TANÚSÍTÁSI JELENTÉS

mySigno API 3.1
v3.1.

HUNG-TJ-66-2014

Verzió:	1.0
Fájl:	HUNG_TJ_66_2014_v10.pdf
Minősítés:	Nyilvános
Oldalak:	31

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2014.08.30	A szerkezet felállítása
v0.02	2014.10.11.	A tanúsítás eredményeit tartalmazó teljes változat
v0.03	2014.10.20	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v1.0	**2014.10.31**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**mySigno API 3.1**
Verzió szám:	**v3.1**
Rövid elnevezés:	**mySigno API 3.1**
Az értékelt termék típusa:	Fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2014. október 06.
Az értékelés módszere:	MIBÉTS
Az értékelés garanciaszintje:	Fokozott (EAL3)
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • fokozott biztonságú elektronikus aláírások létrehozása, • elektronikus aláírások kezdeti ellenőrzése.
Konfigurációs követelmények:	Operációs rendszerek: • Windows 7 • Windows 8 • Windows 8.1 • Amennyiben a fejlesztői környezet az operációs rendszerben nem tartalmazza: Microsoft Ink SDK Fejlesztő környezet: • Microsoft Visual Studio 2013 • Wacom SDK A magánkulcs tárolására szolgáló összetevő: • A konfigurációba ágyazott PKCS#12 formátumú fájl, vagy az InfoProve Core SDK által támogatott tároló

2 Azonosítás

Az értékelt termék neve:	**mySigno API 3.1**
Verzió szám:	**v3.1**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	mySigno.kliens.telepito.31.exe MySignoLibrary.NET.CertificatePackageLibrary.dll MySignoLibrary.NET.ConfigAPI.dll MySignoLibrary.NET.dll MySignoLibrary.NET.Documents.dll MySignoLibrary.NET.Encryption.dll MySignoLibrary.NET.Exceptions.dll MySignoLibrary.NET.PDF.dll MySignoLibrary.NET.PDFInterface.dll MySignoLibrary.NET.PluginSystem.dll MySignoScreenDevice.Plugin.DeviceConfig MySignoScreenDevice.Plugin.dll WacomSTUDevice.Plugin.DeviceConfig WacomSTUDevice.Plugin.dll

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az mySigno API 3.1 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.

Először az mySigno API 3.1 üzemmódjait határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

A mySigno API 3.1 egy üzemmóddal rendelkezik, fokozott biztonságú elektronikus aláírások létrehozására és kezdeti ellenőrzésére alkalmas.

Fokozott biztonságú aláírás létrehozás esetén az mySigno API 3.1képes együttműködni PKCS#12 szoftveres kulcstároló állománnyal, illetve az InfoProve Core SDK az általa támogatott kulcstárolókkal

3.2 Biztonsági funkciók

A mySigno API 3.1 az alábbi biztonsági funkciókat valósítja meg:

- BF1: Fokozott biztonságú elektronikus aláírás létrehozása
- BF2: Fokozott biztonságú elektronikus aláírás kezdeti ellenőrzése
- BF3: Biometrikus adatok védelme
- BF4: Biztonságos üzenetváltás
- BF5 A biztonsági funkcionalitás (TSF) védelme

3.2.1 BF1: Fokozott biztonságú elektronikus aláírás létrehozása

A biztonsági funkció fő célja a digitális aláírás létrehozása. A funkció sikeres végrehajtása esetén létrejön egy digitálisan aláírt (a beállításoktól függően XAdES-EPES vagy XAdES-T szintű) XML csomag, amelyben a digitális aláírás hitelesíti és biztosítja a csomagba fűzött adatok integritását.

3.2.2 BF2: Fokozott biztonságú elektronikus aláírás kezdeti ellenőrzése

A biztonsági funkció fő célja, hogy elvégezze a kapott XML csomag aláírásainak kezdeti ellenőrzését. (XAdES-EPES szinten) Ez a funkció ellenőrzi az aláírás létrehozásának sikerességét és az aláíró tanúsítvány megfelelőségét. A kezdeti ellenőrzés elvárásai a kliens API jellemzően offline működéséhez igazodnak és a rendelkezésre álló adatokból is képesek dolgozni.

3.2.3 BF3: Biometrikus adatok védelme

A biztonsági funkció fő célja, hogy megvédje a begyűjtött biometrikus adatokat az illetéktelen felhasználástól és egyértelműen a dokumentumhoz kössék azt. Ez biztosítja többek között azt is, hogy a biometrikus aláírás adatok a dokumentum tartalmához olyan módon kapcsolódjanak, hogy minden – a biometrikus aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető legyen.

3.2.4 BF4: Biztonságos üzenetváltás

A biztonsági funkció fő célja az aláírást tartalmazó csomagok szerver felé továbbítása. A funkció képes akkor is biztonságos adatcserére a szerver és a kliens API között, ha a kommunikációra kijelölt csatorna maga nem titkosított.

3.2.5 BF5 A biztonsági funkcionalitás (TSF) védelme

A biztonsági funkció fő célja, hogy megvédje a konfigurációs állományt és a kliens szerelvényeit. Ezt egyrészt a konfigurációs állomány digitális aláírásával és ennek ellenőrzésével biztosítja, másrészt a kliens API szerelvényeinek digitális aláírásával. Az utóbbi ellenőrzése az operációs rendszerre hárul.

