényre juttatásával biztosítani kell, hogy a felhasználók hitelesítési adataikat (jelszavaikat, aktivizáló kódjaikat) megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtassák. (OE.Authentication Data Management)
8. Biztosítani kell a hitelesítési adatok és az ezekhez tartozó jogosultságok megfelelő eltávolítását, miután a hozzáférési jogosultság megszűnt (pl. munkahelyváltozás vagy munkaköri felelősség megváltozása következtében). (OE.Disposal of Authentication Data)
9. A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE olyan módon legyen szállítva, telepítve, kezelve és üzemeltetve, amely megőrzi az informatikai biztonságot. (OE.Installation)
10. A TOE IT környezete csak olyan operációs rendszert használhat, mely garantálja a TOE számára a tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét. (OE.Operating System)
11. A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE biztonságkritikus elemei védve legyenek az informatikai biztonságot veszélyeztető fizikai támadásokkal szemben. (OE.Physical Protection)

12. A rendszert megfelelő fizikai biztonság biztosításával védeni kell a kommunikációs képességekre irányuló fizikai támadásokkal szemben. (OE.Communication Protection)
13. Megfelelő sértetlenség védelmet kell biztosítani a felhasználói adatokra és a szoftverre. (OE.Integrity protection of user data and software)
14. Sértetlenség védelmet kell biztosítani a förmverek, a szoftverek, valamint a mentett adatok megváltozásának észlelése érdekében. (OE.Detect modifications of firmware, software, and backup data)
15. A rosszindulatú programkódokat meggátoló beépített eljárásoknak és mechanizmusoknak kell létezniük. (OE.Procedures for preventing malicious code)
16. Automatizált értesítést (vagy más reagálásokat) kell megvalósítani a TSF által felfedett támadások esetében a támadások azonosítása és elrettentése érdekében. (OE.React to detected attacks)
17. Meg kell követelni a letöltések/átvitelek felügyeletét. (OE.Require inspection for downloads)
18. Megbízható útvonalat kell biztosítani a felhasználók és a rendszer között. Megbízható útvonalat kell biztosítani a biztonság-kritikus (TSF) adatok számára, aminek mindkét végpontja megbízhatóan azonosított. (OE.Trusted Path)
19. Funkciók és eljárások alkalmazásával biztosítani kell, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek. (OE.Validation of security function)
20. Jóváhagyott kriptográfiai algoritmusokat kell megvalósítani a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat kell alkalmazni, valamint tanúsított kriptográfiai modulokat kell használni. (OE.Cryptographic functions)
21. Az adatok formájában megjelenő értékeket védeni kell a TOE felé vagy a TOE-tól történő átvitel közben, ahol az átvitel akár egy közbeiktatott nem megbízható komponensen keresztül, akár közvetlenül az emberi felhasználókhoz/tól történik. (OE.Data import/export)
22. Időszakosan ellenőrizni kell mind a rendszer, mind a szoftver sértetlenségét. (OE.Periodically check integrity)

23. A biztonság-kritikus eseményeket azonosítani és felügyelni kell, megkövetelve a rendszervizsgálóktól a naplóbejegyzések kellő (kockázatokkal arányban álló) gyakoriságú átvizsgálását. (OE.Auditors Review Audit Logs)
24. A naplórekordokat védeni kell a jogosulatlan hozzáféréssel szemben abból a célból, hogy biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért. (OE.Protect stored audit records)
25. Amennyiben a napló eseménysor tároló területe megtelt vagy majdnem megtelt, a naplózható események korlátozásával meg kell akadályozni a naplórekordok lehetséges elvesztését. (OE.Respond to possible loss of stored audit records)
26. Pontos időpontot kell biztosítani az időfüggő hitelesítés-szolgáltatásokhoz, valamint a napló események sorrendjének ellenőrizhetőségéhez. (OE.Time stamps)

27. Egy rosszindulatú kód bejutása és károkozása után egy működőképes állapotba kell tudni visszaállni. Ennek az állapotnak mentesnek kell lennie az eredeti rosszindulatú programkódtól. (OE.Object and data recovery free from malicious code)
28. Egy biztonsági komponens hibája esetén meg kell őrizni a rendszer egy biztonságos állapotát, és/vagy helyre kell állítani a rendszert egy biztonságos állapotába. (OE.Preservation/trusted recovery of secure state)
29. Elegendő mentés tárolást és hatékony visszaállítást kell biztosítani a rendszer újra felépíthetősége érdekében. (OE.Sufficient backup storage and effective restoration)

30. A fejlesztési fázisban olyan eszközöket és technikákat kell biztosítani, hogy használatukkal biztosítva legyen a biztonság TOE-ba tervezése. A működtetés során észlelni és javítani kell a hibákat. (OE.Lifecycle security)
31. A gyártónak javítani kell a felhasználók által azonosított biztonsági hibákat. (OE.Repair identified security flaws)

4.2 A biztonságos felhasználás egyéb feltételei

4.2.1 Az értékelés eredményeiből származó feltételek

Az értékelés során elvégzett tesztelési és sebezhetőség elemzési tapasztalatok alapján megállapított konfigurálásra vonatkozó feltételeket be kell tartani:

32. Az Info&AA rendszer éles használata kizárólag a HSM modul támogatására építő üzemmódra szorítkozhat, a szoftveres üzemmód csak tesztelési célokat szolgál.
33. A rendszert csak hardver tokenes azonosítással és hitelesítéssel lehet használni.
34. Az operációs rendszerben be kell kapcsolni a Code Signing ellenőrzést kötelező tulajdonságként, a Code Signing segítségével aláírt futtatható állományok sértetlenségének automatikus ellenőrzésére.
35. A rendszer alapbiztonságát adó InfoAA.sso file előállításához megfelelő adminisztratív intézkedések szükségesek. Ezek biztosítsák az alábbiakat:
    a) Az SSO-k tanúsítványához tartozó magánkulcsok olyan tokenekben generálták, amelyek garantálják a magánkulcs kiolvashatatlanságát és annak hozzáférés védelmét.
    b) Az InfoAA.sso file előállítása a rendszer auditor fizikai jelenlétében történjen, így garantálva a kettős személyi felügyeletet.
    c) Az auditor készítsen jelentést az InfoAA.sso file létrehozásáról, ami terjedjen ki a létrehozás idejére, az alkalmazott tokenek típusára, egyedi azonosító adatára és a tokeneket birtokló személyek adataira.
36. Az SO, PO és RO jogosultságok kiadása során megfelelő adminisztratív intézkedések szükségesek. Ezek biztosítsák az alábbiakat:
    a) Az SO, PO és RO tanúsítványához tartozó magánkulcsok olyan tokenben generálódtak, amik garantálják a magánkulcs kiolvashatatlanságát és annak hozzáférés védelmét.
    b) Az SO jogosultság kiadásáról az SSO, a PO és RO jogosultságok kiadásáról pedig az SO készítsen jelentést, ami terjedjen ki a létrehozás idejére, az alkalmazott tokenek típusára, egyedi azonosító adatára és a tokeneket birtokló személyek adataira.
37. A rendszeradminisztrátor biztosítsa, hogy a felhasználók az általuk használt komponenseken kívül, máshoz futtatási joggal ne férjenek hozzá.
38. Minden indításkor az ACRL profilok helyes betöltődését a rendszeradminisztrátornak ellenőriznie kell.

