Tanúsítási jelentés

Kofax Capture Hitelesítő modul (UserSign)

HUNG-TJ-MIBÉTS-009-2016

Verzió:	1.0
Fájl:	HUNG-TJ-MIBÉTS-009-2016_v10.pdf
Minősítés:	Nyilvános
Oldalak:	18

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2016.03.02.	A szerkezet felállítása
v0.2	2016.03.18.	Belső egyeztetésre kiadott verzió
v0.9	2016.03.21.	Külső egyeztetésre kiadott verzió
v1.0	**2016.03.23.**	**Végleges verzió**

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft.
Tanúsítási divízió

Tartalom

I. Összefoglaló

I.1. A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői

TOE név:	**Kofax Capture Hitelesítő modul (UserSign)**
TOE rövid neve:	UserSign
TOE verzió:	v 1.0.0
Értékelő:	Hunguard Kft. Értékelési Divízió 1123. Budapest, Kékgolyó u. 6.
Értékelés befejezése:	2016. február 26.
Az értékelés módszere:	MIBÉTS
Az értékelés garanciaszintje:	Fokozott (EAL3)

I.2. A tanúsítás tárgya

UserSign modul feladata, hogy a papír dokumentumokból bizonyító erővel bíró hiteles elektronikus másolatok készítésének folyamatát támogassa.

A UserSign modul által támogatott alap funkcionalitás az alábbi:

- Kofax Capture kötegben szereplő TIFF fájlokból PDF dokumentumok előállítása;
- a PDF dokumentum kiegészítése a 13/2005 IHM rendeletben szereplő hiteles másolatképzési rendeletben előírt összes metaadattal;
- a dokumentum elektronikus aláírása;
- elektronikusan aláírt dokumentum kezdeti ellenőrzése.

A modul egy hitelesített elektronikus dokumentumok tárolására felkészített dokumentum archívum számára olyan, belső aláírással ellátott PDF állományokat állít elő, melyek

- a kezelő tevőleges akciójával igazolt módon képi és tartalmi egyezőséget mutatnak a papír eredeti dokumentummal;
- olyan elektronikus aláírást tartalmaznak, melynek érvényessége biztosítja, hogy a letároláskor az archívumba a kezelő által a papír eredetivel képileg és tartalmilag megegyezőnek kijelentett hiteles elektronikus dokumentum kerülhessen.

A UserSign modul az alább megadott szabványoknak, illetve ajánlásoknak megfelelő működést biztosít:

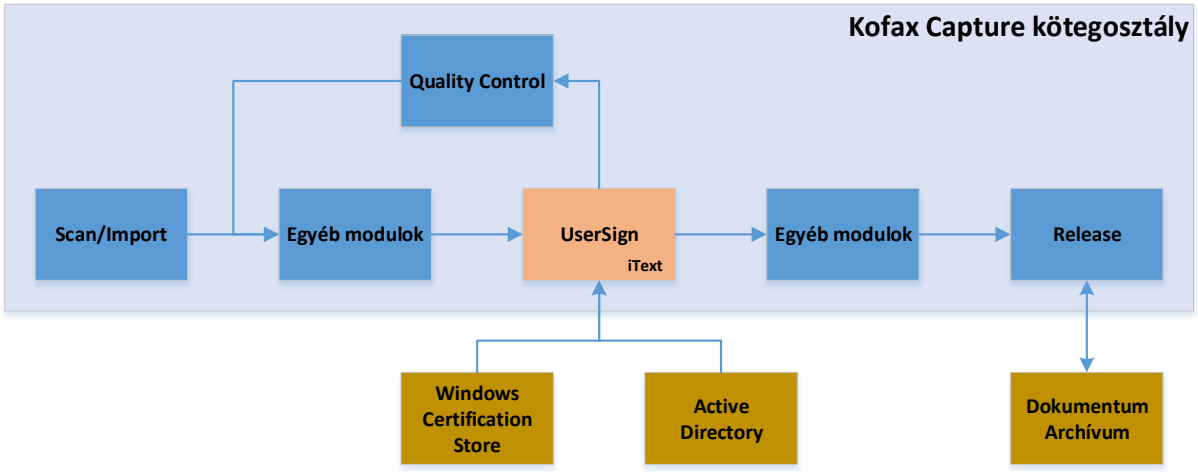
- Tanúsítványok és CRL-ek ellenőrzése, tanúsítási útvonal felépítése és érvényesítése. A tanúsítványlánc felépítésénél az alábbi kiterjesztéseket támogatja:
  - ExtendedKeyUsage,
  - KeyUsage,
  - BasicConstraints,
  - CRLDistributionPoints,
  - SubjectAlternativeName,
  - IssuerAlternativeName,
- elektronikus aláírás formátumok létrehozása és ellenőrzése, az alábbi szabványos formátumokkal:

