TANÚSÍTÁSI JELENTÉS

MultiSigno V3 SDK
aláíró alkalmazás fejlesztő készlet
v3.0.1 /r249/

HUNG-TJ-33-2006

Verzió:	1.0
Fájl:	HUNG_TJ_33_2006_v10.pdf
Minősítés:	Nyilvános
Oldalak:	38

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2006.05.25	A szerkezet felállítása
v0.8	2006.05.26	A tanúsítás eredményeit tartalmazó teljes változat
v0.9	2006.06.05	Utolsó egyeztetésre kiadott változat
v1.0	2006.06.08.	Végleges verzió

A tanúsítási jelentést készítette:

Farkas Gábor
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**MultiSigno V3 aláíró alkalmazás fejlesztő készlet**
Verzió szám:	**3.0.1 r249**
Rövid elnevezés:	**MultiSigno v3.0.1**
Az értékelt termék típusa:	fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2006. május 18
Az értékelés módszere:	a MIBÉTS séma értékelési módszertana1
Az értékelés garanciaszintje:	kiemelt (EAL4)
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • elektronikus aláírás létrehozása; • elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal; • szimmetrikus AES ECB és CBC, 3DES-CBC, RC2 -CBC és aszimmetrikus (RSA, PKCS#1 v1.5) titkosítás és megoldás • időbélyegzés (kérése és ellenőrzése).
Konfigurációs követelmények:	Szoftver konfiguráció: • Operációs rendszer: Windows XP , Windows 2000 • PKCS#11 interfész • A MUSI.DLL és CertDBAPI.dll használatához szükséges DLL-ek: o cmapi.dll ,cmlasn.dll, cppasn1.dll, crlapi.dll srlapi.dll, v2.5.0.1 o libcurl.dll, libcurl2.dll, v7.13.1 o libeay32.dll, ssleay32.dll v0.9.8 o libxml2.dll, v2.6.10 o Cryptlib v5.2.1 Hardver konfiguráció: • CPU: X86-os processzor • RAM: 256 Mbyte vagy több • Diszk hely: 30 Mbyte vagy több • PKCS#11 token

[1] Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:
- 1. számú MIBÉTS kiadvány: **A MIBÉTS nemzeti séma általános modellezése** /0.95 verzió, 2005 február/,
- 2. számú MIBÉTS kiadvány: **Az értékelés és a tanúsítás folyamatai** /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - **A biztonsági előirányzat értékelésének módszertana** /0.95 verzió, 2005 február/,
- 3. . számú MIBÉTS kiadvány: Az értékelés módszertana 4 - **A kiemelt garanciaszint értékelésének módszertana** /0.95 verzió, 2005 február/

2 Azonosítás

Az értékelt termék neve:	**MultiSigno V3 aláíró alkalmazás fejlesztő készlet**
Verzió szám:	**3.0.1 /r249/**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	• MUSI.dll v3.0.1 r249 • CertDBAPI.dll v3.0.1 r249 • dokumentáció

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján a MultiSigno v3.0.1 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.
Először a MultiSigno v3.0.1 két üzemmódját határozzuk meg, melyekre eltérő szabályok vonatkoznak. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmódok

A MultiSigno v3.0.1 két használati esetet különböztet meg, az alábbiak szerint:

- Fokozott biztonságú aláírás létrehozás használati esete:
  - A MultiSigno-t biztonságos aláírás létrehozó eszköz nélkül használják elektronikus aláírások generálására és ellenőrzésére. Használható KHE (kriptográfiai hardver eszköz) vagy PKCS#12 szoftveres kulcstároló állomány.
- Minősített elektronikus aláírás használati esete:
  - Minősített aláírás létrehozása esetén kötelező tanúsított, NHH által nyilvántartásba vett BALE használata. Az aláírás létrehozásához használt tanúsítványnak minősítettnek kell lennie. A BALE-hez való hozzáférés szabványos PKCS#11 interfészen keresztül valósul meg.

A MultiSigno v3.0.1 két működési módban használható: dinamikus és statikus módban.

- Statikus módban a middleware(k) dll-je(i) a BaleAPI osztály létrejöttekor betöltõdnek, és csak az osztály megsemmisítésekor engedi el õket a rendszer. Alkalmazása egyféle middleware használata esetén javasolt.
- Dinamikus módban a middleware(k) dll-je(i) csak akkor töltõdnek be, amikor lekérik a middleware-hez tartozó BaleHandler osztálypéldányt és az osztálypéldány megsemmisítésekor engedi el a rendszer. Robosztusabb működést tesz lehetővé, használata többszálú futattás, illetve többféle middleware párhuzamos alkalmazása esetén javasolt.

3.2 Biztonsági funkciók

A TOE által megvalósított biztonsági funkciók a következőek:

- BF1 Aláírás létrehozása
- BF2 Elektronikus aláírás ellenőrzése
- BF3 Időbélyeg kérések és válaszok kezelése
- BF4 Tanúsítási útvonal felépítése és érvényesség ellenőrzése
- BF5 Tanúsítványtár kezelés
- BF6 Titkosítás és megoldás

3.2.1 BF1 Aláírás létrehozása

A **BF1 Aláírás létrehozása** biztonsági funkció végzi el a fokozott biztonságú vagy minősített elektronikus aláírás létrehozását. Előkészíti az aláírás létrehozást (fájl hozzáadása, magánkulcs kiválasztása, aláírással kapcsolatos adatszerkezetek létrehozása), majd az előkészített információk alapján elkészíti a lenyomatot és az elektronikus aláírást.
A funkció képes az aláírói dokumentum mimeType-jának tárolására, amit a hívó alkalmazás ellenőrizhet.
Az aláírás létrehozás biztonsági funkció az aláírás létrehozási funkció részeként létrehozza a titkosítandó lenyomatot. Az alkalmazható lenyomatoló algoritmusok: SHA-1, SHA-256, SHA-384, SHA-512 [FIPS 180-1], [FIPS 180-2].
A MultiSigno v3.0.1 lehetőséget biztosít fokozott biztonságú és minősített elektronikus aláírások létrehozására. ***Fokozott biztonságú aláírások esetén*** az alábbi kulcstároló eszközöket képes kezelni:

- Saját tanúsítványtárba betöltött PKCS#12-es formátumú kulcstároló fájl,
- kriptográfiai hardver eszköz (saját tanúsítványtáron keresztül).

A biztonsági funkció közvetlenül nem ellenőrzi a **`keyUsage`** kiterjesztést (a kötelezően beállított **`nonRepudiation`** bit mellett opcionálisan a **`digitalSignature`** bit lehet beállítva), a függvénykönyvtár használójának kell ellenőrizni a funkció által visszaadott értéket.
Minősített elektronikus aláírás létrehozása esetén az aláíráshoz használt tanúsítványnak minősített tanúsítványnak (QCStatement kiterjesztés használata) kell lennie. A MultiSigno 3.0.1 képes minősített tanúsítványokhoz tartozó, hardvereszközön (BALE-n) tárolt magánkulcsot használni. A minősített aláírás létrehozásához használt magánkulcshoz tartozó tanúsítványban a **`keyUsage`** kiterjesztésben csak a **`nonRepudiation`** bit lehet beállítva, amit a függvénykönyvtárat használó alkalmazásfejlesztőnek kell ellenőriznie.
A funkció által létrehozott elektronikus aláírás formátuma: Melasz-Ready XAdES-C formátum.
A MultiSigno v3.0.1 az aláírás létrehozását akkor tekinti sikeresnek, ha az aláírás ellenőrzését is végre tudja hajtani.

3.2.2 BF2 Elektronikus aláírás ellenőrzése

Ez a funkció valósítja meg a bemenetként kapott elektronikus aláírás ellenőrzését. A funkciónak átadott elektronikus aláírás ellenőrzés után a hívó alkalmazásnak meg kell vizsgálni az ellenőrzés által visszaadott információkat, amelyek jelzik, hogy az aláírás megfelel-e a hívó alkalmazás által kezdeményezett kezdeti vagy utólagos ellenőrzésnek, illetve további részletek ad az ellenőrzés státuszról.

