Tanúsítási JELENTÉS

mySigno for PDA és mySigno Server elektronikus aláíró rendszerről v1.0

HUNG-TJ-32/2006

Verzió:	1.0
Fájl:	HUNG_TJ_32_2006_v10.pdf
Minősítés:	Nyílt
Oldalak:	35

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2006.05.19	• A szerkezet felállítása.
v0.8	2006.05.22	• A tanúsítás eredményeit tartalmazó teljes változat.
v0.9	2006.05.28.	• Utolsó egyeztetésre kiadott verzió
v1.0	2006.05.29.	• Végleges verzió

A tanúsítási jelentést készítette:

Farkas Gábor
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**mySigno for PDA és mySigno Server aláíró rendszer**
Verzió szám:	**1.0**
Rövid elnevezés:	**mySigno v1.0**
Az értékelt termék típusa:	fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2006. május 29.
Az értékelés módszere:	a MIBÉTS séma értékelési módszertana1
Az értékelés garanciaszintje:	fokozott (EAL3)
Az értékelt termék funkcionalitása:	A mySigno v1.0 egy olyan komplex informatikai rendszerbe illeszkedik, mely az elektronikus aláírások létrehozásán és ellenőrzésén kívül számos egyéb funkcionalitással rendelkezik (kliens oldalon: összetett XML csomagok összeállítása, kézi aláírás elhelyezése, szervert oldalon: aláírt csomagok archiválása, adatbázisba szervezése)
Konfigurációs követelmények:	Kliens operációs rendszer: • Pocket PC 2003 SE A működéshez szükséges egyéb TOE környezeti összetevők: • Pocket PC 2003 SDK • ActiveSync • Embedded Visual Tools Szerver operációs rendszer: • Windows 2003 Server

[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 3 **- A fokozott garanciaszint értékelésének módszertana** /0.95 verzió, 2005 február/

2 Azonosítás

Az értékelt termék neve:	**mySigno for PDA és mySigno Server aláíró rendszer**
Verzió szám:	**1.0**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	• függvénykönyvtár cesigno.dll • dokumentáció

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az mySigno v1.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.

3.1 Szerepkörök

A mySigno v1.0 által kezelt szerepkörök:

- Ügynök: Az a szereplő, aki a csomagot a saját elektronikus aláírásával ellátja, integritását ezzel biztosítva.
- Ellenőrző fél: A szerver oldali automatikus ellenőrző folyamat tölti be ezt a szerepet.

A mySigno v1.0 hatáskörén kívüli, de a biztonságos működéssel összefüggésben lévő szerepkörök:

- Szerver adminisztrátor: Aki a mySigno szerver karbantartását és beállításait jogosult végezni.
- PDA adminisztrátor: Aki a mySigno PDA modul telepítésével, a paraméter fájlok, kulcsok biztonságos PDA-ra juttatásával kapcsolatos feladatokat végzi. Lehetővé teszi az ügynök számára a PIN kód cserét.

3.2 Biztonsági funkciók

A biztonsági követelmények teljesítése érdekében a TOE az alábbi biztonsági funkciókat valósítja meg:

BF1 A felhasználó azonosítása és hitelesítése
BF2 Aláírás létrehozása
BF3 Digitális aláírás ellenőrzése
BF4 Biztonságos üzenetváltás
BF5 Elektronikus aláírás kezdeti ellenőrzése
BF6 Elektronikus aláírás utólagos ellenőrzése
BF7 A TSF védelme

3.2.1 BF1 A felhasználó azonosítása és hitelesítése

A magánkulcshoz való hozzáférés érdekében az aláíró félnek azonosítania/hitelesítenie kell magát.
Kliens oldalon az értékelés hatáskörébe eső életciklus során a TOE felhasználó: az ügynök (aláíró);
A szerver oldalon az értékelés hatáskörébe eső életciklus során a TOE felhasználó: az ellenőrző felet reprezentáló automatikus folyamat.

3.2.1.1 BF1.1 Felhasználó azonosítása és hitelesítése

PDA kliensen aláíró (ügynök) azonosítása/hitelesítése kliens oldalon a magánkulcshoz való hozzáféréshez szükséges PIN kód megadásával.
Szerver oldalon az ellenőrző felet reprezentáló automatikus folyamat azonosítása/hitelesítése az IT környezetet biztosító operációs rendszerhez szükséges azonosítás és hitelesítés valósítja meg.

3.2.1.2 BF1.2 Magánkulcshoz való hozzáférés korlátozása és menedzsmentje

Ügynök magánkulcs védelme: A TOE hatáskörén kívül, telepítéskor megadott, a magánkulcshoz való hozzáféréshez szükséges 6 hosszú betű/szám kombinációjú PIN kód három egymást követő sikertelen megadási kísérlete esetén a mySigno v1.0 törli a magánkulcsot.
A funkció valósítja meg ezen kívül az aláírói hitelesítő adat cseréjét is. Az aláírónak meg kell adni az előző PIN kódot a TOE által biztosított felhasználói interfészen, majd kétszer be kell írnia az új hitelesítő adatot.

