TANÚSÍTÁSI JELENTÉS

InfoSigno AC SDK v1.0.0.6

Attribútum tanúsítványok érvényességét ellenőrző SDK

HUNG-TJ-51-2010

Verzió:	1.0
Fájl:	HUNG-TJ-51-2010_v10.pdf
Minősítés:	Nyilvános
Oldalak:	29

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	**2010.08.27.**	**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:	**InfoSigno AC SDK Attribútum tanúsítványok érvényességét ellenőrző SDK**
Verzió szám:	**v1.0.0.6**
Rövid elnevezés:	**InfoSigno AC SDK**
Az értékelt termék típusa:	Elektronikus aláírás termék
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 alábbi funkciók tartoznak az InfoSigno AC SDK v1.0.0.6 szolgáltatásai közé:
	• Szabványos attribútum tanúsítvány beolvasása;
	• Attribútum tanúsítvány érvényesség ellenőrzése, és ebből következően az alábbi alfunkciók:
	  • A kapcsolódó nyilvános kulcs tanúsítványok feldolgozása, tanúsítási útvonalak érvényesség ellenőrzése, CRL és OCSP feldolgozás;
	  • A tanúsítványokon lévő aláírások ellenőrzése (a tanúsítási útvonal nyilvános kulcs tanúsítványain és az attribútum tanúsítványon lévő digitális aláírás ellenőrzése);
	  • Tanúsítvány visszavonási lista feldolgozása (ACRL) az attribútum tanúsítványokra;
	• Attribútum tanúsítvány elemeinek .NET objektumokra történő leképzése;
	• Az attribútum tanúsítványban található összes mező elérhetővé tétele.

Konfigurációs követelmények:	Az InfoSigno AC SDK függvénykönyvtárnak az alábbi informatikai elemekből álló környezetben kell működnie: • .NET Framework 3.5, • Windows XP Professional, Windows 2000 szerver vagy újabb verziók • Web szerver: Internet Information Server 5.0 vagy újabb verziók • Microsoft SQL szerver 2000 vagy újabb verziók

2 Azonosítás

Az értékelt termék neve:	**InfoSigno AC SDK Attribútum tanúsítványok érvényességét ellenőrző SDK**
Verzió szám:	**v1.0.0.6**
Az értékelt termék alkotó elemei:	Szoftver: • InfoSigno AC SDK: 1.0.0.6 • InfoSigno ACTest: 1.0.1.4 Útmutatók**:** • Az ACTest teszt website telepítői dokumentációja - Attribútum tanúsítványok érvényességét ellenőrző programkönyvtár (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) • Az ACTest tesztprogram felhasználói dokumentációja - Attribútum tanúsítványok érvényességét ellenőrző programkönyvtár (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az InfoSigno AC SDK irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.

3.1 Biztonsági funkciók

A InfoSigno AC SDK az alábbi biztonsági funkciók megvalósításával teljesíti a funkcionális biztonsági követelményekben megfogalmazott célokat:

- BF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése
- BF2 A visszavonási információk feldolgozása
- BF3 Digitális aláírás ellenőrzése
- BF4 Attribútum tanúsítvány érvényesség ellenőrzése
- BF5 Attribútumok visszaadása és megjelenítése
- BF6 ACTest menedzsment

A **Nyilvános kulcs tanúsítványok érvényesség ellenőrzése biztonsági funkció** végzi az attribútum tanúsítványhoz kapcsolódó szabványos nyilvános kulcs tanúsítványok, az AC tulajdonos nyilvános kulcs tanúsítványának, illetve az AC kibocsátó nyilvános kulcs tanúsítványának érvényesség ellenőrzését az RFC5280 szabványnak megfelelően.

A visszavonási információk feldolgozása biztonsági funkció AC esetén ACRL állományok feldolgozását, PKC estén CRL állományok illetve OCSP információk kezelését végzi.

A **Digitális aláírás ellenőrzése biztonsági funkció** hajtja végre a tanúsítási útvonal nyilvános kulcs tanúsítványain és az attribútum tanúsítványon lévő digitális aláírás ellenőrzését. Kiszámítja az aláírt adat lenyomatát, és a tanúsítványban található nyilvános kulcs algoritmus és nyilvános kulcs felhasználásával ellenőrzi az aláírást.

Az Attribútum tanúsítvány érvényesség ellenőrzése biztonsági funkció feladata az attribútum tanúsítványok érvényességének ellenőrzése, és ennek visszaadása a hívó IT környezeti alkalmazásnak, azaz az AC-t használó rendszernek, amely a saját igényei alapján használja fel a TOE által szolgáltatott eredményt.