3.2.3 BF3 Időbélyeg kérések és válaszok kezelése

A MultiSigno v3.0.1 képes időbélyeg kérést kibocsátani az aláírás adott időben való meglétének igazolása céljából. Az RFC 3161-ben specifikáltaknak megfelelően összeállítja az időbélyeg kérést a lenyomattal, és elküldi a kérés paramétereként megadott külső időbélyeg szolgáltatóhoz.
A MultiSigno v3.0.1 az időbélyeg szolgáltatótól kapott időbélyeg válaszra végrehajtja a szükséges szintaktikai és szemantikai ellenőrzéseket, azaz ellenőrzi az időbélyeg válasz elemeit és aláírását.

3.2.4 BF4 Tanúsítási útvonal felépítése és érvényesség ellenőrzése

Ez a biztonsági funkció végzi az aláíró tanúsítványtól a gyökértanúsítványig tartó tanúsítvány lánc elemeinek összegyűjtését és ellenőrzését. A MultiSigno v3.0.1 saját tanúsítványtárából dolgozik, ezt adja át az útvonal tényleges ellenőrzését végző nyílt kódú függvénykönyvtárnak (Certificate Management Library API), melynek feladata a tanúsítványok és visszavonási listák értelmezése és tárolása, tanúsítványok érvényességének vizsgálata.
A biztonsági funkció meghívását a MultiSigno v3.0.1 végzi, de a tényleges útvonal érvényesség ellenőrzést a CML-ben megvalósított függvények végzik (MultiSigno értékelés hatáskörén kívüli összetevőként), melyek az ellenőrzés eredményét visszaadják a hívó MultiSigno v3.0.1 függvénynek, ami értelmezi az érvényesség ellenőrzés eredményét.

3.2.5 BF5 Tanúsítványtár kezelés

A MultiSigno v3.0.1 saját tanúsítványtárat használ a működése során, amihez az alábbi tanúsítványtár funkciókat biztosítja:

- Gyökér tanúsítvány hozzáadása
- Gyökér tanúsítvány eltávolítás
- Gyökér tanúsítvány listázása
- közbenső tanúsítvány hozzáadása
- közbenső tanúsítvány eltávolítás
- közbenső tanúsítvány listázása
- végfelhasználói tanúsítvány hozzáadása
- végfelhasználói tanúsítvány eltávolítás
- végfelhasználói tanúsítvány listázása
- végfelhasználói tanúsítvány exportálása
- PKCS#12 formátumú magánkulcs tárolása
- CRL források megadása
- CRL források törlése
- CRL források listázása
- CRL tárolása

3.2.6 BF6 Titkosítás és megoldás

A MultiSigno v3.0.1 titkosítás és kapcsolódó megoldás biztonsági funkciókat is támogat.
A támogatott aszimmetrikus algoritmusok:

- RSA, PKCS#1 v1.5.

Támogatott szimmetrikus titkosítási algoritmusok:

- AES/ECB és CBC mód,
- 3DES/CBC,
- RC2/CBC.

4 Feltételezések és hatókör

Az értékelés pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

- a biztonsági előirányzat feltételezései (az értékelés tárgyát képező fejlesztő készlet biztonságához szükséges, az informatikai környezetre vonatkozó feltételek),
- a biztonságos felhasználás feltételei (az értékelés tárgyát képező fejlesztő készlet felhasználásával készített alkalmazások biztonságához szükséges, ezen alkalmazások megfelelő kialakítására vonatkozó feltételezések, javaslatok).

4.1 Feltételezések a MultiSigno v3.0.1 informatikai környezetére

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

1. Az engedéllyel rendelkező felhasználók (alkalmazás fejlesztők) megbízhatók a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre (AE.Authorized_Users).
2. A MultiSigno v3.0.1-t megfelelően telepítik és konfigurálják (AE.Configuration).
3. Fokozott biztonságú elektronikus aláírás létrehozása esetén a MultiSigno v3.0.1 által meghívott kriptográfiai funkciók (OpenSSL v0.9.8) megbízhatónak tekinthetők az elvárt kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a MultiSigno v3.0.1 környezete tartalmaz egy vagy több NHH által nyilvántartott, tanúsított BALE-t, mely(ek) tárolják és védik az aláíró magánkulcsát, illetve végrehajtják a digitális aláírást (AE.Crypto_Module).
4. A MultiSigno v3.0.1-mal szembeni támadási potenciált alacsonynak tételezzük fel. (AE.Low).
5. A MultiSigno v3.0.1 környezete fizikailag biztonságos (AE.Physical_Protection).
6. A tanúsítvány és tanúsítvány visszavonási információk a MultiSigno v3.0.1 rendelkezésére állnak (AE.PKI_Info)
7. A MultiSigno v3.0.1 környezete GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről (AE.Time).
8. A MultiSigno v3.0.1 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést (AE.TimeStamp).

4.2 A biztonságos felhasználás egyéb feltételei

1. A MultiSigno v3.0.1 programozói könyvtár az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja az automatikus Policy kezelést és az LDAP alapú CRL kibocsátást, valamint a delta CRL-t. Ezért csak olyan környezetben szabad alkalmazni, ahol önkibocsátott (self issued) tanúsítvány a tanúsítványláncba nem fordul elő. Nem használható olyan rendszerben, ahol a Policy-t automatikusan kell kezelni, LDAP alapú a CRL kibocsátás, vagy delta CRL-t használnak.
2. A MultiSigno v3.0.1 fejlesztő készletet használó aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.
3. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében biztosítani kell a használt PKCS#12 fájl és token eszköz jelszavának lecserélhetőségét.

4. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:
    a. vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
    b. az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.
5. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a MultiSigno v3.0.1 programozói könyvtár funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák azt.
6. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a MultiSigno v3.0.1 programozói könyvtárat, valamint az aláírás-létrehozás és aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő valamennyi összetevőjét egy biztonságos területen valósítsák meg.

4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és a MultiSigno v3.0.1 valamennyi biztonsági funkcióját.

5 A MultiSigno v3.0.1 szerkezeti leírása

Az értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők. A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak:

- fokozott biztonságú elektronikus aláírás létrehozása RSA/1024 algoritmus paraméterekkel, PKCS#12 formátumú fájlban saját tanúsítványtárban vagy kriptográfiai hardver eszközben tárolt magánkulcs használatával.
- minősített elektronikus aláírás létrehozása RSA/1024 algoritmus paraméterekkel BALE használatával.
- elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal;
- aláírás létrehozáshoz lenyomat készítése SHA-1, SHA-256, SHA-384, SHA-512 algoritmusokkal.
- szimmetrikus AES ECB és CBC, 3DES-CBC, RC2 -CBC és aszimmetrikus (RSA, PKCS#1 v1.5) titkosítás és megoldás
- időbélyegzés (kérése és ellenőrzése).

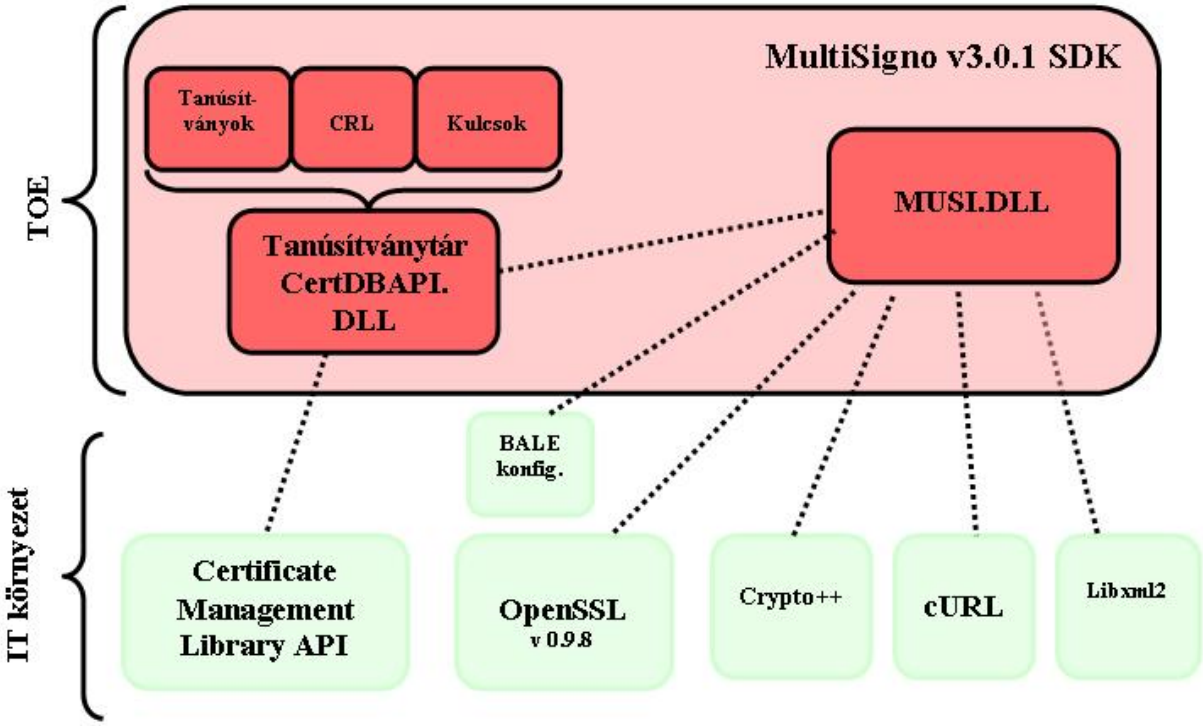
Ennek alapján a MultiSigno v3.0.1 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani.