4 Feltételezések és hatókör

4.1 A biztonsági előirányzatban megfogalmazott a környezet által teljesítendő biztonsági célok

Az értékelés következtetései a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket a mySigno API nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezete teljesítse) az alábbiak:

OE.Trusted_Security_Admin

A mySigno API 3.1 használata előtti, a TOE hatáskörön kívülre eső telepítési feladatokat végző adminisztrátorok megbízhatóak, a mySigno API 3.1 használatára kiképezték őket, rendelkeznek a szükséges eszközökkel a feladataik ellátáshoz.

OE.UserGuide

A klienst használó ügynököt az eszköz használatára kiképezték, ismeri az eszköz fizikai paramétereiből következő, és annak biztonságos alkalmazását garantáló használati szabályokat.

OE.Trusted_EnvCode

A mySigno biztonsági funkcióit hívó alkalmazás és a mySigno API 3.1 által hívott funkciókat megvalósító függvénykönyvtár megbízható a tekintetben, hogy teljesíti a jelen biztonsági előirányzatban IT környezeti feltételezésként előírt, a TOE biztonságos használatát feltételező biztonsági követelményeket.

OE.Packet_Viewers

Mind a kliens eszköz, mind pedig a szerver oldali IT környezet tartalmaz olyan külső megjelenítő alkalmazásokat, melyek képesek a csomagba foglalható formátumok (melyeket az aláírási szabályzat határoz meg) mindegyikének a megjelenítésére. Az aláírás létrehozó 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.

OE.Separation_and_Exclusion

Az aláírás létrehozását és ellenőrzését végző IT környezetben a TOE folyamatok védettek más folyamatok káros beavatkozásai ellen. A mySigno API 3.1 modult csak egy host alkalmazás töltheti be egy időben.

OE.Services_Integrity

A mySigno API 3.1 környezetének (hívó host alkalmazásnak, operációs rendszernek) biztosítania kell olyan eszközöket, mellyel azok ellenőrizni tudják a mySigno API 3.1 szolgáltatások és paraméterek sértetlenségét.

OE.Protected_Verification_Environment

A szerver oldalon biztosítani kell egy védett környezetet és egy ellenőrző alkalmazást egy kézi aláírással kapcsolatban utólag felvetődő vitás esetek rendezésére.

A védett környezetben az ellenőrző alkalmazás meghatározott számú kulcsőr együttes jelenlétében legyen képes visszaállítani a dokumentumhoz kapcsolt kézi aláírás biometrikus

adatait, egyúttal ellenőrizni a csomag digitális aláírásának érvényességét és a kézi aláírással ellátott dokumentum sértetlenségét, mely után egy írásszakértő már képes lehet eldönteni a vitát (valóban a megnevezett személytől származik-e a kézi aláírás).

OE.Host_CLIENT_Machine

Az a gazdaszámítógép, melyen a mySigno API 3.1 fut, közvetlenül az aláíró (ügynök) befolyása és a rendszert működtető szervezet felügyelete alatt áll.

A gazdaszámítógép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.

A TOE-nak az alábbi intézkedéseket kell érvényre juttatnia:

- a gazdaszámítógép vírusvédelemmel ellátott;
- a gazdagép adminisztrátori funkcióihoz való hozzáférés kizárólagosan az ehhez a funkcióhoz hozzárendelt adminisztrátorokra korlátozott (felhasználó és adminisztrátor megkülönböztetése);
- a gazdagép operációs rendszere elutasítja a nem megbízható forrásból letöltött alkalmazások futtatását.

OE.Signatory_Presence

Az elektronikus aláírás létrehozójának (ügynöknek) végig jelen kell lennie attól kezdődően, hogy kifejezte aláírási szándékát, addig, amíg megadja a magánkulcs aktivizálásához szükséges hitelesítő adatát.

4.2 A CWA 14170 és CWA 14171 követelményeknek való megfelelésből adódó feltételek

1. számú feltétel: A mySigno aláíró alkalmazás fejlesztő készlettel létrehozott aláíró alkalmazáshoz olyan CSP driver-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.

Érintett biztonsági követelmény: S_SCA_1

Megjegyzés: Az 1. számú feltétel automatikusan teljesül, ha a biztonsági előirányzat OE.TOE/SCDev_Communications feltétele (környezetre irányuló biztonsági célja) teljesül, így nem képez kiegészítő feltételt.

2. számú feltétel: A mySigno aláíró alkalmazás fejlesztő készlettel létrehozott aláíró alkalmazáshoz olyan CSP driver-t kell alkalmazni, amely képes megőrizni az aláírót hitelesítő adatok bizalmasságát.

Érintett biztonsági követelmény: S_SCA_2

Megjegyzés: A 2. számú feltétel automatikusan teljesül, ha a biztonsági előirányzat OE.Signatory_Authentication_Data_Protection feltétele (környezetre irányuló biztonsági célja) teljesül, így nem képez kiegészítő feltételt.

3. számú feltétel: A mySigno aláíró alkalmazás fejlesztő készletet használó aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és

alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

Érintett biztonsági követelmény: S_SCA_9

Megjegyzés: A 3. számú feltétel automatikusan teljesül, ha a biztonsági előirányzat OE.Host_Platform feltétele (környezetre irányuló biztonsági célja) teljesül, így nem képez kiegészítő feltételt.