Egy AC ellenőrzése a figyelembe vett RFC 3281 ajánlás alapján az alábbi kötelező ellenőrzéseket foglalja magába:

1. Az AC birtokosát hitelesítő (AC-ben hivatkozott) nyilvános kulcs tanúsítvány megtalálása, majd ezen PC teljes hitelesítési útvonalának ellenőrzése az RFC 5280 szerint.
2. Az AC digitális aláírásának kriptográfiai ellenőrzése, valamint az AC kibocsátójának teljes hitelesítési útvonalának ellenőrzése az RFC 5280 szerint.
3. Az AC kibocsátójának nyilvános kulcs tanúsítványára az alábbiak ellenőrzése:
   - megfelel az RFC 5280-ban meghatározott tanúsítvány profilnak,
   - a kulcshasználat (keyusage) kiterjesztés engedélyezi a digitális aláírás ellenőrzésére való felhasználást,
   - a CA (basic constraint) és a kulcshasználat (keyusage) kiterjesztés megtiltja a PC kibocsátást (cA: false, keyCertSign bit: 0)
4. Az AC kibocsátója egy közvetlenül megbízható AC kibocsátó (a közvetlen megbízhatóság konfigurálással vagy más módon érhető el).

5. Az AC kiértékelésének időpontja az AC érvényességén belül van. (azaz a kiértékelés időpontja nagyobb vagy egyenlő, mint notBeforeTime, egyúttal kisebb vagy egyenlő, mint notAfterTime). Egyes alkalmazásokban az ellenőrzés időpontja eltérhet az aktuális időponttól.
6. Az AC által tartalmazott valamennyi kritikus kiterjesztést az ellenőrző alkalmazásnak támogatnia kell (azaz fel kell ismernie a kiterjesztés értékét, a kiterjesztés értékéről meg kell állapítania, hogy elfogadható-e vagy sem, nem elfogadható kiterjesztés érték esetén az AC-t vissza kell utasítani), ellenkező esetben az AC-t vissza kell utasítani.
7. Az AC visszavonási információinak ellenőrzése. Ez az ellenőrzés a két lehetséges visszavonási sémában eltérő szabályokat tartalmaz.

Az Attribútumok visszaadása és megjelenítése biztonsági funkció biztosítja, hogy az ACTest és az InfoSigno AC SDK ellenőrizze az AC-ben szereplő attribútumokat, és megjelenítse a vonatkozó attribútumokat, melyek az alábbiak lehetnek: AuditIdentity; authorityKeyIdentifier; TargetInformation; authenticationInfo; accessIdentity; chargingIdentity; group; role; clerance; egyedi attribútumok.

Az ACTest menedzsment biztonsági funkció kezeli az InfoSigno AC SDK és ACTest alkalmazás konfigurálásával, felhasználók beállításával és biztonsági paraméterek beállításával kapcsolatos feladatokat.

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 InfoSigno AC SDK informatikai környezetére

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

1. A hoszt platform operációs rendszerének az általa futtatott alkalmazások számára elkülönített futási környezetet kell biztosítania. Fentieken túl az alábbi intézkedések teljesülését kell garantálni: a hoszt védett a vírustámadásokkal szemben; a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett; a hoszt platform adminisztrátori funkcióihoz való hozzáférés a platform adminisztrátorokra korlátozott ("hoszt adminisztátor"). A felhasználói fiók különbözik a hoszt adminisztrátoritól a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt áll; a hoszt platform operációs rendszere nem engedi nem megbízható alkalmazások végrehajtását. Alkalmazási megjegyzések: - a hoszt adminisztrátor szerepe eltér a TOE biztonsági adminisztrátor szerepétől. (OE.Host_Platform)
2. A TOE környezetének biztosítania kell az aláírások és az attribútum tanúsítvány ellenőrzéséhez szükséges érvényesítő adatokat. (OE.Validation_Data_Provision)
3. A TOE környezetének a biztonsági adminisztrátorok számára biztosítania kell olyan eszközöket, melyekkel a TOE szolgáltatásainak és paramétereinek sértetlensége kontrollálható. (OE.Services_Integrity)
4. A TOE biztonsági adminisztrátorainak megbízhatónak kell lenniük, a TOE használatára ki kell őket képezni, és rendelkezésükre állnak azok az eszközök, amelyekkel a feladataikat megfelelően el tudják látni. (OE.Trusted_Security_Administrator)
5. A TOE környezete biztosítja a teszteléshez (ACTest) szükséges IT környezetet a tesztekben részt vevő felhasználói adatok tárolásához. (OE.AC_CheckFrame)

4.2 A biztonságos felhasználás egyéb feltétele

6. Az InfoSigno AC SDK működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az InfoSigno AC SDK programozói könyvtárat, valamint az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő valamennyi összetevőt egy biztonságos területen valósítsák meg.