A MultiSigno v3.0.1 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokkal rendelkezik:

- Biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat.
- Elfogad és feldolgoz X509 v3 nyilvános kulcs tanúsítványokat.
- Képes a szükséges tanúsítványok és visszavonási adatok megszerzésére.
- Ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzést is.
- Hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében.
- Minősített aláírás létrehozása esetén együttműködik a magyar jogszabályok által megkövetelt módon minősített aláírás létrehozásához szükséges tanúsított BALE eszközzel, vagy fokozott biztonságú aláírások esetén képes szabványos szoftveres kulcstároló állományok vagy Kriptográfiai hardver eszköz (KHE) biztonságos kezelésére.
- Gyűjti, tárolja és karbantartja a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat.
- Képes automatikusan választani több magán rejtjelező kulcsból, ha nyilvános kulcs alapú megoldást végez.
- Elektronikus aláírás formátum: Melasz-Ready XAdES.

5.1 Architektúra

Az 1. ábra a MultiSigno v3.0.1 struktúráját és az IT környezetbe való beágyazódását mutatja be.



1. ábra A MultiSigno v3.0.1 és környezete

A MultiSigno v3.0.1 értékelés hatáskörébe eső összetevők az alábbiak:

- MultiSigno **CertDBAPI**: A tanúsítványtár szolgáltatásokat végző összetevő.
- MultiSigno **MultiSigno**: Az elektronikus aláírással, kriptográfiával kapcsolatos szolgáltatások.

A MultiSigno v3.0.1 IT környezetéhez tartozó összetevők, melyek nem részei jelen értékelésnek:

- **Crypto ++ v5.2.1**: Kriptográfia műveletek végrehajtása (lenyomatolás, szimmetrikus és asszimetrikus titkosítás, kulcsgenerálás).
- **Libxml2 v2.6.10**: XML struktúrák értelmezése, előállítása.
- **OpenSLL v0.9.8:** Tanúsítványok értelmezése, http és https kapcsolatok felépítése, aláírás érték létrehozása és ellenőrzése, PKCS 7 és PKCS 12 csomagok értelmezése és létrehozása.
- **cURL 7.13.1:** Http és https kapcsolatok felépítése (OpenSLL segítségével).
- **Certificate Management Library (CML) v2.5.0.1:** Tanúsítványok és visszavonási listák értelmezése és tárolása, valamint tanúsítványok érvényességének vizsgálata.

5.2 Alrendszerek

A MultiSigno v3.0.1-nak az alábbi hat alrendszere van:

- AR1: Tanúsítványtár kezelését végző alrendszer
- AR2: Kriptográfiai alrendszer
- AR3: MultiSigno elektronikus aláírás szolgáltatási alrendszer
- AR4: Kiegészítő funkciókat végző alrendszer

5.2.1 Az AR1 (Tanúsítványtár kezelését végző) alrendszer:

- Megvalósítja a BF4 **Tanúsítási útvonal felépítése és érvényesség ellenőrzése** biztonsági funkciót, azáltal, hogy az aláírás ellenőrzéséhez szükséges tanúsítási útvonal felépítéséhez összegyűjti, tárolja, kezeli a tanúsítványokat.
- Megvalósítja a BF5 **Tanúsítványtár kezelés** biztonsági funkciót, azáltal, hogy gondoskodik a tanúsítványtárral kapcsolatos szolgáltatásokról.
- Közreműködik a BF1 **Aláírás létrehozása** biztonsági funkció megvalósításában, mert biztosítja az aláírás létrehozásához szükséges megfelelő tanúsítványhoz és magánkulcshoz való hozzáférést.
- Közreműködik a BF2 **Elektronikus aláírás ellenőrzése** biztonsági funkció megvalósításában, mert a tanúsítványok és kulcsok biztonságos kezelésével hozzájárul az aláírás érvényességének ellenőrzéséhez.
- Közreműködik a BF6 **Titkosítás és megoldás** biztonsági funkció megvalósításában, mert biztosítja és kezeli ezen funkció működéséhez szükséges tanúsítványokat.

5.2.2 Az AR2 (Kriptográfiai) alrendszer:

- Megvalósítja a BF6 **Titkosítás és megoldás** biztonsági funkciót azáltal, hogy megfelelő paraméterezéssel meghívja a tényleges titkosítási, megoldási függvényeket.
- Közreműködik a BF1 **Aláírás létrehozása** biztonsági funkció megvalósításában, mert elvégzi az aláírás létrehozásához szükséges kriptográfiai funkciók megfelelő paraméterekkel történő meghívását.
- Közreműködik a BF2 **Elektronikus aláírás ellenőrzése** biztonsági funkció megvalósításában, mert elvégzi az aláírás ellenőrzéséhez szükséges kriptográfiai funkciók megfelelő paraméterekkel történő meghívását.
- Közreműködik a BF3 **Időbélyeg kérések és válaszok kezelése** biztonsági funkció megvalósításában, mert elvégzi az időbélyeg kéréshez szükséges kriptográfiai funkciók meghívását, valamint az időbélyegen szereplő aláírás ellenőrzéséhez szükséges kriptográfiai funkciók megfelelő paraméterekkel történő meghívását.
- Közreműködik a BF4 **Tanúsítási útvonal felépítése és érvényesség ellenőrzése** biztonsági funkció megvalósításában,mert hozzájárul a tanúsítványokon lévő aláírások ellenőrzéséhez.
- Közreműködik a BF5 **Tanúsítványtár kezelés** biztonsági funkció megvalósításában, mert elvégzi a kulcsadatok kezelését.

5.2.3 Az AR3 (MultiSigno elektronikus aláírás szolgáltatási) alrendszer:

- Megvalósítja a BF1 **Aláírás létrehozása** biztonsági funkciót azáltal, hogy elektronikus aláírást hoz létre.
- Megvalósítja a BF2 **Elektronikus aláírás ellenőrzése** biztonsági funkciót azáltal, hogy a kapott elektronikus aláírásra elvégzi annak ellenőrzését.
- Megvalósítja a BF3 **Időbélyeg kérések és válaszok kezelése** biztonsági funkciót azáltal, hogy időbélyeg kérést bocsát ki, és ellenőrzi a kapott időbélyeg választ.
- Közreműködik a BF4 **Tanúsítási útvonal felépítése és érvényesség ellenőrzése** biztonsági funkció megvalósításához, mert kezdeményezi a Tanúsítványtár kezelési alrendszer felé az útvonal felépítését és ellenőrzését.
- Közreműködik a BF6 **Titkosítás és megoldás** biztonsági funkció megvalósításában, mert interfészt biztosít a nyílt forrású kriptográfiai modulokhoz és kezeli a minősített elektronikus aláíráshoz szükséges BALE-t.

5.2.4 Az AR4 (Kiegészítő funkciókat végző) alrendszer:

- Nem valósít meg biztonsági funkciót és nem is közreműködik ezekben.