4.2.2 MSZ CWA 14167-1 követelményeknek való megfelelés

Az Info&AA 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 Info&AA rendszer biztosítja (azaz teljes mértékben megfelel a követelménynek), egy másik részét pedig támogatja (azaz részben megfelel a követelménynek).
A követelmények egy harmadik csoportjában az Info&AA 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:

39. Az IT környezet biztosítsa és kezelje a rendszeradminisztrátor, a rendszerüzemeltető és rendszervizsgáló szerepköröket.
40. Az IT környezet biztosítsa a megfelelő HSM modul használatát az attribútum tanúsítványokat aláíró kulcs tárolására, illetve a HSM modul tanúsításakor meghatározott felhasználási feltételek betartását.
41. A naplózás tárolási hibája miatt végzett tevékenységek naplózása érdekében IT és nem IT eljárásokat kell foganatosítani.
42. A napló események digitális aláírásának az ellenőrzését (vagyis a napló sértetlenségének igazolását) az IT környezetnek kell biztosítania.
43. Az attribútum tanúsítvány kérelem adatainak a bizalmasságát az IT környezet biztosítsa.
44. Időszakonként az Info&AA rendszerben alkalmazott algoritmusokról ellenőrizni kell, hogy azok megfelelnek-e a "Biztonságos algoritmusok[1]" című dokumentumban meghatározott követelményeknek.
45. IT és nem IT eljárásokat kell foganatosítani az alábbi követelmények teljesüléséhez: [[SO2.1]; [SO2.2]; [SO2.3]; [SO3.1] NQCA; [SA1.2]; [KM1.2]; [KM1.3]; [KM1.4]; [KM1.7]; [KM3.1]; [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; [BK2.2]; [BK3.1]; [BK3.2]; [R1.1]; [R1.2]; [R1.4]; [R1.5] QCA; [R1.6]; [R2.1]; [CG2.2]; [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1];

4.3 Az értékelés hatóköre

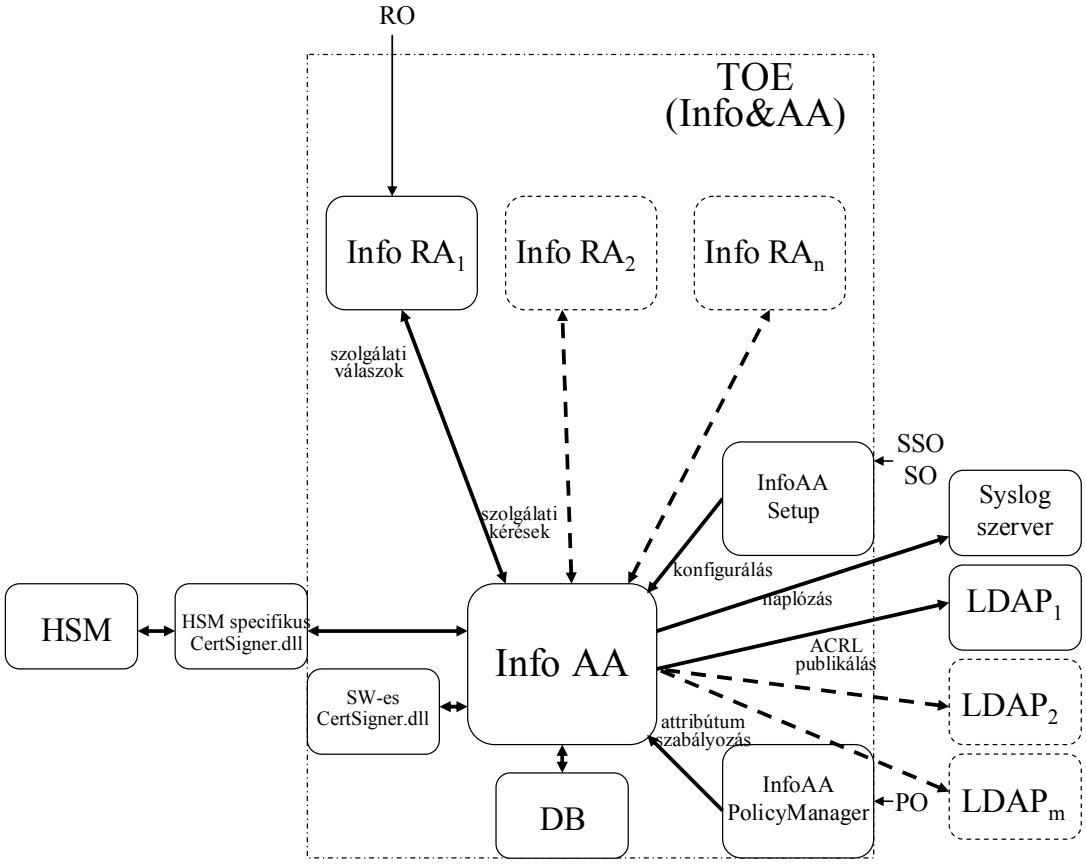
Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az Info&AA v1.0 valamennyi biztonsági funkcióját.

[1] Lásd ETSI SR 002 176-1 v2.0.0

5 Az Info&AA v1.0 szerkezeti leírása

5.1 Architektúra

Az Info&AA v1.0 fő összetevőit és fizikai hatókörét az 1. ábra szemlélteti, külön megjelenítve benne az értékelés tárgyát.