- PAdES-BASIC.

UserSign modul a TOE-ra vonatkozó követelményeket az alábbi mértékadó dokumentumban foglaltaknak megfelelően támogatja:

- CWA 14170
- CWA 14171
- 13/2005 IHM rendelet
- ETSI TS 102 778-2 v1.2.1

I.3. A TOE biztonsági környezete és határai



1. ábra: Környezeti modell

A TOE-nak az 1. ábrán található UserSign modul felel meg, a környezeti modell további elemei a TOE hatókörén kívül esnek.

UserSign a Kofax Capture egyedi fejlesztésű moduljaként (Custom Module) lett megvalósítva. Működési környezete így egy Kofax Capture köteg, mely egy olyan Kofax Capture kötegosztály (kötegdefiníció) példánya, amelyhez a UserSign modult a folyamat implementálója hozzáadta.

A UserSign modul a Kofax Capture által biztosított módon fogadja és adja ki a hitelesítendő dokumentumokat. Feladata elvégzéséhez az alábbi külső komponensekre van szükség:

- Windows Certification Store: A Windows operációs rendszerek által biztosított tanúsítványtár.
- Active Directory: A felhasználó teljes nevét biztosítja.

UserSign modul biztonsági tartományát az operációs rendszer és a Kofax biztonsági beállításai biztosítják. A telepítési leírás alapján konfigurálva az operációs rendszer és Kofax is csak a szükséges jogosultságokat biztosítja a felhasználók számára.

I.4. A rendszer főbb komponenseinek azonosítása

Értékelt TOE verzió: UserSign 1.0.0

Futtatható saját szoftver elemek

Fájlnév	Verzió	Fejlesztő
SecurityLib.dll	1.0.0.0	User
UserSign.AEX	1.0.5882.22198	User
UserSign.exe	1.0.5882.22198	User
UserSignLib.dll	1.0.5882.22198	User
Encrypt.exe	1.0.5882.22198	User

A futtatható állományok SHA256 lenyomatai:

SecurityLib.dll A5E2777FF519B319DCB4A596C4A324E2422415E8EEE0067C6232556AB8A480F1

UserSign.AEX 9A2690DE016F0DD2B041C6F7463FDBD0ED2D21E4D927F71D8C2990F8BF2B297D

UserSign.exe 379EB4653E87221BBE06D92CC2B10AC848F358EF9408096E35E7CDDE141FAAA6

UserSignLib.dll 84DF4E6494BDFD51FA231065538B281846C5A0456D4EEB1EBF874E2E74D4A3CF

Encrypt.exe 21B256553F73A70902E0E91B1B31D20B54B7AF6A9B0CBF7127B1396C8A9B53A6

Felhasznált komponensek listája

Fájlnév	Verzió	Fejlesztő
AxInterop.AcroPDFLib.dll	1.0.0.0	Adobe
Interop.AcroPDFLib.dll	1.0.0.0	Adobe
itextkey.xml	5.5.6.0	iText Software
itextsharp.dll	5.5.6.0	iText Software
itextsharp.licensekey.dll	1.0.3.0	iText Software
nlog.config	2.0.0.0	nLog project (Open source)
NLog.dll	2.0.0.0	nLog project (Open source)