6 Dokumentáció

Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek) az alábbiak:

- a **fejlesztésre alkalmas MUSI.dll és CertDBAPI.dll v3.0.1 r249**
- "MultiSigno v3.0.1 –Ú**tmutató**" /Reference Manual/

A fejlesztésre alkalmas MultiSigno v3.0.1 a fejlesztésekhez szükséges dll-t tartalmazza

MultiSigno v3.0.1 – Útmutató bemutatja a MultiSigno v3.0.1 fejlesztő készletet, tartalmazza az adminisztrátori és felhasználói, illetve a fejlesztőknek szóló útmutatást

7 Tesztelés

A tesztelés során a MultiSigno v3.0.1 fejlesztő készlet kulcs, tanúsítvány és CRL kezeléssel, valamint az aláírással és az aláírás ellenőrzéssel kapcsolatos függvényeit kerültek ellenőrzésre.
A MultiSigno v3.0.1 értékelése során kialakított és alkalmazott tesztek két csoportba sorolhatóak:

- PKITS teszt,
- Saját fejlesztésű értékelői teszt.

7.1 PKITS teszt

A MultiSigno v3.0.1 fejlesztő készleten az értékelők elvégezték a NIST által javasolt PKITS teszteket, annak eldöntésére, hogy a tanúsítványlánc érvényességének ellenőrzése megfelel-e az RFC 3280-ban kötelezően előírt elvárásoknak. A tesztelés eredményei az alábbiak:

- PKITS 4.1 Aláírás ellenőrzés:
  a 4.1.1 - 4.1.4 A tesztek sikeresen lefutottak, a MultiSigno v3.0.1 fejlesztőkészlet csak RSA tanúsítványokkal működik.
- PKITS 4.2 Érvényességi időszakok
  A 4.2.1 - 4.2.8 A tesztek sikeresen lefutottak.
- PKITS 4.3 Név-lánc ellenőrzés
  A 4.3.1 - 4.3.6, 4.3.9 tesztek sikeresen lefutottak.
- PKITS 4.4 Alap CRL teszt
  A 4.4.1 - 4.4.21 tesztek sikeresen lefutottak.
- PKITS 4.5 Önkibocsátott tanúsítványláncok ellenőrzése
  A MultiSigno v3.0.1 nem kezeli azokat a tanúsítványláncokat, amelyek önkibocsátott tanúsítványokat tartalmaznak.
- PKITS 4.6 Alapvető megkötések ellenőrzése
  A 4.6.1 - 4.6.17 tesztek a 4.6.15 és a 4.6.17 tesztek kivételével sikeresen lefutottak. /A 4.6.15-ös és a 4.6.17-es tesztek önkibocsátott tanúsítványokat tartalmaznak. A MultiSigno v3.0.1 nem kezeli azokat a tanúsítványláncokat, amelyek önkibocsátott tanúsítványokat tartalmaznak./
- PKITS 4.7 Kulcshasználat
  A 4.7.1 - 4.7.5 tesztek sikeresen lefutottak.
- PKITS 4.8-4.12 Policy tesztek
  A MultiSigno v3.0.1 nem kezeli a Policy kiterjesztéseket a tanúsítványokban.
- PKITS 4.13 Name Constraints
  A 4.13.1 - 4.13.38 tesztek a 4.13.14 és a 4.13.19 tesztek kivételével sikeresen lefutottak.
  /A 4.13.14-es teszt esetben nem tudja betölteni a PKCS#12 kulcsfájlt, mert a DN név nem RFC 2253 formátumú, s a MultiSigno v3.0.1 ezt elvárja. A 4.13.19-es teszt önkibocsátott tanúsítványokat tartalmaz. A MultiSigno v3.0.1 nem kezeli azokat a tanúsítványláncokat, amelyek önkibocsátott tanúsítványokat tartalmaznak./
- PKITS 4.14 Kibocsátási hely
  A MultiSigno v3.0.1 nem kezeli az LDAP alapú CRL kibocsátási helyeket, csak a HTTP, HTTPS protokolon keresztülieket.
- PKITS 4.15 Delta CRL
  A MultiSigno v3.0.1 nem kezeli a Delta CRL-eket.
- PKITS 4.16 Egyéni tanúsítvány kiterjesztések
  A 4.16.1 - 4.16.2 tesztek sikeresen lefutottak.

7.2 Saját fejlesztésű értékelői teszt

Az értékelők megvizsgálták a MultiSigno v3.0.1 fejlesztő készletet, hogy helyesen kezeli-e az aláírás ideje környékén visszavont tanúsítványokat.
Két teszt futott le. Mindkét esetben a CRL kibocsátása 24 óránként történik.

- Az első esetben az aláírás ideje előtt, de még a következő CRL kibocsátása előtt visszavonták az aláírói tanúsítványt. Az értékelők azt várták, hogy az aláírás ellenőrzése az utólagos ellenőrzés során érvénytelen eredményt ad.
- A második esetben közvetlenül az aláírás után, de még a következő CRL kibocsátása előtt visszavonták az aláírói tanúsítványt. Az értékelők azt várták, hogy az aláírás ellenőrzése az utólagos ellenőrzés során érvényes eredményt ad.

Mindkét esetben az aláírási csomag elkészítése után közvetlenül sor került az ellenőrzésre. Az ellenőrzés érvényesnek mutatta az aláírásokat, azzal a kikötéssel, hogy még nem felel meg az utólagos ellenőrzés feltételeinek. Ez az eredmény az elvárt, hiszen az aláírás idején aktuális CRL-ben nincs benne az aláíró tanúsítvány.
Mindkét esetben sor került az aláírás ideje után 24 órával is az ellenőrzésekre.

- Az első esetben az ellenőrzés azt adta, hogy az aláírás érvénytelen, mivel a tanúsítvány vissza lett vonva. Ez volt az elvárt eredmény.
- A második esetben az ellenőrzés azt adta, hogy az aláírás érvényes. Ez volt az elvárt eredmény.

Összefoglalva a teszteredményeket megállapítható, hogy a MultiSigno v3.0.1 fejlesztő készlet a tesztelés során megfelelően működött, a várt teszt eredményeket produkálta.

8 Az értékelt konfiguráció

8.1 Hardver

Hardver konfiguráció:

- CPU: X86-os processzor
- RAM: 256 Mbyte vagy több
- Diszk hely: 30 Mbyte vagy több
- PKCS#11 token

8.2 Szoftver

Szoftver konfiguráció:

- Operációs rendszer: Windows XP , Windows 2000
- PKCS#11 interfész
- A MUSI.DLL és CertDBAPI.dll használatához szükséges DLL-ek:
  - cmapi.dll ,cmlasn.dll, cppasn1.dll, crlapi.dll srlapi.dll, v2.5.0.1
  - libcurl.dll, libcurl2.dll, v7.13.1
  - libeay32.dll, ssleay32.dll v0.9.8
  - libxml2.dll, v2.6.10
  - Cryptlib v5.2.1

8.3 BALE

A MultiSigno v3.0.1 minősített aláírás létrehozása esetén NHH által nyilvántartásba vett biztonságos aláírás létrehozó eszköz használata kötelező. A MultiSigno v3.0.1 a BALE eszközt PKCS#11 interfészen keresztül éri el.

9 Az értékelés eredményei

A MultiSigno v3.0.1 fejlesztő készlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került, kiemelt garanciaszinten.

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy **a MultiSigno v3.0.1 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.**

A fenti megállapítás a kiemelt garanciaszint (EAL4) követelményeinek teljesítésén alapul. Az alábbiak azt mutatja meg, hogy az egyes garanciaösszetevőket hogyan teljesíti a MultiSigno v3.0.1 fejlesztő készlet, illetve mely fejlesztői bizonyítékok támogatták ennek kimutatását.