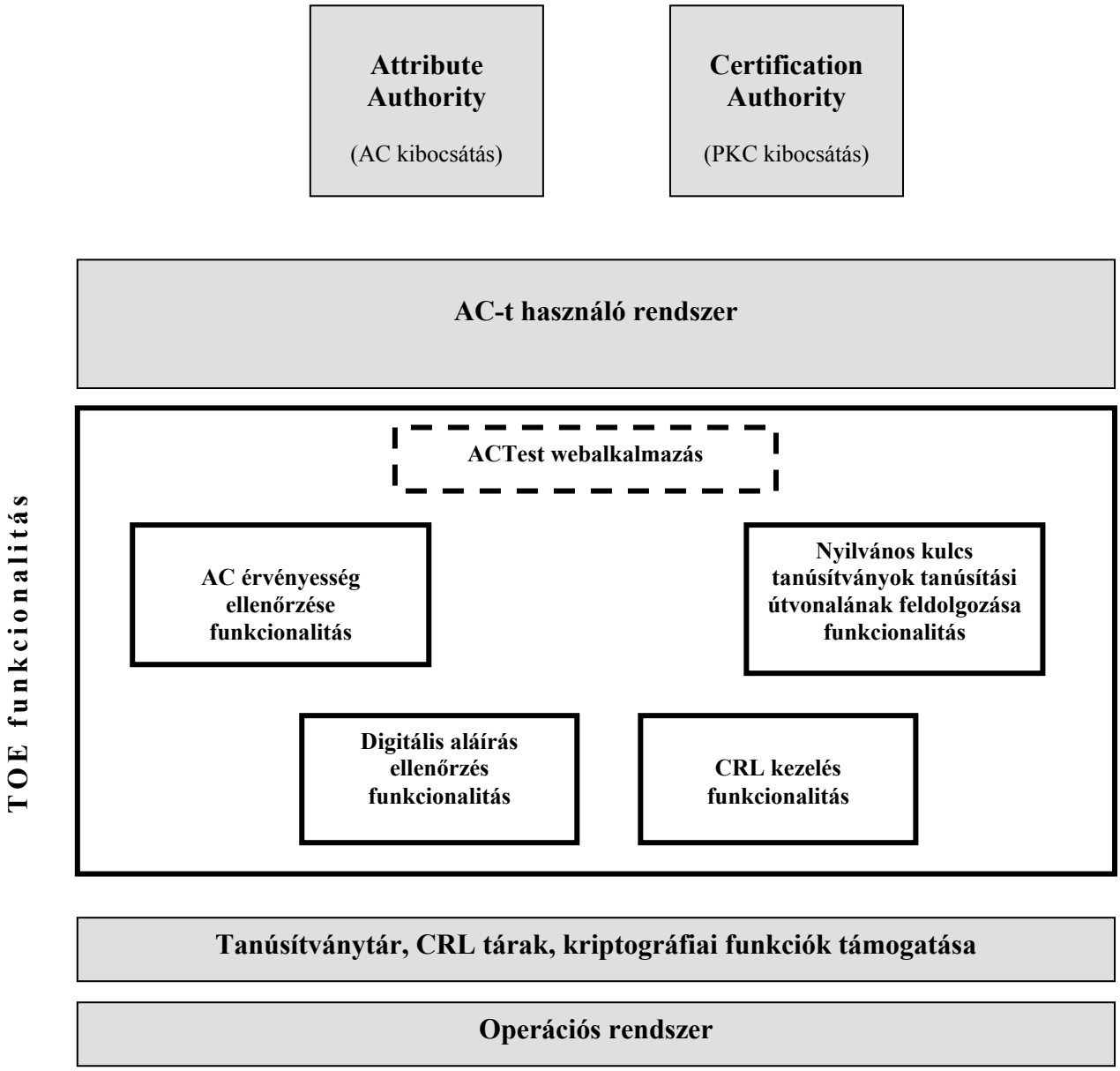
4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az InfoSigno AC SDK valamennyi biztonsági funkcióját.