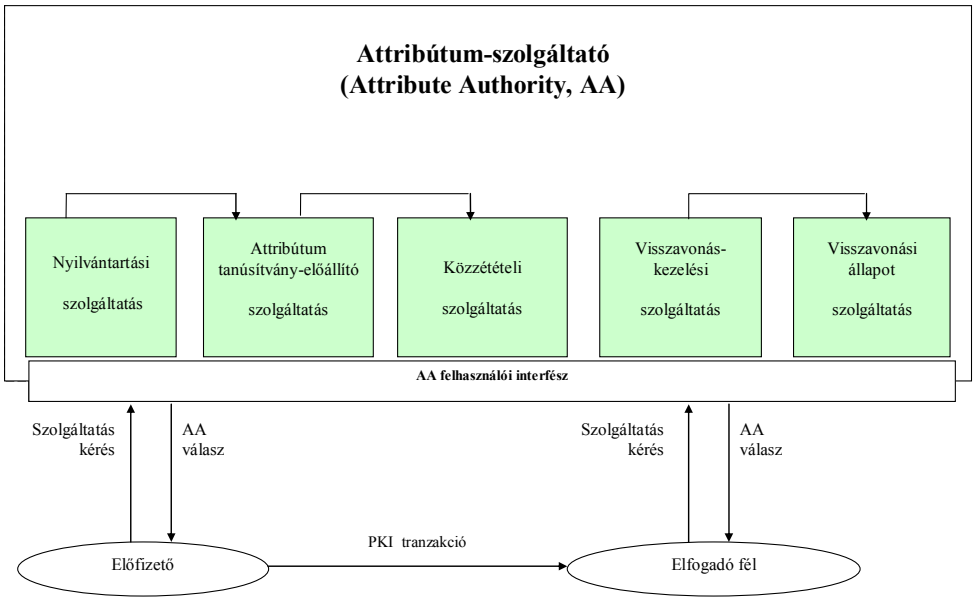
1. ábra: Az Info&AA v1.0 fizikai hatóköre

Felhasználók (a működő Info&AA-hoz közvetlenül hozzáférő, bizalmi munkakört betöltő személyek): SSO, SO, RO, PO.

Egyéb felhasználók (a működő Info&AA-hoz közvetlenül hozzá nem férő, bizalmi munkakört betöltő személyek): ADM és SA .

Külső felhasználók az Info&AA-hoz közvetlenül nem férhetnek (csak az RO közvetítésével kérhetnek szolgáltatást, illetve az LDAP-ból tölthetik le az attribútum visszavonási listákat).

Az Info&AA attribútum tanúsítványok (AC) kezelését (előállítását, szétosztását, visszavonását, visszavonás állapot kezelését) végző megbízható hitelesítés szolgáltató rendszer, ahogyan azt az 2. ábra szemlélteti.



2. ábra: Az Info&AA logikai hatóköre

Az **attribútum tanúsítvány** egy olyan adatszerkezet, amelyet az attribútum-szolgáltató (AA) digitálisan aláírt, és amely bizonyos attribútum értékeket birtokosának (előfizető) azonosító információihoz köt.

A **nyilvántartási szolgáltatás** az előfizető azonosságát és egyéb sajátos tulajdonságát vizsgálja. E szolgáltatás eredményeit az attribútum tanúsítvány-előállító szolgáltatásnak továbbítják.

Az **attribútum tanúsítvány-előállító szolgáltatás** a nyilvántartási szolgáltatás által megvizsgált azonosság és más jellemzők alapján attribútum tanúsítványt állít elő és ír alá.

A **közzétételi szolgáltatás** szétosztja az attribútum tanúsítványokat az előfizetők között, és ha az előfizető beleegyezik, az érintett felek között is. Ez a szolgáltatás a Hitelesítés-szolgáltató szabályzataira és gyakorlatára vonatkozó információkat is szétoszt az előfizetők és az érintett felek között.

A **visszavonás-kezelési szolgáltatás** feldolgozza a visszavonással kapcsolatos kérelmeket és jelentéseket a szükséges teendők meghatározása érdekében. E szolgáltatás eredményeit a visszavonási állapot szolgáltatásán keresztül osztják szét.

A **visszavonási állapot szolgáltatás** az attribútum tanúsítványok visszavonási állapotára vonatkozóan nyújt információt az érintett feleknek. Ez a szolgáltatás rendszeres időközönként frissített attribútum tanúsítvány visszavonási állapotinformáción (ACRL) alapul.

5.2 Alrendszerek

Az Info&AA rendszernek az alábbi alrendszerei vannak:

- AR1: Kliens (InfoAA RA)
- AR2: Attribútum-szabályozó (InfoAA Policy Manager)
- AR3: Konfiguráló (InfoAA Setup)
- AR4: Szerver (InfoAA)
- AR5: Segédkönyvtárak (DLL-k)

6 Tesztelés

6.1 A fejlesztők tesztelése

A fejlesztő tesztelési stratégiája a következő volt:

A fejlesztő által tervezett tesztesetek összességében lefedték a TOE fő funkcionalitását, valamennyi tesztelhető biztonsági funkciót, az összes külső interfészt, illetve az alrendszerek közötti belső interfészeket is.

A tesztesetek az alábbiak szerint csoportosíthatók:

- Telepítés: A tesztesetek lefuttatása során a telepítőkészletek felhasználásával a TOE működőképes állapota áll elő.
- InfoAA konfiguráció: A tesztesetek a TOE konfigurációjának teljes körű ellenőrzésére alkalmasak.
- Policy Manager funkcionalitás: A tesztesetek az AC kollekciók készítésének és beállításainak ellenőrzését végzik.
- Attribútum tanúsítvány kezelés - RA funkcionalitás: A tesztesetek az AC-k kérése, felfüggesztése, aktiválása és visszavonása, illetve a beállítási hiba ellenőrzésére szolgálnak.
- Jogosultságkezelés: A tesztesetek a különböző szerepkörök jogosultságainak ellenőrzése során a negatív, elutasítást kiváltó szituációkat ellenőrzik.
- Konfigurációs fájl ellenőrzés: A tesztesetek a rendszer integritás sérüléséből fakadó hibaágak lekezelését ellenőrzik.

6.2 Az értékelők tesztelése

Az értékelő független tesztelését saját környezetében végezte.

Az értékelő azt a tesztelési stratégiát választotta, hogy:

- először teljes mértékben megismételte a fejlesztők által végrehajtott tesztelést,
- majd független tesztesetet hajtott végre, melyek a jogosultságkezelésre és a CRL profil állományok integritás ellenőrzésére terjedtek ki.

A független tesztelés során hiba nem lépett fel.

