TANÚSÍTÁSI JELENTÉS

eSign Toolkit
minősített elektronikus aláíráshoz
v2.1.0

HUNG-TJ-043-2008

Verzió:	1.0
Fájl:	Hung-TJ-043-2008_v10.pdf
Minősítés:	Nyilvános
Oldalak:	37

Változáskezelés

Verzió	Dátum	A változás leírása
v0.5	2008.11.09	• A szerkezet felállítása.
v0.8	2008.11.11.	• A tanúsítás eredményeit tartalmazó teljes változat.
v0.9	2008.11.17.	• Utolsó egyeztetésre kiadott változat
v1.0	**2008.12.01.**	• **Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
Hunguard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**eSign Toolkit fejlesztőkészlet v2.1.0**
Verzió szám:	**V2.1.0.2**
Rövid elnevezés:	**eSign Toolkit v2.1.0**
Az értékelt termék típusa:	fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2008. november 02.
Az értékelés módszere:	a MIBÉTS séma értékelési módszertana1
Az értékelés garanciaszintje:	fokozott (EAL3)
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • TEXT/XML formátumú dokumentumokra szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C és XAdES-XL, valamint RFC 3852 szerinti CMS) elektronikus aláírás létrehozása, • TEXT/XML formátumú dokumentumokra létrehozott, szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás ellenőrzése, • X.509 v3 tanúsítványok és tanúsítványláncok kezelése (az RFC 5280 alapján), • időbélyegzés kérés készítése és az időbélyeg válasz ellenőrzése (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve), • visszavonási információk (CRL és OCSP) kezelése (az RFC 5280 és RFC 2560 alapján), • különböző PKCS#11-es felületen keresztül elérhető biztonságos aláírás-létrehozó eszközökkel (BALE) való együttműködési képesség.

[1] Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- **A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (v1.0, 2008 június) - 5. számú segédlet: ÉRTÉKELÉSI MÓDSZERTAN**

Konfigurációs követelmények:

Szoftver konfiguráció:

- Operációs rendszer: Windows XP SP2
- PKCS#11 interfész (BALE felé)
- OpenSSL v0.9.8.h
- Zlib v1.2.3
- Libxslt v1.1.24
- libxml v2.7.1

2 Azonosítás

Az értékelt termék neve:	**eSign Toolkit fejlesztőkészlet v2.1.0**
Verzió szám:	**V2.1.0.2**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	• NoregPKI2.dll v2.1.0.2 • OpenSSL v0.9.8.h • Zlib v1.2.3 • Libxslt v1.1.24 • libxml v2.7.1 • dokumentáció

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az eSign Toolkit v2.1.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.
Először az eSign Toolkit v2.1.0 két üzemmódját határozzuk meg, melyekre eltérő szabályok vonatkoznak. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmódok

Az eSign Toolkit v2.1.0 két üzemmódot különböztet meg:

- Fokozott biztonságú aláírás létrehozás üzemmód
    - Az eSign Toolkit v2.1.0-t biztonságos aláírás létrehozó eszköz nélkül használják elektronikus aláírások generálására és ellenőrzésére.
- Minősített elektronikus aláírás létrehozás üzemmód
    - Minősített aláírás létrehozása esetén kötelező a BALE használata, illetve nem megbízható környezetben a BALE és az aláírás létrehozó alkalmazás (TOE) között megbízható útvonal kiépítésére van szükség. Az aláírás létrehozásához használt tanúsítványnak minősítettnek kell lennie. Az eSign Toolkit v2.1.0 a BALE-hez való hozzáférést PKCS#11 interfészen keresztül valósítja meg.

3.2 Biztonsági funkciók

A TOE által megvalósított biztonsági funkciók a következőek:

- BF1 Aláírás létrehozása
- BF2 Aláírás ellenőrzése
- BF3 Időbélyeg kérés
- BF4 Időbélyeg ellenőrzés
- BF5 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése
- BF6 Szabványos aláírás formátumú aláírás
- BF7 működési paraméterek beállítása

3.2.1 BF1 Aláírás létrehozása

A **BF1 Aláírás létrehozása** biztonsági funkció hozza létre az aláírói dokumentumra és az aláírási információkra az elektronikus aláírást az aláírói magánkulcs felhasználásával.

Az eSign Toolkit v2.1.0 lehetőséget biztosít fokozott biztonságú és minősített elektronikus aláírások létrehozására. A magánkulcsot tokenből (PKCS#11 felületen keresztül), fokozott biztonságú aláírások esetén fájlból is (PEM kulcsfájlból) képes kezelni.

A magánkulcs közvetlen aktivizálása előtt az eSign Toolkit v2.1.0 a paraméterként kapott aláíró hitelesítő adatot használja az aláíró hitelesítéséhez.

Minősített elektronikus aláírás létrehozása esetén az eSign Toolkit v2.1.0 kommunikációt kezdeményez az aláírás létrehozását ténylegesen végző BALE-vel. Az aláíró által kiválasztott tanúsítványhoz tartozó magánkulccsal és az ennek megfelelő algoritmussal (ami az eSign Toolkit v2.1.0 esetén az RSA algoritmus legalább 1024 bit kulcshosszal) létrehozza az aláírást. A BALE eszköz végzi a magánkulcs aktivizáláshoz szükséges aláíró hitelesítő adat bekérést. Ez esetben az aláírás létrehozásához használt tanúsítványnak minősített tanúsítványnak kell lennie (qCStatement kiterjesztés használatával - ETSI TS 101 862 v1.3.3), és a keyUsage kiterjesztésben csak a nonRepudiation bit lehet beállítva.

Fokozott biztonságú aláírás létrehozása esetén

- Aktivizálja a PEM kulcsfájlban tárolt magánkulcsot, és az RSA algoritmus legalább 1024 bit kulcshossz használatával létrehozza a lenyomatra az aláírást, amit beletesz az XML aláírásba.

vagy

- Kezdeményezi a KHE (Kriptográfiai hardver eszköz) felé az aláírás létrehozását, majd a kapott aláírás érték felhasználásával összeállítja az XML aláírást.