5 Az InfoSigno AC SDK szerkezeti leírása

5.1 Architektúra

Az 1. ábra a TOE-t alkotó összetevőket mutatja azok tágabb üzemeltetési környezetébe eső más komponensekkel együtt. A szürke mezők a működtetési környezet által biztosított szolgáltatásokat jelentik, a fehér dobozok pedig a TOE logikai határaiba eső funkcionalitást mutatják.



1. ábra A TOE logikai határai és üzemeltetési környezete

Az 1.ábrán látható InfoSigno AC SDK és IT környezeti alkotóelemek szerepe:

Attribute Authority: Az attribútum tanúsítványok kibocsátását végző szervezet, rendszer.
Certification Authority: Az attribútum tanúsítványokhoz kapcsolódó nyilvános kulcsú tanúsítványok (AC tulajdonos, AC kibocsátó nyilvános kulcsú tanúsítványainak) kibocsátását végző szervezet.
AC-t használó rendszer: Az attribútum tanúsítványok által tartalmazott engedélyek feldolgozását végző rendszer. Ennek bemenete a TOE által szolgáltatott érvényesség ellenőrzés eredménye, az attribútum tanúsítványban tartalmazott attribútumokkal.

A InfoSigno AC SDK által biztosított funkcionalitás az alábbiakat foglalja magába:

1. **Attribútum tanúsítvány megfelelés ellenőrzése**
   Az attribútum tanúsítvány érvényesség ellenőrzése az RFC 3281-ben specifikált szerkezeti profil szerint, az alábbi megszorításokkal:
   - az AC kibocsátás egyszintű jogosultság kiosztás alapján történik (AA alatt nem állhat másik AA)
   - az alábbi opcionális tulajdonságokat az értékelt TOE verzió nem támogatja:
     - Proxying
     - Use of ObjectDigestInfo
     - AA Controls
     - Attribute Encryption

2. **Az AC által megjelölt PKI tanúsítvány érvényességének ellenőrzése**
   Az attribútum tanúsítvány ellenőrzésében szerepet játszó nyilvános kulcsú tanúsítványok (AC tulajdonos és az AC kibocsátó nyilvános kulcs tanúsítványai) érvényesség ellenőrzése az RFC 5280 által meghatározott módon, az AC kibocsátó tanúsítványa esetén kiegészítve az RFC 3281 vonatkozó követelményeivel (RFC 3281 4.5 fejezet).

3. **Attribútum tanúsítvány eredményének visszaadása és az aláírt attribútumok megjelenítése/továbbítása**
   Ezt a funkciót az InfoSigno AC ellenőrző alkalmazás végzi. Meghívja az InfoSigno AC SDK megfelelő funkcióit, és érvényes AC esetén megjeleníti/továbbítja az attribútumokat az azokat felhasználó IT környezeti összetevők felé.

A fenti fő funkcionalitást az alábbi szolgáltatások meghívásával hajtja végre a TOE:

Az attribútum tanúsítványokra vonatkozó visszavonás állapot (ACRL) feldolgozása

A TOE támogatja mindkét alábbi visszavonási sémát:
- „visszavonás nélküli” séma („never revoke” scheme)
- „AC-beli mutató” séma („Pointer in AC” scheme)

Az attribútum tanúsítvány visszavonási lista (ACRL) érvényesség ellenőrzése során a TOE megvizsgálja a tanúsítványok ellenőrzésében szerepet játszó ACRL-ek érvényességét. A TOE csak teljes visszavonási lista feldolgozását kezeli a tanúsítvány crlDistributionPoint kiterjesztésben mutatott lista feldolgozásával, delta CRL-eket nem kezel.

A nyilvános kulcs tanúsítványokra vonatkozó visszavonás állapot (CRL/OCSP) feldolgozása

A tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése során a TOE megvizsgálja a nyilvános kulcs tanúsítványok ellenőrzésében szerepet játszó CRL-ek érvényességét. A TOE csak teljes CRL feldolgozását kezeli a tanúsítvány crlDistributionPoint kiterjesztésben mutatott CRL feldolgozásával, delta CRL-eket nem dolgoz fel.

Az Online Certificate Status Protocol (OCSP) követelményei lehetővé teszik, hogy a TOE online tanúsítvány állapot kéréseket kezdeményezzen a nyilvános kulcs tanúsítványokra vonatkozóan, és ellenőrizze az OCSP válaszokat.