Az értékelt konfiguráció elemei:

Operációs rendszerek:

- Windows 7 Professional
- Windows 7 Ultimate
- Windows 7 Enterprise
- Windows Server 2008 Standard Edition with Service Pack 1
- Windows Server 2008 Standard x64 Edition (64-Bit) with Service Pack 1
- Windows Server 2008 Enterprise Edition with Service Pack 1
- Windows Server 2008 Enterprise x64 Edition (64-Bit) with Service Pack 1
- Windows Server 2008 Datacenter Edition with Service Pack 1
- Windows Server 2008 Datacenter x64 Edition (64-Bit) with Service Pack 1
- Windows Server 2008 Standard Edition with Service Pack 2
- Windows Server 2008 Standard x64 Edition (64-Bit) with Service Pack 2
- Windows Server 2008 Enterprise Edition with Service Pack 2
- Windows Server 2008 Enterprise x64 Edition (64-Bit) with Service Pack 2
- Windows Server 2008 Datacenter Edition with Service Pack 2
- Windows Server 2008 Datacenter X64 Edition (64-Bit) with Service Pack 2
- Windows Vista Business Edition with Service Pack 1
- Windows Vista Business x64 (64-Bit) Edition with Service Pack 1

- Windows Vista Enterprise Edition with Service Pack 1
- Windows Visita Enterprise x64 (64-Bit) Edition with Service Pack 1
- Windows Vista Business Edition with Service Pack 2
- Windows Vista Business x64 Edition (64-Bit) with Service Pack 2
- Windows Vista Enterprise Edition with Service Pack 2
- Windows Vista Enterprise x64 Edition (64-Bit) with Service Pack 2

Környezeti modulok:

- Kofax Capture 9.00.1237 (Service Pack 2) vagy frissebb
- Adobe Reader DC 2015.010.20056 vagy frissebb
- .NET Framework 3.5

II. A tanúsítás jellemzése

Jelen tanúsítás az elektronikus aláírás termékkel szembeni elvárások teljesülését vizsgálja, azon belül annak megerősítését, hogy a vizsgált termék által nyújtott biztonsági szolgáltatások papíralapú dokumentumokról elektronikus úton készített másolatok rendszerében hitelesnek - joghatás kiváltására alkalmasnak - tekinthetők-e.

II.1. Az alkalmazott értékelési módszer

A UserSign termék értékelésére a MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) értékelési módszertant alkalmazták. 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.

II.2. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Rendszer értékelési jelentés:

- Kofax Capture Hitelesítő modul (UserSign) ÉRTÉKELÉSI JELENTÉS v1.0

Mértékadó követelményrendszernek való megfelelés elemzés:

- Kofax Capture Hitelesítő modul (UserSign) megfelelése a CWA 14170:2004 és CWA 14171:2004 követelményeinek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS v 1.0
- Kofax Capture Hitelesítő modul (UserSign) megfelelése a 13/2005. (X. 27.) IHM rendeletben meghatározott követelményeknek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS v 1.0

II.3. Az értékeléshez felhasznált fejlesztői bizonyítékok

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

Fájlnév	Verzió
Bizt.szerk. leírása - UserSign - ADV_ARC.docx	2016.02.24
Konfiguráció lista - UserSign - ALC_CM.docx	2016.02.24
Életciklus meghatározás - UserSign - ALC_LCD.docx	2016.02.24
UserSign - ADV_FSP_2016.02.24.docx	2016.02.24
FP - UserSign - ADV_FSP_2015.02.24.docx	2016.02.24
Konfiguráció menedzsment - UserSign - ALC_CM.docx	2016.02.24
A fejlesztés biztonsága - UserSign - ALC_DVS.docx	2016.02.24
UserSign - ADV_TDS.docx	2016.02.24
Tesztelési dokumentáció - UserSign - ATE_FUN.docx	2016.02.24
Telepítés és Üzemeltetés - AGD_PRE_OPE.docx	2016.02.24
"Felhasználói_leírás - UserSign - AGD_OPE - 2016.02.24.docx"	2016.02.24
TOE terv - UserSign - ADV_TDS.docx	2016.02.24
Tesztlefedettség elemzés - UserSign - ATE_COV.docx	2016.02.24
Szállítási eljárások - UserSign - ALC_DEL.docx	2016.02.24
UserSign biztonsági előirányzat_v1.0.doc	1.0