Fokozott biztonságú aláírás létrehozása esetén a keyUsage kiterjesztésben a kötelezően beállított nonRepudiation bit mellett opcionálisan a digitalSignature bit lehet még beállítva.

A funkció által létrehozott elektronikus aláírás formátuma megfelel a következőknek: RFC 3852 (CMS), ETSI TS 101903 v1.2.2 (XAdES).

Lenyomat készítés

Az aláírás létrehozás biztonsági funkció ezen alfunkciója hozza létre a lenyomatot, amire az aláírás készül. Az aláírás létrehozása során az aláírandó adatokra alkalmazott lenyomatoló algoritmus: SHA-1 [FIPS 180-1].

Megengedett dokumentum formátumok:

Az eSign Toolkit v2.1.0 a következő dokumentum formátumok aláírását engedi meg: TXT/XML.

Támogatott aláírás formátumok:

A funkció által támogatott elektronikus aláírás formátumok: XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL, CMS.

3.2.2 BF2 Elektronikus aláírás ellenőrzése

Ez a biztonsági funkció valósítja meg az elektronikus aláírás ellenőrzését az aláíró tanúsítványának felhasználásával.

Az aláírás ellenőrzés folyamata három lépésből áll: első lépésben a funkció megnézi, hogy kapcsolódik-e időbélyeg az aláíráshoz. Amennyiben nem, akkor végrehajtja a **BF3 Időbélyeg kérés** és a **BF4 Időbélyeg ellenőrzés** biztonsági funkciókat. Az ellenőrzés második lépéseként az aláírás érvényességének megállapításához szükséges információk összegyűjtését végzi, amennyiben ez még nem áll rendelkezésre. Ezt a **BF5 Tanúsítványlánc felépítése és érvényesség ellenőrzése** biztonsági funkció végzi el. Végül a harmadik lépésben kerül sor az elektronikus aláírás ellenőrzésére.

Az aláírás ellenőrzés által visszaadott értékekből a meghívó alkalmazás dönthet az alábbi három lehetséges állapot közül:

- befejezetlen;
- sikeres;
- sikertelen.

Sikeres esetben befejeződött az összes érvényesítő adat összegyűjtése, és az aláírás ezek alapján érvényesnek tekinthető.

Sikertelen ellenőrzés olyan esetben történhet, ha például az aláírás formátuma nem megfelelő vagy a digitális aláírás értéke érvénytelen.

Befejezetlen esetben nincs elegendő információ az aláírás érvényességének pozitív megállapításhoz.

A funkció által ellenőrizni képes elektronikus aláírás formátumok: XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL, XAdES-A, CMS. Az alábbi szabványoknak megfelelőséget is képes ellenőrizni: XAdES v1.2.2, MELASZ-ready v1.0.

3.2.3 BF3 Időbélyeg kérés

Az eSign Toolkit v2.1.0 biztosítja az időbélyeg kérés képességét**.** Az RFC 3161-ben specifikáltaknak megfelelően összeállítja az időbélyeg kérést a hash értékkel, és elküldi a külső időbélyeg szolgáltatóhoz.

3.2.4 BF4 Időbélyeg ellenőrzés

Az eSign Toolkit v2.1.0 a szolgáltatótól kapott időbélyeg választ importálja, és elvégzi a szükséges ellenőrzéseket: ellenőrzi a válasz státuszt, azt, hogy érvényes-e az időbélyegen lévő aláírás, valamint ellenőrzi az időbélyeg aláírásához használt tanúsítvány érvényességét.

3.2.5 BF5 Tanúsítási útvonal felépítése és érvényesség ellenőrzése

Ez a biztonsági funkció végzi az aláíró tanúsítványból kiindulva a megbízható pontig (gyökértanúsítványig) tartó tanúsítvány lánc elemeinek összegyűjtését.

Az eSign Toolkit v2.1.0 az IT környezet által sértetlenségében megvédett konfigurációs fájlból vagy a registry-ből olvassa be a kulcsadat tárolók elérését, amiket a tanúsítási útvonal érvényesség ellenőrzése során felhasznál. Ezen fájl tartalmának módosítása kívül esik a TOE hatókörén.

A tanúsítási útvonal felépítéséhez az eSign Toolkit v2.1.0 betöltésekor lefut egy inicializáló rutin, amely elvégzi az elérési helyek inicializálását.

A konfigurációs fájl vagy a registry, valamint a tanúsítványokat és CRL-eket tároló könyvtár feltöltése kívül esik a TOE hatókörén.

Az eSign Toolkit v2.1.0 az érvényesség ellenőrzés során a végtanúsítványra **visszavonási információkat (CRL) gyűjt** be, amennyiben a CRL-eket tároló könyvtár nem tartalmazza azt. A paraméterezhető türelmi idő letelte után a TOE-t meghívó alkalmazásnak kell megismételnie a visszavonási információk lekérését, hogy az aláírás érvényességének ellenőrzése a legfrissebb CRL-ek alapján történjen meg. A TOE ellenőrzi a tanúsítványokon és a CRL-eken lévő aláírásokat.

A **tanúsítványlánc tanúsítványai**ra megnézi, hogy az érvényességi idejükbe beleesik-e az aláíráshoz csatolt időbélyegben szereplő időpont. A tanúsítványlánc felépítésekor azt is megvizsgálja, hogy a kibocsátott tanúsítványok érvényességi ideje beleesik-e a kibocsátó tanúsítvány érvényességi idejébe (kagyló modell). Azt is megvizsgálja, hogy szerepel-e a visszavonási listán a tanúsítvány, és amennyiben igen, akkor az időbélyeg által meghatározott időpontban visszavont állapotú volt-e.