Tanúsítási útvonal érvényesség ellenőrzés szolgáltatás

A **tanúsítási útvonal érvényesség ellenőrzése** gondoskodik az attribútum tanúsítványhoz kapcsolódó nyilvános kulcs tanúsítvány (AC tulajdonos nyilvános kulcs tanúsítványának), illetve az AC kibocsátó nyilvános kulcs tanúsítványának érvényesség ellenőrzéséről. Ez a funkcionalitás a tanúsítási útvonal érvényességének ellenőrzésével és a tanúsítási útvonal felépítésével foglalkozik. A feldolgozás megfelel az RFC 5280 szabványnak.

A nyilvános kulcs tanúsítványok esetén *háromféle* tanúsítványt különböztetünk meg:
- **Megbízható pontok**: Ezek önaláírt tanúsítványok, melyek nem igényelnek semmilyen érvényesség ellenőrzést. A megbízható pont (önaláírt tanúsítvány) általában tanúsítvány formában jelenik meg. A megbízható pont elsődleges célja a megkülönböztető név (Distinguished Name), a nyilvános kulcs és az algoritmus azonosító megállapítása. A megbízható pontok hozzáadását, törlését, menedzselését az InfoSigno AC SDK hatáskörén kívül, a Windows tanúsítványtárban kell kezelni.
- **Közbenső tanúsítványok**: Ezek a hitelesítés-szolgáltatók (CA-k) számára kibocsátott tanúsítványok. Egy tanúsítási útvonal minden tanúsítványa ennek tekintendő, kivéve a megbízható pontot és a végtanúsítványt.
- **Végtanúsítvány:** A tanúsítási útvonal legutolsó tanúsítványa, melyet a szóban forgó egyed (aláíró) részére bocsátottak ki.

A nyilvános kulcs tanúsítványok érvényességének ellenőrzése során a tanúsítványhoz felépíthető teljes tanúsítási útvonalat figyelembe kell venni.

Az InfoSigno AC SDK a nyilvános kulcs tanúsítványok ellenőrzésekor a **keyUsage**, **extendedKeyUsage** és a **basicConstraints** biztonsággal kapcsolatos tanúsítvány kiterjesztési ellenőrzéseket veszi számításba.

PKI aláírás ellenőrzése szolgáltatás

A PKI aláírás ellenőrzése során az InfoSigno AC SDK feldolgozza az aláírási információkat és a nyilvános kulcsot használja az aláírás ellenőrzéséhez. A PKI aláírás ellenőrzésével kapcsolatos funkció a tanúsítási útvonal sikeres ellenőrzésétől függ.

6 Tesztelés

6.1 A fejlesztők tesztelése

A fejlesztő tesztelési munkája az alábbiakkal összegezhető:

- A tesztelést egy erre fejlesztett külön alkalmazás (ACTest) végzi.
- A tesztelés Webes felületen, úgynevezett portleteken keresztül történik.
- A portletek az attribútum tanúsítvány különböző rész elemeit vizsgálják.
- A tesztelés a teljes attribútum lehetőséget lefedi, alapos és elégséges.
- A tesztelés környezete megfelelt az ST-ben leírt működési környezetnek.

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, TOE azon részein, mely nem jelent meg hangsúlyosan a fejlesztői tesztelésben:, döntően az „Adminisztrálás” és a „Bejelentkezés” TSFI-re koncentrálva..

A független tesztelés során hiba nem lépett fel.

7 Az értékelt konfiguráció

Szoftver elemek:

- ACTest.dll (v1.0.1.4) - (InfoSigno ACTest bináris)
- ACSDK.dll (v1.0.0.6) - (InfoSigno AC SDK bináris)
- InfoSigno.dll (v3.0.0.92) - (InfoSigno PKI SDK bináris)
- SoftwareActivationLibrary.dll (v1.0.0.0) - (InfoSigno szoftveres védelem bináris)

3. fél által fejlesztett dll-ek:

- crypto.dll (1.5.0.0) - (BouncyCastle.Crypto (BCC) bináris)
- nunit.core.dll (v2.4.8.0) - (BCC test framework bináris)
- nunit.core.interfaces.dll (v2.4.8.0) - (BCC test framework bináris)
- nunit.framework.dll (v2.4.8.0) - (BCC test framework bináris)

Útmutató elemek:

- Az ACTest teszt website telepítői dokumentációja
- Az ACTest tesztprogram felhasználó dokumentációja