II.4. Az értékelési folyamat tanúsítási szempontú ellenőrzése

A tanúsítási jelentés készítői a teljes értékelési folyamatot figyelemmel kísérték, ellenőrizték:

- az értékelési folyamatok módszertani szempontú ellenőrzésével;
- különböző szakértői megbeszéléseken való részvétellel.

III. Az értékelés eredményei

III.1. A garanciális biztonsági követelményeknek való megfelelés

Az értékelés módszertana a MIBÉTS termékekre vonatkozó értékelési módszertanát (KIB 28. számú ajánlása) követte, az eredmények leírása is az ott meghatározott jelöléseket alkalmazza.

III.1.1. A biztonsági előirányzat értékelése

Értékelői feladatelem	határozat
ASE_INT: Biztonsági előirányzat, Bevezetés	megfelelt
ASE_CCL: Biztonsági előirányzat, Megfelelőségi nyilatkozatok	megfelelt
ASE_SPD: Biztonsági előirányzat, Biztonsági probléma meghatározás	megfelelt
ASE_OBJ: Biztonsági előirányzat, Biztonsági célok	megfelelt
ASE_ECD: Biztonsági előirányzat, Kiterjesztett biztonsági követelmények	megfelelt
ASE_REQ: Biztonsági előirányzat, Biztonsági követelmények	megfelelt
ASE_TSS: Biztonsági előirányzat, Az értékelés tárgya összefoglaló előírása	megfelelt

III.1.2. A fejlesztés értékelése

Értékelői feladatelem	határozat
ADV_ARC.1: Biztonsági szerkezet leírás	megfelelt
ADV_FSP.3: Funkcionális specifikáció teljes összegzéssel	megfelelt
ADV_TDS.2: Szerkezeti terv	megfelelt

III.1.3. Az útmutatók értékelése

Értékelői feladatelem	határozat
AGD_OPE.1: Üzemeltetési felhasználói útmutató	megfelelt
AGD_PRE.1: Előkészítő eljárások	megfelelt

III.1.4. Az életciklus támogatás értékelése

Értékelői feladatelem	határozat
ALC_CMC.3: Engedélyezéssel kapcsolatos intézkedések	megfelelt
ALC_CMS.3: A megvalósítási reprezentáció CM lefedettsége	megfelelt
ALC_DEL.1: Szállítási eljárások	megfelelt
ALC_DVS.1: A biztonsági intézkedések azonosítása	megfelelt
ALC_LCD.1: A fejlesztő által meghatározott életciklus modell	megfelelt

III.1.5. A tesztelés értékelése

Értékelői feladatelem	határozat
ATE_FUN.1: Funkcionális tesztelés	megfelelt
ATE_COV.2: A lefedettség vizsgálata	megfelelt
ATE_DPT.1: Az alap terv tesztelése	megfelelt
ATE_IND.2: Független tesztelés - minta	megfelelt

III.1.6. A sebezhetőség értékelése

A sérülékenység vizsgálat során olyan tesztesetek kerültek végrehajtásra, amelyek a TOE biztonsági funkcióinak megkerülését tesztelték.

Ezt kiegészítette a forráskódban a biztonságkritikus (elsősorban a kriptográfiai műveleteket végrehajtó) kódrészletek vizsgálata.