3.2.2 BF2 Aláírás létrehozása

Ez a biztonsági funkció hozza létre az ügynök által kiválasztott csomagra az elektronikus aláírást. Ehhez elkészíti a lenyomatot, amire az aláírást készíti, az aláírás létrehozás számára elfogadható formátumra hozza.
Az aláírás létrehozása során az aláírandó adatokra alkalmazott lenyomatoló algoritmus: SHA-1 [FIPS 180-1].
A lenyomatkészítés előtt a mySigno v1.0 egyértelműen jelzi az ügynöknek, hogy a PDA eszköz kijelzőjén látható csomagra fokozott biztonságú aláírás készül, amely jelzésre az ügynöknek pozitív választ kell adnia.
A mySigno v1.0 lehetőséget biztosít a hatáskörén kívül eső életciklus fázisban telepített külső megjelenítő alkalmazások meghívására.
A mySigno v1.0 aláírás előtt megvizsgálja a kapott dokumentum kiterjesztését, és amennyiben az aláírási szabályzatban meghatározott formátumok közül egyikkel sem egyezik, akkor nem hajtja végre az aláírandó dokumentumokhoz való hozzáadását.
A mySigno v1.0 az aláírás előtt lehetőséget ad az aláíró tanúsítvány adatainak (név, kibocsátó, érvényességi idő) megtekintésére.
Az ügynöknek az aláírás létrehozására adott pozitív válasza és a **BF1** biztonsági funkcióban specifikált hitelesítése után a TOE elektronikus aláírást hoz létre a számított lenyomatra az RSA kriptográfiai algoritmussal, 1024 bit kulcshosszal, a PKCS#1 v1.5-nek megfelelően.
Az aláírást a mySigno v1.0 az alábbi szabályok alapján készíti el:

- Az elektronikus aláírásban csak az aláíró tanúsítvány azonosítója szükséges.
- A [keyinfo] elemben csak az aláíró tanúsítványt kell megadni.
- A kötelező aláírási tulajdonságok:
    - Aláírás ideje
    - Aláírási szabályzat azonosítója
    - Aláírói tanúsítvány

3.2.3 BF3 Digitális aláírás ellenőrzése

A mySigno v1.0 képes a **„BF2 Aláírás létrehozás”** alatt meghatározottak szerint létrehozott digitális aláírás ellenőrzésére. A folyamat kiszámítja az aláírt adat lenyomatát, majd az ügynök nyilvános kulcs tanúsítványában található nyilvános kulcs és az RSA/1024 algoritmus felhasználásával ellenőrzi a digitális aláírás értéket, valamint a nyilvános kulcs tanúsítvány érvényességi idejét. Amennyiben a kiszámított lenyomat és a digitális aláírás ellenőrzése során kapott érték megegyezik és a tanúsítvány érvényességi idejébe beleesik a PDA eszköz által szolgáltatott idő, akkor a digitális aláírás érték helyes.
A funkció további ellenőrzéseket nem végez.

3.2.4 BF4 Biztonságos üzenetváltás

A kliens a szerverrel kommunikál az 1. ábrán látható kommunikációs csatornán. Ez a biztonsági funkció a kliens és a szerver közötti kommunikáció bizalmasságáról, sértetlenségéről és hitelességéről gondoskodik. Csomag szinkronizálás ((kliens)

3.2.4.1 BF4.1 Üzenet aláírása (PDA kliens hitelesítése)

- elektronikus aláírás RSA/1024 algoritmussal és kulcshosszal a továbbított csomag sértetlenségének biztosításához és a PDA eszköz azonosításához (Ehhez az eszközön tárolt magánkulcsra van szükség. Az aláírás ellenőrzése a szerver oldalon történik, ott az eszköz nyilvános kulcsához kell hozzáférni a csomag feldolgozó folyamatnak.)

3.2.4.2 BF4.2 Üzenet rejtjelezése (PDA kliens oldalon)

- RSA/1024 algoritmus és kulcshossz a TOE által titkosítandó csomag szimmetrikus kulcsának rejtjelezéséhez
- AES/256 titkosító kulcs a továbbítandó csomag rejtjelezéséhez

Frissítés letöltése és visszaigazolás küldése

3.2.4.3 BF4.3 Üzenet aláírása (szerver hitelesítése)

Elektronikus aláírás RSA/1024 algoritmussal és kulcshosszal a továbbított csomag sértetlenségének biztosításához és a szerver azonosításához (Ehhez az eszközön tárolt magánkulcsra van szükség. Az aláírás ellenőrzése a kliens oldalon történik, ott a szerver nyilvános kulcsához kell hozzáférni a csomag feldolgozó folyamatnak.)

3.2.4.4 BF4.4 Üzenet rejtjelezése (szerver oldalon)

- RSA/1024 algoritmus és kulcshossz a TOE által titkosítandó csomag szimmetrikus kulcsának rejtjelezéséhez
- AES/256 titkosító kulcs a továbbítandó csomag rejtjelezéséhez

3.2.4.5 BF4.5 Kliens üzenet megoldása és hitelesítése

A mySigno szerver a rajta tárolt magánkulccsal megoldja a kommunikációs kulcsot RSA/1024 algoritmussal, majd a kommunikációs kulccsal a kapott üzenetet (AES/256).
A mySigno szerver a PDA kliens nyilvános kulcsával ellenőrzi az üzenet hitelességét.
A szerver a PDA kliens nyilvános kulcsához a TOE IT környezetéhez tartozó, a beérkezett csomagok és egyéb ellenőrzéshez szükséges információkat tartalmazó adatbázis felé való kommunikációt biztosító interfészen fér hozzá.