4. számú feltétel: A mySigno aláíró alkalmazás fejlesztő készlet 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.

Érintett biztonsági követelmény: S_I/O_1

Megjegyzés: Az 4. számú feltétel automatikusan teljesül, ha a biztonsági előirányzat OE.Host_Platform feltétele (környezetre irányuló biztonsági célja) teljesül, így nem képez kiegészítő feltételt.

5. számú feltétel: A mySigno aláíró alkalmazás fejlesztő készlet működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a programozói könyvtár és az aláíró alkalmazás funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezeket.

Érintett biztonsági követelmény: S_I/O_2

Megjegyzés: Az 5. számú feltétel automatikusan teljesül, ha a biztonsági előirányzat OE.Host_Platform feltétele (környezetre irányuló biztonsági célja) teljesül, így nem képez kiegészítő feltételt.

6. számú feltétel: A mySigno aláíró alkalmazás fejlesztő készlet működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a programozói könyvtárat és az aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

Érintett biztonsági követelmény: S_VER_1

Megjegyzés: A 6. számú feltétel automatikusan teljesül, ha a biztonsági előirányzat OE.Host_Platform feltétele (környezetre irányuló biztonsági célja) teljesül, így nem képez kiegészítő feltételt.

7. számú feltétel: Olyan külső megjelenítőt szabad használni, ami tájékoztatja az aláírót, hogy egyéb aláírt adatok vannak beágyazva az aláírói dokumentumba, nem képes adat módosításra, és képes az általa kezelt formátum szintaktikai ellenőrzésére, beleértve az aktív kódok jelenlétének felismerését, valamint az aktív kódok által végrehajtott módosítások jelzését.

Érintett biztonsági követelmény: S_SDP_7, S_SDP_8, S_SDP_9, S_SDP_12

Megjegyzés: Kiegészítő feltételt képez.

8. számú feltétel: A mySigno API-t csak olyan környezetben szabad alkalmazni, amelyben a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni, illetve csak olyan aláírási szabályzat szerint működhet, amely legfeljebb a következő X.509 v3 tanúsítvány kiterjesztéseket használja fel:

- ExtendedKeyUsage,
- KeyUsage,
- BasicConstraints,
- CRLDistributionPoints,
- SubjectAlternativeName,
- IssuerAlternativeName,
- OCSP No check - id-pkix-ocsp-nocheck,
- OCSP AuthorityInfoAccess,
- QC statement.

Érintett biztonsági követelmény: F_ISV_3, S_SAV_7

Megjegyzés: Kiegészítő feltételt képez.

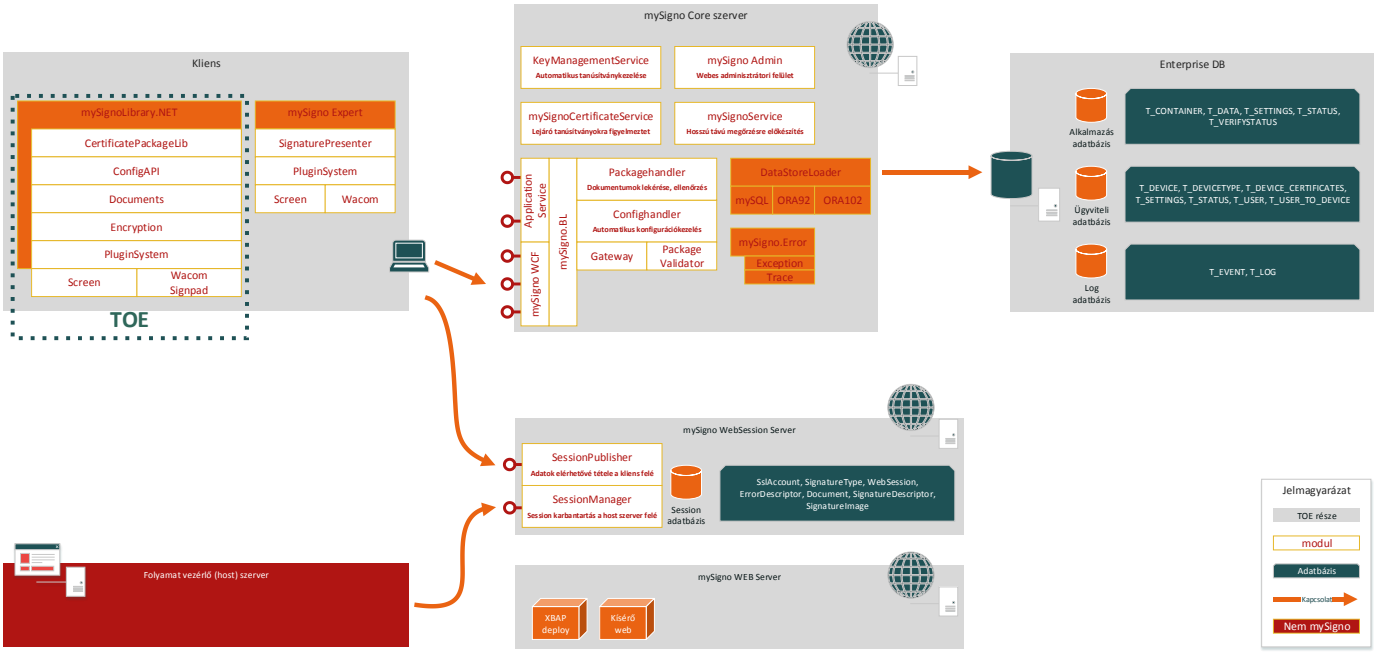
5 A mySigno API 3.1 szerkezeti leírása

A mySigno API 3.1 legfontosabb biztonsági tulajdonságai az alábbiak:

- kézi aláírásból biometrikus adatokat képez, majd egyértelműen, illetéktelen felhasználástól és hozzáféréstől védve az aláírt dokumentumhoz köti,
- a kézi aláírás bitképét, az aláírásból számított biometrikus adatokat és az ezzel aláírt dokumentumokat is tartalmazó csomag sértetlenségét és hitelességét megvédi (fokozott biztonságú elektronikus aláírás létrehozásával, illetve ennek kezdeti ellenőrzésével),
- a kézi és fokozott biztonságú elektronikus aláírást tartalmazó csomagok titkosítja a szerver felé továbbítás előtt,
- indításkor a konfigurációs állományon szerver oldalon elhelyezett fokozott biztonságú elektronikus aláírás érvényességét ellenőrzi.

5.1 Az értékelés tárgya biztonsági környezete és határai

A mySigno API 3.1 egy kliens-szerver architektúrában felépülő zárt rendszer részét képezi. Az 1. ábra a teljes rendszert tekinti át, meghatározva ezen belül a mySigno API 3.1 helyzetét.



1. ábra: a mySigno rendszer felépítése

Az ábrán a mySigno API 3.1 pontozott vonallal van jelölve (TOE).

6 Dokumentáció

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

Telepítési kézikönyv:	INFOSCOPE_mySigno_telepitesi_v3.3	3.3
Fejlesztői dokumentáció:	INFOSCOPE_mySigno_fejlesztoi_v3.3.docx	3.3
	mySigno 2010 P2 Quickstart v4.2.docx	4.2

7 Tesztelés

7.1 A fejlesztők tesztelése

A fejlesztők a teszteket automata programmal valósították meg. A teszt során az összes biztonsági funkcióhoz teszteket rendeltek, és a funkcióhoz tartozó interfészeket minden paraméterre kiterjedően tesztelték. A tesztelés során alkalmazott teszt konfiguráció Windows 8 alatt futó virtuális gép volt, amelyet a fejlesztők az értékelők rendelkezésére bocsátottak. A fejlesztő a tesztjeit minden általa támogatott konfiguráción elvégezte.

A fejlesztők a TOE-t az összes ST-ben szereplő konfiguráción (OS változaton) tesztelték. A tesztek mindegyike sikeresen lefutott, a tervekkel megegyező eredményeket hozva.

7.2 Az értékelők tesztelése

Az értékelők áttekintették a fejlesztői teszteket, és megállapították, hogy a fejlesztők automata tesztekkel, megismételhető módon végezték a tesztelést. Az értékelésre átadott tesztelhető TOE és teszt dokumentáció minden olyan elemet tartalmazott, amely a tesztek megértéséhez és független megismétléséhez szükséges. A teszteléshez az automata teszt program forráskódja is átadásra került, így a teljes teszt metódus ismert volt az értékelők előtt. Az értékelők az automata tesztek révén minden fejlesztői tesztet megismételtek az értékelésre átadott konfiguráción, illetve azon a részen, ahol a fejlesztői tesztek hatékonysága és a lehetséges sebezhetőségek indokolttá tették, az értékelők saját teszteket is végrehajtottak.

A fejlesztői tesztek megismétlése sikeresen, hiba nélkül lefutottak. A tesztesetek eredménye minden esetben megfelelt az elvárt eredménynek.

8 Az értékelt konfiguráció

Értékelt mySigno API verzió: 3.1 mely az alábbi fájlokból áll:

mySigno.kliens.telepito.31.exe
SHA256: 5BB88B61B4E749D870B147AC716281DAC3EC2A35BB578A6F5FD752E4B1F8EE9F

MySignoLibrary.NET.CertificatePackageLibrary.dll v2.1.1.0
SHA256: 7CAD31EF5AEFBC7D940C394DA2CCD6ED4D51D424497A0E26C512148E51AF9ADF

MySignoLibrary.NET.ConfigAPI.dll v3.1.0.0
SHA256: B463A16CF2FBE98331AD6D9F96EDD6A634C1464E1237A3796C85AAFC59183711

MySignoLibrary.NET.dll v3.0.5.1
SHA256: 5247629157301FFF09603541CB001689D958B1057FF059AA04E4975E1825F3F2

MySignoLibrary.NET.Documents.dll v2.2.1.0
SHA256: DAA82B515C2E9E1D0B6343FDA4C3F53A85FA5842810F879537D951071D3C6B4E

MySignoLibrary.NET.Encryption.dll v3.1.0.0
SHA256: 4A99ACEAEA6AE3A296F9570CE005EBE9591F0EF6B25B8DC1436905FF31E7CA46

MySignoLibrary.NET.Exceptions.dll v2.2.1.0
SHA256: 4C224D9456C20157D82327B95AB21EA9F81046486B3DA6BCD97BF54776497D8F