Környezeti elemek:

- Windows XP SP3
- .NET 3.5
- Microsoft SQL Server 2008 Express
- IIS 5.0

8 Az értékelés eredményei

Az InfoSigno AC SDK 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 InfoSigno AC SDK v1.0 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés másik következtetése az alábbi:

Az InfoSigno AC SDK v1.0 a 4.2 fejezetben megfogalmazott informatikai és nem informatikai környezetére vonatkozó feltételek teljesülése esetén megfelel a CEN CWA 14171 által az elektronikus aláírások ellenőrzésére vonatkozó biztonsági követelményrendszer azon követelményeinek, amelyek attribútum tanúsítványok ellenőrzése esetén értelmezhetők.

8.1 A biztonsági előirányzat értékelése

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

Az értékelés alapja az alábbi dokumentum:

- InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **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:

- InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **Biztonsági előirányzat** (v1.0)
- **Biztonsági szerkezet leírás** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Funkcionális specifikáció** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **TOE terv** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Megvalósítási reprezentáció** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Az ACTest teszt website telepítői dokumentációja** (v1.0)
- **Az ACTest tesztprogram felhasználó dokumentációja** (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:

- InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **Biztonsági előirányzat** (v1.0)
- **Funkcionális specifikáció** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **TOE terv** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Az ACTest teszt website telepítői dokumentációja** (v1.0)
- **Az ACTest tesztprogram felhasználó dokumentációja** (v1.0)
- **A szállítási eljárások leírása -** Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (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:

Az Info&AA rendszerre kidolgozott, az InfoSigno AC SDK (+ InfoSigno ACTest) TOE-ra is érvényes fejlesztői bizonyítékok:

- **A konfiguráció kezelés dokumentációja -** Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A fejlesztés biztonság dokumentációja** - Attribútum-szolgáltató szoftver (Info&AA) (v1.00)
- **Az életciklust meghatározó dokumentáció** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **Infoscope Fejlesztési konvenciók, C#, C/C++ (**v1.01)
- **A fejlesztő eszközök dokumentációja** - Attribútum-szolgáltató szoftver (Info&AA) (v1.0)

Az InfoSigno AC SDK (+ InfoSigno ACTest) TOE-ra érvényes egyedi fejlesztői bizonyítékok:

- InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **Biztonsági előirányzat** (v1.0)
- **A tesztelésre alkalmas értékelés tárgya(v**1.0.0.6 és v1.0.1.4
- **Konfiguráció lista** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **A szállítási eljárások leírása -** Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (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:

- InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **Biztonsági előirányzat** (v1.0)
- **Biztonsági szerkezet leírás** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Funkcionális specifikáció** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **TOE terv** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Az ACTest teszt website telepítői dokumentációja** (v1.0)
- **Az ACTest tesztprogram felhasználó dokumentációja** (v1.0)
- **A konfiguráció kezelés dokumentációja -** Attribútum-szolgáltató szoftver (Info&AA) (v1.0)
- **A tesztelésre alkalmas értékelés tárgya(**1.0.0.6 és 1.0.1.4)
- **Az ACTest tesztprogram dokumentációja -**Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 +ACTest v1.0.1.4) (v1.0)
- **Tesztlefedettség elemzés - ATE_COV.2** Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 +ACTest v1.0.1.4) (v1.0)
- **Tesztmélység elemzés - ATE_DPT.2** Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 +ACTest v1.0.1.4) (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:

- InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **Biztonsági előirányzat** (v1.0)
- **Biztonsági szerkezet leírás** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Funkcionális specifikáció** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **TOE terv** - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
- **Forráskód Lásd: „**Megvalósítási reprezentáció - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)”
- **Az ACTest teszt website telepítői dokumentációja** (v1.0)
- **Az ACTest tesztprogram felhasználó dokumentációja** (v1.0)
- **A tesztelésre alkalmas értékelés tárgya(**1.0.0.6 és 1.0.1.4
- **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 nem adott a tanúsítási jelentésbe megjelenítendő megjegyzést, illetve javaslatot.