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja, /s az ezt leíró fejlesztői bizonyíték/
Konfiguráció menedzselés	ACM_CAP.4	Az értékelésre átadott szoftver (fejlesztő készlet) egyedi azonosításra került. A konfiguráció lista leírja a MultiSigno v3.0.1 alkotó konfiguráció elemeket, megfelelve az ACM_SCP-ben megadott minimális körnek(megvalósítási reprezentáció, tervezési dokumentációk, tesztelési dokumentáció, fejlesztői útmutató, a konfiguráció menedzselés dokumentáció, valamint a biztonsági hibák). A konfiguráció lista elemeit a dokumentált rendszer szerint kezelik MultiSigno v3.0.1 – **A konfiguráció menedzselés dokumentációja**
	ACM_SCP.2	A konfiguráció menedzselés dokumentációban megadott konfiguráció lista tartalmazza a konfiguráció menedzselés rendszer által nyomon követendő, a CC és a MIBÉTS által megkövetelt minimális konfiguráció elem készletet. A konfiguráció menedzselés dokumentáció leírja az egyes konfiguráció elem állapotok nyomon követésének módját a TOE teljes életciklusa során. MultiSigno v3.0.1 – **A konfiguráció menedzselés dokumentációja**
	ACM_AUT.1	A konfiguráció menedzselés terv tartalmazza a MultiSigno megvalósítási reprezentációhoz való hozzáférést felügyelő automatizmusok leírását. Az automatizált hozzáférés ellenőrzési intézkedések hatékonyan gátolják a MultiSigno megvalósítási reprezentációjának jogosulatlan módosításait. MultiSigno v3.0.1 – **A konfiguráció menedzselés dokumentációja**

Kiszállítás és működtetés	ADO_DEL.2	A szállítási eljárások alkalmasak a biztonsági cél kielégítésére (vagyis annak garantálása, hogy a szállítási eljárások kielégítően biztosítják, hogy a kifejlesztett értékelés tárgya sértetlenül jut el a felhasználó telephelyére, valamint detektálhatók a szállítás során végrehajtott módosítások és álcázásos próbálkozások). A szállítási dokumentáció leírja, hogy a különböző eljárások és technikai intézkedések milyen módon járulnak hozzá a fejlesztői eredeti példány és a felhasználó telephelyén megkapott verzió közötti módosítások vagy más ellentmondások észleléséhez. A szállítási dokumentáció leírja, hogy a különböző mechanizmusok és eljárások hogyan teszik lehetővé az álcázási kísérletek észlelését, még olyan esetekben is, amikor a fejlesztő nem küldött semmit sem a felhasználónak. A szállítási eljárásokat alkalmazzák. MultiSigno v3.0.1 – Ú**tmutató** /Reference Manual/
	ADO_IGS.1	A dokumentáció megadja és leírja a biztonságos telepítéséhez, generálásához és indításához szükséges eljárásokat illetve azokat a lépéseket, amelyek a MultiSigno biztonságos telepítéséhez, generáláshoz és indításához szükségesek. MultiSigno v3.0.1 – **Útmutató** /Reference Manual/
Fejlesztés	ADV_FSP.2	A funkcionális specifikáció informális módon leírja a megvalósítandó biztonsági funkciókat és azok külső interfészeit. Teljes körűen meghatározza a biztonsági funkciókat. Illetőleg meggyőző indoklást tartalmaz arról, hogy teljes mértékben bemutatta a biztonsági funkciókat. A funkcionális specifikáció lefed minden biztonsági előirányzatban szereplő funkcionális biztonsági követelményt. MultiSigno - **Funkcionális specifikáció**
	ADV_HLD.2	A magas szintű terv az összes szükséges informális magyarázatot tartalmazza. Leírja a biztonsági funkciókat az alrendszerek szintjén, azonosítja a biztonsági funkciók által megkövetelt összes hardvert, förmvert és szoftvert. Az alrendszerek interfészeit leírja az egyes alrendszerek interfészeit azok célja és használati módja szerint, valamint megadja a következmények részleteit, a kivételeket és hibaüzeneteket. A biztonsági funkciókat pontosan írja le. A biztonsági funkciók között nincs olyan függőségi kapcsolat, mely nem szerepel a magas szintű tervben A magas szintű terv lefedi a biztonsági előirányzat összes funkcionális biztonsági követelményét. MultiSigno - **Magas szintű terv**
	ADV_LLD.1	Az alacsony szintű terv az összes szükséges informális magyarázatot tartalmazza. Leírja a biztonsági funkciókat a modulok szintjén és az összes modul célját, valamint a modulok közötti kapcsolatokat. Leírja a modulok interfészeit, azok célja és használatának módja szerint, valamint részletezi a hatásokat, kivételeket, illetve hibaüzeneteket. Az alacsony szintű terv a funkcionális biztonsági követelmények pontos leképezése és lefedi a biztonsági előirányzat összes funkcionális biztonsági követelményét MultiSigno - **Alacsony szintű terv**
	ADV_IMP.1	A megvalósítási reprezentáció (pontosabban annak biztonsági szempontból kritikus része) pontosan képezi le az érintett funkcionális biztonsági követelményeket MultiSigno - **Forráskód**

	ADV_RCR.1	A biztonsági előirányzat összefoglaló előírása és a funkcionális specifikáció közötti megfeleltetés-elemzés alapján megállapítható, hogy a funkcionális specifikáció a MultiSigno biztonsági funkcióinak helyes és teljes reprezentációja. A funkcionális specifikáció és a magas szintű terv közötti megfeleltetés-elemzés alapján megállapítható, hogy a magas szintű terv helyes és teljes megvalósulása a funkcionális specifikációnak. A magas szintű terv és az alacsony szintű terv közötti megfeleltetés-elemzés alapján megállapítható, hogy az alacsony szintű terv helyes és teljes megvalósulása a magas szintű tervnek. Az alacsony szintű terv és a megvalósítás reprezentáció részhalmaza közötti megfeleltetés-elemzés alapján megállapítható, hogy a részhalmaz helyes és teljes megvalósulása az alacsony szintű terv azon részének, melyet a megvalósítási reprezentáció finomított. MultiSigno– **Megfeleltetés elemzések**
Útmutató dokumentumok	AGD_ADM.1	Az adminisztrátoroknak (is) szóló útmutatás: • leírja az adminisztrátor rendelkezésére álló adminisztratív biztonsági funkciókat és interfészeket, • leírja a MultiSigno biztonságos üzemeltetéséhez szükséges adminisztrálás módját, • tartalmazza az azokkal a funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos feldolgozási környezetben felügyelni kell. • leír minden olyan feltételezést, mely a biztonságos üzemeltetés szempontjából lényeges felhasználói viselkedéssel kapcsolatos. • leír minden, az adminisztrátor ellenőrzése alá tartozó biztonsági paramétert, szükség esetén jelezve a biztonságos értékeket is. • leírja a végrehajtandó adminisztrátori funkcióhoz kapcsolódó, biztonsági szempontból lényeges események típusát, beleértve a biztonsági tulajdonságok megváltoztatását is. • konzisztens az értékeléshez beadott többi dokumentációval, leír minden, a MultiSigno informatikai környezetére vonatkozó, az adminisztrátor számára lényeges biztonsági követelményt. MultiSigno v3.0.1 – **Útmutató** /Reference Manual/
	AGD_USR.1	A felhasználóknak szóló útmutatás: • leírja a nem adminisztrátor felhasználók rendelkezésére álló valamennyi interfész és funkció leírását, • leírja a MultiSigno által biztosított, felhasználók által hozzáférhető biztonsági funkciók használatát, • megadja a felhasználó által hozzáférhető azon funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos feldolgozási környezetben felügyelni kell, • leír minden olyan felhasználói feladatot, amely a MultiSigno biztonságos üzemeltetéséhez szükséges, beleértve a biztonsági környezet leírásában szereplő, a felhasználói viselkedésre vonatkozó feltételezéseket is, • konzisztens az értékeléshez beadott többi dokumentációval, leír minden, a MultiSigno informatikai környezetére vonatkozó, a felhasználó számára lényeges biztonsági követelményt. MultiSigno v3.0.1 – **Útmutató** /Reference Manual/

