TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft, mint a 9/2005. (VII.21.) IHM rendelet alapján a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt, a Nemzeti Média és Hírközlési Hatóság nyilvántartásában szereplő elektronikus aláírási termékeket tanúsító szervezet és a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

tanúsítja,

hogy a

WSG Szerver Üzemeltető Kft.

által kifejlesztetett

SMTR Tranzakció-kezelő és Archiváló szerver

v1.0.0

az 1.számú mellékletben áttekintett funkcionalitással, valamint
a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

alkalmas

a digitális archiválás szabályairól szóló 114/2007. (XII. 29.) GKM rendelet szerint fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumok megőrzésére

szolgáló informatikai rendszerben való felhasználásra.

Jelen tanúsítvány a HUNG-TJ-DA-001-2012. számú tanúsítási jelentés alapján került kiadásra.
Az értékelés garanciaszintje: MIBÉTS kiemelt (mely megfelel a CC EAL4 garanciaszintjének).
Készült a WSG Szerver Üzemeltető Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-DA-001-2012**.
A tanúsítás kelte: 2012. február 29.
A tanúsítvány érvényességi ideje: visszavonásig.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők,
összesen 9 oldalon.

PH.

Endrődi Zsolt Tanúsítási igazgató	dr. Szabó István Ügyvezető igazgató

1. számú melléklet

Az SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0 legfontosabb tulajdonságainak összefoglalása

Az SMTR v1.0 egy tranzakciós központ (SMTR rendszer) szolgáltatásait megvalósító egyedi szoftver termék, mely egyúttal egy speciális, zárt elektronikus archiválási szolgáltatást is megvalósít.

Az SMTR v1.0 az alábbi szolgáltatásokat biztosítja: Befogadás, Megőrzés, Kibocsájtás, Ellenőrzés, Kripto eszköz ellátás.

A tanúsítás logikai hatókörébe az alábbi funkciók és biztonsági funkciók tartoznak:
Funkciók:

- valós idejű tranzakciós adatok (tokenek) fogadása, dekódolása, sértetlenség és hitelesség szempontjából történő ellenőrzése, napi összesítése
- napi aggregált tranzakciós adatok fogadása, sértetlenség és hitelesség szempontjából történő ellenőrzése, az összesített valós idejű tranzakciós adatokkal való egybevetése
- napi aggregált tranzakciós adatok hosszú távú archiválása
- hiteles kimutatások készítése a napi aggregált tranzakciós adatokból
- távoli ellenőrzési felület biztosítása EO felhasználók számára
- hardver kriptográfiai eszköz egyedi előállítása a terminálok számára

Biztonsági funkciók:

- felhasználó azonosítás és hitelesítés
- hozzáférés ellenőrzés
- biztonsági naplózás
- távoli hozzáférési lehetőség biztosítása (GSA és EO felhasználók számára)
- helyi adminisztrálási lehetőség biztosítása (SSO, SO, TO és AO felhasználók számára)

2. számú melléklet

A biztonságos felhasználás feltételei

A tanúsítás pozitív következtetése az alábbi feltételek együttes teljesülésén múlik.[1]

1. számú feltétel:

Az IT és nem IT környezetnek biztosítania kell az alábbi szerepköröket:

- Rendszergazda: az operációs rendszereket, alkalmazásokat telepíti, és alap konfigurációt állít be,
- DB adminisztrátor: adatbázis jogokat ad ki, adatbázis visszaállítást végez,
- Napló auditor (rendszervizsgáló): naplót olvas és elemez,
- Operátor: a rendszer működését követi nyomon a monitoring segítségével, adatbázis mentést és log mentést végez.

Ezen szerepköröket különböző megbízható személyekre bízzák, akik ne töltsenek be egyetlen SMTR szoftver szerepkört sem.

A Rendszergazda, DB adminisztrátor, Napló auditor és Operátor szerepkörök azonosítása álnév alapján nem történhet.

A felhasználókat össze kell tudni kapcsolni a Rendszergazda, DB adminisztrátor, Napló auditor (rendszervizsgáló) és Operátor szerepkörökkel.

Érintett követelmények: [MA1.1] [MA1.2] [MA1.3] [IA1.4]

2. számú feltétel:

Egy biztonsági tisztviselő munkakört betöltő felhasználó nem lehet független rendszervizsgáló.

Érintett követelmény: [MA1.4]

3. számú feltétel:

Az IT és nem IT környezetnek biztosítania kell, hogy az SMTR szoftver működési környezetét alkotó rendszerelemek rendelkezzenek a helyes és biztonságos telepítéshez és működtetéshez szükséges útmutatókkal, illetve a rendszerben valósítsanak meg védelmet a vírusokkal és kártékony szoftverekkel szemben.