3.2.6 BF6 Szabványos aláírás formátumú aláírás

Ez a biztonsági funkció az alábbi szabványos aláírás formátumokat támogatja:

- aláírás létrehozásakor:
  - XAdES v1.2.2 szerinti XAdES-EPES, XAdES-T, XAdES-C és XAdES-XL,
  - MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C és XAdES-XL,
  - RFC 3852 szerinti CMS.
- aláírás ellenőrzésekor:
  - XAdES v1.2.2 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL, és XAdES-A,
  - MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A,
  - RFC 3852 szerinti CMS.

3.2.7 BF7 Működési paraméterek beállítása

Ez a biztonsági funkció meghatározza a konfigurációs paraméterek elérhetőségét a Windows Registry gyűjtő és elérési út értékeinek beállításával, vagy egy XML konfigurációs fájl kijelölésével.

4 Feltételezések és hatókör

Az értékelés pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

- a biztonsági előirányzatból adódó feltételek (az értékelés tárgyának biztonságához szükséges, az informatikai környezetre vonatkozó feltételezések),
- a CWA 14170 és a CWA 14171 követelményeinek való megfelelés érdekében teljesítendő feltételek
- a biztonságos felhasználás egyéb feltételei.

4.1 Feltételezések az eSign Toolkit v2.1.0 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. Az eSign Toolkit v2.1.0 fejlesztőkészletet megfelelően telepítik és konfigurálják (AE.Configuration).
3. Az eSign Toolkit v2.1.0 által meghívott kriptográfiai funkciók (például OpenSSL) megbízhatóan valósítják meg az eSign Toolkit v2.1.0 által hívott kriptográfiai funkciókat. Minősített elektronikus aláírás létrehozása esetén az eSign Toolkit v2.1.0 környezete tartalmaz egy (vagy több) NHH által nyilvántartott, tanúsított BALE-t, mely tárolja és védi az aláíró magánkulcsát, illetve végrehajtja a digitális aláírást. (AE.Crypto_Module)
4. A fejlesztői környezetben az eSign Toolkit v2.1.0 függvény-gyűjtemény védett a jogosulatlan fizikai hozzáféréssel szemben. (AE.Physical_Protection).
5. A tanúsítvány és tanúsítvány visszavonási információk az eSign Toolkit v2.1.0 rendelkezésére állnak (AE.PKI_Info).
6. A környezet GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről (AE.Time).
7. Az eSign Toolkit v2.1.0 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést (AE.TimeStamp).

4.2 A CWA 14170 és 14171 követelményeknek való megfelelés feltételei

1. számú CWA feltétel (az F_ISV_3 funkcionális követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjtemény a tanúsítványlánc ellenőrzésekor a kagylóhéj modellt követi, azaz minden tanúsítvány érvényességi időintervallumának benne kell lennie az őt kibocsátó tanúsítvány érvényességi időintervallumában. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a kibocsátott CRL nem teljes. Ezért csak olyan környezetben szabad alkalmazni, ahol egy kibocsátott tanúsítvány nem érvényes tovább, mint az őt kibocsátó tanúsítvány, valamint a tanúsítványokhoz kiadott CRL teljes.

2. számú CWA feltétel (az S_SCA_9 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjteménnyel fejlesztett 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. számú CWA feltétel (az S_SCA_12 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjtemény tartalom típusként a text/xml típust tárolja el. Ezért kizárólag e típusnak megfelelő adatok aláírására használható.

4. számú CWA feltétel (az S_I/O_1 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjtemény nem rendelkezik önvédelmi funkcióval, ezért működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

- vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
- az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

5. számú CWA feltétel (az S_I/O_2 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az eSign Toolkit v2.1.0 függvény-gyűjtemény funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

6. számú CWA feltétel (az S_VER_1 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az eSign Toolkit v2.1.0 függvény-gyűjtemény valamennyi aláírás-létrehozás vagy aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

4.3 A biztonságos felhasználás egyéb feltételei

Az eSign Toolkit v2.1.0 az alábbi üzemmódokat különbözteti meg:

- minősített elektronikus aláírást létrehozó üzemmód (a „QualifiedSignature” környezeti változó értéke nem 0)
- fokozott biztonságú elektronikus aláírást létrehozó üzemmód (a „QualifiedSignature” környezeti változó értéke 0)

1. számú egyéb feltétel
Minősített elektronikus aláírás létrehozása esetén a „minősített elektronikus aláírást létrehozó üzemmód”-ot kell beállítani a „QualifiedSignature” környezeti változó értékének helyes beállításával.

4.4 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az eSign Toolkit v2.1.0 valamennyi biztonsági funkcióját.

5 Az eSign Toolkit v2.1.0 szerkezeti leírása

Az értékelés tárgya (az eSign Toolkit v2.1.0 függvénygyűjtemény) az alábbi tulajdonságokkal rendelkezik:

- képes szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C és XAdES-XL, valamint RFC 3852 szerinti CMS) elektronikus aláírás létrehozására,
- képes szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás ellenőrzésére,
- képes X.509 v3 tanúsítványok és tanúsítványláncok kezelése (az RFC 5280 alapján),
- alkalmas időbélyegzés kérés készítésére és az időbélyeg válasz ellenőrzésére (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve),
- képes visszavonási információk (CRL és OCSP) lekérdezésére a hitelesítés-szolgáltatóktól (a tanúsítványból kiolvasott elérési helyről),
- képes együttműködni különböző aláírás-létrehozó eszközökkel (ALE) és biztonságos aláírás-létrehozó eszközökkel (BALE).