3.2.4.6 BF4.6 Szerver üzenet megoldása és hitelesítése

A PDA kliens a rajta tárolt eszköz magánkulccsal megoldja a kommunikációs kulcsot RSA/1024 algoritmussal, majd a kommunikációs kulccsal a kapott üzenetet (AES/256).
A PDA kliens a szerver nyilvános kulcsával ellenőrzi az üzenet hitelességét.
A szerver nyilvános kulcsához való hozzáféréshez a PDA kliens telepítése során a szerver üzenet hitelesítéshez használt kulcspárjának nyilvános kulcs tanúsítványát importálni kell.

3.3 BF5 Aláírás kezdeti ellenőrzése

A kezdeti ellenőrzés a TOE szerver oldali összetevője köré épülő IT környezet (hosztalkalmazás) által fogadott csomagban szereplő aláírás első ellenőrzése, melyet a csomag fogadása után a lehető leghamarabb végre kell hajtani.

A TOE ellenőrzi, hogy szerepelnek-e a kötelező aláírási tulajdonságok, majd –amennyiben nem talál–, **időbélyeget kér** az aláírási szabályzat által kijelölt időbélyegzés szolgáltatótól az ügynök aláírás adott időben való meglétének bizonyításához.
Az időbélyeg válasz érvényesítése esetén az időbélyeget a TOE a csomagba foglalja.
Amennyiben a funkció talál érvényes időbélyeget, akkor a biztonsági funkció a kezdeti ellenőrzés második lépését hajtja végre, azaz összegyűjti az aláírás ellenőrzéséhez szükséges érvényesítő adatokat.
Az összegyűjtendő érvényesítő adatok:

- visszavonási információk;
- tanúsítványlánc információk.

A TOE végrehajtja az aláírás ellenőrzését a rendelkezésre álló érvényesítő adatok alapján, aminek a lehetséges kimenetele: sikeres, sikertelen, befejezetlen.
Befejezetlen státusz esetén a türelmi idő (amely paraméterként adható meg) eltelte után megismétli az adatok összegyűjtését az időbélyeghez képest legfrissebb visszavonási információk begyűjtése érdekében.
A funkció részeként a szerver oldali alkalmazás az aláírt PDA felől érkező csomagok tárolására szolgáló adatbázis felé küldés előtt ún. érkeztető aláírással látja el a csomagokat.

3.3.1 BF6 Aláírás utólagos ellenőrzése

Ez a biztonsági funkció hajtja végre a kezdeti ellenőrzés során összegyűjtött adatok alapján az aláírás utólagos ellenőrzését. Ehhez csak a már korábban összegyűjtött információkat használja. A funkció két állapottal tér vissza: sikeres vagy sikertelen (ez utóbbi akkor, ha nem építhető fel az útvonal a rendelkezésre álló adatokból, vagy van érvénytelen elem az útvonalban ezen adatok alapján).

3.3.2 BF7 A TSF védelme

A mySigno v1.0 a PIN kódot annak felhasználása után azonnal törli a memóriából, annak biztosítása érdekében, hogy más folyamatok még véletlenül se férhessenek hozzá.

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 az mySigno v1.0 informatikai környezetére

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

1. A mySigno v1.0 biztonságos működéséhez szükséges kulcsokat és a mySigno v1.0 biztonsági funkcióit biztonságos módon telepítetik a PDA eszközre (A.Init_PDA).
2. A PDA eszközt elektronikus aláírás létrehozására csak feltöltött akkumulátorral használják az adatvesztés elkerülése érdekében (A.PDA_Physical_Security).
3. Feltételezzük, hogy a PDA kliens kizárólag a regisztrált ügynök felügyelete alatt marad. Az eszközt az ügynök felügyelete nélkül más személynek átadni tilos. (A.Signer_Only).
4. A mySigno PDA klienst futtató PDA közvetlenül az aláíró befolyása és a rendszert működtető szervezet felügyelete alatt áll (A.Host_PDA_Machine).
5. Az aláírás létrehozását és ellenőrzését végző informatikai környezetben a mySigno folyamatai védettek más folyamatok káros beavatkozásai ellen. A mySigno v1.0 modult csak egy hívó alkalmazás tölti be egy időben (A.Separation_and_Exclusion)
6. A PDA modul tárolására szolgáló könyvtár tartalmát a kliens eszköz felhasználója nem módosítja (A.AccessControl).
7. A mySigno biztonsági adminisztrátora megbízható, képzett és rendelkezik a feladatai ellátáshoz szükséges hozzáférésekkel és jogosultságokkal (Trusted_Security_Administrator).
8. A biztonsági adminisztrátor vagy a mySigno v1.0-t hívó alkalmazás számára eszköz áll rendelkezésre, amellyel ellenőrizhető a mySigno szolgáltatásainak és paramétereinek a sértetlensége (A.Services_Integrity).
9. Az aláíró ügynök végig jelen van attól kezdődően, hogy kifejezte aláírási szándékát, addig, amíg megadja a magánkulcs aktiválásához szükséges hitelesítő adatát (A.Signatory_Presence).
10. Feltételezzük, hogy a PDA eszköz tartalmaz olyan külső megjelenítő alkalmazásokat, melyek képesek a csomagba foglalható formátumok (melyeket az aláírási szabályzat határoz meg) mindegyikének a megjelenítésére. Az aláírás létrehozó PDA kliens és az aláírás ellenőrző felet jelentő szerver alkalmazás IT környezete pontosan ugyanazon formátumokat ismeri és tudja megjeleníteni, illetve ezen külső alkalmazások a két oldalon egyforma konfigurációs beállításokkal működnek. Ezen külső alkalmazások kívül esnek a TOE hatáskörén (A.Packet_Viewers).
11. Az aláírás ellenőrzését végző szerver fizikailag védett a külső támadók közvetlen támadásai ellen (A.Physical_Security).
12. A mySigno v1.0 szerver oldali modult futtató gazdaszámítógép közvetlenül az ellenőrző (természetes vagy jogi személy) befolyása és felügyelete alatt áll, ami garantálja, hogy a biztonsági intézkedéseket megfelelően alkalmazzák (A.Host_Server_Machine).
13. A mySigno v1.0 szerver oldali modul hozzáféréssel rendelkezik az aláírás ellenőrzéséhez szükséges összes érvényesítő adathoz (A.Access_to_Validation_Data).