Érintett követelmény: [SO1.1]

4. számú feltétel:

Az IT és nem IT környezetnek a folyamatos működés biztosítása érdekében biztosítania kell, hogy:

- az éles helyszínen két párhuzamos, egymásnak tartalékot jelentő alrendszer fusson,
- egy monitoring rendszernek biztosítani kell az összes komponens állapotának és elérhetőségének figyelését,
- egy mentési és egy helyreállítási funkciónak biztosítani kell, hogy a mentésben tárolt adatok alapján a rendszer mentési időpontjában érvényes állapota visszaállítható.

Érintett követelmények: [SO2.1] [SO2.2] [SO2.3] [LA1.1] [LA1.2] [LA2.1] [LA2.2]

[1] Az érintett követelmények hivatkozásában a Nemzeti Hírközlési Hatóság Hivatala: Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre (2008. június) c. dokumentum jelöléseit alkalmaztuk.

5. számú feltétel:

Az üzemeltetési környezetnek megbízható (pontos és szinkronizált) időforrást kell biztosítania az SMTR számára, a naplózott események időpontjának pontos jelzésére, valamint az elektronikus archiválás befogadással és kibocsátással kapcsolatos időfüggő funkcióihoz. Az SMTR szoftveren kívüli elemek is ugyanezt a megbízható időforrást alkalmazzák a naplózott esemény idejének jelzésére.

Érintett követelmények: [SO3.1] [AA8.1] [AR1.3]

6. számú feltétel:

Az SMTR oldali IIS csak kölcsönös autentikációt elváró SSL kapcsolatot engedjen kiépíteni és az SMTR oldali tűzfal csak a játékszerverekhez regisztrált IP címről tegye lehetővé VPN kapcsolat kiépítését, a VPN-en belül csak kölcsönös autentikációt elváró SSL kapcsolatot engedjen kiépíteni. A gépi felhasználó (játékszerver) által kezdeményezett adatkapcsolat befejezése után az IIS a kiépített SSL session-t bontsa le. A kiépített SSL session lebontását az IIS megfelelő konfigurálásával kell biztosítani (pl. a ConnectionTimeout változó default 120 sec értékének meghagyásával).

Az SMTR szoftveren kívüli elemek felhasználói számára hozzáférés-ellenőrzést a környezetnek kell biztosítania.

Az SMTR szoftveren kívüli elemek által kezelt érzékeny maradvány információkat a környezetnek kell megvédenie.

Érintett követelmények: [IA1.1] [IA1.2] [IA1.5] [SA1.1] [SA1.2]

7. számú feltétel:

Biztosítani kell az SMTR szoftveren kívüli elemek felhasználóira a hitelesítő adatok egyediségét.

Érintett követelmény: [IA1.3]

8. számú feltétel:

Az SMTR szoftver humán felhasználói hitelesítő adataikat (2048 bites RSA magánkulcsok) a hardver kripto tokenen aktivizálják PIN kódjuk megadásával. A hardver kripto tokennek biztosítani kell a blokkolást (3 egymás utáni sikertelen hitelesítési kísérlet után). Az SMTR szoftveren kívüli elemek felhasználóira az elvárt blokkolást szintén a környezetnek kell biztosítania.

Érintett követelmények: [IA2.1] [KM3.1]

9. számú feltétel:

Az authentikációs RSA kulcsokat, az SMTR aláíró magánkulcsot és a terminál aláíró kulcsot CC tanúsított kriptográfiai eszközben kell előállítani és tárolni. A kulcs előállításnak minden esetben meg kell felelnie az ETSI ALGO csoport által kiadott TS 102 176-1 dokumentum aktuális verziójában leírt kriptográfiai követelményeknek. Az eszközök elosztását biztonságosan kell végezni.

Érintett követelmények: [KM1.2] [KM1.3] [KM2.1] [KM4.2] [KM6.2] [IA3.1]

10. számú feltétel:

Az IT és nem IT környezetnek biztosítani kell, hogy a kulcsok cseréje azok érvényességi ideje előtt hajtódjon végre. A több klónozott kriptográfiai hardver modulban tárolt TrHwEnc magánkulcs érvényessége a teljes életciklusra szól. Amennyiben valamelyik HSM modul elveszik vagy a magánkulcs egyéb módon kompromittálódik, valamennyi klónozott HSM modult meg kell semmisíteni.

A kód aláíró magánkulcs életciklusa a külső CA által rá kiadott tanúsítvány életciklusával megegyezik. Érvényességi ideje 2 év, melynek lejárta előtt a kódot újra alá kell írni egy új (vagy meghosszabbított) tanúsítványhoz tartozó magánkulccsal.