Ellenőrzésre kerültek a TOE által használt harmadik feles alkalmazások a nyílt sérülékenység adatbázisok által.

A fenti vizsgálatok nem tártak fel kockázatokat, így az értékelés eredménye alapján a TOE üzemeltetési környezetében ellenáll egy megemelt-alap támadó képességgel rendelkező támadónak.

Értékelői feladatelem	határozat
AVA_VAN.2: Sebezhetőség vizsgálat	megfelelt

III.2. A CWA14170:2004 és a CWA 14171:2004 megfeleltetés eredménye

III.2.1. A TOE megfelelése a funkcionális követelményeknek[1]

Funkcionális követelmény	Teljesülés
F_SCA_1	megfelelt
F_SDP_1	megfelelt
F_SDP_2	megfelelt
F_SDP_3	megfelelt
F_SAV_1	megfelelt
F_SAV_2	megfelelt
F_SAV_3	megfelelt
F_SIC_1	megfelelt
F_SIC_2	megfelelt
F_SIC_3	megfelelt

[1] A követelmény rövidítések a CWA dokumentumokból készített tanúsítói funkcionális követelménypontok azonosítói

F_DTBSF_1	megfelelt
F_DTBSF_2	megfelelt
F_DHC_1	megfelelt
F_DHC_2	megfelelt
F_SSC_1	megfelelt
F_SSC_2	nem vonatkozik
F_SSC_3	nem vonatkozik
F_SSC_4	nem vonatkozik
F_SSC_5	megfelelt
F_SSC_6	megfelelt
F_SSC_7	megfelelt
F_SSC_8	megfelelt
F_SSA_1	megfelelt
F_SDC_1	megfelelt
F_SDOC_1	megfelelt
F_I/O-1	környezetnek kell biztosítania
F_I/O-2	megfelelt
F_I/O-3	megfelelt
F_ISV-1	megfelelt
F_ISV-2	nem vonatkozik
F_ISV-3	megfelelt
F_USV-1	nem vonatkozik
F_human_1	nem vonatkozik
F_human_2	nem vonatkozik
F_human_3	nem vonatkozik
F_human_4	nem vonatkozik
F_human_5	nem vonatkozik
F_human_6	nem vonatkozik
F_human_7	nem vonatkozik
F_machine_1	nem vonatkozik
F_machine_2	megfelelt

F_general_1	megfelelt
F_protocol	megfelelt
F_format	megfelelt
F_principles	megfelelt

III.2.2. A vizsgált rendszer megfelelése a biztonsági követelményeknek[2]

Biztonsági követelmény	Teljesülés
S_SCA_1	megfelelt
S_SCA_2	megfelelt
S_SCA_3	nem vonatkozik
S_SCA_4	nem vonatkozik
S_SCA_5	megfelelt
S_SCA_6	megfelelt
S_SCA_7	nem vonatkozik
S_SCA_8	nem vonatkozik
S_SCA_9	megfelelt
S_SCA_10	megfelelt
S_SCA_11	megfelelt
S_SCA_12	megfelelt
S_SDP_1	megfelelt
S_SDP_2	megfelelt
S_SDP_3	megfelelt
S_SDP_4	megfelelt
S_SDP_5	megfelelt
S_SDP_6	megfelelt
S_SDP_7	megfelelt
S_SDP_8	megfelelt
S_SDP_9	megfelelt
S_SDP_10	megfelelt
S_SDP_11	megfelelt
S_SDP_12	megfelelt
S_SAV_1	megfelelt
S_SAV_2	megfelelt
S_SAV_3	megfelelt
S_SAV_4	megfelelt
S_SAV_5	megfelelt
S_SAV_6	megfelelt
S_SAV_7	megfelelt
S_SAV_8	megfelelt
S_SIC_1	megfelelt
S_SIC_2	megfelelt
S_SIC_3	megfelelt
S_SIC_4	megfelelt
S_SIC_5	megfelelt

[2] A követelmény rövidítések a CWA dokumentumokból készített tanúsítói biztonsági követelménypontok azonosítói