4.2 A biztonságos felhasználás egyéb feltételei

1. A mySigno v1.0 kriptográfiai modul az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a CRL-t más tanúsítvánnyal ellenőrzik, mint a végfelhasználó tanúsítványokat. A tanúsítványlánc felépítésekor a kibocsájtó-tulajdonos egyezőséget binárisan ellenőrzi. Ezért csak olyan környezetben szabad alkalmazni, ahol önkibocsátott (self issued) tanúsítvány a tanúsítványláncba nem fordul elő, a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni, valamint a tanúsítványláncban a kibocsájtó-tulajdonos név egyezőség bináris.
2. Az mySigno v1.0-át 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 mySigno v1.0 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.
4. Az mySigno v1.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék Az mySigno v1.0 programozói könyvtár funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.
5. Az mySigno v1.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az mySigno v1.0 programozói könyvtárat, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

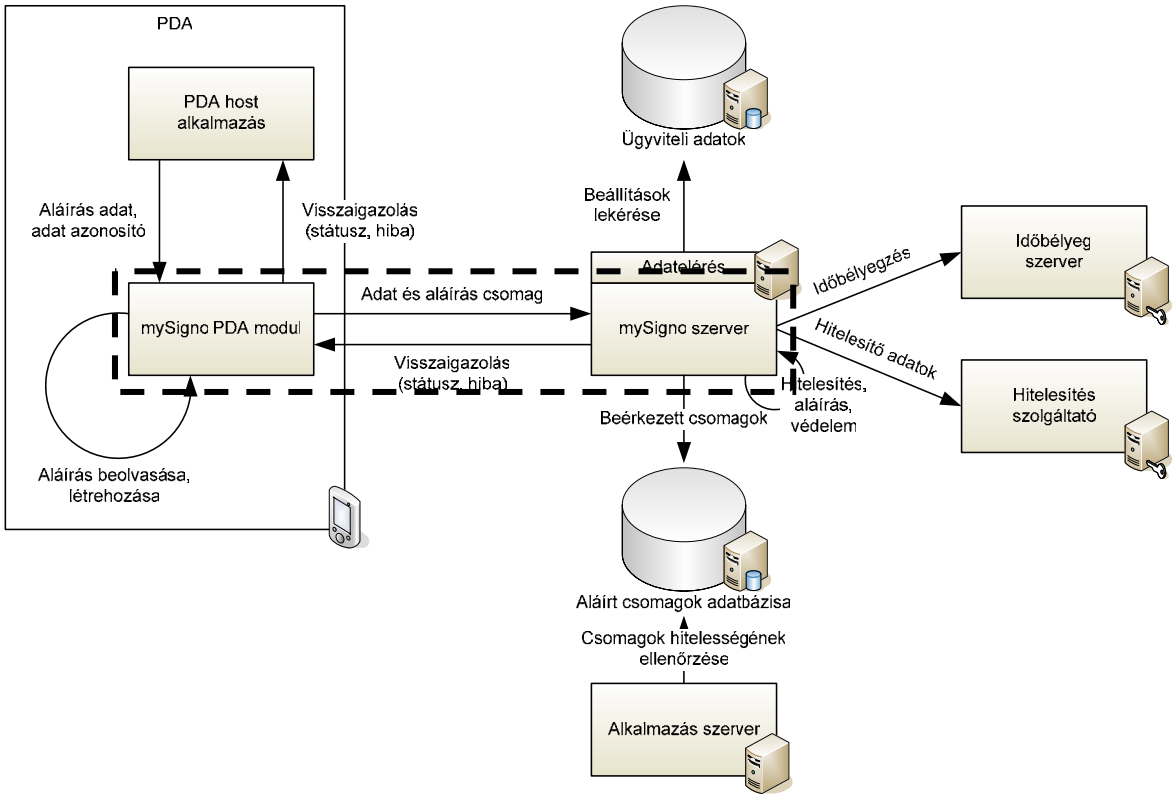
4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az mySigno v1.0 valamennyi biztonsági funkcióját.

5 Az mySigno v1.0 szerkezeti leírása

5.1 Architektúra

Az 1. ábra az mySigno v1.0 struktúráját és az IT környezetbe való beágyazódását mutatja be. Az ábrán szaggatott vonallal jelzett elemek képezik a TOE határait.