MySignoLibrary.NET.PDF.dll v1.0.0.0
SHA256: 14746861BA5535EBA7F060FE8155AEDBF9E3C0421A5CA78E2C20197966534063

MySignoLibrary.NET.PDFInterface.dll v1.0.0.0
SHA256: C1B23E1C18BCF649809E93FE69D6AACA2F65CD23B6A8F0C6ABE336D1D6F6E863

MySignoLibrary.NET.PluginSystem.dll v2.1.7.0
SHA256: B48F290525F9A8FEE347C30E5D2DF7027408797C5732DEB92185E17BC152C926

MySignoScreenDevice.Plugin.DeviceConfig
SHA256: 1A8F8E2BA5FEA9CE30D86F18E0B714A63A06FB6D94C54A7C01FCD3D174176B88

MySignoScreenDevice.Plugin.dll v2.1.2.0
SHA256: 45D19A0902A5A36DD918969543C07A928EFB5DEAB09FC943819832979B46ED5E

WacomSTUDevice.Plugin.DeviceConfig
SHA256: DC68E103B49FB3CB06802E729604480259621E7214055542A229CEA8B49C0776

WacomSTUDevice.Plugin.dll v2.1.6.0
SHA256: 27E1D65F812B02E36CE3F8AB304D7004BAE8BF05F10CAC61463B61EA418D40CE

Az értékelt konfiguráció elemei:

Operációs rendszerek:
- Windows 7
- Windows 8
- Windows 8.1
- Amennyiben a fejlesztői környezet az operációs rendszerben nem tartalmazza: Microsoft Ink SDK

Fejlesztő környezet:
- Microsoft Visual Studio 2013
- Wacom SDK

A magánkulcs tárolására szolgáló összetevő:

A konfigurációba ágyazott PKCS#12 formátumú fájl, vagy az InfoProve Core SDK által támogatott tároló

9 Az értékelés eredményei

A mySigno API 3.1 értékelés az informatikai termékek technológia szempontú biztonsági értékelésére kidolgozott MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertant használta.

A MIBÉTS értékelési módszertana a KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlásának (Az E-közigazgatási Keretrendszer követelménytár, 2009) részét képezi az alábbi címen: „Termékekre vonatkozó értékelési módszertan”.

Az értékelés garanciaszintje MIBÉTS **fokozott**, mely a CC (Common Criteria, MSZ ISO/IEC 15408) szerinti **EAL3**-as szintnek felel meg.

Az értékelés fő következtetése az alábbi:

Az értékelés tárgya megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az 4. fejezetekben megfogalmazott feltételek teljesülése esetén a mySigno API 3.1 függvénykönyvtár alkalmas fokozott biztonságú elektronikus aláírások létrehozására és kezdeti ellenőrzésére.

9.1 A biztonsági előirányzat értékelése

Ez az alfejezet a mySigno API 3.1biztonsági előirányzata értékelési eredményeit foglalja össze.

Az értékelés alapja az alábbi dokumentum:

Biztonsági előirányzat	INFOSCOPE_mySigno_ST_v1.0.5.doc INFOSCOPE_mySigno_ST_v1.0.6_lite.pdf	1.0.5 1.0.6

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Biztonsági előirányzat	ASE_INT.1 Bevezetés	A követelményeknek **megfelelt**.
	ASE_CCL.1 Megfelelőségi nyilatkozatok	A követelményeknek **megfelelt**.
	ASE_SPD.1 Biztonsági probléma meghatározás	A követelményeknek **megfelelt**.
	ASE_OBJ.2 Biztonsági célok	A követelményeknek **megfelelt**.
	ASE_ECD.1 Kiterjesztett biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_REQ.2 Biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_TSS.1 Az értékelés tárgya összefoglaló előírása	A követelményeknek **megfelelt**.

9.2 A fejlesztés értékelése

Ez az alfejezet a mySigno API 3.1 tervezési dokumentációit értékeli a biztonsági funkcióik megfelelő leírása és magyarázata szempontjából.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági szerkezet leírás	INFOSCOPE_mySigno_FS_v1.4.4.docx	1.4.4
Funkcionális specifikáció	INFOSCOPE_mySigno_FS_v1.4.4.docx	1.4.4
TOE terv	INFOSCOPE_mySigno_HLD_v311.docx	3.1.1

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Fejlesztés	ADV_ARC.1 A biztonsági szerkezet leírás	A követelményeknek **megfelelt**.
	ADV_FSP.3 Funkcionális specifikáció teljes összegzéssel	A követelményeknek **megfelelt**.
	ADV_TDS.2 Szerkezeti terv	A követelményeknek **megfelelt**.