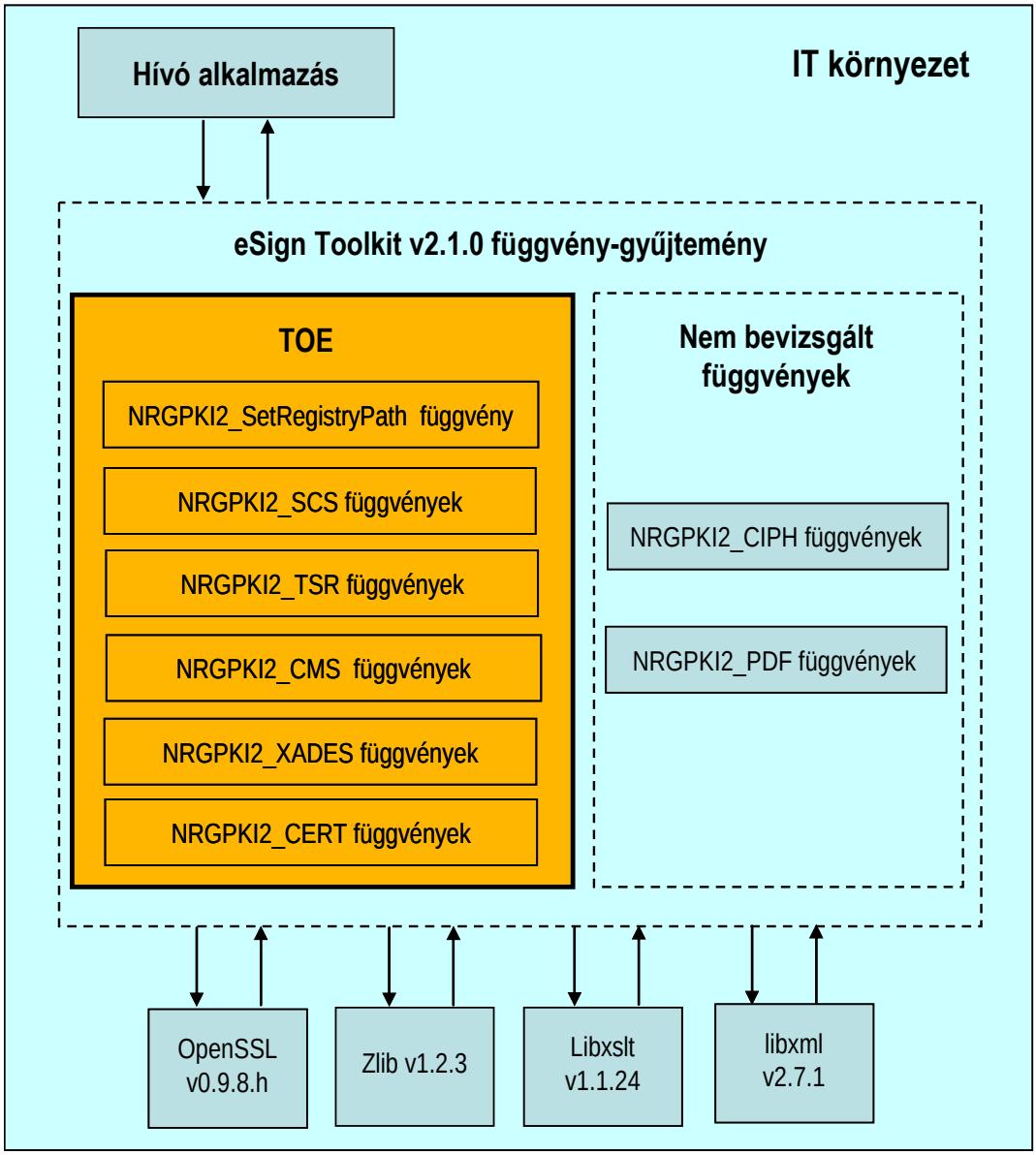
Az eSign Toolkit v2.1.0 szoftverfejlesztők számára készült, zárt rendszerben felhasználásra kerülő, nyilvános kulcs szolgáltatásokat biztosító C nyelven írt függvénygyűjtemény, olyan funkcionalitással, mellyel elektronikus aláírások létrehozása, ellenőrzése, az ellenőrzéshez érvényesítő információk feldolgozása, tanúsítási útvonal felépítése, tanúsítványok érvényességének ellenőrzése, visszavonási információk érvényesség ellenőrzése, időbélyeg kérése és ellenőrzése, OCSP kérése és ellenőrzése valósítható meg.

Az eSign Toolkit v2.1.0 az OpenSSL funkcióira épít, azokat felhasználja működése során, ezen keresztül valósítja meg a legtöbb kriptográfiai funkcionalitást. A kriptográfiai token eszközök kezelése PKCS#11 felületen keresztül történik.

A DLL különféle programozási nyelvi környezetből hívható felülettel rendelkezik, szoftver fejlesztői csomagban kerül forgalomba.

5.1 Architektúra

Az 1 ábra az eSign Toolkit v2.1.0 struktúráját és az IT környezetbe való beágyazódását –a TOE határaival - mutatja be.



1 ábra: Az eSign Toolkit v2.1.0 és környezete

Az eSign Toolkit v2.1.0 függvény csoportokból áll:

- Az NRGPKI2_SetRegistryPath függvény beállítja a konfigurációs paramétereket.
- Az NRGPKI2_SCS_xxx függvények kezelik az intelligens kártyán (PKCS11-en keresztül) vagy PEM fájlban tárolt magánkulcsot.
- Az NRGPKI2_TSR_xxx függvények az időbélyegzéssel kapcsolatos feladatokat végzik el.
- Az NRGPKI2_CMS_xxx függvények kezelik a CMS formátumú elektronikus aláírásokat.
- Az NRGPKI2_XAdES_xxx függvények kezelik a XAdES formátumú elektronikus aláírásokat.

- Az NRGPKI2_PDF_xxx függvények kezelik a PDF formátumú elektronikus aláírásokat.
- Az NRGPKI2_CERT_xxx függvények tanúsítványra vonatkozó információkat adnak.
- Az NRGPKI2_CIPH_xxx függvények titkosítást és dekódolást végeznek.

Az NRGPKI2_CIPH_xxx és az NRGPKI2_PDF_xxx függvények nem képezték a vizsgálat tárgyát (tehát a TOE részét sem).