1. ábra A mySigno v1.0 határai

5.1.1 A mySigno PDA modul funkcionális elemei

1. 1Az aláírás létrehozásának előkészítése
    a. Egy csomag kiválasztása aláírásra vagy a kiválasztás visszavonása
    b. Az aláírandó csomag tartalmának megjelenítése
    c. Alkalmazandó aláírási szabályzat
    d. Az aláírási tulajdonságok kiválasztása/megjelenítése.
    e. Az aláíráshoz használt tanúsítvány (és ezáltal a magánkulcs) kiválasztása
    f. Az aláírás egyértelmű szándékának kifejezése és az ügynök hitelesítése
2. Az aláírandó csomagok formázását/lenyomatolását végző összetevő
3. A fokozott biztonságú elektronikus aláírás létrehozását végző összetevő
    a. Az aláírói magánkulcs aktivizálása.
    b. Fokozott biztonságú elektronikus aláírás létrehozása
    c. Az elektronikus aláírás visszaadása
4. Csomagszinkronizálás kezdeményezés szerver felé biztonságos csatornán
    a. a szerverhez továbbított csomag hitelesítése kliens eszköz aláírással
    b. a szerverhez továbbított csomag rejtjelezése
    c. a szervertől érkezett szoftverfrissítések fogadása (szerver aláírás ellenőrzése, rejtjelezés megoldása)

5.1.2 A mySigno szerver funkcionális elemei

A klienstől beérkezett aláírt adatok automatikus feldolgozása (Kezdeti és utólagos ellenőrzés

1. Az ellenőrzés előkészítését végző összetevő
    a. A beérkezett csomag szintaktikai ellenőrzése
    b. Aláírási szabályzat alkalmazása (mySigno v1.0 rögzített aláírási szabályokkal dolgozik)
2. Az érvényesítő adatok összegyűjtését és kezelését végző összetevő
    a. az aláírt tulajdonságok megfelelőségének ellenőrzése,
    b. az aláírás idejének meghatározása,
    c. érvényes tanúsítvány útvonal felépítése,
    d. a tanúsítvány útvonal érvényességének ellenőrzése.
3. Aláírásokat ellenőrző összetevő
    a. a csomagra számolt ügynök elektronikus aláírás;
    b. az ügynök tanúsítványokhoz tartozó útvonalat alkotó tanúsítványok elektronikus aláírásai;
    c. az önaláírt gyökér tanúsítvány aláírása (megbízható pont);
    d. az összegyűjtött érvényesítési adatokon szereplő aláírások (CRL-eken szereplő aláírások).
4. Az ellenőrzés eredményének továbbítása az ellenőrzési folyamat végén

5.1.3 A mySigno v1.0 környezetének elemei

1. Kliens oldal:
    a. a PDA hosztalkalmazás
    b. infoSigno modul a PKCS#12 tanúsítványban tárolt adatokhoz való hozzáférés biztosításához
    c. ügynök tanúsítványt és magánkulcsot tároló fájlok
2. Szerver oldal:
    a. hitelesítés szolgáltatóval való kommunikáció
    b. időbélyeg szolgáltatóval való kapcsolat
    c. aláírás adatbázis (aláírt csomagok adatbázisát kezelő adatbázis kezelő rendszer)
    d. Oracle adabázis (A mySigno szerver bizonyos beállításait tartalmazza.)

5.2 Alrendszerek

A mySigno v1.0-nak az alábbi három alrendszere van:

- AR1: Aláírás létrehozó alrendszer
- AR2: Aláírás ellenőrző alrendszer
- AR3: Kommunikációs alrendszer

5.2.1 Az AR1 (Aláírás létrehozó) alrendszer:

- Megvalósítja a **BF1 A felhasználó azonosítása és hitelesítése** biztonsági funkciót, bekérve és ellenőrizve a **BF2 Aláírás létrehozása** funkcióhoz szükséges aláíró hitelesítő adatot.
- Megvalósítja a **BF2 Aláírás létrehozása** biztonsági funkciót, megvalósítva a mySigno PDA oldali modul által kitűzött fő biztonsági célt, a fokozott biztonságú elektronikus aláírás készítését.
- Megvalósítja a **BF3 Elektronikus aláírás ellenőrzése** biztonsági funkciót, elvégezve a digitális aláírás ellenőrzését.

- Megvalósítja a **BF7 A TSF (a biztonsági funkciók) védelme** biztonsági funkciót, elvégezve az aláíró hitelesítő adat felhasználás utáni azonnali törlését a memóriából.

5.2.2 Az AR2 (Aláírás ellenőrző) alrendszer:

- Megvalósítja a **BF5 Elektronikus aláírás kezdeti ellenőrzése** biztonsági funkciót, elvégezve a kezdeti aláírás ellenőrzéssel kapcsolatos feladatokat.
- Megvalósítja a **BF6 Elektronikus aláírás utólagos ellenőrzése** biztonsági funkciót, elvégezve a BF5 funkció által összegyűjtött adatok alapján az elektronikus aláírás ellenőrzését.

5.2.3 Az AR3 (Kommunikációs) alrendszer:

- Megvalósítja a **BF4 Biztonságos üzenetváltás** biztonsági funkciót, végrehajtva a csomagok szinkronizálásának, a státusz továbbításának és a szoftverfrissítések letöltésének kezdeményezését, illetve meghívva a biztonságos üzenetváltás aláírási és rejtjelezési funkcióit megvalósító biztonsági funkciókat.

6 Dokumentáció

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

- "mySigno PDA és Szerver elektronikus aláíró rendszer v1.0 – **Adminisztrátori felület (Útmutató)**"
- "mySigno v1.0 – **A biztonságos telepítési, generálási és indítási eljárások leírása**"
- „mySigno v1.0 **Install csomag**”

7 Tesztelés

A TOE fejlesztése során kialakított és alkalmazott tesztek a következők:

- A magánkulcshoz való hozzáférés érdekében az aláíró vagy ellenőrző félnek azonosítása / hitelesítése.
- A kiválasztott csomag elektronikus aláírása. Ehhez a lenyomat elkészítése, amire az aláírás készül, az aláírás létrehozás számára elfogadható formátumra hozatala.
- A kiválasztott csomagra létrehozott digitális aláírás ellenőrzésére.
- A kliens és a szerver közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének ellenőrzése.
- A magánkulcs aktivizálása és felhasználása után annak memóriából történő törlése.