10 Mellékletek

10.1 Az InfoSigno AC SDK megfelelése az MSZ CWA-14167-1:2006 követelményeinek

A 8. fejezetben foglaltak szerint az értékelés döntően annak megállapítására irányult, hogy az értékelés tárgya kielégíti-e a biztonsági előirányzatban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az InfoSigno AC SDK fejlesztő készletre (mint elektronikus aláírási termékre) ugyanakkor az alábbi alábbi nemzetközi követelményrendszer is vonatkozik:

- CEN/ISSS/E-Sign 14171:2004 CEN Workshop Agreement: General guidelines for electronic signature verification /May 2004/

A fenti dokumentumokban megfogalmazott funkcionális és biztonsági követelményeknek való megfelelőséget külön is vizsgálta az értékelés, melynek módszere a következő volt:
Az értékelés az egyes követelményekre külön-külön határozatot hozott, hogy az alábbiakból melyik vonatkozik az adott követelményre:

- megfelel,
- nem felel meg,
- nem vonatkozik rá a követelmény,
- feltétellel megfelel.

Egyetlen követelményre sem születhet "nem megfelel" határozat, mert ez az egész értékelés tárgyára nézve "nem megfelelt" eredménnyel járna.

A "feltétellel megfelel" határozat olyan feltételt támaszt (nem az értékelés tárgyára, hanem annak működtetési környezetére, vagy egy kiegészítő termékre), melynek kielégítése szükséges az értékelés tárgyának jövőbeli biztonságos használathoz.

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- 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.

Követelmény azonosító	Követelmény	Határozat
F_ISV-1	Az érvényesítő adatokat az ellenőrzőnek be kell gyűjtenie, és amennyiben létezik, az aláírási szabályzat minden követelményét teljesítenie kell.	**Megfelelt**
F_ISV-2	Ha szükség lehet utólagos ellenőrzésre, az érvényesítő adatoknak tartalmazniuk kell annak bizonyítékát, hogy a felhasznált tanúsítvány lánc érvényes volt az aláírás létrehozásának időpontjában.	**Nem vonatkozik rá**
F_ISV-3	Ha szükség lehet utólagos ellenőrzésre, az érvényesítő adatoknak tartalmazniuk kell annak bizonyítékát, hogy	**Megfelelt**

	a felhasznált tanúsítvány lánc érvényes volt az aláírás létrehozásának időpontjában.	
F_USV-1	Az utólagos ellenőrzés során a kezdeti ellenőrzés során begyűjtött érvényesítő adatok ellenőrzésénél az aláírási szabályzat minden követelményét teljesíteni kell.	**Nem vonatkozik rá**
F_human_1	Az aláírás-ellenőrző rendszernek eszközt kell biztosítania a felhasználó számára, amelyen keresztül az kommunikálni tud a rendszerrel. Ha az aláírt adatokhoz egynél több aláírás van hozzárendelve, akkor ennek a kommunikációnak azzal kell kezdődnie, hogy kijelzésre kerül az aláírások száma, amelyek feltehetően léteznek, és fel kell kínálni, hogy melyik legyen az ellenőrizendő.	**Nem vonatkozik rá**
F_human_2	Az aláírás-ellenőrző rendszernek interaktív eszközt kell biztosítania a felhasználó számára, hogy megnézhesse az aláírási szabályzat teljes egészét, vagy legalább az alkalmazási területre és feltételekre vonatkozó részeket.	**Nem vonatkozik rá**
F_human_3	A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az “Ami megjelenik, azt írták alá.” követelményt. Ha valamilyen okból az aláírói dokumentum nem jeleníthető meg pontosan a megfelelő módon, akkor ezt a felhasználói interfésznek világosan jeleznie kell.	**Megfelelt**
F_human_4	A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az “Ami megjelenik, azt írták alá.” követelményt. Ha valamilyen okból az aláírói dokumentum nem jeleníthető meg pontosan a megfelelő módon, akkor ezt a felhasználói interfésznek világosan jeleznie kell.	**Megfelelt**
F_human_5	A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az “Ami megjelenik, azt írták alá.” követelményt.	**Nem vonatkozik rá**
F_human_6	A felhasználói interfészekre teljesüljenek az F_principles egyszerűségre és hibamentességre vonatkozó speciális elvárásai.	**Megfelelt**
F_human_7	A kezdeti aláírás-ellenőrzési folyamat kimenő állapota az alábbiak egyike legyen: „érvényes” állapot (sikeres ellenőrzés), „érvénytelen” állapot (sikertelen ellenőrzés), „befejezetlen ellenőrzés” állapot (befejezetlen ellenőrzés)	**Megfelelt**
F_machine_1	Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére	**Megfelelt**