Érintett követelmény: [KM3.2]

11. számú feltétel:

Az IT és nem IT környezetnek biztosítani kell, hogy az alábbi kulcsok érvényessége az alábbi módon ellenőrzésre kerüljön.

- TrHwEnc RSA kulcsnak nincs tanúsítványa, érvényességét szervezeti eljárásokkal kell figyelni, 4 év után cserélni kell.
- kód aláíró magánkulcshoz tartozó tanúsítvány ellenőrzése a kódon lévő aláírásokat ellenőrző OS feladata.
- TrSwEnc1 és TrSwEnc2 RSA kulcsokhoz nincs tanúsítvány, a nyilvános kulcsok a Tranzakciós DLL-ben vannak, melyek szétosztását és ellenőrzését szervezeti eljárásokkal biztosítják.

Érintett követelmény: [KM3.3]

12. számú feltétel:

AZ SMTR rendszerben használt kulcsokat biztonságos törlési folyamatokkal kell megsemmisíteni oly módon, hogy többé azok ne legyenek visszanyerhetők amikor lejár az élettartamuk, vagy a rendszerből kivonásra kerülnek. A megsemmisítést dokumentálni kell.

Érintett követelmények: [KM5.1] [KM5.2] [KM5.3] [KM5.4]

13. számú feltétel:

Minden magán/titkos kulcsot biztonságosan kell tárolni. Az érvényesítő aláíró, igazolásokat aláíró, visszaigazolásokat aláíró magánkulcsok mentését vagy letétbe helyezését tiltani kell. A környezetnek biztosítania kell, hogy az infrastrukturális és rendszervezérlési kulcsok mentése és helyreállítása csak jogosult személy (pl. biztonsági tisztviselő) által hajtható végre.

A dekódoláshoz szükséges TrHwEnc magánkulcs klónozását (szoftveres generálás, majd több kriptográfiai eszközbe másolását) biztonságosan kell megvalósítani.

Érintett követelmények: [KM6.1] [KM6.3] [KM6.4] [KM6.5]

14. számú feltétel:

Az IT és nem IT környezetnek biztosítani kell az SMTR szoftver által generált naplóesemények tekintetében az alábbiakat:

- a naplóeseményeknek egy független syslog szerverre, valamint egy tartalék naplóba továbbítását (TCP protokoll alkalmazásával),
- a naplóesemények illetéktelen módosításának, törlésének megakadályozását (a napló sorok láncolt formában történő digitális aláírásával),
- a napló tárolási hibák miatt szükséges naplóesemények generálását,
- a naplóesemények megjelenítését (szűrő és kereső funkciókkal kiegészítve) egy erre felhatalmazott szerepkört betöltő felhasználó (rendszervizsgáló) számára,
- a naplózott események alapján a biztonság potenciális megsértésének észlelése esetén riasztás (e-mail értesítés a rendszergazda számára) generálását,
- a naplóállományok archiválását legalább 90 napra,
- az archivált naplóállományokban az események típusa szerinti keresési lehetőséget,
- az archivált naplóállomány bejegyzéseinek védelmét a módosítástól és a jogosulatlan törléstől.

Érintett követelmények: [AA1.1] [AA2.1] [AA2.2] [AA4.1] [AA4.2] [AA5.1] [AA5.2] [AA6.1] [AA7.1], [AR1.1] [AR1.2] [AR1.4] [AR2.1] [AR3.1] [LA1.1] [LA1.2] [LA2.1] [LA2.2]

15. számú feltétel:

Az IT és nem IT környezetnek biztosítani kell az SMTR szoftveren kívüli elemek naplózására az elvárt információk rögzítését, valamint azt, hogy ne naplózzanak le védetlen formában kritikus biztonsági paramétereket.

Érintett követelmények: [AA1.1] [AA3.1]

16. számú feltétel:

Az IT és nem IT környezetnek biztosítani kell, hogy

- az SMTR rendszer rendelkezik egy mentési funkcióval,
- a mentésben tárolt adatok alapján a rendszer mentési időpontjában érvényes állapota visszaállítható, az archivált adatokhoz tartozó adatbázist is beleértve,
- a mentés védett a módosítás és a jogosulatlan törlés, valamint a hozzáférhetetlenné válás ellen,
- a mentésben kritikus biztonsági paraméterek és más bizalmas információk csak titkosított formában tárolhatók,
- megfelelő eljárások biztosítsák, hogy a mentett adatok a rendszer és a benne tárolt adatok mentéskori állapotát hitelesen rögzítik,
- az SMTR rendszer rendelkezzen egy helyreállítási funkcióval, amely képes egy mentésből helyreállítani a rendszert,
- a rendszerüzemeltető érhesse el a mentési és a helyreállítási funkciókat.