9.3 Az útmutatók értékelése

Ez az alfejezet a mySigno API 3.1 útmutató dokumentációját értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Telepítési kézikönyv	INFOSCOPE_mySigno_telepitesi_v3.3 INFOSCOPE_mySigno_fejlesztoi_v3.3.docx mySigno 2010 P2 Quickstart v4.2.docx	3.3 3.3 4.2
Fejlesztői dokumentáció	INFOSCOPE_mySigno_fejlesztoi_v3.3.docx	3.3

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

9.4 Az életciklus támogatás értékelése

Ez az alfejezet a mySigno API 3.1 fejlesztése során a fejlesztői környezetben betartott biztonsági intézkedéseket értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Konfiguráció lista	mySigno_konfiguracio_lista_v3.2.doc	3.2
A konfiguráció kezelés dokumentációja	INFOSCOPE_mySigno_konfiguracio_kezeles_v3.1.docx	3.1
A fejlesztés biztonság dokumentációja	INFOSCOPE_mySigno_DVS_v1.0.docx	1.00
Az életciklus meghatározás dokumentációja	INFOSCOPE_mySigno_eletciklus_meghatarozas_v3.1.docx	3.1
A szállítási eljárások leírása	mySigno 3.1 Telepítési kézikönyv 1. fejezete (Szállítás)	3.3

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Életciklus támogatás	ALC_CMC.3 Engedélyezéssel kapcsolatos intézkedések	A követelményeknek **megfelelt**.
	ALC_CMS.3 A megvalósítási reprezentáció CM lefedettsége	A követelményeknek **megfelelt**.
	ALC_DEL.1 A szállítási eljárások	A követelményeknek **megfelelt**.
	ALC_DVS.1 A biztonsági intézkedések azonosítása	A követelményeknek **megfelelt**.
	ALC_LCD.1 A fejlesztő által meghatározott életciklus modell	A követelményeknek **megfelelt**.

9.5 A tesztelés értékelése

Ez az alfejezet azt vizsgálja és értékeli, hogy a mySigno API 3.1 a tervdokumentációkban megadottaknak megfelelően működik-e, valamint összhangban van-e a biztonsági előirányzatában megfogalmazott funkcionális biztonsági követelményeivel.

Az értékelés alapját az alábbi fejlesztői és értékelői bizonyítékok képezték:

A tesztelésre alkalmas TOE	mySigno API	3.1
Tesztelési dokumentáció	INFOSCOPE_mySigno_Test_Documentation_v1.2	1.2

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

9.6 A sebezhetőség értékelése

Ez az alfejezet a mySigno API 3.1-ben lévő hibák, gyengeségek meglétét és a velük való visszaélések lehetőségét kívánja meghatározni vagy kizárni. Mindez a fejlesztő és az értékelő elemzésén alapul, valamint értékelői tesztelés egészíti ki.

Az értékelés alapját az összes fejlesztői bizonyíték képeztek (lásd 14.2)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
A sebezhetőség felmérése	AVA_VAN.2 Sebezhetőség vizsgálat	A követelményeknek **megfelelt**.

10 Értékelői megjegyzések és javaslatok

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

11 Mellékletek

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

A mySigno API 3.1 fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN CWA 14170:2004 munkacsoport egyezmény: Security requirements for signature creation applications /May 2004/
- CEN CWA 14171:2004 munkacsoport egyezmény: General guidelines for electronic signature verification /May 2004/

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

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

Egyetlen követelményre sem születhet "nem megfelel" határozat, mert ez az egész értékelés tárgyára nézve "nem felel meg" 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.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

Az mySigno API 3.1 fejlesztő készlet (A 4. 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 és a kezdeti ellenőrzésre vonatkozik.**

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

11.1 Az mySigno API 3.1 megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_SCA_1	Megfelel	alkalmaz
F_SDP_1	Megfelel	kezel
F_SDP_2	Megfelel	kezel
F_SDP_3	Megfelel	kezel
F_SAV_1	Megfelel	megvalósít
F_SAV_2	Megfelel	megvalósít
F_SAV_3	Megfelel	alkalmaz
F_SIC_1	Megfelel	megvalósít
F_SIC_2	Megfelel	megvalósít
F_SIC_3	Nem vonatkozik rá a követelmény	-

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_DTBSF_1	Megfelel	alkalmaz
F_DTBSF_2	Megfelel	alkalmaz
F_DHC_1	Megfelel	alkalmaz
F_DHC_2	Nem vonatkozik rá a követelmény	-
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	Megfelel	megvalósít
F_SDOC_1	Megfelel	alkalmaz
F_I/O-1	Nem vonatkozik rá a követelmény	
F_I/O-2	Megfelel	alkalmaz
F_I/O-3	Megfelel	megvalósít, alkalmaz
F_ISV-1	Megfelel	alkalmaz
F_ISV-2	Nem vonatkozik rá a követelmény	-
F_ISV-3	Feltétellel megfelel (8 számú CWA feltétel)	alkalmaz
F_USV-1	Nem vonatkozik rá a követelmény	-
F_human_1	Nem vonatkozik rá a követelmény	-
F_human_2	Nem vonatkozik rá a követelmény	-
F_human_3	Nem vonatkozik rá a követelmény	-
F_human_4	Nem vonatkozik rá a követelmény	-
F_human_5	Nem vonatkozik rá a követelmény	-
F_human_6	Megfelel	megvalósít
F_human_7	Megfelel	alkalmaz

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_machine_1	Megfelel	alkalmaz
F_machine_2	Nem vonatkozik rá a követelmény	-
F_general_1	Megfelel	megvalósít
F_protocol	Megfelel	alkalmaz
F_format	Megfelel	alkalmaz
F_principles	Megfelel	megvalósít