Az életciklus támogatása	ALC_DVS.1	A fejlesztés bizalmasságát és sértetlenségét garantáló szabályok vizsgálata alapján kijelenthető, hogy az alkalmazott biztonsági intézkedések kielégítők. Az értékelő a helyszíni szemlén (megfigyeléssel, mintavételi vizsgálattal és személyes kérdésekkel) megállapította, hogy a leírt biztonsági intézkedéseket be is tartják MultiSigno – **A fejlesztési biztonság dokumentációja**
	ALC_LCD.1	Az alkalmazott életciklus modell (Microsoft Solution Framework) lefedi a fejlesztési és karbantartási folyamatot. Az életciklus modell által leírt eljárások, eszközök és technikák használata pozitív módon hozzájárul a MultiSigno fejlesztéséhez és karbantartásához. MultiSigno – **Az életciklust meghatározó dokumentáció**
	ALC_TAT.1	A fejlesztő eszközök dokumentációja alapján megállapítható, hogy minden fejlesztő eszköz jól meghatározott. Egyértelműen megadja az implementációban használt valamennyi utasítás jelentését, valamint az összes megvalósítás-függő opció jelentését. MultiSigno – **A fejlesztő eszközök dokumentációja**
Tesztelés	ATE_FUN.1	A tesztelési dokumentáció tartalmazza a teszt terveket, a teszt eljárások leírását és a várt eredményeket, valamint a teszt eredményeit. Azonosítja a tesztelendő biztonsági funkciókat és leírja a végrehajtott tesztek célját. A leírt teszt konfiguráció megegyezik a biztonsági előirányzatban megadott értékelendő konfigurációval. A tesztelési tervek és a megfelelő teszt eljárások leírásai összhangban vannak egymással. A teszt eljárások leírása a megismételhetőséghez szükséges kellő részletességgel meghatározza a kezdeti tesztfeltételeket, beleértve a sorrendiséget befolyásoló függőségeket, amennyiben léteznek ilyenek valamint az egyes biztonsági funkciók kiváltását (teszt input) és az ezek eredményeként várható reakciókat. A várható teszteredmények megadása megfelelő (egyértelműek, megfelelnek a tesztmódszerből adódó működésnek). A tesztelési dokumentációban leírt, várt eredmények megfelelnek a teszt tényleges eredményeivel. MultiSigno – **Tesztelési dokumentáció**
	ATE_COV.2	A teszt lefedettség elemzés alapján megállapítható, hogy a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikáció közötti megfeleltetés pontos. Minden biztonsági funkció esetén alkalmas a várt viselkedés bemutatásához és megfelelően ellenőrzik az összes biztonsági funkciót. A teszt lefedettség elemzés alapján megállapítható, hogy a funkcionális specifikációban leírt biztonsági funkciók és a tesztelési dokumentációban szereplő tesztek közötti megfeleltetés teljes /minden biztonsági funkcióhoz és ezek külső interfészeihez tartozik teszt/. MultiSigno v3.0.1 – **Teszt lefedettség elemzés**

	ATE_DPT.1	A teszt mélység lefedettség elemzés alapján megállapítható, hogy a tesztelési dokumentációban azonosított tesztek és a magas szintű terv közötti megfeleltetés pontos. A leírt tesztelési módszer minden biztonsági funkció esetén alkalmas a várt viselkedés bemutatásához és megfelelően ellenőrzik az összes biztonsági funkciót. A teszt mélység elemzés alapján megállapítható, hogy a magas szintű tervben leírt biztonsági funkciók és a tesztelési dokumentációban szereplő tesztek közötti megfeleltetés teljes /vagyis a magas szintű tervben leírt minden alrendszerhez és minden belső interfészhez tartozik teszt/. MultiSigno v3.0.1 – **Teszt mélység elemzés**
	ATE_IND.2	A tesztelt MultiSigno v3.0.1 -t megfelelően telepítették, és ismert állapotban volt. A fejlesztő a független teszteléshez biztosította az értékelő számára azt a környezetet és erőforrás-készletet, amivel a saját tesztelését végezte Az értékelő megismételte a tesztelést a fejlesztő tesztelési dokumentációjában leírt terv tesztek egy mintára valamint megtervezett egy teszt készletet és végrehajtotta valamint dokumentálta azokat. MultiSigno v3.0.1 – **A tesztelésre alkalmas MultiSigno v3.0.1**
A sebezhetőség felmérése	AVA_MSU.2	Az útmutató helytelen használhatóságának elemzése alapján megállapítható, hogy az útmutató a MultiSigno v3.0.1 valamennyi működési módjában útmutatást ad a biztonságos működtetésre MultiSigno v3.0.1 **Az útmutató helytelen használhatóságának elemzése**
	AVA_SOF.1	A MultiSigno v3.0.1 nem alkalmaz nem kriptográfiai, valószínűségi vagy permutációs mechanizmusokat. Ezért a biztonsági funkcióerősség elemzésre nincs szükség, az erre vonatkozó követelmény kielégítettnek tekinthető.
	AVA_VLA.2	Az értékelő az áthatolás tesztelések eredményei, valamint a sebezhetőségi elemzések következtetései alapján megállapította, hogy a MultiSigno v3.0.1 a tervezett (cél)környezetében képes ellenállni egy alacsony támadási képességgel rendelkező támadónak. Az értékelő jelentést írt az összes kihasználható sebezhetőségről és maradvány sebezhetőségről MultiSigno v3.0.1 - **Sebezhetőség elemzés**

Az értékelés másik következtetése az alábbi:
A MultiSigno v3.0.1 fejlesztő készlet (A 4.2 fejezetben megfogalmazott feltételek teljesülése esetén) **megfelel a CEN CWA 14170:2004 és CEN CWA 14171:2004 által az elektronikus aláíró alkalmazásokra támasztott valamennyi olyan funkcionális és garanciális biztonsági követelménynek, mely a fejlesztő készletre vonatkozik.**

10 Értékelői megjegyzések és javaslatok

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

11 Mellékletek

A 9. fejezetben foglaltak szerint az értékelés döntően annak megállapítására irányult, hogy az értékelés tárgya kielégíti-e a biztonsági előirányzatban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

A MultiSigno v3.0.1 fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN CWA 14170:2004 munkacsoport egyezmény: Security requirements for signature creation applications /May 2004/
- CEN CWA 14171:2004 munkacsoport egyezmény: 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.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

A MultiSigno v3.0.1 fejlesztő készlet (A 4.2 fejezetben megfogalmazott feltételek teljesülése esetén) **megfelel a CEN CWA 14170:2004 és CEN CWA 14171:2004 által az elektronikus aláíró alkalmazásokra támasztott valamennyi olyan funkcionális és garanciális biztonsági követelménynek, mely a fejlesztő készletre vonatkozik.**

Mivel az értékelés 9. fejezetben megfogalmazott fő következtetése ettől látszólag független állítást fogalmaz meg, így indoklásra szorul.

A jelen tanúsítási jelentés alapját képező értékelés egy olyan biztonsági előirányzatból indult ki, mely a korábbi hazai (aláíró alkalmazások támogatását megvalósító fejlesztő készletekre vonatkozó) értékelésektől eltérően nem a CWA 14170 és CWA 14171 mértékadó követelményrendszer általános, hanem a MultiSigno v3.0.1-ra vonatkozó konkrét követelményrendszert határozza meg az értékelés viszonyítási alapjaként. Ez teljes mértékben összhangban van a MIBÉTS (és a CC) módszertanával, ugyanakkor nem teszi összehasonlíthatóvá a jelen értékelés eredményét a korábbi értékelési eredményekkel.

A fentiek indokolják, hogy a biztonsági előirányzatnak való megfelelés mellett (ami az értékelés fő következtetése), megfogalmazásra került a CEN követelményeknek való megfelelőség is.

A két következtetés nincs ellentmondásban egymással, kiegészítik egymást.

Az alábbiak (táblázatos formában) a CEN követelményeknek való megfelelésre vonatkozó vizsgálat eredményét foglalja össze.

11.1 A MultiSigno v3.0.1 megfelelése a funkcionális követelményeknek.

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	**megfelel**
F_SDP_2	**megfelel**
F_SDP_3	**megfelel**
F_SAV_1	**megfelel**
F_SAV_2	**megfelel**
F_SAV_3	**megfelel**
F_SIC_1	**nem vonatkozik rá a követelmény**
F_SIC_2	**nem vonatkozik rá a követelmény**
F_SIC_3	**megfelel**
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**megfelel**
F_SSC_1	**nem vonatkozik rá a követelmény**
F_SSC_2	**nem vonatkozik rá a követelmény**
F_SSC_3	**megfelel**
F_SSC_4	**nem vonatkozik rá a követelmény**
F_SSC_5	**megfelel**
F_SSC_6	**megfelel**
F_SSC_7	**megfelel**
F_SSC_8	**megfelel**
F_SSA_1	**nem vonatkozik rá a követelmény**
F_SDC_1	**nem vonatkozik rá a követelmény**
F_SDOC_1	**megfelel**
F_I/O-1	**nem vonatkozik rá a követelmény**
F_I/O-2	**megfelel**
F_I/O-3	**megfelel**
F_ISV-1	**megfelel**
F_ISV-2	**megfelel**
F_ISV-3	**feltétellel megfelel (1)**
F_USV-1	**megfelel**
F_human_1	**nem vonatkozik rá a követelmény**
F_human_2	**nem vonatkozik rá a követelmény**
F_human_3	**nem vonatkozik rá a követelmény**
F_human_4	**nem vonatkozik rá a követelmény**
F_human_5	**megfelel**
F_human_6	**nem vonatkozik rá a követelmény**
F_human_7	**megfelel**
F_machine_1	**megfelel**
F_machine_2	**megfelel**
F_general_1	**nem vonatkozik rá a követelmény**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	**nem vonatkozik rá a követelmény**