Érintett követelmények: [BK1.1] [BK1.2] [BK1.3] [BK2.1] [BK2.2] [BK2.3] [BK3.1] [BK3.2]

17. számú feltétel:

Az SMTR rendszer TSA1 és TSA2 paramétereit úgy kell konfigurálni, hogy mindkét TSA minősített időbélyeg szolgáltató legyen.

Érintett követelmények: [IN2.5] [LA4.1]

18. számú feltétel:

Az IT vagy nem IT környezetnek biztosítani kell, hogy a Rendszergazdák vagy a DB adminisztrátorok az archivált napi aggregált tranzakciós adatok tartalmát ne ismerhessék meg.

Érintett követelmény: [LA3.1]

19. számú feltétel:

Legalább évente az AO aktivizálja a „Felülhitelesítés indítása” funkciót.

Az üzemeltetési környezetnek biztosítania kell egy olyan eljárásrendet, mely garantálja, hogy az adatok az off-line adathordozókról (szalagok, cd-k stb.) is törlődjenek a megőrzési idő lejártát követő egy éven belül felülírással vagy megsemmisítéssel..

Érintett követelmény: [LA6.1]

20. számú feltétel:

Az SMTR szoftver működési környezetét alkotó rendszerelemek naplózzák az alábbiakat:

- az archivált adatok rendelkezésre állásának megőrzésével kapcsolatos, biztonsági szempontból jelentős események (mentés, helyreállítás, load-balance problémák a két párhuzamos hardveren, stb.),
- az archivált adatok sértetlenségének megőrzésével kapcsolatos, biztonsági szempontból jelentős események (pl. helyreállítás).

Érintett követelmény: [LA7.1]

3. számú melléklet

A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások

1. A MIBÉTS értékelési módszertana (mely a Közigazgatási Informatikai Bizottság 28. számú ajánlásának /Az E-közigazgatási Keretrendszer követelménytár, 2009/ részét képezi az alábbi címen: Termékekre vonatkozó értékelési módszertan)
2. Nemzeti Hírközlési Hatóság Hivatala: Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre (2008. június)
3. Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model - CCMB-2009-07-001 - Version 3.1, Revision 3Final, July 2009.
4. Common Criteria for Information Technology Security Evaluation, Part 2:Security Functional Components - CCMB-2009-07-002 - Version 3.1, Revision 3 Final, July 2009.
5. Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Components - CCMB-2009-07-003 - Version 3.1, Revision 3 Final, July 2009.
6. Common Methodology for Information Technology Security Evaluation, Evaluation methodology - CCMB-2009-07-004 - Version 3.1, Revision 3 Final, July 2009.
7. ISO/IEC 15408-1: 2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
8. ISO/IEC 15408-2: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
9. ISO/IEC 15408-3: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
10. ISO/IEC 18045: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Methodology for IT Security Evaluation

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Biztonsági előirányzat 1.00
- Az előkészítő eljárások leírása: Telepítési kézikönyv - Tranzakciós szerver v1.0.0
- Üzemeltetési felhasználói útmutatók:
- Felhasználói kézikönyv - Desktop alkalmazások v1.0.0
- Felhasználói kézikönyv - Külső ellenőr webalkalmazás v 1.0.0
- Felhasználói kézikönyv - Játékszerver adminisztrátor webalkalmazás v1.0.0
- Felhasználói kézikönyv - HSM alkalmazások v1.0.0
- Biztonsági szerkezet leírás v 1.00
- Funkcionális specifikáció v1.00
- TOE terv v1.00
- Megvalósítási reprezentáció v1.00
- Saját fejlesztésű forráskódok v1.0.0
- Konfiguráció lista v1.00
- A konfiguráció kezelés dokumentációja v1.00
- A fejlesztés biztonság dokumentációja v1.00
- Az életciklus meghatározás dokumentációja v1.00
- A fejlesztő eszközök dokumentációja v1.00
- A szállítási eljárások leírása v1.00
- A tesztelésre alkalmas TOE v1.0.0
- Tesztelési terv v1.0.0
- Tesztelési dokumentáció v1.0.0
- Teszt lefedettség elemzés v1.00
- Teszt mélység elemzés v1.00

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0 ÉRTÉKELÉSI JELENTÉS v1.0
- Az SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0 rendszer megfelelése az elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó műszaki biztonsági követelményeknek v1.0

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0 a MIBÉTS módszertana szerint került független értékelésre és tanúsításra.

Az értékelés garanciaszintje

MIBÉTS kiemelt (mely megfelel a CC EAL4 garanciaszintjének)