7 Az értékelt konfiguráció

Telepítő csomagok:

- infoaa_installer.exe (1.0.0.1)- (az InfoAA.exe telepítő alkalmazása)
- infoaara_installer.exe (1.0.0.0) - (az InfoAARA.exe telepítő alkalmazása)
- infoaapm_installer.exe (1.0.0.0) - (az InfoAAPolicyManager.exe telepítő alkalmazása)

Szoftver elemek:

- InfoAASsoSetup.exe (2.0.0.3) – (a 3 SSO kezdeti meghatározását, fiókjuk beállítását végző alkalmazás)
- InfoAASetup.exe (1.0.0.0) - az InfoAA.exe beállítását végző alkalmazás
- InfoAARA.exe (1.0.0.0) - regisztrációs alkalmazás
- InfoAA.exe (0.1.0.401) – attribútum tanúsítványokat kezelő szerver oldali alkalmazás
- InfoAAPolicyManager.exe (1.0.0.0) – attribútum kollekciók szerkesztését biztosító alkalmazás
- BusinessEntities.dll (1.0.0.0) - attribútum tanúsítványokhoz kapcsolódó általános segédkönyvtár
- CertSigner.dll (2.0.0.14) - szoftveres aláíró könyvtár (teszt üzemmódhoz)
- PkiMiddleware.dll (1.0.0.0) - a konfigurációs állományok és a szolgáltatói kérések aláírását, valamint a különböző tisztviselők (SSO, SO, RO, PO) beléptetését végző segédkönyvtár
- Repository.dll (1.0.0.0) - a konfigurációs állományok mentését és betöltését támogató segédkönyvtár
- aa.sql - adatbázis generáló script

Környezeti elemek:

- CertSigner.dll (2.0.0.9)[2] - aláíró könyvtár nCipher nShield HSM modulhoz
- Windows XP SP3
- Microsoft SQL Server 2008 Express
- OpenLDAP 2.2.29
- Syslogd server: syslog-win32-0.3

[2] A HUNG-T-048/2009 regisztrációs számú InfoCA v2.5 komponenseként tanúsított dll.

8 Az értékelés eredményei

Az Info&AA v1.0 az informatikai termékek technológia szempontú biztonsági értékelésére kidolgozott MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertan szerint független értékelésre és tanúsításra került.

Az értékelés garanciaszintje MIBÉTS kiemelt, mely a CC (Common Criteria, MSZ ISO/IEC 15408) szerinti EAL4-es szintnek felel meg

Az értékelés fő következtetése az alábbi:

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy az Info&AA v1.0 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés másik következtetése az alábbi:

Az Info&AA v1.0 a 4.2 fejezetben megfogalmazott informatikai és nem informatikai környezetére vonatkozó feltételek teljesülése esetén megfelel az MSZ CWA 14167-1:2006 által az elektronikus aláírásokhoz tartozó tanúsítványokat kezelő megbízható rendszerekkel szemben támasztott biztonsági követelményrendszer azon követelményeinek, amik attribútum tanúsítvány kiadó rendszer esetén értelmezhető.

8.1 A biztonsági előirányzat értékelése

Ez az alfejezet a TOE biztonsági előirányzata értékelési eredményeit foglalja össze.

Az értékelés alapja az alábbi dokumentum:

- **Attribútum-szolgáltató szoftver (Info&AA) v1.0 – Biztonsági előirányzat** (v1.0)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Biztonsági előirányzat	ASE_INT.1 Bevezetés	A követelményeknek **megfelelt**.
	ASE_CCL.1 Megfelelőségi nyilatkozatok	A követelményeknek **megfelelt**.
	ASE_SPD.1 Biztonsági probléma meghatározás	A követelményeknek **megfelelt**.
	ASE_OBJ.1 Biztonsági célok	A követelményeknek **megfelelt**.
	ASE_ECD.1 Kiterjesztett biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_REQ.1 Biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_TSS.1 Az értékelés tárgya összefoglaló előírása	A követelményeknek **megfelelt**.

8.2 A fejlesztés értékelése

Ez az alfejezet A TOE tervezési dokumentációit értékeli a biztonsági funkcióik megfelelő leírása és magyarázata szempontjából.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

- Attribútum-szolgáltató szoftver (Info&AA) v1.0 - **Biztonsági előirányzat** (v1.0)
- **Biztonsági szerkezet leírás** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Funkcionális specifikáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **TOE terv** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Megvalósítási reprezentáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Forráskód** (lásd „Megvalósítási reprezentáció - Attribútum-szolgáltató szoftver (Info&AA) v1.0” dokumentum 2. fejezete)
- **A bizalmi munkakörök áttekintése** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- InfoAA **Adminisztrátori kézikönyv** (v1.0)
- InfoAA **RA kézikönyv** (v1.0)
- InfoAA **Policy Manager kézikönyv** (v1.0)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Fejlesztés	ADV_ARC.1 A biztonsági szerkezet leírás értékelése	A követelményeknek **megfelelt**.
	ADV_FSP.4 A teljes funkcionális specifikáció értékelése	A követelményeknek **megfelelt**.
	ADV_TDS.3 Az alap moduláris terv értékelése	A követelményeknek **megfelelt**.
	ADV_IMP.1 A megvalósítási reprezentáció értékelése	A követelményeknek **megfelelt**.

8.3 Az útmutatók értékelése

Ez az alfejezet A TOE útmutató dokumentációját értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

- Attribútum-szolgáltató szoftver (Info&AA) v1.0 - **Biztonsági előirányzat** (v1.0)
- **Funkcionális specifikáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **TOE terv** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A szállítási eljárások leírása** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Telepítési kézikönyv** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- **A bizalmi munkakörök áttekintése** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- **InfoAA Adminisztrátori kézikönyv** (v1.0)
- **InfoAA RA kézikönyv** (v1.0)
- **InfoAA Policy Manager kézikönyv** (v1.0)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Útmutató dokumentumok	AGD_PRE.1 Az előkészítő eljárások értékelése	A követelményeknek **megfelelt**.
	AGD_USR.1 Az üzemeltetési felhasználói útmutató értékelése	A követelményeknek **megfelelt**.

8.4 Az életciklus támogatás értékelése

Ez az alfejezet A TOE fejlesztése során a fejlesztői környezetben betartott biztonsági intézkedéseket értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

- Attribútum-szolgáltató szoftver (Info&AA) v1.0 - **Biztonsági előirányzat** (v1.0)
- a tesztelésre alkalmas Info&AA rendszer,
- **Konfiguráció lista** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A konfiguráció kezelés dokumentációja** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A fejlesztés biztonság dokumentációja** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Az életciklust meghatározó dokumentáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A fejlesztő eszközök dokumentációja** - Attribútum-szolgáltató szoftver (Info&AA) v1.0 (v1.0)
- **Infoscope Fejlesztési konvenciók, C#, C/C++** (v1.01)
- **A szállítási eljárások leírása** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **saját fejlesztésű forráskódok** (az implementáció reprezentáció egy részhalmaza)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Életciklus támogatás	ALC_CMC.4 A konfiguráció kezelés képességének értékelése	A követelményeknek **megfelelt**.
	ALC_CMS.4 A konfiguráció kezelés hatókörének értékelése	A követelményeknek **megfelelt**.
	ALC_DEL.1 A szállítás értékelése	A követelményeknek **megfelelt**.
	ALC_DVS.1 A fejlesztés biztonságának értékelése	A követelményeknek **megfelelt**.
	ALC_LCD.1 Az életciklus meghatározás értékelése	A követelményeknek **megfelelt**.
	ALC_TAT.1 A fejlesztői eszközök és technikák értékelése	A követelményeknek **megfelelt**.