11.2 A mySigno API 3.1 megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SCA_1	Feltétellel megfelel (OE.TOE/SCDev_ Communications)	részben megvalósít + külső környezeti elvárás
S_SCA_2	Feltétellel megfelel (OE.Signatory_Authentication_ Data_Protection)	részben megvalósít + külső környezeti elvárás
S_SCA_3	Nem vonatkozik rá a követelmény	-
S_SCA_4	Nem vonatkozik rá a követelmény	-
S_SCA_5	Megfelel	támogat
S_SCA_6	Megfelel	megvalósít
S_SCA_7	Nem vonatkozik rá a követelmény	-
S_SCA_8	Nem vonatkozik rá a követelmény	-
S_SCA_9	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás
S_SCA_10	Megfelel	alkalmaz
S_SCA_11	Megfelel	alkalmaz
S_SCA_12	Megfelel	alkalmaz
S_SDP_1	Megfelel	alkalmaz
S_SDP_2	Megfelel	megvalósít -
S_SDP_3	Nem vonatkozik rá a követelmény	-
S_SDP_4	Nem vonatkozik rá a követelmény	-
S_SDP_5	Megfelel	alkalmaz
S_SDP_6	Megfelel	támogat
S_SDP_7	Feltétellel megfelel (7 számú CWA feltétel)	részben megvalósít + külső környezeti elvárás
S_SDP_8	Feltétellel megfelel (7 számú CWA feltétel)	részben megvalósít + külső környezeti elvárás

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SDP_9	Feltétellel megfelel (7 számú CWA feltétel)	részben megvalósít + külső környezeti elvárás
S_SDP_10	Megfelel	alkalmaz
S_SDP_11	Megfelel	alkalmaz
S_SDP_12	Feltétellel megfelel (7 számú CWA feltétel)	külső környezeti elvárás
S_SAV_1	Megfelel	alkalmaz
S_SAV_2	Megfelel	alkalmaz
S_SAV_3	Megfelel	alkalmaz
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	Feltétellel megfelel (8 számú CWA feltétel)	alkalmaz
S_SAV_8	Megfelel	megvalósít
S_SIC_1	Megfelel	megvalósít
S_SIC_2	Megfelel	alkalmaz
S_SIC_3	Megfelel	alkalmaz
S_SIC_4	Megfelel	megvalósít
S_SIC_5	Megfelel	megvalósít
S_SAC_1	Nem vonatkozik rá a követelmény	-
S_SAC_2	Nem vonatkozik rá a követelmény	-
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	-

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SAC_12	Nem vonatkozik rá a követelmény	-
S_DTBSF_1	Megfelel	alkalmaz
S_DHC_1	Megfelel	alkalmaz
S_DHC_2	Nem vonatkozik rá a követelmény	-
S_DHC_3	Megfelel	alkalmaz
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	Megfelel	megvalósít
S_I/O_1	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás
S_I/O_2	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás
S_I/O_3	Nem vonatkozik rá a követelmény	-
S_VER_1	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás

11.3 A tanúsított termékek listájába javasolt szöveg

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

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

- *Fokozott biztonságú elektronikus aláírás létrehozása a Crypto API által támogatott algoritmus paraméterekkel, szoftver tokenben tárolt magánkulcs használatával.*
- *Elektronikus aláírás kezdeti ellenőrzése a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal, RSA 2048 algoritmus támogatással.*
- *Aláírás létrehozáshoz lenyomat készítése SHA-256 algoritmusokkal.*

Ennek alapján a mySigno API 3.1 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani."

12 Biztonsági előirányzat

A jelen tanúsítási jelentés részét képező végleges biztonsági előirányzatot különálló dokumentumként csatoljuk. A fejlesztő megítélése szerint a biztonsági előirányzat egyes részei üzleti titkot tartalmaznak, ezért nyilvánosságra ezektől mentes "lite" verziót bocsájt.

13 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

API	**A**pplication **P**rogramming **I**nterface
CC	**C**ommon **C**riteria (Közös szempontok)
CEN	**C**omité **E**uropeen de **N**ormalization (Európai Szabványügyi Bizottság)
CWA	**C**EN **W**ork **A**greement (CEN munka megállapodás)
DHC	**D**ata **H**ashing **C**omponent (adatlenyomat-készítő összetevő)
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
ETSI TS	**ETSI T**echnical **S**pecification
MIBÉTS	**M**agyar **I**nformatikai **B**iztonsági **É**rtékelési és **T**anúsítási **S**éma
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**ignature **C**reation **A**pplication (aláírást létrehozó alkalmazás)
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	**S**ecure **H**ash **A**lgorithm
SIC	**S**igner's **I**nteraction **C**omponent (aláíróval kölcsönható összetevő)
SSC	**S**CDev/**S**CA **C**ommunicator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikátor összetevő)
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- mySigno API 3.1 Biztonsági előirányzat v1.05
- mySigno API 3.1 (fuggvénykönyvtár) v3.1 Értékelési jelentés v1.0