A tesztelés a következő platformokon és konfigurációban lett elvégezve:

- Kliens oldal:
  - Windows Mobile 2003 SE operációs rendszer
  - HP iPAQ HX4700 és Fujitsu-Siemens LOOX 720 PDA hardver
- Szerver oldal:
  - Windows 2003 Server operációs rendszer.

A fejlesztők által végzett tesztelésről az értékelők megalapították, hogy:

- minden biztonsági funkciót és ezek minden külső interfészét tesztelték,
- minden alrendszert és ezek minden belső interfészét tesztelték,

így megfelel mind a tesztelés lefedettségére, mind pedig a tesztelés mélységére vonatkozó elvárásoknak.

A fejlesztők tesztelésre átadták az értékelőknek az mySigno v1.0 futtatható változatát és automatizált teszt rendszerét, egyúttal saját környezetükben és harmadik helyen is biztosították a közös tesztelést.

Az értékelők független tesztelést végeztek az értékelés tárgyára (a fejlesztőknél, saját tesztkörnyezetükben, illetve harmadik félnél is). Az alkalmazott tesztkonfigurációk különbözők voltak, annak megfelelően, hogy a biztonsági előirányzat deklarálja az értékelés tárgyának platform függetlenségét.

A független tesztelés eredményei megfeleltek a várakozásoknak (a tapasztalt tényleges eredmények megegyeztek a teszt tervben szereplő elvárt eredményekkel).

8 Az értékelt konfiguráció

A mySigno v1.0 egy összetett rendszerbe illeszkedő, fokozott biztonságú elektronikus aláírások létrehozására és ellenőrzésére alkalmas függvénykönyvtár. Kliens és szerver oldali összetevőkkel rendelkezik.

A TOE informatikai környezetének elemei:

- Gazdagép operációs rendszere:
  - Kliens:
    Operációs rendszer:
    Pocket PC 2003 SE
    A működéshez szükséges egyéb TOE környezeti összetevők:
    Pocket PC 2003 SDK
    ActiveSync
    Embedded Visual Tools
  - Szerver
    Operációs rendszer:
    Windows 2003 Server
    Kommunikáció:
    IP alapú kapcsolatok fogadás az ügynökök PDA-ja felől, elérés az adatbázis és az Active Directory serverek felé
- A PKCS#12-ben tárolt adatokhoz való hozzáférést támogató összetevők (kriptográfiai szolgáltatások), melyek kriptográfiai interfészt adnak, amit az aláíró alkalmazás meghív az aláírás létrehozása érdekében.
- Az ügynök számára a dokumentum megjelenítését lehetővé tevő szoftver, illetve jelzés, ha ennek a jellemzői nem teljesen felelnek meg a dokumentum által megkövetelt tulajdonságoknak (színhasználat, a szükséges szabályzatok megléte, …)
- A magánkulcs tárolására szolgáló összetevő:
  - Kliens: PKCS#12 formátumú fájl.
  - Szerver: PKCS#12 formátumú fájl.

Az értékelés eredményei az alábbi platformon és konfigurációban lettek ellenőrizve, tesztelve.

PDA hardver és szoftver konfiguráció:

Paraméter	Követelmény
operációs rendszer	Pocket PC 2003 SE
képernyő felbontás	VGA (640x480)
kommunikáció	IP szintű kapcsolat
szabad tárterület	az alkalmazás számára min. 5 Mbyte
billentyűzet	nem szükséges
Bluetooth	nem szükséges

Szerver hardver és szoftver konfiguráció:

Paraméter	Követelmény
operációs rendszer	Windows 2003 Server
processzor	Intel Xeon, Minimum 3GHz, 1MB, ajánlott két processzorra bővíthető alaplappal
memória	Minimum 2GB
szabad tárterület	a szolgáltatás telepítéséhez legalább 15 Mbyte
hálózati kapcsolat	IP alapú kapcsolatok fogadás az ügynökök PDA-ja felől, elérés az aláírás adatbázis és az ügyviteli adatok tárolója felé, Gigabites hálózati kártya