11.2 A MultiSigno v3.0.1megfelelése a biztonsági követelményeknek.

Biztonsági követelmény	Teljesülés
S_SCA_1	**megfelel**
S_SCA_2	**megfelel**
S_SCA_3	**megfelel**
S_SCA_4	**megfelel**
S_SCA_5	**megfelel**
S_SCA_6	**megfelel**
S_SCA_7	**nem vonatkozik rá a követelmény**
S_SCA_8	**nem vonatkozik rá a követelmény**
S_SCA_9	**feltétellel megfelel (2)**
S_SCA_10	**megfelel**
S_SCA_11	**megfelel**
S_SCA_12	**megfelel**
S_SDP_1	**megfelel**
S_SDP_2	**nem vonatkozik rá a követelmény**
S_SDP_3	**nem vonatkozik rá a követelmény**
S_SDP_4	**nem vonatkozik rá a követelmény**
S_SDP_5	**nem vonatkozik rá a követelmény**
S_SDP_6	**nem vonatkozik rá a követelmény**
S_SDP_7	**nem vonatkozik rá a követelmény**
S_SDP_8	**nem vonatkozik rá a követelmény**
S_SDP_9	**nem vonatkozik rá a követelmény**
S_SDP_10	**megfelel**
S_SDP_11	**megfelel**
S_SDP_12	**nem vonatkozik rá a követelmény**
S_SAV_1	**nem vonatkozik rá a követelmény**
S_SAV_2	**megfelel**
S_SAV_3	**megfelel**
S_SAV_4	**nem vonatkozik rá a követelmény**
S_SAV_5	**nem vonatkozik rá a követelmény**
S_SAV_6	**nem vonatkozik rá a követelmény**
S_SAV_7	**megfelel**
S_SAV_8	**nem vonatkozik rá a követelmény**
S_SIC_1	**nem vonatkozik rá a követelmény**
S_SIC_2	**nem vonatkozik rá a követelmény**
S_SIC_3	**nem vonatkozik rá a követelmény**
S_SIC_4	**nem vonatkozik rá a követelmény**
S_SIC_5	**nem vonatkozik rá a követelmény**
S_SAC_1	**megfelel**
S_SAC_2	**megfelel**
S_SAC_3	**nem vonatkozik rá a követelmény**
S_SAC_4	**feltétellel megfelel (3)**
S_SAC_5	**nem vonatkozik rá a követelmény**
S_SAC_6	**feltétellel megfelel (3)**
S_SAC_7	**megfelel**

S_SAC_8	**nem vonatkozik rá a követelmény**
S_SAC_9	**nem vonatkozik rá a követelmény**
S_SAC_10	**nem vonatkozik rá a követelmény**
S_SAC_11	**nem vonatkozik rá a követelmény**
S_SAC_12	**nem vonatkozik rá a követelmény**
S_DTBSF_1	**megfelel**
S_DHC_1	**megfelel**
S_DHC_2	**megfelel**
S_DHC_3	**megfelel**
S_SSC_1	**megfelel**
S_SSC_2	**nem vonatkozik rá a követelmény**
S_SSC_3	**nem vonatkozik rá a követelmény**
S_SSC_4	**nem vonatkozik rá a követelmény**
S_SSA_1	**nem vonatkozik rá a követelmény**
S_SDC_1	**nem vonatkozik rá a követelmény**
S_I/O_1	**feltétellel megfelel (4)**
S_I/O_2	**feltétellel megfelel (5)**
S_I/O_3	**nem vonatkozik rá a követelmény**
S_VER_1	**feltétellel megfelel (6)**

11.3 A tanúsított termékek listájába javasolt szöveg

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

"Az értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők A MultiSigno v3.0.1 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokat támogatja:

- *Biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat.*
- *Elfogad és feldolgoz X509 v3 nyilvános kulcs tanúsítványokat.*
- *Képes a szükséges tanúsítványok és visszavonási adatok megszerzésére.*
- *Ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzést is.*
- *Hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében.*
- *Minősített aláírás létrehozása esetén együttműködik a magyar jogszabályok által megkövetelt módon minősített aláírás létrehozásához szükséges tanúsított BALE eszközzel, vagy fokozott biztonságú aláírások esetén képes szabványos szoftveres kulcstároló állományok vagy kriptográfiai hardver eszköz (KHE) biztonságos kezelésére.*
- *Gyűjti, tárolja és karbantartja a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat.*
- *Képes automatikusan választani több magán rejtjelező kulcsból, ha nyilvános kulcs alapú megoldást végez.*

A MultiSigno v3.0.1 fejlesztő készlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került, kiemelt garanciaszinten. Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy a MultiSigno v3.0.1 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket."

12 Biztonsági előirányzat

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

13 Fogalmak és rövidítések

13.1 Fogalmak

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

biztonsági 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.

biztonsági funkció szabályzata
A biztonsági funkció által érvényre juttatott biztonsági szabályzat.

biztonsági jellemző
Szubjektumokkal, használókkal és/vagy objektumokkal társított olyan információ, amelyet az értékelés tárgyára vonatkozó biztonsági szabályzat érvényre juttatására használnak.

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

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

értékelés tárgya
Az az informatikai termék vagy rendszer, valamint a hozzá kapcsolódó adminisztrátori és felhasználói útmutatók (jelen esetben fejlesztői útmutató), amelyre az értékelés irányul.

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

értékelési séma
Olyan igazgatási és szabályozási keret, amely szerint az értékelő szervezet egy adott közösségben alkalmazza a CC-t.

értékelő szervezet
Az a testület, amely egy adott közösség keretein belül az úgynevezett értékelési séma révén valósítja meg a CC-t.

felhasználó
Az a személy, aki a MultiSigno v3.0.1-t alkalmazást használja, azaz a MultiSigno v3.0.1 szolgáltatásait igénybe kívánja venni.

funkcióerősség
Az értékelés tárgya valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén.

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

kulcs, aláíró kulcs
Elektronikus aláírás létrehozásához használt magánkulcs.

kulcs, hitelesítő kulcs
Az azonosításhoz, hitelesítéshez és jogosultság ellenőrzéséhez használt magánkulcs.

kulcs, dekódoló kulcs
Dekódoláshoz használt magánkulcs.

kulcstároló
Kulcsot tároló hardver eszköz (token, PKCS#11, ALE, BALE), vagy titkosítással védett kulcsot tároló fájl (PKCS#12).

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

tanúsítási útvonal felépítése
Egy tanúsítványhoz a tanúsítvány lánc kialakítása, úgy, hogy minden tanúsítványt az azt kibocsátó hitelesítés szolgáltató tanúsítványa kövessen. A tanúsítvány lánc a megbízható legfelső szintű tanúsítvánnyal kezdődik, ezt nulla vagy több közbenső tanúsítvány követi, és a végtanúsítvánnyal végződik.

tanúsítási útvonal érvényesítése
A tanúsítási útvonala érvényesíteni kell, mielőtt a végtanúsítvány hitelessége elfogadásra kerülne. A tanúsítási útvonal érvényesítése a tanúsítási útvonalban szereplő minden egyes tanúsítványra a PKIX szabvány szerint előírt ellenőrzések elvégzését jelenti.

tanúsítvány, megbízható legfelső szintű tanúsítvány
Olyan önaláírt tanúsítvány, amely nem igényel tanúsítási útvonal érvényesítést. A tanúsítvány láncban az első helyen szerepel.

tanúsítvány, közbenső tanúsítvány
Olyan, hitelesítés szolgáltató számára kiadott tanúsítvány, amely a tanúsítvány láncban nem az első és nem az utolsó helyen szerepel.