8.5 A tesztelés értékelése

Ez az alfejezet azt vizsgálja és értékeli, hogy A TOE a tervdokumentációkban megadottaknak megfelelően működik-e, valamint összhangban van-e a biztonsági előirányzatában megfogalmazott funkcionális biztonsági követelményeivel.

Az értékelés alapját az alábbi fejlesztői és értékelői bizonyítékok képezték:

- Attribútum-szolgáltató szoftver (Info&AA) v1.0 - **Biztonsági előirányzat** (v1.0)
- **Biztonsági szerkezet leírás** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Funkcionális specifikáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **TOE terv** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Telepítési kézikönyv** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- **A bizalmi munkakörök áttekintése** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- **InfoAA Adminisztrátori kézikönyv** (v1.0)
- **InfoAA RA kézikönyv** (v1.0)
- **InfoAA Policy Manager kézikönyv** (v1.0)
- **A konfiguráció kezelés dokumentációja** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A tesztelésre alkalmas TOE**
- Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztelési terv** (v1.0)
- Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztelési dokumentáció** (v1.0)
- Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztlefedettség elemzés** - ATE_COV.2 (v1.0)
- Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztmélység elemzés** - ATE_DPT.2 (v1.0)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Tesztelés	ATE_FUN.1 A funkcionális tesztelés értékelése	A követelményeknek **megfelelt**.
	ATE_COV.2 A teszt lefedettség elemzés értékelése	A követelményeknek **megfelelt**.
	ATE_DPT.2 A teszt mélység elemzés értékelése	A követelményeknek **megfelelt**.
	ATE_IND.2 A független tesztelés értékelése	A követelményeknek **megfelelt**.

8.6 A sebezhetőség értékelése

Ez az alfejezet A TOE-ben lévő hibák, gyengeségek meglétét és a velük való visszaélések lehetőségét kívánja meghatározni vagy kizárni. Mindez a fejlesztő és az értékelő elemzésén alapul, valamint értékelői tesztelés egészíti ki.

Az értékelés alapját az alábbi fejlesztői és értékelői bizonyítékok képezték:

- Attribútum-szolgáltató szoftver (Info&AA) v1.0 - **Biztonsági előirányzat** (v1.0)
- **Biztonsági szerkezet leírás** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Funkcionális specifikáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **TOE terv** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Forráskód** (lásd „Megvalósítási reprezentáció - Attribútum-szolgáltató szoftver (Info&AA) v1.0” dokumentum 2. fejezete)
- **Telepítési kézikönyv** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- **A bizalmi munkakörök áttekintése** - Info&AA Attribútum tanúsítvány kibocsátó szoftver (v1.0)
- **InfoAA Adminisztrátori kézikönyv** (v1.0)
- **InfoAA RA kézikönyv** (v1.0)
- **InfoAA Policy Manager kézikönyv** (v1.0)
- **A tesztelésre alkalmas TOE**
- **Nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására**

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
A sebezhetőség felmérése	AVA_VAN.3 A sebezhetőség értékelése	A követelményeknek **megfelelt**.

9 Értékelői megjegyzések és javaslatok

Az értékelő által megfogalmazott javaslatok bekerültek mind a tanúsítvány 2. számú mellékletébe, mind jelen tanúsítási jelentés 4.2.1 alfejezetébe.

10 Mellékletek

10.1 Az Info&AA v1.0 megfelelése az MSZ CWA-14167-1:2006 követelményeinek

Az alábbi táblázat az MSZ CWA-14167-1 követelményeknek való megfelelésre vonatkozó vizsgálat eredményét foglalja össze. Az értékelés az egyes követelményekre külön-külön határozatot hozott, hogy az alábbiakból melyik vonatkozik az adott követelményre:

- **Az Info&AA v1.0 rendszer teljesíti** (azaz teljes mértékben megfelel a követelménynek)
- **Az Info&AA v1.0 rendszer támogatja** (azaz részben megfelel a követelménynek, de a környezetnek is támogatást kell nyújtania),
- **A környezetnek kell biztosítania** (azaz az Info&AA v1.0 rendszer nem vállalja fel a követelmény teljesítését, a megvalósítást az IT és nem IT környezettől várja el),
- **Az Info&AA v1.0 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.

Ssz	A követelmény azonosítója	A követelmény rövid leírása	Határozat az Info&AA v1.0 rendszerre
Általános funkcionális és biztonsági követelmények			
Menedzselés (M)			
M1 Rendszer- és biztonságkezelés			
1	[M1.1]	Különböző jogokkal bíró munkaköröket kell biztosítani.	**az Info&AA v1.0 rendszer támogatja**
2	[M1.2]	Legalább a következő munkakörök szükségesek:	**az Info&AA v1.0 rendszer támogatja**
3	[M1.3]	Felhasználók és munkakörök összekapcsolási képessége.	**az Info&AA v1.0 rendszer támogatja**
Rendszerek és működésük (SO)			
SO1 Üzemeltetés menedzselése			
4	[SO1.1]	Útmutatók biztosítása (helyes és biztonságos működtetés).	**az Info&AA v1.0 rendszer teljesíti**
SO2 A folyamatos szolgáltatás biztosítása			
5	[SO2.1]	99.9%-os rendelkezésre állás (tanúsítvány szétosztás, visszavonás kezelés, visszavonás állapot szolgáltatás).	**a környezetnek kell biztosítania**
6	[SO2.2]	Katasztrófahelyzetben is a működés (alternatív TWS)	**a környezetnek kell biztosítania**
7	[SO2.3]	Biztonságos áttérés a katasztrófa-helyreállító rendszerre.	**a környezetnek kell biztosítania**

