TANÚSÍTÁSI JELENTÉS

SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0

/ Elektronikus archiválási szoftver /

HUNG-TJ-DA-001-2012

Verzió:	1.0
Fájl:	Hung-TJ-DA-001-2012_v10.pdf
Minősítés:	Nyilvános
Oldalak:	22

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2012.02.08	A szerkezet felállítása
v0.02	2012.02.11	A tanúsítás eredményeit tartalmazó teljes változat
v0.03	2012.02.13	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v1.0	**2012.02.29**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői

Az értékelt termék neve:	**SMTR Tranzakció-kezelő és Archiváló szerver v1.0**
Verzió szám:	**v1.0.0**
Rövid elnevezés:	**SMTR v1.0**
Az értékelt termék típusa:	Elektronikus archiválási szoftver
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2012. február 8.
Az értékelés módszere:	MIBÉTS /CEM, Common Evaluation Methodology, v3.1/
Az értékelés garanciaszintje:	MIBÉTS kiemelt /mely megfelel a CC EAL4 szintnek/
Az értékelt termék funkcionalitása:	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 (a biztonsági előirányzatában részletezett módon) az alábbi szolgáltatásokat biztosítja: Befogadás, Megőrzés, Kibocsájtás, Ellenőrzés, Kripto eszköz ellátás.
Mértékadó jogszabály	114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól

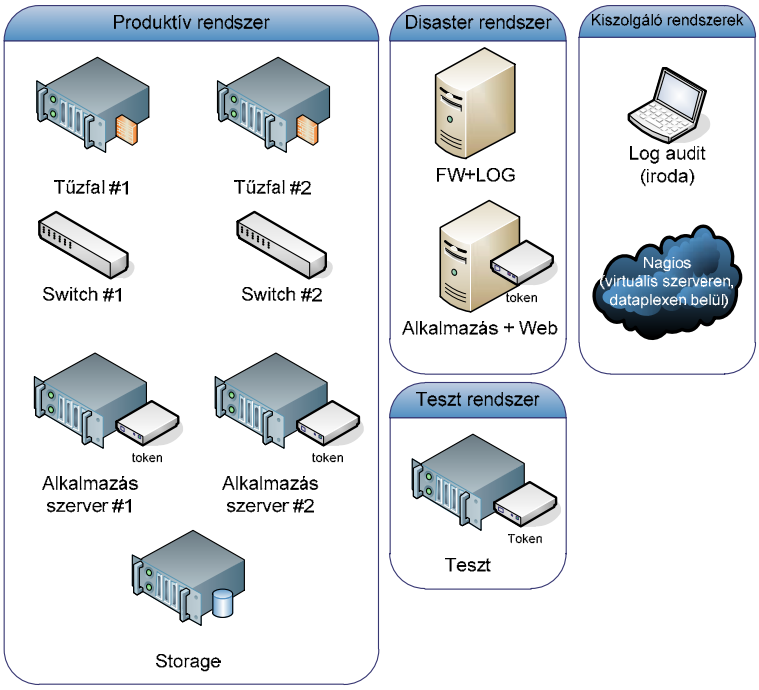
1.2 Azonosítás

Fejlesztő neve:	**WSG Szerver Üzemeltető Kft.**
Az értékelt termék neve:	**SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0**
Verzió szám:	**1.0.0**

1.3 A tanúsítás tárgya, biztonsági környezete és határai

Az SMTR v1.0 egy tranzakciós központ (SMTR rendszer) szolgáltatásait megvalósító egyedi szoftver termék, mely egyúttal egy speciális, zárt elektronikus archiválási szolgáltatást is megvalósít, biztosítva a következő szolgáltatásokat Befogadás, Megőrzés, Kibocsájtás, Ellenőrzés, Kripto eszköz ellátás.

Az SMTR v1.0 egy nagyobb informatikai rendszer (az SMTR rendszer) része. Az 1. ábra az SMTR rendszer fizikai architektúráját mutatja, ezen belül a jelen tanúsítási jelentés tárgyát képező SMTR v1.0 az alkalmazás szervereken futó speciális szoftver.



1. ábra: A teljes SMTR rendszer fizikai architektúrája

Az értékelés tárgya biztonsági környezetéhez tartozik az ábrán jelzett elsődleges helyszín (produktív rendszer), másodlagos helyszín (disaster vagy katasztrófa rendszer), teszt rendszer, illetve kiszolgáló rendszerek.

Szintén a környezet (tehát nem a TOE) része a produktív, a disaster és a teszt rendszerekben működtetett egyéb hardver és szoftver eszközök (tűzfalak, switch-ek, storage, log audit, Nagios, egyéb hálózati elemek), sőt az alkalmazás szerver hardver kiszolgálója és operációs rendszere is.