	és az elektronikus aláírás formátumának meghatározására.	
F_machine_2	A 2-es típusú API-k az elektronikus aláírások hitelesítését és/vagy ellenőrzését kell lehetővé tenniük, illetve be kell szerezniük az aláírói információkat, az output állapotot és az érvényesítő adatokat.	**Megfelelt**
F_general	A rendszer által megvalósított aláírás-ellenőrzési folyamatnak meg kell felelnie egy ember számára olvasható formájú leírásnak, feltételezve, hogy az aláírási szabályzat minden feldolgozási szabálya világosan meghatározott.	**Megfelelt**
F_protocol	Az aláírás-ellenőrzési alkalmazásnak szabványos protokollt kell használnia a megbízható szolgáltatóval (szolgáltatókkal) történő kommunikáció során.	**Megfelelt**
F_format	Az aláírás-ellenőrzési alkalmazásnak képesnek kell lennie szabványos formátumok kezelésére	**Megfelelt**
F_principles	A felhasználói felületek tervezésekor számos elvet figyelembe kell venni: …..	**Megfelelt**
B_Secure area	Az aláírás-ellenőrzés folyamattal kölcsönhatásba lépő összes összetevőt egy biztonságos területen kell megvalósítani.	**Lásd alább**
B_Secure area/ Software module	A biztonságos területet technikailag egy **szoftver modulban** valósítják meg, melyben a biztonsági ellenintézkedések szoftverben vannak megvalósítva.	**Feltétellel megfelelt**
B_Secure area/ Tamper-evident module	A biztonságos területet technikailag egy m**ódosítást-jelző modulban** valósítják meg, ahol a biztonsági ellenintézkedéseket olyan módon valósítják meg, hogy a manipuláció ugyan nem akadályozható meg, de a felhasználó észlelheti azt.	**Nem vonatkozik rá**
B_Secure area/ Tamper-resistant module	A biztonságos területet technikailag egy **módosításnak ellenálló modulban** valósítják meg, ahol a biztonsági ellenintézkedéseket olyan módon valósítják meg, hogy a manipuláció reális erőfeszítésekkel nem megvalósítható.	**Nem vonatkozik rá**

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 InfoSigno AC SDK egy olyan szoftverfejlesztő könyvtár, mely felhasználásával attribútum tanúsítványok érvényessége ellenőrizhető.

Az InfoSigno AC SDK szolgáltatásai közé az alábbi funkciók tartoznak:

- *Szabványos attribútum tanúsítvány beolvasása;*
- *Attribútum tanúsítvány érvényesség ellenőrzése, és ebből következően az alábbi alfunkciók:*
  - *A kapcsolódó nyilvános kulcs tanúsítványok feldolgozása, tanúsítási útvonalak érvényesség ellenőrzése, CRL és OCSP feldolgozás;*
  - *A tanúsítványokon lévő aláírások ellenőrzése (a tanúsítási útvonal nyilvános kulcs tanúsítványain és az attribútum tanúsítványon lévő digitális aláírás ellenőrzése);*
  - *Tanúsítvány visszavonási lista feldolgozása (ACRL) az attribútum tanúsítványokra;*
- *Attribútum tanúsítvány elemeinek .NET objektumokra történő leképzése;*
- *Az attribútum tanúsítványban található összes mező elérhetővé tétele.*

Az InfoSigno AC SDK az attribútum tanúsítványok feldolgozása során az alábbi szabványokat, ajánlásokat veszi figyelembe:

- *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*

Az InfoSigno ACTest egy az InfoSigno AC SDK függvényeire épülő web alapú alkalmazás. Segítségével az InfoSigno AC SDK összes funkciója kipróbálható, ellenőrizhető, tesztelhető."

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
- InfoSigno AC SDK Biztonsági előirányzat v1.0
- InfoSigno AC SDK 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
InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribútum tanúsítványok érvényességét ellenőrző SDK - **Biztonsági előirányzat**	1.0
Az ACTest teszt website telepítői dokumentációja	1.0
Az ACTest tesztprogram felhasználó dokumentációja	1.0
Biztonsági szerkezet leírás - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
Funkcionális specifikáció - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
TOE terv - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
Megvalósítási reprezentáció - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
Konfiguráció lista - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	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 tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
Az ACTest tesztprogram dokumentációja - Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
Tesztlefedettség elemzés - ATE_COV.2 Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
Tesztmélység elemzés - ATE_DPT.2 Attribútum tanúsítványok érvényességét ellenőrző SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)	1.0
A tesztelésre alkalmas értékelés tárgya	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 14171: 2004 General guidelines for electronic signature verification
- 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