SO3 Időszinkronizáció			
8	[SO3.1] NQCA	Állítást kell megfogalmazni az idő pontosságára.	**a környezetnek kell biztosítania**
Azonosítás és hitelesítés (IA)			
IA1 A felhasználó hitelesítése			
9	[IA1.1]	Kötelező felhasználói azonosítás és hitelesítés.	**az Info&AA v1.0 rendszer támogatja**
10	[IA1.2]	A felhasználó kijelentkezése után kötelező az újrahitelesítés.	**az Info&AA v1.0 rendszer támogatja**
11	[IA1.3]	Egyedi hitelesítő adatok.	**az Info&AA v1.0 rendszer támogatja**
IA2 Hitelesítési hiba			
12	[IA2.1]	A sikertelen hitelesítési kísérletek korlátozása.	**az Info&AA v1.0 rendszer támogatja**
IA3 A titok ellenőrzése			
13	[IA3.1]	Mechanizmus a titkok ellenőrzésére.	**az Info&AA v1.0 rendszer támogatja**
Rendszer-hozzáférés ellenőrzés (SA)			
SA1 Rendszer-hozzáférés ellenőrzés			
14	[SA1.1]	Azonosított egyének hozzáférésének ellenőrzése, korlátozása.	**az Info&AA v1.0 rendszer támogatja**
15	[SA1.2]	Hozzáférés védelem az érzékeny maradvány információkra.	**a környezetnek kell biztosítania**
Kulcs kezelés (KM)			
KM1 Kulcs generálás			
16	[KM1.1]	A tanúsítvány aláíró kulcsokat biztonságos kriptográfiai modulban (HSM) kell generálni.	**az Info&AA v1.0 rendszer támogatja**
17	[KM1.2]	A HSM-et értékelni és tanúsítani kell.	**a környezetnek kell biztosítania**
18	[KM1.3]	Kettős személyi ellenőrzés a szolgáltatói kulcsgenerálásnál.	**a környezetnek kell biztosítania**
19	[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	-
20	[KM1.7]	A kulcs generálás algoritmusa biztonságos legyen.	**a környezetnek kell biztosítania**

KM2 Kulcs elosztás			
21	[KM2.1]	A magán/titkos kulcsokat tilos nyílt formában szétosztani.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
22	[KM2.2]	A még tanúsítványba nem foglalt nyilvános kulcsokat biztonságos környezetben kell tartani.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
23	[KM2.3]	Szabványos kriptográfiai kulcselosztó módszer használata.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
24	[KM2.4]	A szolgáltatói nyilvános kulcsok szétosztásánál fenn kell tartani a sértetlenséget és hitelességét.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
25	[KM2.5]	Az önaláírt tanúsítvány jellemzői:	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
26	[KM2.6]	Önaláírt tanúsítványra biztonságos lenyomat készítése.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
KM3 Kulcs használat			
27	[KM3.1]	A HSM-hez hozzáférés ellenőrzést kell alkalmazni.	**a környezetnek kell biztosítania**
28	[KM3.4]	El kell különíteni az aláíró kulcsokat.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
29	[KM3.5]	Jogosult kulcshasználat csak életcikluson belül történhet.	**az Info&AA v1.0 rendszer teljesíti**
30	[KM3.6]	Kulcshasználat előtt tanúsítvány érvényesség ellenőrzés.	**az Info&AA v1.0 rendszer teljesíti**
KM4 Kulcs csere			
31	[KM4.1]	I és RV kulcsokat rendszeresen (pl. évente) cserélni kell.	**a környezetnek kell biztosítania**
32	[KM4.2]	A kulcs cserét biztonságosan kell végrehajtani.	**a környezetnek kell biztosítania**
KM5 Kulcs megsemmisítés			
33	[KM5.1	Tanúsítvány aláíró kulcsok végleges megsemmisítése.	**a környezetnek kell biztosítania**
34	[KM5.2]	Kivont rendszerek kulcsait meg kell semmisíteni.	**a környezetnek kell biztosítania**
35	[KM5.3]	Kulcs kinullázás képessége.	**a környezetnek kell biztosítania**
36	[KM5.4]	Biztonságos SW kulcstörlési folyamatok alkalmazása.	**a környezetnek kell biztosítania**

KM6 Kulcs tárolása, mentése és helyreállítása			
37	[KM6.1]	Minden magán/titkos kulcsot biztonságosan kell tárolni.	**a környezetnek kell biztosítania**
38	[KM6.2]	A TA kulcsokat HSM-ben kell tárolni.	**a környezetnek kell biztosítania**
39	[KM6.3]	Az I és RV kulcsokat HKE-ben kell tárolni.	**a környezetnek kell biztosítania**
40	[KM6.4]	Kulcs exportálás csak védett módon.	**a környezetnek kell biztosítania**
41	[KM6.5]	Kulcsokat csak jogosult személy (pl. SO) kezelheti.	**a környezetnek kell biztosítania**
42	[KM6.6]	TA magánkulcsok kezelése kettős személyi ellenőrzés alatt.	**a környezetnek kell biztosítania**
43	[KM6.7]	Tilos aláíró magánkulcsot menteni, letétbe helyezni.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
KM7 Kulcs archiválás			
44	[KM7.1]	Tilos az aláíró magánkulcsok archiválása.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
Naplózás (AA)			
AA1 Napló adatok generálása			
45	[AA1.1]	A következő események naplózása feltétlenül szükséges:	**az Info&AA v1.0 rendszer támogatja**
AA2 Napló adatok garantált rendelkezésre állása			
46	[AA2.1]	Karban kell tartani a naplózási adatokat.	**a környezetnek kell biztosítania**
47	[AA2.2]	A naplóbejegyzéseket nem szabad automatikusan felülírni.	**a környezetnek kell biztosítania**
AA3 Naplózási paraméterek			
48	[AA3.1]	Minden naplórekordnak tartalmaznia kell a következőket:…	**az Info&AA v1.0 rendszer teljesíti**
AA4 A napló választható áttekintése			
49	[AA4.1]	Gondoskodni kell a naplóesemények közötti keresésről.	**a környezetnek kell biztosítania**
50	[AA4.2]	A naplórekordot ember által olvashatóan kell megjeleníteni.	**a környezetnek kell biztosítania**
AA5 Korlátozott naplómegtekintés			
51	[AA5.1]	A naplót csak jogosultsággal lehessen olvasni.	**a környezetnek kell biztosítania**
52	[AA5.2]	Meg kell akadályozni a naplózási rekordok módosítását.	**az Info&AA v1.0 rendszer támogatja**
AA6 Riasztás generálása			
53	[AA6.1]	Riasztás kell a biztonság potenciális megsértése esetén.	**a környezetnek kell biztosítania**
AA7 A napló adatok sértetlenségének garantálása			
54	[AA7.1] NQCA	Biztosítani kell a napló adatok sértetlenségét.	**az Info&AA v1.0 rendszer támogatja**