S_SAC_1	megfelelt
S_SAC_2	megfelelt
S_SAC_3	megfelelt
S_SAC_4	megfelelt
S_SAC_5	nem vonatkozik
S_SAC_6	nem vonatkozik
S_SAC_7	megfelelt
S_SAC_8	megfelelt
S_SAC_9	nem vonatkozik
S_SAC_10	nem vonatkozik
S_SAC_11	nem vonatkozik
S_SAC_12	nem vonatkozik
S_DTBSF_1	megfelelt
S_DHC_1	megfelelt
S_DHC_2	megfelelt
S_DHC_3	megfelelt
S_SSC_1	nem vonatkozik
S_SSC_2	nem vonatkozik
S_SSC_3	megfelelt
S_SSC_4	megfelelt
S_SSA_1	megfelelt
S_SDC_1	megfelelt
S_I/O_1	megfelelt
S_I/O_2	megfelelt
S_I/O_3	megfelelt
S_VER_1	megfelelt

III.3. A 13/2005 IHM rendeletben szereplő követelményeknek való megfeleltetés eredménye

Követelmény	Teljesülés
Általános_szabály_1_elv /4. § (1)/	megfelelt
Általános_szabály_2_folyamat /4. § (2)/	megfelelt
Általános_szabály_3_metadatok /4. § (3)/	megfelelt
Általános_szabály_4_részleges_másolat /4. § (3a)/	nem támogatott
Általános_szabály_5_aláírás /4. § (4)/	megfelelt
Általános_szabály_6_dokumentum-csoportok /4. § (5)/	nem támogatott
Általános_szabály_7_érvényességi_idő /4. § (6)/	környezet által megvalósítandó
Általános_szabály_8_feljogosítás /4. § (7)/	környezet által megvalósítandó
Általános_szabály_9_hozzájárulás /4. § (8)/	környezet által megvalósítandó
Általános_szabály_10_dokumentáltság /4. § (9)/	környezet által megvalósítandó
Általános_szabály_11_másolatkészítési_rend /4. § (10)/	környezet által megvalósítandó
Általános_szabály_12_dokumentumformátum /4 § (11)/	megfelelt
Automatikus_másolatkészítés_1_feltételek /4/A § (1)/	nem támogatott
Automatikus_másolatkészítés_2_mintavételezés /4/A § (2)/	nem támogatott
Automatikus_másolatkészítés_3_hitelesítés /4/A § (3)/	nem támogatott
Automatikus_másolatkészítés_4_kivételek /4/A § (4)/	nem vonatkozik
Közokirat_másolata_1_előírt_formátum /5 § (1)/	nem támogatott
Közokirat_másolata_2_eltérések /5 § (2)/	környezet által megvalósítandó
Közokirat_másolata_3_automatikus_másolatkészítés /5 § (3)/	nem támogatott
Közokirat_másolata_4_egyedi_ellenőrzés /5 § (4)/	környezet által megvalósítandó
Közokirat_másolata_5_kiszervezhetőség /5 § (5)/	környezet által megvalósítandó

Okirat_másolata_1_kiállított:_képi_vagy tartalmi_megfelelés /6 § (1)/	környezet által megvalósítandó
Okirat_másolata_2_őrzött:_képi_megfelelés /6 § (2)/	környezet által megvalósítandó
Számviteli_bizonylat_másolata_1_képi_megfelelés /7 § (1)-(2)/	környezet által megvalósítandó

III.4. A biztonságos felhasználás feltételei

III.4.1. Az üzemeltetési környezetre vonatkozó biztonsági célok

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

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

OE.AUDIT_GENERATION Az üzemeltetési környezet biztosítsa a biztonsági szempontból releváns események észlelését és rögzítését.

OE.AUDIT_PROTECTION Az üzemeltetési környezet biztosítsa a napló információk védelmét.