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

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

tanúsítvány, visszavont
Olyan tanúsítvány, amely már nem használható vagy nem megbízható. A hitelesítés-szolgáltató, amely a tanúsítvány kibocsátotta, a tanúsítványt különféle okokból vonhatja vissza. Az okok között szerepel a kulcs feltételezett vagy tényleges kompromittálódása, a tanúsítvány alanynak távozása az adott szervezettől, stb. A tanúsítvány visszavonási lista tartalmazza az összes visszavont és még nem lejárt tanúsítványt. Opcionálisan a tanúsítvány visszavonási lista tartalmazhat visszavont és már lejárt tanúsítványokat is.

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

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

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

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

XAdES
Az XMLDSIG szabvány továbbfejlesztése, az EU elektronikus aláírásra vonatkozó (1999/93/EC) direktívája szerint.

XMLDSIG
XML elektronikus aláírás szintaktikáját és feldolgozását leíró szabvány.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

AES	**A**dvanced **E**ncryption **S**tandard
ALE	**A**láírás-**l**étrehozó **e**szköz
API	**A**pplication **P**rogramming **I**nterface
AR	**Al**rendszer
BALE	**B**iztonságos **a**láírás-**l**étrehozó **e**szköz
BF	**B**iztonsági **f**unkció
CC	**C**ommon **C**riteria (Közös szempontok)
CCRA	**C**ommon **C**riteria **R**ecognition **A**rrangement (a Közös szempontok szerint kibocsátott tanúsítványok kölcsönös elismeréséről szóló nemzetközi megállapodás)
CEM	**C**ommon **E**valuation **M**ethodology (Közös értékelési módszertan)
CEN	**C**omité **E**uropeen de **N**ormalization (Európai Szabványügyi Bizottság)
CRL	**C**ertificate **R**evocation **L**ist (tanúsítvány visszavonási lista)
CWA	**C**EN **W**ork **A**greement (CEN munka megállapodás)
DHC	**D**ata **H**ashing **C**omponent (adatlenyomat-készítő összetevő)
DN	**D**istinguised **N**ame (megkülönböztetett, egyedi név)
DTBS	**D**ata **t**o **b**e **S**igned (aláírandó adat)
DTBSF	**D**ata **t**o **b**e **S**igned **F**ormatter (aláírandó adat formattáló)
EAL	**E**valuation **A**ssurance **L**evel (értékelési garanciaszint)
ETSI	**E**uropean **T**elecommunication **S**tandard **I**nstitute
FIPS	**F**ederal **I**nformation **P**rocessing **S**tandard
IT	**I**nformáció **t**echnológia
MIBÉTS	**M**agyar **I**nformatikai **B**iztonsági és **É**rtékelési **S**éma
PKCS	**P**ublic **K**ey **C**ryptography **S**tandard
PKI	**P**ublic **K**ey **I**nfrastructure
RFC	**R**equest **f**or **C**omment
RSA	**R**ivest, **S**hamir, and **A**dleman (az RSA algoritmus)
SAC	**Signer's Authentication Component (aláírót hitelesítő összetevő)**
SAV	**S**ignature **A**ttribute **V**iewer (aláírási tulajdonság megjelenítő összetevő)
SCA	**S**ecure **C**reation **A**pplication (aláírás-létrehozó alkalmazás)
SDC	**S**igner's **D**ocument **C**omposer (aláírói dokumentum szerkesztő)
SDO	**S**igned **D**ata **O**bject (aláírt adat objektum)
SDOC	**S**igned **D**ata **O**bject **C**omposer (aláírt adat objektum szerkesztő)
SDP	**S**igner's **D**ocument **P**resenter (aláírói dokumentumot megjelenítő összetevő)

SHA-1	**S**ecure **H**ash **A**lgorithm
SIC	**S**igner's **I**nteraction **C**omponent (aláíróval kölcsönható összetevő)
SLC	**S**ignature **L**ogging **C**omponent (aláírás naplózó összetevő)
SSA	**S**CDev - **S**CA **A**uthenticator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti hitelesítés összetevője)
SSC	**S**CDev - **S**CA **C**ommunicator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikátor összetevő)
SSCD	**S**ecure **S**ignature-**C**reation **D**evice (biztonságos aláírás-létrehozó eszköz)
ST	**S**ecurity **T**arget (biztonsági előirányzat)
SOF	**S**trenght **o**f **F**unction (funkcióerősség)
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)
XAdES	**XML A**dvanced **E**lectronic **S**ignature (XML formátumú elektronikus aláírás)
XML	E**x**tensible **M**arkup **L**anguage
XMLDSIG	**XML-D**igital **Sig**nature Syntax and Processing

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- MultiSigno v3.0.1 Biztonsági előirányzat v1.0
- MultiSigno v3.0.1 Értékelési jelentés v1.0

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

Cím	verzió	Fájlnév
Biztonsági előirányzat	v1.0	MultiSigno_ST_v10.pdf
Funkcionális specifikáció	v1.0	MultiSigno_FS_v10.doc
Magas szintű terv	v1.0	MultiSigno_HLD_v10.doc
Alacsony szintű terv (MultiSigno SDK Dokumentáció)	v3.0.1	"html_060428" alkönyvtár
megvalósítás	v3.0.1	"include_060428, "src_060428" és "bin_060428" alkönyvtárak
Megfeleltetés elemzések	v1.0	MultiSigno_RCR_v10.doc
Tesztelési dokumentáció	v1.0	MultiSigno_Test_Documentation.doc
Teszt lefedettség elemzés	v1.0	MultiSigno_Test_Cov_v10.doc
Teszt mélység elemzés	v1.0	MultiSigno_Test_Depth_v10.doc
Útmutató (MultiSigno 3.0 Manual)	2006.04.28	MultiSigno_SDK_man.rtf
A konfiguráció menedzselés dokumentációja	v1.0	MultiSigno_Conf_Mgmt_v10.doc
A fejlesztési biztonság dokumentációja	v1.0	MultiSigno_DVS_v10.doc
Az életciklust meghatározó dokumentáció	v1.0	MultiSigno_LCDf_v10.doc
A fejlesztő eszközök dokumentációja	v1.0	MultiSigno_TAT_v10.doc
Az útmutató helytelen használhatóságának elemzése	v1.0	MultiSigno_Misuse_v10.doc
Sebezhetőség elemzés	v1.0	MultiSigno_Vulnerability_Analysis.doc
Folyamatábrák	v.1.0	"Folyamatábrák" alkönyvtár
MultiSigno 3 - Rendszerterv - Implementációs modell	2006.01.06	MS3-Komponensmodell.pdf
MultiSigno 3 - Rendszerterv - Felhasználási esetek megvalósításai	2006.01.06	MS3-Kovetelmenyrealizaciok.pdf
Logikai architektúra a MultiSigno 3 rendszertervhez	2006.01.06	MS3-Logikai_Architektura.pdf
MultiSigno 3.0 Specifikáció	v2.0	MS3-specifikacio_v2.pdf
MultiSigno 3.0 Manual	2006.04.28	MultiSigno_SDK_man.rtf

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- 1. számú MIBÉTS kiadvány: A MIBÉTS nemzeti séma általános modellezése /0.95 verzió, 2005 február/,
- 2. számú MIBÉTS kiadvány: Az értékelés és a tanúsítás folyamatai /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - A biztonsági előirányzat értékelésének módszertana /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 4 - A kiemelt garanciaszint értékelésének módszertana /0.95 verzió, 2005 február/

14.4 Az értékeléshez felhasznált egyéb dokumentumok

Az értékelés figyelembe vette az alábbi mértékadó követelményrendszereket is:

- Az elektronikus aláírásról szóló 2001. Évi XXXV.törvény
- CEN CWA 14170:2004 munkacsoport egyezmény: Security Requirements fro Signature Creation System
- CEN CWA 14171:2004 munkacsoport egyezmény: General guidelines for electronic signature verification
- CEN CWA 14172-4:2001 munkacsoport egyezmény: Signature-creation application and general gudelines for electronic signature verification
- ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 101 862 v1.3.3 Qualified Certificate profile
- ETSI SR 002 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)
- RSA Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
- SHA-1 Secure Hash Algorithm /FIPS PUB 180-1/
- RFC3161 Time-Stamp Protocol (TSP)
- RFC3275 XML Digital Signatures (XMLDSig)
- RFC3280 Certificate and Certificate Revocation List (CRL) Profile
- PKCS#1 RSA Cryptographic Standard /RFC2313/
- PKCS #11 v2.11: Cryptographic Token Interface Standard
- PKCS #12 v1.0 Personal Information Exchange Information Standard