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

fejlesztői bizonyíték	Cím	verzió
Megvalósítás		
futtatható saját szoftver elemek	Az egyes komponensek és SHA256 lenyomataik: MySignoLibrary.NET.CertificatePackageLibrary.dll, 7CAD31EF5AEFBC7D940C394DA2CCD6ED 4D51D424497A0E26C512148E51AF9ADF MySignoLibrary.NET.ConfigAPI.dll, B463A16CF2FBE98331AD6D9F96EDD6A6 34C1464E1237A3796C85AAFC59183711 MySignoLibrary.NET.dll, 5247629157301FFF09603541CB001689 D958B1057FF059AA04E4975E1825F3F2 MySignoLibrary.NET.Documents.dll, DAA82B515C2E9E1D0B6343FDA4C3F53A 85FA5842810F879537D951071D3C6B4E MySignoLibrary.NET.Encryption.dll, 4A99ACEAEA6AE3A296F9570CE005EBE9 591F0EF6B25B8DC1436905FF31E7CA46 MySignoLibrary.NET.Exceptions.dll, 4C224D9456C20157D82327B95AB21EA9 F81046486B3DA6BCD97BF54776497D8F MySignoLibrary.NET.PDF.dll, 14746861BA5535EBA7F060FE8155AEDB F9E3C0421A5CA78E2C20197966534063 MySignoLibrary.NET.PDFInterface.dll, C1B23E1C18BCF649809E93FE69D6AACA 2F65CD23B6A8F0C6ABE336D1D6F6E863 MySignoLibrary.NET.PluginSystem.dll, B48F290525F9A8FEE347C30E5D2DF702 7408797C5732DEB92185E17BC152C926 MySignoScreenDevice.Plugin.DeviceConfig, 1A8F8E2BA5FEA9CE30D86F18E0B714A6 3A06FB6D94C54A7C01FCD3D174176B88 MySignoScreenDevice.Plugin.dll, 45D19A0902A5A36DD918969543C07A92 8EFB5DEAB09FC943819832979B46ED5E	 v2.1.1.0 v3.1.0.0 v3.0.5.1 v2.2.1.0 v3.1.0.0 v2.2.1.0 v1.0.0.0 v1.0.0.0 v2.1.7.0 v2.1.2.0

	WacomSTUDevice.Plugin.DeviceConfig, DC68E103B49FB3CB06802E7296044802 59621E7214055542A229CEA8B49C0776 WacomSTUDevice.Plugin.dll, 27E1D65F812B02E36CE3F8AB304D7004 BAE8BF05F10CAC61463B61EA418D40CE	v2.1.6.0
harmadik fél által fejlesztett szoftver komponensek	InfoProve Core SDK	v3.2.0.1
Fejlesztői dokumentációk		
Biztonsági előirányzat	INFOSCOPE_mySigno_ST_v1.0.5.doc INFOSCOPE_mySigno_ST_v1.0.6_lite.pdf	1.0.5 1.0.6
Telepítési kézikönyv	INFOSCOPE_mySigno_telepitesi_v3.3 INFOSCOPE_mySigno_fejlesztoi_v3.3.docx mySigno 2010 P2 Quickstart v4.2.docx	3.3 3.3 4.2
Fejlesztői dokumentáció	INFOSCOPE_mySigno_fejlesztoi_v3.3.docx	3.3
Üzemeltetési kézikönyv	INFOSCOPE_mySigno_fejlesztoi_v3.3.docx	3.3
Biztonsági szerkezet leírás	INFOSCOPE_mySigno_FS_v1.4.4.docx	1.4.4
Funkcionális specifikáció	INFOSCOPE_mySigno_FS_v1.4.4.docx	1.4.4
TOE terv	INFOSCOPE_mySigno_HLD_v311.docx	3.1.1
Funkcionális biztonsági követelmények	SFRs.doc	1.0
Konfiguráció lista	mySigno_konfiguracio_lista_v3.2.doc	3.2
A konfiguráció kezelés dokumentációja	INFOSCOPE_mySigno_konfiguracio_kezeles_v3.1.docx	3.1
A fejlesztés biztonság dokumentációja	INFOSCOPE_mySigno_DVS_v1.0.docx	1.00
Az életciklus meghatározás dokumentációja	INFOSCOPE_mySigno_eletciklus_meghatarozas_v3.1.docx	3.1
A szállítási eljárások leírása	mySigno 3.1 Telepítési kézikönyv 1. fejezete (Szállítás)	3.3
A tesztelésre alkalmas TOE		3.3.1
Tesztelési dokumentáció	INFOSCOPE_mySigno_Test_Documentation_v1.2	1.2
Teszt lefedettség elemzés	INFOSCOPE_mySigno_Test_Documentation_v1.2	1.2
Teszt mélység elemzés	INFOSCOPE_mySigno_Test_Documentation_v1.2	1.2

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 2, September 2006.
- [Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
- KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlás „Termékekre vonatkozó értékelési módszertan”

14.4 Az tanúsításhoz felhasznált egyéb dokumentumok

Az értékelés figyelembe vette az alábbi mértékadó követelményrendszereket is:

- Az elektronikus aláírásról szóló 2001. évi XXXV. törvény
- CEN CWA 14170:2004 - Security requirements for signature creation applications
- CEN CWA 14171:2004 - General guidelines for electronic signature verification
- ETSI TS 102 176-1 v2.1.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- RFC 5280 PKIX - Certificate and Certificate Revocation List (CRL) Profile
- SHS Secure Hash Standard /FIPS PUB 180-3/
- PKCS#1 RSA Cryptography Standard v2.1, June 2002