Az eSign Toolkit v2.1.0 az IT környezet elemeit (harmadik fél által fejlesztett, nyilvánosan elérhető és szabadon felhasználható függvények) az alábbi feladatok elvégzéséhez használja:

- OpenSSL: általános kriptográfiai műveletek végrehajtása,
- Libxml: XML kezelés,
- Libxslt: XML megjelenítés,
- ZLIB: tömörítés.

Az eSign Toolkit v2.1.0 biztonsági funkciói szempontjából az OpenSSL és a libxml csomagok biztosítanak közvetve TOE biztonsági funkciót támogató funkciót.

5.2 Alrendszerek

Az eSign Toolkit v2.1.0-nak az alábbi alrendszerei vannak:

- AR1: Paraméter beállítás
- AR2: Kulcskezelés
- AR3: Időbélyegzés
- AR4: CMS csomagolás
- AR5: XAdES csomagolás

6 Dokumentáció

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

- a **fejlesztésre alkalmas NOREGPKI2.DLL v2.1.0.2**
- NOREGPKI.doc - **FEJLESZTŐI DOKUMENTÁCIÓ**

A fejlesztésre alkalmas eSign Toolkit v2.1.0 a fejlesztésekhez szükséges dll-t tartalmazza

A NOREGPKI.doc - **FEJLESZTŐI DOKUMENTÁCIÓ** bemutatja az eSign Toolkit v2.1.0 fejlesztő készletet, tartalmazza az adminisztrátori és felhasználói, illetve a fejlesztőknek szóló útmutatást

7 Tesztelés

7.1.1 A fejlesztő tesztelési munkájának áttekintése

A fejlesztő bár tesztelte a függvénykészletet, de nem dokumentálta le a tesztelés eredményeit.

Ezért a fejlesztői tesztelést teljes egészében az értékelő által végrehajtott független tesztelésnek kellett pótolnia.

7.1.2 Az értékelő tesztelési munkájának áttekintése

Az értékelő független tesztelését saját környezetében végezte.

A fejlesztői tesztelés hiányosságai miatt a független tesztelés stratégiájaként a biztonsági előirányzatban leírt biztonsági funkciók specifikus részleteit, illetve a teljes folyamat tesztelését irányozta elő az értékelői teszt. Valamennyi biztonsági funkcióra készült egy átfogó, vagy több részletet kielemző teszteset. Összességében 119 darab független teszt került megtervezésre.

A tesztek a következő 4 csoportba sorolhatóak:

- OCSP kérés – válasz tesztelése (21 teszteset),
- időbélyeg kérés - válasz tesztelése (22 teszteset),
- PKITS tesztek (67 teszteset),
- kiegészítő tesztek (9 teszteset).

Az OCSP kérés – válasz tesztelését az értékelő egy automata OCSP szerverrel (ocsp_test_server.exe) illetve egy előre megírt teszt programmal (ocsptest.exe) végezte. A program létrehozot egy aláírást, elhelyezett benne egy időbélyeget, és elvégzte a tanúsítványlánc ellenőrzését OCSP-t használva a végfelhasználói tanúsítványra. Az eSign Toolkit függvénykönyvtár a tanúsítványlánc ellenőrzésekor, ha (hibás válasz miatt) nem tud OCSP ellenőrzést végrehajtani, akkor CRL ellenőrzést hajt végre.

Az időbélyeg kérés – válasz tesztelését során az értékelő egy automata TSA szerverrel (tsa_test_server.exe) illetve egy előre megírt teszt programmal (tsatest.exe) végezte. A program létrehozott egy aláírást, elhelyezett benne egy időbélyeget, és elvégzte a tanúsítványlánc ellenőrzését időbélyeg kérést használva a végfelhasználói tanúsítványra. A dokumentum aláíró tanúsítványa Aladin eToken kriptográfiai hardver eszközben volt tárolva..

A kiegészítő tesztek azokat a biztonsági függvényeket, alrendszereket, API függvényeket tesztelte, melyek az előző tesztesetekből kimaradtak.

A PKITS tesztek a felvállalt funkcionalitásnak megfelelő PKITS tanúsítványlánc felépítő és ellenőrző teszteseteket tartalmazták. A tesztelés során lokális időbélyeg szolgáltató volt használva (tsa_test_server.exe).

A független tesztelés a legutolsó végrehajtásakor hiba nem lépett fel.

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 SP2
- PKCS#11 interfész (BALE felé)
- OpenSSL v0.9.8.h
- Zlib v1.2.3
- Libxslt v1.1.24
- libxml v2.7.1
    - o

8.3 BALE

Az eSign Toolkit v2.1.0 minősített aláírás létrehozása esetén NHH által nyilvántartásba vett biztonságos aláírás létrehozó eszköz használata kötelező. A TOE a BALE eszközt PKCS#11 interfészen keresztül éri el.

9 Az értékelés eredményei

Az eSign Toolkit v2.1.0 fejlesztőkészlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került, fokozott garanciaszinten.

Az értékelés megállapította, a tanúsítás pedig megerősítette az alábbiakat: **az eSign Toolkit v2.1.0 megfelel a biztonsági előirányzatának, azaz kielégíti az "eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – Biztonsági előirányzat" című dokumentumban megfogalmazott funkcionális és garanciális biztonsági követelményeket.**

A fenti megállapítás a fokozott garanciaszint (EAL3) követelményeinek teljesítésén alapul. Az alábbiak azt mutatja meg, hogy az egyes garanciaösszetevőket hogyan teljesíti az eSign Toolkit v2.1.0 fejlesztő készlet, illetve mely fejlesztői bizonyítékok támogatták ennek kimutatását.