AA8 A napló időbejegyzéseinek garantálása			
55	[AA8.1]	Megbízható időforrást kell alkalmazni a naplóhoz.	**a környezetnek kell biztosítania**
Archiválás (AR)			
AR1 Archív adatok generálása			
56	[AR1.1]	Képesnek kell lenni archívum létrehozására.	**a környezetnek kell biztosítania**
57	[AR1.2]	Archiválni kell: (tanúsítványok, CRL-ek, naplók)	**a környezetnek kell biztosítania**
58	[AR1.3]	Minden bejegyzésnek tartalmaznia kell az időpontot.	**a környezetnek kell biztosítania**
59	[AR1.4]	Archívumban kritikus biztonsági paraméter csak védetten.	**a környezetnek kell biztosítania**
AR2 Szelektálható keresés			
60	[AR2.1]	Az archívumra biztosítani kell egy keresési lehetőséget.	**a környezetnek kell biztosítania**
AR3 Az archivált adatok sértetlensége			
61	[AR3.1]	Az archívum bejegyzéseit védeni kell a módosítástól.	**a környezetnek kell biztosítania**
Mentés és helyreállítás (BK)			
BK1 Mentés generálása			
62	[BK1.1]	Léteznie kell egy mentési funkciónak.	**a környezetnek kell biztosítania**
63	[BK1.2]	A mentett adatokból a rendszer visszaállítható legyen.	**a környezetnek kell biztosítania**
64	[BK1.3]	A mentési funkció meghívható legyen (jogosultan).	**a környezetnek kell biztosítania**
BK2 A mentési információ sértetlensége és bizalmassága			
65	[BK2.1] NQCA	A mentést védeni kell a módosítás ellen.	**a környezetnek kell biztosítania**
66	[BK2.2]	Kritikus biztonsági paraméterek csak titkosított formában tárolhatók.	**a környezetnek kell biztosítania**
BK3 Helyreállítás			
67	[BK3.1]	Biztosítani kell egy helyreállítási funkciót.	**a környezetnek kell biztosítania**
68	[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			
69	[GE1.1]	A szolgáltatások által létrehozott üzenetre biztosítani kell: (üzenet és visszajátszás elleni védelem, létrehozási időpont)	**az Info&AA v1.0 rendszer teljesíti**

Regisztráció szolgáltatás (R)			
R1 Tanúsítvány kérelem			
70	[R1.1]	A tanúsítvány kérést szükség esetén védeni kell.	**a környezetnek kell biztosítania**
71	[R1.2]	Megfelelő mechanizmus szükséges a birtoklás bizonyítására.	**a környezetnek kell biztosítania**
72	[R1.4]	Mechanizmus kell a tanúsítvány kérelmek jóváhagyására.	**az Info&AA v1.0 rendszer teljesíti**
73	[R1.6]	A regisztráció üzeneteit alá kell írni.	**az Info&AA v1.0 rendszer teljesíti**
R2 Tanúsítvány kérelem			
74	[R2.1]	Az alanyra vonatkozó információ bizalmasságát védeni kell.	**a környezetnek kell biztosítania**
R3 Regisztráció szolgáltatás naplózása			
75	[R3.1]	A regisztráció alábbi eseményeit kötelező naplózni:	**az Info&AA v1.0 rendszer teljesíti**
Tanúsítvány előállítás szolgáltatás (CG)			
CG1 Tanúsítvány előállítás			
76	[CG1.1]	Biztosítani kell a tanúsítvány kérelem üzenet védelmét.	**az Info&AA v1.0 rendszer támogatja**
77	[CG1.2]	A tanúsítvány kérelmet biztonságosan kell feldolgozni.	**az Info&AA v1.0 rendszer teljesíti**
78	[CG1.3]	Biztosítani kell a birtoklás bizonyításának az ellenőrzését.	**az Info&AA v1.0 rendszerre a követelmény nem vonatkozik**
79	[CG1.5]	Meg kell felelni a meghatározott profiloknak.	**az Info&AA v1.0 rendszer teljesíti**
80	[CG1.6] NQCA	A tanúsítványoknak meg kell felelniük az alábbiaknak:	**az Info&AA v1.0 rendszer teljesíti**
CG2 Tanúsítvány megújítás			
81	[CG2.1]	A tanúsítvány megújítás során védekezni kell a tanúsítvány helyettesítés támadás ellen.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
82	[CG2.2]	I és RV kulcsokra a tanúsítvány megújításnak teljesítenie kell a KM.4 (kulcs csere) feltételeit is.	**a környezetnek kell biztosítania**
83	[CG2.3]	Biztosítani kell a TA tanúsítványok időbeli megújítását.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
84	[CG2.4]	Biztonságos mechanizmus kell az alany kulcsainak újra hitelesítésére és/vagy kulcs megújítására.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**

CG3 Felülhitelesítés			
85	[CG3.1]	Felülhitelesítés alkalmazása esetén biztosítania kell:…	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
CG4 A tanúsítvány előállítás szolgáltatás naplózása			
86	[CG4.1]	A tanúsítvány előállítás alábbi eseményeit kell naplózni:	**az Info&AA v1.0 rendszer teljesíti**
Tanúsítvány szétosztás szolgáltatás (D)			
D1 Szétosztás kezelés			
87	[D1.1]	A tanúsítvány szétosztás csak alanyoknak és az engedélyezett érintett feleknek.	**a környezetnek kell biztosítania**
88	[D1.2]	A szétosztás folyamata [D1.1]-nek megfelelő legyen.	**a környezetnek kell biztosítania**
D2 Objektumok exportja/importja			
89	[D2.1]	A tanúsítványtárra hozzáférés-ellenőrzési politika kell.	**a környezetnek kell biztosítania**
Visszavonás kezelés szolgáltatás (RM)			
RM1 Tanúsítvány állapotváltozás kérések			
90	[RM1.1]	A visszavonás/felfügg kérelmek végrehajtása 24 órán belül.	**a környezetnek kell biztosítania**
91	[RM1.2]	Minden kérelmet hitelesíteni és érvényesíteni kell.	**az Info&AA v1.0 rendszer teljesíti**
92	[RM1.3]	Visszavont tanúsítványt nem lehet újra használatba venni.	**az Info&AA v1.0 rendszer teljesíti**
93	[RM1.4]	TA kulcs- tanúsítványok visszavonása kettős ellenőrzéssel.	**a környezetnek kell biztosítania**
94	[RM1.5]	Állapot változtatását csak a következők kezdeményezhetik:	**a környezetnek kell biztosítania**
95	[RM1.6]	A tanúsítvány állapot adatbázist azonnal frissíteni kell.	**az Info&AA v1.0 rendszer teljesíti**
RM2 Tanúsítvány felfüggesztés/visszavonás			
96	[RM2.1]	Tanúsítvány visszavonása, még katasztrófát követően is.	**a környezetnek kell biztosítania**
97	[RM2.2]	Időszakos frissítő üzenetek használata esetén:…	**az Info&AA v1.0 rendszer teljesíti**
98	[RM2.3]	Valós idejű üzenetek használata esetén:….	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
RM3 A Visszavonás kezelés naplózása			
99	[RM3.1]	A visszavonás kezelés alábbi eseményeit kötelező naplózni:	**az Info&AA v1.0 rendszer teljesíti**