9 Az értékelés eredményei

Az mySigno v1.0 fejlesztő készlet 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, hogy **az mySigno v1.0 megfelel a biztonsági előirányzatának, kielégíti az abban 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 mySigno v1.0 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.3	Az értékelésre átadott szoftver (fejlesztő készlet) egyedi azonosításra került. A szoftver kijelzi verzió számát (v1.0). A konfiguráció lista valamennyi eleme következetesen erre a névre és verziószámra (v1.0) hivatkozik. A konfiguráció lista egyedileg azonosít minden konfiguráció elemet. A konfiguráció menedzselés tervben leírt hozzáférés ellenőrzési intézkedések képesek a konfiguráció elemekhez történő jogosulatlan hozzáférés megakadályozására mySigno v1.0 – **A konfiguráció menedzselés dokumentációja**
	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: megvalósítási reprezentáció; tervezési dokumentáció; teszt dokumentáció; útmutató dokumentációk, konfiguráció menedzselés dokumentáció. A konfiguráció menedzselés dokumentáció leírja az egyes konfiguráció elem állapotok nyomon követésének módját a mySigno teljes életciklusa során. mySigno v1.0 – **A konfiguráció menedzselés dokumentációja**
Kiszállítás és működtetés	ADO_DEL.1	A szállítási eljárások alkalmasak a biztonsági cél kielégítésére (vagyis annak garantálása, hogy a szállítási eljárások kielégítően biztosítják, hogy a kifejlesztett értékelés tárgya sértetlensége nem sérül a felhasználó telephelyére történő szállítás során) A szállítási eljárásokat alkalmazzák. "mySigno v1.0 – **Adminisztrátori felület** "
	ADO_IGS.1	A dokumentáció megadja és leírja a biztonságos telepítéséhez, generálásához és indításához szükséges eljárásokat illetve azokat a lépéseket, amelyek az mySigno v1.0 biztonságos telepítéséhez, generáláshoz és indításához szükségesek. "mySigno v1.0 – **Adminisztrátori felület** "
Fejlesztés	ADV_FSP.1	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. "mySigno v10.- **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. "mySigno v1.0- **Magas szintű terv**"
	ADV_RCR.1	A biztonsági előirányzat összefoglaló előírása és a funkcionális specifikáció közötti megfeleltetés-elemzés alapján megállapítható, hogy a funkcionális specifikáció a mySigno v1.0 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. „mySigno v1.0 – **Megfeleltetés elemzések**”
Útmutató dokumentumok	AGD_ADM.1	Az adminisztrátoroknak (is) szóló útmutatás: • leírja az adminisztrátor rendelkezésére álló adminisztratív biztonsági funkciókat és interfészeket, • leírja az mySigno v1.0 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, az mySigno v1.0 informatikai környezetére vonatkozó, az adminisztrátor számára lényeges biztonsági követelményt. "mySigno v1.0 – **Adminisztrátori felület** "

	AGD_USR.1	A felhasználóknak szóló útmutatás: • leírja a nem adminisztrátor felhasználók rendelkezésére álló valamennyi interfész és funkció leírását, • leírja az mySigno v1.0 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 az mySigno v1.0 biztonságos üzemeltetéséhez szükséges, beleértve a biztonsági környezet leírásában szereplő, a felhasználói viselkedésre vonatkozó feltételezéseket is, • konzisztens az értékeléshez beadott többi dokumentációval, leír minden, az mySigno v1.0 informatikai környezetére vonatkozó, a felhasználó számára lényeges biztonsági követelményt. "mySigno v1.0 – **Adminisztrátori felület** "
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 megállapította, hogy a leírt eljárások alkalmazásának eredményét bemutató bizonyítékok (napló fájl, mentéseket tartalmazó fájlok) léteznek, illetve a leírt biztonsági intézkedéseket be is tartják. "mySigno v1.0 – **A fejlesztési biztonság 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. "mySigno v1.0 – **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/. "mySigno v1.0 – **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/. "mySigno v1.0 – **Teszt mélység elemzés**"
	ATE_IND.2	A tesztelt mySigno-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. "mySigno v1.0 – **A tesztelésre alkalmas mySigno v1.0**"
A sebezhetőség felmérése	AVA_MSU.1	Az útmutató helytelen használhatóságának elemzése alapján megállapítható, hogy az útmutató az mySigno v1.0 valamennyi működési módjában útmutatást ad a biztonságos működtetésre "mySigno v1.0 **Az útmutató helytelen használhatóságának elemzése**"
	AVA_SOF.1	A mySigno v1.0 kizárólag a BF1 (A felhasználó azonosítása és hitelesítése) biztonsági funkcióban alkalmaz valószínűségi vagy permutációs mechanizmusokat (PIN bekérése és ellenőrzése). Ezért a biztonsági funkcióerősség elemzés erre a mechanizmusra szorítkozik. A funkcionális specifikáció, a magas szintű terv, a felhasználói útmutató és az adminisztrátori útmutató alapján megállapítható, hogy minden valószínűségi vagy permutációs mechanizmushoz tartozik SOF követelmény. A SOF követelmények helyessége megállapítást nyert. "mySigno v1.0 –**Biztonsági funkcióerősség elemzés**"
	AVA_VLA.1+	Az értékelő az áthatolás tesztelések eredményei, valamint a sebezhetőségi elemzések következtetései alapján megállapította, hogy az mySigno v1.0 a tervezett (cél)környezetében képes ellenállni egy alacsony támadási képességgel rendelkező támadónak. Az értékelő jelentést írt az összes kihasználható sebezhetőségről és maradvány sebezhetőségről „mySigno v1.0 **- Sebezhetőség elemzés**"

Az értékelés másik következtetése az alábbi:
Az mySigno v1.0 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.**

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 mySigno v1.0 fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN/ISSS/E-Sign 14170:2004 CEN Workshop Agreement: Security requirements for signature creation applications /May 2004/
- CEN/ISSS/E-Sign 14171:2004 CEN Workshop Agreement: General guidelines for electronic signature verification /May 2004/

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

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

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

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

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- interjú: a fejlesztőkkel való személyes konzultációk során kapott információk alapján,
- dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- tapasztalat: a program felhasználói felületének működtetése, illetve a tesztelés során szerzett „felhasználói” tapasztalatokból leszűrt következtetések alapján,
- teszt: az értékelők által végzett tesztelés eredményei alapján,
- forrás kód: a fejlesztők által átadott forráskód értékelők általi elemzése alapján.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

Az mySigno v1.0 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.**

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 mySigno v1.0-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 mySigno v1.0 megfelelése a funkcionális követelményeknek.