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja
Konfiguráció menedzselés	ACM_CAP.3	Az értékelésre átadott szoftver (fejlesztő készlet) egyedi azonosításra került. A konfiguráció lista leírja az eSign Toolkit v2.1.0 alkotó konfiguráció elemeket, megfelelve az ACM_SCP-ben megadott minimális körnek. A konfiguráció lista elemeit a dokumentált rendszer szerint kezelik **megfelelt**
	ACM_SCP.1	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. **megfelelt**
Kiszállítás és működtetés	ADO_DEL.1	Az eSign Toolkit v2.1.0 függvény-gyűjtemény szállítását és átadását minden esetben a termék gyártója végzi. **megfelelt**
	ADO_IGS.1	Az útmutató megadja és leírja a biztonságos telepítéséhez, generálásához és indításához szükséges eljárásokat. Az útmutatóban megadott telepítési, generálási és indítási eljárások leírják azokat a lépéseket, amelyek az eSign Toolkit v2.1.0 biztonságos telepítéséhez, generáláshoz és indításához szükségesek. **megfelelt**
Fejlesztés	ADV_FSP.1	A funkcionális specifikáció informális módon leírja a megvalósítandó biztonsági funkciókat és azok külső interfészeit. Teljes körűen meghatározza a biztonsági funkciókat. A funkcionális specifikáció lefed minden biztonsági előirányzatban szereplő funkcionális biztonsági követelményt. **megfelelt**

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja
	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. **megfelelt**
	ADV_RCR.1	A biztonsági előirányzat összefoglaló előírása és a funkcionális specifikáció közötti megfeleltetés-elemzés alapján megállapítható, hogy a funkcionális specifikáció a TOE 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. **megfelelt**
Útmutató dokumentumok	AGD_ADM.1	Az útmutatóra teljesülnek az alábbiak: • Az eSign Toolkit v2.1.0 függvénykönyvtár működését befolyásoló konfigurációs paraméterek állítása kitüntetett szerepkört igényel. Ilyen a függvénykönyvtárhoz tartozó Registry bejegyzések beállítása, a program által használt konfigurációs fájl beállítása, valamint a használt kulcsok, CRL-ek megfelelő könyvtárba helyezése. Az útmutató ezeket megfelelő alapossággal leírja. • Az útmutató leírja a használt Registry kulcs helyét, beállítási módját és az egyes változók szerepét. • Az eSign Toolkit v2.1.0 függvénykönyvtár egyes funkciói azonos jogosultsággal használhatók (a jogosultságok beállítása a felhívó program, vagy a működési környezet feladata). A működéshez szükséges Registry kulcsok az útmutatóban megfelelően dokumentálva vannak. • Az eSign Toolkit v2.1.0 függvénykönyvtár egyes funkciói adott funkcionalitással rendelkeznek, s ezt leírja az útmutató. • Az útmutató önmagában ellentmondásmentes, más dokumentumokkal összevetve sem tartalmaz ellentmondást. **megfelelt**

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja
	AGD_USR.1	Az útmutatóra teljesülnek az alábbiak: • Az eSign Toolkit v2.1.0 függvénykönyvtár egyes funkciói azonos jogosultsággal használhatók. A felhívható funkciók, azok felhívási módjai, a visszakapott értékek az útmutatóban megfelelően le vannak dokumentálva. • A biztonsági funkciókat az egyes függvények felhívásán keresztül lehet elérni, ami az útmutatóban megfelelő módon dokumentált. • Az eSign Toolkit v2.1.0 függvénykönyvtár egyes funkcióinak be és kimenő paraméterei, visszaadott hibaértékei megfelelő módon leírásra kerültek az útmutatóban. • Az eSign Toolkit v2.1.0 függvénykönyvtár használata egyértelműen van dokumentálva az útmutatóban. A függvénykönyvtár használata kötött, ami példákon keresztül is szemléltetve van. • Az útmutató önmagában ellentmondásmentes, és nem mond ellent más egyéb dokumentumnak sem. **megfelelt**
Az életciklus támogatása	ALC_DVS.1	Az értékelő a helyszíni szemlén (megfigyeléssel, mintavételi vizsgálattal és személyes kérdésekkel) megállapította, hogy a leírt biztonsági intézkedéseket be is tartják **megfelelt**
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. **megfelelt**
	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. A teszt lefedettség elemzés alapján megállapítható, hogy minden biztonsági funkcióhoz tartozik teszt, így a tesztelés lefedi a funkcionális specifikációban leírt biztonsági funkcionalitást. **megfelelt**

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja
	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. A teszt mélység elemzés alapján megállapítható, hogy minden alrendszerhez tartozik teszt, így a tesztelés lefedi a magas szintű tervben meghatározott biztonsági funkcionalitást. **megfelelt**
	ATE_IND.2	A független (értékelői) tesztelésre az értékelő telephelyén került sor. A tesztelt konfiguráció a biztonsági előirányzatnak megfelelő volt. Az eSign Toolkit v2.1.0-át a független teszteléshez megfelelően telepítették, valamint ismert állapotban volt. Mivel a fejlesztői tesztelést az értékelő végezte el, ezért a független tesztelés lényegében a „fejlesztői” tesztelés teljeskörű megismétlésének és ellenőrzésének tekinthető. A független tesztelésről külön dokumentáció készült, mely a tesztkészletben szereplő tesztekről rögzített minden szükséges információt. Ennél a független tesztelésnél a tényleges teszteredmények megegyeztek a várt eredményekkel **megfelelt**
A sebezhetőség felmérése	AVA_MSU.1	Az útmutató egyértelmű és belső ellentmondásoktól mentes: nem tartalmaz olyan félrevezető részeket, melyek alapján a függvény-gyűjteményt meghívó alkalmazás fejlesztője félreérthetné teendőit, és a TOE-ra vagy a TOE által nyújtott biztonságra nézve hátrányos módon alkalmazza a leírtakat. Az útmutató teljes: nem mond ellent a más értékelői tevékenység végrehajtása közben szerzett TOE-val kapcsolatos tapasztalatoknak. Az útmutató megalapozott: nem támaszt olyan követelményeket a TOE használatával vagy működési környezetével szemben, melyek nem felelnek meg az ST-nek, vagy indokolatlanul nagy terhet jelentenek a biztonság fenntartásához A TOE kizárólag a rendelkezésre bocsátott leírás alapján biztonságosan konfigurálható és használható Az útmutató kielégítő a felhasználó (alkalmazás fejlesztő) számára a függvény-gyűjtemény által biztosított biztonsági funkciók hatékony adminisztrálásához és használatához, valamint a nem biztonságos állapotok észleléséhez. **megfelelt**
	AVA_SOF.1	Az eSign Toolkit v2.1.0 nem alkalmaz valószínűségi vagy permutációs mechanizmusokat. **megfelelt**
	AVA_VLA.1	A fejlesztő sebezhetőségi elemzése a TOE-ban használt verziókat érintő nyilvánvaló sebezhetőséget nem tárt fel. Azonosítatlan sebezhetőségek nem maradtak. Az értékelés során ellenőrzésre került, hogy a használt modulokra (OpenSSL, libxml, libxslt, zlib) nem jelentek meg újabb veszélyek a vizsgált adatbázisokban. A fejlesztő sebezhetőségi elemzése nem mond ellent sem az ST-nek, sem a fejlesztői útmutatónak **megfelelt**