Visszavonás állapot szolgáltatás (RS)			
RS1 Visszavonás állapot adatok			
100	[RS1.1]	Csak megbízható tanúsítvány visszavonás kezelő szolgáltatásoktól származó üzenet dolgozható fel.	**az Info&AA v1.0 rendszer teljesíti**
101	[RS1.2]	OCSP üzenetek sértetlenségét és hitelességét ellenőrizni kell.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
102	[RS1.3]	OCSP válaszokra garantálni kell, hogy a tanúsítvány-állapot adatbázisból valóban a kért tanúsítványra vonatkozó választ kapták.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
RS2 Állapot kérés/válasz			
103	[RS2.1]	Minden választ digitálisan alá kell írni.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
104	[RS2.2]	Aláírni csak biztonságos algoritmussal.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
-	[RS2.3]	törölve	-
105	[RS2.4]	A válasz üzenetnek tartalmaznia kell az aláírás idejét.	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**
RS3 A tanúsítvány visszavonás állapot naplózása			
106	[RS3.1]	A tanúsítvány visszavonás alábbi eseményeit kell naplózni:…	**az Info&AA v1.0 rendszerre nem vonatkozik a követelmény**

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 Info&AA v1.0 egy olyan speciális elektronikus aláírás termék, amely különböző attribútum-szolgáltatást biztosító funkciókkal rendelkezik.
Az Info&AA v1.0 felhasználói az attribútum-szolgáltató operátorai és adminisztrátorai.
Az Info&AA v1.0 az alábbi attribútum-szolgáltatásokat támogatja:

a) *attribútum regisztráció szolgáltatás,*
b) *attribútum tanúsítvány igénylés szolgáltatás,*
c) *attribútum tanúsítvány előállítás szolgáltatás,*
d) *attribútum tanúsítvány szétosztás szolgáltatás,*
e) *attribútum tanúsítvány visszavonás kezelés szolgáltatás,*
f) *attribútum tanúsítvány visszavonás állapot szolgáltatás.*

A támogatott szolgáltatásokon belül az alábbiakat valósítja meg:

- *attribútum tanúsítvány előállítás (már kiadott PKI tanúsítványokhoz kapcsolódó, X.509 és RFC 3281 szabványoknak megfelelő attribútum tanúsítványok generálása),*
- *attribútum tanúsítvány visszavonás kezelés (már kiadott attribútum tanúsítványok visszavonása, felfüggesztése, újra aktiválása),*
- *attribútum tanúsítvány visszavonás állapot szolgáltatás (a visszavont és felfüggesztett attribútum tanúsítványokat tartalmazó, X.509 és RFC 5280 szabványoknak megfelelő ACRL-ek előállítása és LDAP-ba publikálása)"*

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 cél
Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

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.

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.

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

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.

AR	Alrendszer
ADV (Assurance: Development)	Fejlesztés értékelése
AGD (Assurance: Guidance documents)	Útmutató dokumentumok értékelése
ALC (Assurance: Life cycle support)	Életciklus támogatás értékelése
ASE (Assurance: Security Target)	Biztonsági előirányzat értékelése
ATE (Assurance: Tests)	Tesztelés értékelése
AVA (Assurance:Vulnerability assessment)	Sebezhetőségi elemzés értékelése
CA (Certification Authority)	Hitelesítés-Szolgáltató
CC (Common Criteria)	Közös szempontok
CEM (Common Evaluation Methodology)	Közös értékelési módszertan
CM (Configuration management)	Konfiguráció kezelés
EAL (Evaluation Assurance Level)	Értékelési garanciaszint
ETR (Evaluation Technical Report)	Értékelési jelentés
ETSI (European Telecommunication Standards Institute)	Európai Telekommunikációs Szabványok Intézete
KIB	Közigazgatási Informatikai Bizottság
MIBÉTS	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
ST (Security Target)	Biztonsági előirányzat
TOE (Target of Evaluation)	TOE, Értékelés tárgya
TSF (TOE Security Functionality)	A TOE biztonsági funkcionalitása

13 Felhasznált dokumentumok

13.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérelem a tanúsítás kérelmezéséhez
- Info&AA v1.0 Biztonsági előirányzat v1.0
- Info&AA v1.0 Értékelési jelentés v1.0

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
Attribútum-szolgáltató szoftver (Info&AA) v1.0 - **Biztonsági előirányzat**	1.0
Telepítési kézikönyv - Info&AA Attribútum tanúsítvány kibocsátó szoftver v1.0	1.0
A bizalmi munkakörök áttekintése - Info&AA Attribútum tanúsítvány kibocsátó szoftver v1.0	1.0
InfoAA Adminisztrátori kézikönyv	1.0
InfoAA RA kézikönyv	1.0
InfoAA Policy Manager kézikönyv	1.0
Biztonsági szerkezet leírás - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
Funkcionális specifikáció - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
TOE terv - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
Megvalósítási reprezentáció - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
Konfiguráció lista - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
A konfiguráció kezelés dokumentációja - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
A fejlesztés biztonság dokumentációja - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
Az életciklust meghatározó dokumentáció - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
A fejlesztő eszközök dokumentációja - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
Infoscope Fejlesztési konvenciók, C#, C/C++	1.01
A szállítási eljárások leírása - Attribútum-szolgáltató szoftver (Info&AA) v1.0	1.0
A tesztelésre alkalmas értékelés tárgya	1.0
Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztelési terv**	1.0
Attribútum-szolgáltató szoftver (Info&AA) v1.0 Tesztelési dokumentáció	1.0
Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztlefedettség elemzés** - ATE_COV.2	1.0
Attribútum-szolgáltató szoftver (Info&AA) v1.0 **Tesztmélység elemzés** - ATE_DPT.2	1.0

13.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) – Part 1: Introduction and general model
- Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) – Part 2: Security functional components
- Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) – Part 3: Security assurance components
- Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2)
- MSZ/ISO/IEC 15408:2003 Informatika – Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai
- KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlás „Termékekre vonatkozó értékelési módszertan”

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 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 3281: An Internet Attribute Certificate Profile for Authorization
- RFC 4476: Attribute Certificate (AC) Policies Extension
- ITU-T X.509-2000 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile