TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. (1123 Budapest, Kékgolyó u. 6.) mint a NAH által NAT-6-0048/2015 számon akkreditált terméktanúsító szervezet**,**

tanúsítja, hogy az

INFO*SYS Kft.

által fejlesztett

TikettPro EMT modul

V2.11.68.68

verziója

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).

Jelen Tanúsítvány a **HUNG-TJ-MIBÉTS-012-2016** számú
Tanúsítási Jelentés alapján került kiadásra.

Készült az INFO*SYS Kft. (*1063 Budapest, Szinyei Merse u. 5.*) megbízásából.
A Tanúsítvány regisztrációs száma: **HUNG-T-MIBÉTS-012-2016**
A Tanúsítvány érvényességének kezdete: *2016. december 06.*
A Tanúsítvány érvényességének vége: *2019. december 06*.
Jelen Tanúsítvány állításait éves felülvizsgálati eljárásokkal meg kell erősíteni.
A Tanúsítvány terjedelme 5 oldal az érvényességi feltételeket és egyéb jellemzőket tartalmazó mellékletekkel együtt.

Kelt: Budapest, 2016. december 06.

PH.

Endrődi Zsolt	Szűcs Ákos Balázs
Tanúsítási igazgató	Ügyvezető igazgató

1. számú melléklet

A Tanúsítvány érvényességi feltételei

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, amelyet 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 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.

2. számú melléklet

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)

3. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A Tanúsítvány a HUNG_TMK-1_20160726 azonosító számú, a terméktanúsító szervezet által működtetett, akkreditált tanúsítási rendszer alapján lett kiállítva.

Jelen Tanúsítvány az alábbi értékelési dokumentumok alapján került kiadásra:

Rendszer Értékelési Jelentés:

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

Az értékelés garancia szintje: MIBÉTS Fokozott (EAL3)

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)