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	**megfelel**
F_SDP_2	**megfelel**
F_SDP_3	**megfelel**
F_SAV_1	**megfelel**
F_SAV_2	**megfelel**
F_SAV_3	**nem vonatkozik rá a követelmény**
F_SIC_1	**megfelel**
F_SIC_2	**megfelel**
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	**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	**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	**megfelel**
F_USV-1	**megfelel**

F_human_1	**megfelel**
F_human_2	**nem vonatkozik rá a követelmény**
F_human_3	**megfelel**
F_human_4	**megfelel**
F_human_5	**megfelel**
F_human_6	**megfelel**
F_human_7	**megfelel**
F_machine_1	**megfelel**
F_machine_2	**megfelel**
F_general_1	**megfelel**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	**megfelel**

11.2 Az mySigno v1.0 megfelelése a biztonsági követelményeknek.

Biztonsági követelmény	Teljesülés
S_SCA_1	**megfelel**
S_SCA_2	**megfelel**
S_SCA_3	**nem vonatkozik rá a követelmény**
S_SCA_4	**nem vonatkozik rá a követelmény**
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 (1)**
S_SCA_10	**megfelel**
S_SCA_11	**megfelel**
S_SCA_12	**megfelel**
S_SDP_1	**megfelel**
S_SDP_2	**megfelel**
S_SDP_3	**megfelel**
S_SDP_4	**nem vonatkozik rá a követelmény**
S_SDP_5	**megfelel**
S_SDP_6	**megfelel**
S_SDP_7	**nem vonatkozik rá a követelmény**
S_SDP_8	**megfelel**
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	**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	**megfelel**
S_SIC_1	**megfelel**
S_SIC_2	**nem vonatkozik rá a követelmény**
S_SIC_3	**nem vonatkozik rá a követelmény**
S_SIC_4	**megfelel**
S_SIC_5	**megfelel**
S_SAC_1	**megfelel**
S_SAC_2	**megfelel**
S_SAC_3	**megfelel**
S_SAC_4	**megfelel**
S_SAC_5	**nem vonatkozik rá a követelmény**
S_SAC_6	**megfelel**
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	**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 (2)**
S_I/O_2	**feltétellel megfelel (3)**
S_I/O_3	**nem vonatkozik rá a követelmény**
S_VER_1	**feltétellel megfelel (4)**

11.3 A tanúsított termékek listájába javasolt szöveg

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

*„A **mySigno PDA és Szerver v1.0.0** (röviden mySigno v1.0.0 vagy mySigno) aláírás létrehozó és ellenőrző rendszer fokozott biztonságú elektronikus aláírások létrehozására és ellenőrzésére alkalmas függvénykönyvtár. Kliens és szerver oldali összetevőkkel rendelkezik. A függvénykönyvtár C++ nyelven készült, az aláírás létrehozására és ellenőrzésére tartalmaz függvényhívásokat, és rendelkezik felhasználó (aláíró) által látható képernyőkezelő függvényekkel.*
A mySigno elektronikus aláírás létrehozása olyan egyéb funkcionalitással rendelkező rendszerbe épül, amely kézi aláírások létrehozását és feldolgozását teszi lehetővé a felhasználók számára.

A kézi aláírások létrehozása, azok megbízhatósága kívül esik a mySigno értékelés hatókörén, az értékelés a fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére szorítkozik.

Az mySigno v1.0 fejlesztő készlet 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, hogy az mySigno v1.0 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 az mySigno v1.0-t alkalmazást használja, azaz az mySigno v1.0 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.

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
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	**S**igner's **A**uthentication **C**omponent (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
- *mySigno v1.0 Biztonsági előirányzat v1.0*
- *mySigno v1.0 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	fájl név
Biztonsági előirányzat	v1.0	mySigno_ST_v10.pdf
Aláírási szabályzat	v1.0	mySigno_A_Signature_Policy.doc
Funkcionális specifikáció	v1.0	mySigno_FS_v10.doc
Magas szintű terv	v1.0	mySigno _HLD_v10.doc
Megfeleltetés elemzések	v1.0	mySigno_RCR_v10.doc
Tesztelési dokumentáció - Adminisztrátori felület	v1.0	mySigno_Admin_Test_Documentation_v10.doc
Tesztelési dokumentáció - PDA modul	v1.0	mySigno_PDA_Test_Documentation_v10.doc
Tesztelési dokumentáció - Szerver modul	v1.0	mySigno_Server_Test_Documentation_v10.doc
Teszt lefedettség elemzés	v1.0	mySigno_Test_Coverage_Analysis_v10.doc
Teszt mélység elemzés	v1.0	mySigno_Test_Depth_Analysis_v10.doc
Adminisztrátori felület (Útmutató)	v1.0	mySigno_Admin_v10.doc
A konfiguráció menedzselés dokumentációja	v1.0	mySigno_ACM_v10.doc
A fejlesztési biztonság dokumentációja	v1.0	mySigno_DVS_v10.doc
Az útmutatók helytelen használhatóságának elemzése	v1.0	mySigno_Misuse_Analysis_v10.doc
Biztonsági funkcióerősség elemzés	v1.0	mySigno _SOF_Analysis_v10.doc
Sebezhetőség elemzés	v1.0	mySigno_Vulnerability_Analysis_v10.doc
mySigno for PDA Specifikáció	-	mySigno_Specification_final.doc
TOE leírás	-	mySigno_TOE_desription.doc

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 3 - A fokozott 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