Az alábbi táblázat azt mutatja meg, hogy az egyes garanciaösszetevőket mely fejlesztői bizonyítékok támogatták.

Garancia-osztály	Garancia-család	garanciaösszetevők sorszáma és elnevezése és a **megfelelő fejlesztői bizonyíték**	
Konfiguráció kezelés	ACM_CAP	3	ACM_CAP.3 A jogosultságok ellenőrzése **A konfiguráció kezelés dokumentációja**
	ACM_SCP	1	ACM_SCP.1 Az értékelés tárgya konfiguráció kezelésének lefedettsége **A konfiguráció kezelés dokumentációja**
Kiszállítás és működtetés	ADO_DEL	1	ADO_DEL.1 A szállítás eljárásai Nem volt szükség külön dokumentációra
	ADO_IGS	1	ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai Nem volt szükség külön dokumentációra
Fejlesztés	ADV_FSP	1	ADV_FSP.1 Informális funkcionális specifikáció **Fejlesztői dokumentáció**
	ADV_HLD	2	ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés **Magas szintű terv**
	ADV_RCR	1	ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése **Megfelelés elemzés**
Útmutató dokumentumok	AGD_ADM	1	AGD_ADM.1 Az adminisztrátori útmutató **Fejlesztői dokumentáció**
	AGD_USR	1	AGD_USR.1 A felhasználói útmutató **Fejlesztői dokumentáció**
Az életciklus támogatása	ALC_DVS	1	ALC_DVS.1 A biztonsági intézkedések azonosítása **A fejlesztés biztonság dokumentációja**
Tesztelés	ATE_COV	2	ATE_COV.2 A teszt lefedettség elemzése **Teszt lefedettség elemzés**
	ATE_DPT	1	ATE_DPT.1 A magas szintű terv tesztelése **Teszt mélység elemzés**
	ATE_FUN	1	ATE_FUN.1 Funkcionális tesztelés **Tesztelési dokumentáció**
	ATE_IND	2	ATE_IND.2 Független tesztelés - mintán **A tesztelésre alkalmas eSignTK (NoregPKI2.h és NoregPKI2.dll)**
A sebezhetőség felmérése	AVA_MSU	1	AVA_MSU.1 Az útmutatók vizsgálata **Fejlesztői dokumentáció**
	AVA_SOF	1	AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése Nem volt szükség külön dokumentációra
	AVA_VLA	1	AVA_VLA.1 A sebezhetőség független elemzése **Sebezhetőség elemzés**

10 Értékelői megjegyzések és javaslatok

Az értékelő nem adott a tanúsítási jelentésbe megjelentendő 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.

Az eSign Toolkit v2.1.0 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:

Az eSign Toolkit v2.1.0 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.**

A 4-esfejezetben megfogalmazott feltételek teljesülése esetén az eSign Toolkit v2.1.0 függvény-gyűjtemény fokozott biztonságú és minősített elektronikus aláíró és ellenőrző alkalmazások fejlesztésére egyaránt alkalmazható.

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 az eSign Toolkit v2.1.0-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 Az eSign Toolkit v2.1.0 megfelelése a funkcionális követelményeknek.

Funkcionális követelmény	Teljesülés
F_SCA_1	megfelel
F_SDP_1	megfelel
F_SDP_2	megfelel
F_SDP_3	megfelel
F_SDP_4	megfelel
F_SAV_1	megfelel
F_SAV_2	nem vonatkozik rá a követelmény
F_SAV_3	megfelel
F_SIC_1	nem vonatkozik rá a követelmény
F_SIC_2	nem vonatkozik rá a követelmény
F_SIC_3	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
F_SSC_4	nem vonatkozik rá a követelmény
F_SSC_5	nem vonatkozik rá a követelmény
F_SSC_6	nem vonatkozik rá a követelmény
F_SSC_7	nem vonatkozik rá a követelmény
F_SSC_8	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
F_ISV-1	megfelel
F_ISV-2	megfelel
F_ISV-3	feltétellel megfelel (1. számú CWA feltétel)

Funkcionális követelmény	Teljesülés
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	megfelel
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 Az eSign Toolkit v2.1.0megfelelése 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	nem vonatkozik rá a követelmény
S_SCA_6	nem vonatkozik rá a követelmény
S_SCA_7	nem vonatkozik rá a követelmény
S_SCA_8	nem vonatkozik rá a követelmény
S_SCA_9	feltétellel megfelel (2. számú CWA feltétel)
S_SCA_10	megfelel
S_SCA_11	megfelel
S_SCA_12	feltétellel megfelel (3. számú CWA feltétel)
S_SDP_1	megfelel
S_SDP_2	nem vonatkozik rá a követelmény
S_SDP_3	megfelel
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	megfelel
S_SAV_2	nem vonatkozik rá a követelmény
S_SAV_3	megfelel
S_SAV_4	nem vonatkozik rá a követelmény

Biztonsági követelmény	Teljesülés
S_SAV_5	nem vonatkozik rá a követelmény
S_SAV_6	nem vonatkozik rá a követelmény
S_SAV_7	megfelel
S_SAV_8	megfelel
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	nem vonatkozik rá a követelmény
S_SAC_2	megfelel
S_SAC_3	nem vonatkozik rá a követelmény
S_SAC_4	nem vonatkozik rá a követelmény
S_SAC_5	nem vonatkozik rá a követelmény
S_SAC_6	nem vonatkozik rá a követelmény
S_SAC_7	nem vonatkozik rá a követelmény
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	nem vonatkozik rá a követelmény
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. számú CWA feltétel)
S_I/O_2	feltétellel megfelel (5. számú CWA feltétel)
S_I/O_3	nem vonatkozik rá a követelmény
S_VER_1	feltétellel megfelel (6. számú CWA feltétel)

11.3 Automatikus érvényesség

Bizonyos funkcionális és biztonsági követelmények automatikusan teljesülnek az eSign Toolkit v2.1.0 függvény-gyűjtemény felhasználásával fejlesztett elektronikus aláíró alkalmazásokra, feltéve, hogy a függvény-gyűjteményt helyesen használják. Az alkalmazásra automatikusan teljesülő követelmények a következők:

F_DTBSF_1
F_DTBSF_2
F_DHC_1
F_DHC_2
F_SDOC_1
F_protocol
F_format
S_SCA_10
S_SCA_11
S_SCA_12
S_DHC_1
S_DHC_2
S_DHC_3

11.4 A tanúsított termékek listájába javasolt szöveg

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

„Az eSign Toolkit v2.1.0 egy C nyelven írt függvény-gyűjtemény (fejlesztői programkönyvtár).

A függvény-gyűjtemény az alábbi fő funkciókat biztosítja, illetve támogatja:

- *TEXT/XML formátumú dokumentumokra szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C és XAdES-XL, valamint RFC 3852szerinti CMS) elektronikus aláírás létrehozása,*
- *TEXT/XML formátumú dokumentumokra létrehozott, szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás ellenőrzése,*
- *X.509 v3 tanúsítványok és tanúsítványláncok kezelése (az RFC 5280 alapján),*
- *időbélyegzés kérés készítése és az időbélyeg válasz ellenőrzése (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve),*
- *visszavonási információk (CRL és OCSP) kezelése (az RFC 5280 és RFC 2560 alapján),*
- *különböző PKCS#11-es felületen keresztül elérhető biztonságos aláírás-létrehozó eszközökkel (BALE) való együttműködési képesség.*

A fenti fő funkciók alapján az eSign Toolkit v2.1.0 függvény-gyűjtemény segítségével alkalmazások széles köre fejleszthető, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatások biztosítására használhatók.”

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 az eSign Toolkit v2.1.0-t alkalmazást használja, azaz az eSign Toolkit v2.1.0 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.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

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)
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)
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
KM	**K**onfiguráció **m**enedzsment
MIBÉTS	**M**agyar **I**nformatikai **B**iztonsági és **É**rtékelési **S**éma
PKCS	**P**ublic **K**ey **C**ryptography **S**tandard
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Information Standard
PKI	**P**ublic **K**ey **I**nfrastructure
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)
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
- eSign Toolkit v2.1.0 Biztonsági előirányzat v1.0
- eSign Toolkit v2.1.0 Értékelési jelentés v1.0

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

	cím	verzió
eSignTK_ST_v10.doc	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – BIZTONSÁGI ELŐIRÁNYZAT	1.0
eSignTK_CM_v10.doc	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 - A KONFIGURÁCIÓ KEZELÉS DOKUMENTÁCIÓJA	1.0
eSignTK_DVS_v10.doc	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – A FEJLESZTÉS BIZTONSÁG DOKUMENTÁCIÓJA	1.0
NOREGPKI.doc	NOREGPKI2.DLL - FEJLESZTŐI DOKUMENTÁCIÓ	2.1.0.2
eSignTK_ATE_TEST_v10.rtf	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – TESZTELÉSI DOKUMENTÁCIÓ	1.0
eSignTK_ATE_COV_v10.rtf	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – TESZT LEFEDETTSÉG ELEMZÉS	1.0
eSignTK_ATE_DPT_v10.rtf	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – TESZT MÉLYSÉG ELEMZÉS	1.0
eSignTK_HLD_v10.doc	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – MAGAS SZINTŰ TERV	1.0
eSignTK_RCR_v10.doc	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – MEGFELELÉS ELEMZÉS	1.0
eSignTK _VA_v10.doc	eSign Toolkit minősített elektronikus aláíráshoz v2.1.0 – SEBEZHETŐSÉG ELEMZÉS	1.0
A tesztelésre alkalmas TOE	NoregPKI2.dll, NoregPKI2.h	2.1.0.2

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- ISO/IEC 15408:2005 Information technology — Security techniques — Evaluation criteria for IT security (Part 1,2,3)
- ISO/IEC 18045:2005 Information technology — Security techniques — Methodology for IT security evaluation
- KIB 25. ajánlás A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (v1.0, 2008 június)

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 for Signature Creation System
- CEN CWA 14171:2004 munkacsoport egyezmény: General guidelines 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 v2.0.0 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/
- RFC 2560 X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999
- RFC3161 Time-Stamp Protocol (TSP)
- RFC3275 XML Digital Signatures (XMLDSig)
- RFC3852 Cryptographic Message Syntax (CMS)
- RFC5280 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
- MELASZ-ready v1.0 Egységes MELASZ formátum elektronikus aláírásokra v1.0, 2006 február