OE.AUDIT_REVIEW Az üzemeltetési környezet biztosítsa a napló információk megjelenítését szűrés alapján.

OE.Configuration A TOE úgy legyen telepítve és konfigurálva, hogy biztonságos állapotban tudjon működni.
Megjegyzés: A helyes telepítés és konfigurálás az üzemeltetési útmutatóban leírtaknak megfelelően történjen.

OE.CORRECT_TSF_OPERATION Az üzemeltetési környezet biztosítsa a lehetőséget a TSF tesztelésére, hogy a TSF megfelelő működése a felhasználónál biztosítva legyen.
Megjegyzés: A TOE futatható állományainak és konfigurációs fájljainak, valamint biztonsági funkciót befolyásoló adat helyességének ellenőrzése az üzemeltetési környezet feladata.

OE.CRYPTOGRAPHY_ALT A TOE által használt kriptográfiai algoritmusok feleljenek meg az Európai Unión belüli jogszabályoknak. Az elektronikus aláíráshoz használható kriptográfiai algoritmusokat egységesen szabályozzák az Európai Unióban, aktuális információ a következő normatívákból nyerhető
ETSI TS 119 312[3]. A specifikációk folyamatosan megújításra kerülnek, ezért a felhasználónak folyamatosan figyelemmel kell kísérnie az elektronikus aláírás létrehozatalához használható kriptográfiai algoritmusokra vonatkozó normatívák változását, s az annak megfelelő algoritmusokat és paramétereket alkalmazó modulverziót kell használnia.

OE.DISPLAY_BANNER Az üzemeltetési környezet jelenítsen meg figyelmeztetést a rendszer felhasználásáról.

OE.MANAGE Az üzemeltetési környezet az összes szükséges eszközt biztosítsa az adminisztrátorok számára a TOE biztonságának menedzseléséhez és védje ezeket a funkciókat a jogosulatlan használat ellen.

OE.MEDIATE Az üzemeltetési környezet védje a felhasználói adatokat a biztonsági szabályzatnak megfelelően.

[3] A tanúsítvány kiadásakor az aktuális verzió v1.1.1 (2014-11)

OE.NO_EVIL Az üzemeltetés helyszínén legyen biztosítva, hogy az adminisztrátorok nem rosszindulatúak, megfelelően képzettek és követik az adminisztrátori útmutatókat.

OE.PHYSICAL Az üzemeltetés helyszínén legyen biztosítva a fizikai biztonság megfelelő szintje, ami biztosítja, hogy a TOE-t nem lehet befolyásolni, és védett „side-channel attack" támadások ellen.

OE.RESIDUAL_INFORMATION Az üzemeltetési környezet biztosítsa, hogy a védett erőforrásban található információk ne kerüljenek ki az ellenőrzés alól az erőforrás hozzárendelésének megváltozása során.

OE.SELF_PROTECTION Az üzemeltetési környezet biztosítson egy végrehajtási tartományt, ami védi az erőforrásokat a külső behatás, befolyásolás vagy jogosulatlan közzététel ellen.

OE.TIME_STAMPS; OE.TIME_TOE Az üzemeltetési környezet biztosítson megbízható időbélyegeket és időforrást, és az adminisztrátor számára biztosítsa a lehetőséget az időbélyegek által használt megbízható idő beállítására.

OE.TOE_ACCESS Az üzemeltetési környezet biztosítson mechanizmusokat a TOE logikai hozzáférés védelmére.

OE.TOE_PROTECTION Az üzemeltetési környezet védje meg a TOE-t és a TOE erőforrásait a külső behatás, befolyásolás, jogosulatlan közzététel és módosítás ellen.

OE.ARCHIVE Az üzemeltetési környezet biztosítsa az aláírás érvényességének folyamatos megállapíthatóságának fenntartását.

OE.CERT A szervezet által használt aláíró tanúsítvány feleljen meg az alábbi követelményeknek:

- a tanúsítványhoz tartozó tanúsítványlánc egyes elemeiben az ugyanarra a névre vonatkozó issuer name és subject name esetén a whitespace karakterterek használata egyezzen meg,
- a tanúsítványhoz tartozó tanúsítványlánc egyes elemeiben az ugyanarra a névre vonatkozó issuer name és subject name esetén a kis és nagybetűk használata egyezzen meg,
- amennyiben a tanúsítványhoz tartozó tanúsítványlánc bármelyik elemére több name constraint vonatkozik, akkor nem fordulhat elő, hogy egyes constraint-eket a subject name, másokat a subjectAltName teljesít.

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

A TOE konfigurációs állományában a UserSignMode paramétert „live" értékre kell állítani.

III.5. Javaslatok

Az alábbi javaslatok a rendszer jelenlegi vizsgálata szempontjából nem tartoznak az értékelés hatókörébe, de a környezeti biztonságot nagymértékben növelhetik.

1. számú javaslat

A futtató környezetet megalapozó operációs rendszer biztonságos működéshez esetlegesen kiadott javító csomagokat rendszeres időközönként fel kell telepíteni.

2. számú javaslat

Amennyiben a jövőben 64 bites operációs rendszeren is futtatni fogják az értékelés tárgyát, akkor a 64 bit-es platformon a Microsoft .Net Framework 4.0-ra talált CVE-2010-3228 JIT fordító sebezhetőség kihasználhatóságának megakadályozása érdekében a 64 bites operációs rendszeren telepíteni kell az operációs rendszernek megfelelő KB2160841 javítócsomagot.

IV. Javaslat a Tanúsítvány szövegezésére

IV.1. Javaslat a Tanúsítvány főlapjának szövegezésére

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Nemzeti Fejlesztési Minisztérium IKF/1262-1/2016-NFM számú Kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a

User Rendszerház Kft.

által fejlesztett

Kofax Capture Hitelesítő modul (UserSign) v1.0.0

mint informatikai biztonsági funkciókat megvalósító szoftver termék

megfelel

a KIB 28-as Ajánlásában szereplő MIBÉTS módszertan szerinti

fokozott biztonsági szintnek

(mely megfelel a CC EAL 3-es szintjének).

Jelen tanúsítvány a HUNG-TJ-MIBÉTS-009-2016. számú tanúsítási jelentés alapján került kiadásra.

Készült a USER Rendszerház Kft. (1025 Budapest, Szépvölgyi u. 86/b) megbízásából.

A tanúsítvány regisztrációs száma: HUNG-T-MIBÉTS-009-2016

A tanúsítás kelte: 2016. március 23.

A tanúsítvány érvényességi ideje /évenkénti felülvizsgálat mellett/: 2019. március 23.

Mellékletek: feltételrendszer, dokumentumok

IV.2. Javaslat a Tanúsítvány mellékleteire

Javasoljuk, hogy a Tanúsítvány mellékleteiben a következők szerepeljenek:

- A biztonságos felhasználás feltételei lásd az alábbi fejezetet
  III.4 A biztonságos felhasználás feltételei
- A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások lásd az alábbi fejezetet:
  II.1 az alkalmazott módszertan
- A tanúsítási eljárás egyéb jellemzői
  - A tanúsításhoz figyelembe vett, fejlesztőtől független dokumentumok
  - A követelményeknek való megfelelést ellenőrzés vizsgálat garancia szintje

V. Hivatkozások

Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról

2001. évi XXXV törvény az elektronikus aláírásról

13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól

MIBÉTS 2009 Termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében kidolgozott dokumentum, v4 2008.09.19) (a KIB 28-as számú Ajánlás része)

CWA 14170:2004; Security requirements for signature creation applications

CWA 14171:2004; General guidelines for electronic signature verification

ETSI TS 102 778-1 v1.2.1 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1 PAdES Overview – Profile based on ISO 32000-1,

ETSI TS 102 778-2 v1.2.1 Part 2: PAdES Basic – Profile based on ISO 32000-1