Tanúsítási jelentés

TikettPro EMT modul

V2.11.68.68

HUNG-TJ-MIBÉTS-012-2016

Verzió:	1.0
Fájl:	HUNG-TJ-MIBÉTS-012-2016_v10.pdf
Minősítés:	Nyilvános
Oldalak:	13

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2016.11.14.	A szerkezet felállítása
v0.2	2016.12.02.	Belső egyeztetésre kiadott verzió
v0.9	2016.12.05.	Külső egyeztetésre kiadott verzió
v1.0	**2016.12.06.**	**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:	**TikettPro Elektronikus Másodpéldány Tároló**
TOE rövid neve:	TikettPro EMT modul
TOE verzió:	V2.11.68.68
Fejlesztő:	INFO*SYS Kft. 1063 Budapest, Szinyei Merse u. 5.
Értékelő:	Hunguard Kft. Értékelési Divízió 1123 Budapest, Kékgolyó u. 6.
Értékelés befejezése:	2016. december 01.
Az értékelés módszere:	MIBÉTS
Az értékelés garanciaszintje:	Fokozott (EAL3)

I.2. A tanúsítás tárgya

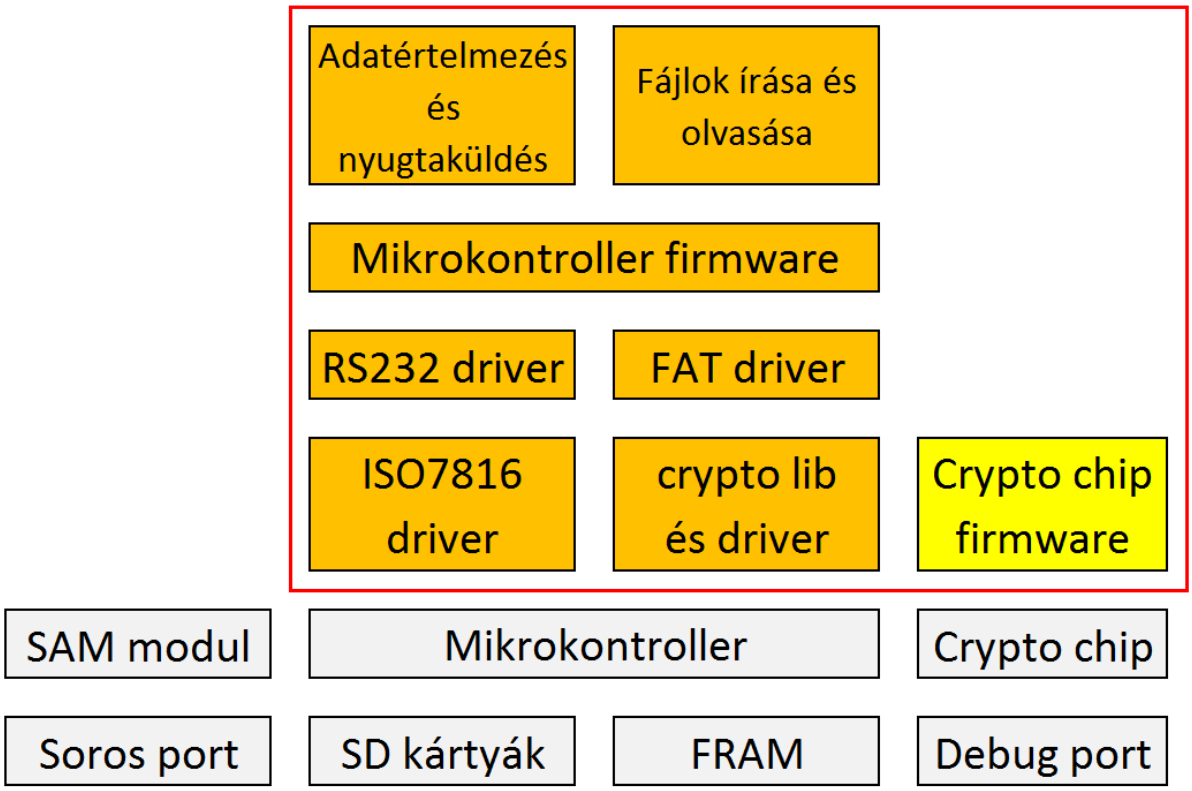
A termék célja, hogy a közösségi közlekedés jegykiadási területén, jegykiadáskor keletkezett bizonylatok (számlák, nyugták stb.) biztonságos és zárt rendszerben történő tárolását, illetve a tárolt adatok külső eszközre történő archiválását biztosítsa a 23/2014. (VI. 30.) NGM rendelet 17.§ (1) bekezdésben szabályozottak szerint.

Fontosabb funkciók:

- megőrzésre szánt adatok (bizonylatok - kinyomtatott számlák, nyugták- másodpéldányai) fogadása, tárolása;
- megőrzött bizonylatokat tároló állományok (másodpéldányok) digitális aláírása (utólagos módosítás kizárása);
- másodpéldányok fizikai védelme (EMT lezárása –tokozása-, plombálás);
- tárolt dokumentumok lekérdezésének biztosítása (soros porton, EMT protokoll segítségével).

I.3. A TOE biztonsági környezete és határai

A TOE az EMT-n futó szoftver (a mikrokontrollerhez feltöltött firmware-rel együtt). Az alábbi ábra szemlélteti az implementációt és a TOE határát:



1. ábra A TOE alkotóelemei, definíciója és határvonala (piros vonallal jelölve)

Minden más eszköz az EMT architektúrában (a hardverelemek, mint a mikrokontroller, az SD kártyák, a crypto chip, a SAM modul, az FRAM és a tápellátás) a működési környezet részének tekinthető. Ezért a felsorolt elemek nem részei a TOE-nak. Különösen, a szervizes munkaállomása és a szoftvere kívül esnek a TOE határán.

Az EMT TikettPro fizikai interfészei

Az EMT modul három interfésszel rendelkezik:

- Kommunikációs port: 10 pines csatlakozóval rendelkező soros port, amelyen keresztül a kommunikáló fél (jegykiadó gép) csatlakozni képes az EMT modulhoz. Normál működés esetén ezen a porton érkezik minden hasznos adat, amit az EMT modulnak tárolnia és őriznie kell.
- Debug port: egy pines csatlakozóval rendelkező soros port, amelyen keresztül a szervizes munkatárs a szerviz funkciókat el tudja érni, inicializálni, illetve karban tudja tartani az eszközt. Szerviz üzemben ezen a porton keresztül történik a firmware feltöltése, az eszköz inicializálása (nyugtakiadó géphez rendelése), valamint a hardver diagnosztizálása (ha korábban blokkolt állapotba került az eszköz).
- SD kártya csatlakozási felület: az EMT modulban az adatok tárolása SD kártyákon történik. Az SD kártya természeténél fogva eltávolítható. Az eltávolításra csak a doboz megbontása után van lehetőség, így a dobozon lévő plomba/matrica érvényessége igazolja az SD kártyák sértetlenségét. Az SD kártya kivételével az SD kártya bármely szabványos SD kártya olvasó által olvasható, azon FAT16, vagy FAT32 fájlrendszeren lévő fájlokban a nyugtainformáció és a napló is rendelkezésre áll.

I.4. A rendszer főbb komponensének azonosítása

Értékelt TOE verzió:

Fájlnév	Verzió	SHA256 lenyomat
2.11.68.68.bin	V2.11.68.68	0A4D776287881E85209095897C33D9C9 80B69070B1AAB1A029A8B0F78A299CA1

II. A tanúsítás jellemzése

Jelen tanúsítás a biztonsági előirányzatában (ST) lefektetetett követelmények teljesülését vizsgálja.

II.1. Az alkalmazott értékelési módszer

A TikettPro EMT modul 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 feleltethető meg.

II.2. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Rendszer Értékelési Jelentés:

- TikettPro EMT modul V2.11.68.68 ÉRTÉKELÉSI JELENTÉS v1.0

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
EMT_modul_STv10.docx	1.0
EMT_modul_ADV_ARC.docx	1.0
EMT_modul_ADV_FSP.docx	1.0
EMT_modul_ADV_TDS.docx	1.0
EMT_modul_ALC_CM.docx	1.0
EMT_modul_ALC_DEL.docx	1.0
EMT_modul_ALC_DVS.docx	1.0
EMT_modul_ALC_LCD.docx	1.0
EMT_modul_ATE_COV.docx	1.0
EMT_modul_ATE_FUN.docx	1.0
Üzemeltetői_kézikönyv_v1.0_pdf.doc	1.0
TikettPro_EMT_telepitesi_leiras_v1.6.docx	1.6
tikettpro_emt_rendszerleiras_v2.10.doc	2.10
tpEMT_tesztelesi_dokumentacio_v1.2_tanusitasi_tesztek.doc	1.2

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 alap támadó képességgel rendelkező támadónak.

Értékelői feladatelem	határozat
AVA_VAN.2: Sebezhetőség vizsgálat	megfelelt

IV. Következtetések

Az értékelés fő következtetése az alábbi:

A TikettPro EMT modul V2.11.68.68 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés eredménye alapján a Tanúsító megállapítja, hogy a TikettPro EMT modul V2.11.68.68, mint informatikai biztonsági funkciókat megvalósító szoftver termék megfelel a KIB 28-as Ajánlásában szereplő MIBÉTS módszertan szerinti fokozott biztonsági szintnek (ami megfeleltethető a CC EAL 3-es szintjének).

V. A biztonságos felhasználás feltételei

V.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 TikettPro EMT modul nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezete teljesítse) az alábbiak:

OE.MEGBÍZHATÓ_ADMIN: A TOE adminisztrátorának megbízhatónak kell lennie és maradéktalanul követnie kell a munkautasításokban foglalt utasításokat.

OE.RIASZTÁS: A TOE adminisztrátorának a hibajelzés után a lehető leghamarabb vizsgálnia és értékelnie kell a kritikus naplóbejegyzéseket, amelyeket a TOE állított elő és tárolt.

OE.PUBLIKUS_KULCS: A szervizesnek kötelessége a publikus kulcsot kinyerni a TOE-ból és azt megfelelő módon tárolni.

OE.NAPLÓ_ANALÍZIS: A TOE központi adminisztrátorának rendszeres időközönként analizálnia kell a TOE által generált naplóbejegyzéseket, ellenőriznie kell a napló integritását és a naplóban foglaltaknak megfelelően reagálnia kell.

OE.SZERVIZ_INTERVALLUM: A TOE szervizei közötti időnek A telepítési útmutatóban meghatározottnak kell lennie ahhoz, hogy az eddigiekben megfogalmazott biztonsági célok teljesülhessenek.

OE.TOE_FIZIKAI_KÖRNYEZET: A TOE olyan helyre van beépítve, ahonnan illetéktelenek csak aránytalanul nagy erőforrás igénybevételével tudnák csak kiszerelni.

OE.HW: A TOE olyan eszközön legyen implementálva, mely alkalmas az EMT modulban lévő szoftverek futtatásához, a fenyegetések kivédéséhez.

OE.SW_FEJLESZTÉS_BIZTONSÁGA: A TOE szoftver frissítéseit biztonságos, megbízható környezetben hozzák létre megbízható eszközökön. Csak arra feljogosított személy férjen hozzá ezekhez az eszközökhöz és a szoftverekhez.

OE.TOE_SZÁLLÍTÁS: A TOE-t csak biztonságos módon, emberi felügyelet mellett lehet a szerviz helyszínéről a nyugtakiadó géphez és viszont szállítani.

OE.KRIPTOGRÁFIAI_MEGFELELÉS: A TOE senkinek sem teheti láthatóvá az adatelem privát kulcsait. A TOE nem biztosíthat interfészt a megosztott kulcsok kinyerésére sem az üzemi használat során (az üzemi tartományban).

OE.TÁRTERÜLET: A nyugtaadatok és a napló tárolására szolgáló SD kártya kapacitása kellően nagy legyen, hogy ne következhessen be adatvesztés a TOE szervizintervallumán belül.

OE.BIZTONSÁGOS_KME: A TOE központi menedzsment eszköze biztonságosan van konfigurálva és használva, különösen az alábbi komponensek vonatkozásában: az operációs rendszere naprakész, a legújabb frissítések telepítve vannak az operációs rendszer gyártójának ajánlásai szerint, naprakész rosszindulatú kód elleni védelemmel rendelkezik. Az eszközön nem lehet más általános célú számítástechnikai szoftver (pl. fordítóprogramot nem tartalmazhat), illetve nem futhat rajta semmilyen szolgáltatás a működéséhez feltétlenül szükséges szolgáltatásokon túl.

OE.KME_HOZZÁFÉRÉS_SZABÁLYOZÁS: A TOE központi menedzsment eszköze (KME) hozzáférései kontrolláltak. A beléptetés nem automatikus és a használat visszaellenőrizhető (a KME naplózásának köszönhetően). A hozzáférés korlátozás alapja lehet fizikai (pl. fizikai hozzáférés korlátozás a KME-hez), és/vagy logikai (pl. az operációs rendszer által nyújtott azonosító és hitelesítő eszközzel).

OE.KME_KAPCSOLAT: A TOE és a TOE központi menedzsment eszköze közötti kapcsolatnak megbízható linknek kell lennie.

OE.KME_FIZIKAI_KÖRNYEZET: A TOE központi menedzsment eszköze biztonságos helyen van tárolva. A KME csak a TOE menedzsmentje esetén van használatban.

OE.ADATOK_ELLENŐRZÉSE: A TOE-ból kinyert adatok ellenőrzését biztosítani kell a KME eszközön.

OE.SW_VÉDELEM: Szoftver (firmware) frissítést a TOE-re telepítésével összefüggő feladatokat kizárólag a gyártói szerviz megbízható adminisztrátora végezheti.

V.2. Javaslatok

Az Értékelési Jelentés kilenc javaslatot tesz a termékkel kapcsolatban. A Tanúsító ezekkel a javaslatokkal egyetért és nyomatékosan felhívja a fejlesztő figyelmét azok figyelembevételére.

VI. Hivatkozások, rövidítések

VI.1. A követelményeket tartalmazó dokumentum

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)

VI.2. Figyelembe vett mértékadó dokumentumok

Common Criteria for Information Technology Security Evaluation (September 2012 -version 3.1, revision 4) – Part 1: Introduction and general model

Common Criteria for Information Technology Security Evaluation (September 2012 -version 3.1, revision 4) – Part 2: Security functional components

Common Criteria for Information Technology Security Evaluation (September 2012 -version 3.1, revision 4) – Part 3: Security assurance components

Common Methodology for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4)

VI.2.1. Rövidítések

ADV (Assurance: Development)	Fejlesztés értékelése
AGD (Assurance: Guidance documents)	Útmutató dokumentumok értékelése
ALC (Assurance: Life cycle support)	Életciklus támogatás értékelése
ASE (Assurance: Security Target)	Biztonsági előirányzat értékelése
ATE (Assurance: Tests)	Tesztelés értékelése
AVA (Assurance:Vulnerability assessment)	Sebezhetőségi elemzés értékelése
CC (Common Criteria)	Közös szempontok
CEM (Common Evaluation Methodology)	Közös értékelési módszertan
CM (Configuration management)	Konfiguráció kezelés
EAL (Evaluation Assurance Level)	Értékelési garanciaszint
ETR (Evaluation Technical Report)	Értékelési jelentés
KIB	Közigazgatási Informatikai Bizottság
MIBÉTS	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
ST (Security Target)	Biztonsági előirányzat
TOE (Target of Evaluation)	TOE, Értékelés tárgya