Az értékelés tárgyának 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)

Az SMTR v1.0 telepítő készletének elemei és azok lenyomata:

Arch.Service.Setup.msi
SHA256 Hash: E4F60D6AC1A50727A5CA986AF6A25E6B1E55E98CCB5737A483182CD4BDC31323

CryptoAuth.HsmStarter.Setup.msi
SHA256 Hash: 79EB59CAF8A1D364C763A62AA1A5D3A8B39F8A8BC065A99394FCD0173E33DB21

CryptoAuth.HsmTool.Setup.msi
SHA256 hash: 7D1571E1DC2B4CB08EFCBE366DC65F31FD96347E2C7074BA4967CCFDF71D9F4

CryptoAuth.Service.Setup.msi
SHA256 hash: 4D25CFD0E1B0EC256574B04182A1936CA47A296D751F5EA991A6E94006D62325

SMTR.Security.WS.zip
SHA256 hash: 2BB8E747CFC4A5B7C34E59723F527CFBB634A2041A69394B35718EC2CA6E072A

SMTRAdmin.Win.Setup.msi
SHA256 hash: E3B88B6261BF6AC3F61C6ED49C07B0A41790D876AE5AEB2A13AEFC6601F1BC46

SMTRAdmin.WS.zip
SHA256 hash: 0552FBD9106FE142BE4C4F8A13F223CD7A1CF2C77E591C4E95FEC69C7482F980

SMTRExternal.Web.zip
SHA256 hash: 7AE9428648C27C41B2771515EEDE8E11AA1DC6612C40D00549FEA1D13E389C86

SMTRExternal.WS.zip
SHA256 hash: 5E00131422CCDE6A10B13D9E4B0BEFA6DB2616C5944687B0811B6EE1A510667E

SMTRGameServer.Internal.Web.zip
SHA256 hash: C78C9BFB0EC34DFE91E9002785540682538369BEC1A27F260834DB189B2CD231

SMTRGameServer.Internal.WS.zip
SHA256 hash: 30AD74E9D7F2AD30D9BD0913D8C93CBFDE59FCABFF7F5FC7A53488605DDB58B9

SMTRGameServer.Web.zip
SHA256 hash: 0124936E8197D54FC074DC750E7A84BEF82FA25E6725BCB7492E5E3C88A997FA

SMTRGameServer.WS.zip
SHA256 hash: 3598F417901142545EF26744F8C3BF3963B19C45C9C93231FBD781F7F06682B6

2 A tanúsítás jellemzése

2.1 Az alkalmazott tanúsítási és értékelési módszer

Az alábbiakban az értékelés és tanúsítás során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

Az elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó műszaki biztonsági követelményeknek való megfelelésnek értékelési és tanúsítási módszertana

Jelen tanúsítási jelentés az alábbi meghatározó dokumentumban definiált követelményrendszert tekinti viszonyítási alapként:

- Nemzeti Hírközlési Hatóság Hivatala: Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre (2008. június)

A követelményrendszer egyes elemeit az 114/2007. (XII. 29.) GKM rendelettel (a digitális archiválás szabályairól) összhangban az alábbiak szerint módosítottuk:

- Archivált adat érvényességi láncára minősített szolgáltató által kibocsátott időbélyegző elhelyezése elegendő. Érintett követelmények [LA4.1] és [LA4.2]
- Az elektronikus úton kiállított igazolásokat az archiválási szolgáltatónak *fokozott biztonságú elektronikus aláírással*, valamint minősített szolgáltató által kibocsátott időbélyegzővel kell ellátni. Érintett követelmény [DS2.5]

Valamennyi követelmény esetében jelen tanúsítási jelentés külön-külön határozatot hoz az alábbi három lehetséges pozitív eredménnyel:

- az adott követelményt az SMTR Tranzakció-kezelő és Archiváló szerver (SMTR szoftver) **teljesíti,**
- az adott követelményt az SMTR Tranzakció-kezelő és Archiváló szerver (SMTR szoftver) **támogatja** (az informatikai vagy a nem informatikai környezetre megfogalmazott működtetési feltétel teljesülése esetén a követelmény teljesül),
- az SMTR Tranzakció-kezelő és Archiváló szerver (SMTR szoftver) az adott követelmény kielégítését az IT és nem IT **környezettől várja el** (vagyis ezen követelményt az SMTR szoftver nem támogatja, azt az informatikai rendszer más elemeinek kell kielégíteni).

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

A "támogatja" és a „környezettől várja el” határozat olyan feltételt támaszt (nem az értékelés tárgyára, hanem annak működtetési környezetére, vagy egy kiegészítő termékre), melynek kielégítése szükséges a mértékadó jogszabályban előírt követelmények teljesüléséhez és jelen tanúsítás érvényességéhez.

MIBÉTS termékértékelési és tanúsítási módszertan

Az SMTR v1.0 értékelése során az informatikai termékek technológia szempontú biztonsági értékelésére kidolgozott MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertant használtuk.

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”.

A MIBÉTS értékelési módszertana az alábbi nemzetközi mértékadó dokumentumok honosított változata (CC: [1]- [3], CEM: [4])

[1]: Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 1: Introduction and general model
[2]: Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 2: Security functional components
[3]: Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 3: Security assurance components
[4]: Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2)

Az [1]- [4] dokumentumokat az alábbi nemzetközi szabványként is elfogadták:

[5]: ISO/IEC 15408-1: 2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
[6]: ISO/IEC 15408-2: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
[7]: ISO/IEC 15408-3: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
[8]: ISO/IEC 18045: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Methodology for IT Security Evaluation

Az értékelés garanciaszintje MIBÉTS kiemelt, mely a CC (Common Criteria, MSZ ISO/IEC 15408) szerinti EAL4-es szintnek felel meg.

2.2 A tanúsításhoz felhasznált értékelési jelentések azonosítása

Szoftverbiztonsági értékelési jelentés:

> SMTR Tranzakció-kezelő és Archiváló szerver v1.0.0 ÉRTÉKELÉSI JELENTÉS v1.0 /SMTR_ETR_v1.0.doc/

Mértékadó követelményrendszernek való megfelelés elemzés:

> 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 /SMTR_Conformance_v1.0.doc/

2.3 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

Fejlesztői dokumentációk		
cím	Filenév (.pdf)	verzió
Biztonsági előirányzat	SMTR_biztonsagi_eloiranyzat_v1.00	1.00
Az előkészítő eljárások leírása: Telepítési kézikönyv - Tranzakciós szerver	SMTR_telepitesi_kezikony_v1.0.0_20120206	1.0.0
Üzemeltetési felhasználói útmutatók: Felhasználói kézikönyv - Desktop alkalmazások Külső ellenőr webalkalmazás Játékszerver adminisztrátor webalkalmazás HSM alkalmazások	 SMTR_felhasznaloi_kezikony_desktopapp_v1.0.0 SMTR_Felhasznaloi_kezikonyv_eowebapp_v1.0.0 SMTR_Felhasznaloi_kezikonyv_gsawebapp_v1.0.0 SMTR_Felhasznaloi_kezikonyv_hsm_v1.0.0	 1.0.0 1.0.0 1.0.0 1.0.0
Biztonsági szerkezet leírás	SMTR_biztonsági_szerkezet_v1.00_20120202	1.00
Funkcionális specifikáció: Funkcionális specifikáció áttekintés Használati esetek Használati eset naplózások Interface Specification	 SMTR_funkcionalis_specifikacio_v1.00_20120201 SMTR_UseCase_dokumentacio_v0.7_20120120 SMTR_UseCase_Log_v0.2_20120206 SMTR_Interface_specification_v1.7_20111025	 1.00 0.7 0.2 1.7
TOE terv: TOE terv áttekintés Rendszerterv	 SMTR_TOE_terv_v1.00_20120206 SMTR_Rendszerterv_v0.8_20120129	 1.00 0.8
Megvalósítási reprezentáció	SMTR_megvalositasi_reprezentacio_v1.0	1.00
Saját fejlesztésű forráskódok	\\Hungserver1\transserv\Deliverables\ADV\Source\ src_20120206_v1.0.0 alkönyvtár	1.0.0
Konfiguráció lista	SMTR_konfiguracio_lista_v1.00_20120206	1.00
A konfiguráció kezelés dokumentációja	SMTR_konfiguracio_kezeles_v1.00_20120202	1.00
A fejlesztés biztonság dokumentációja	SMTR_fejlesztes_biztonsag_v1.00_20120206	1.00
Az életciklus meghatározás dokumentációja	SMTR_eletciklus_meghatarozas_v1.00_20120206	1.00
A fejlesztő eszközök dokumentációja	SMTR_ fejleszto_eszkozok_v1.00_20120206	1.00
A szállítási eljárások leírása	SMTR_szallitasi_dokumentacio_v1.00_20120206	1.00
A tesztelésre alkalmas TOE	\\Hungserver1\transserv\Deliverables\TOE\v1.0.0_ 20120206 alkönyvtár	1.0.0
Tesztelési terv: Teszt terv Archiválás teszt terv Biztonsági teszt terv	 SMTR_TesztTerv_v0.4_20120120 SMTR_ArchivalasTesztTerv_v0.02_20120201 SMTR_BiztonsagiTesztTerv_v0.02_20120105	 0.05 0.02 0.03
Tesztelési dokumentáció	\\Hungserver1\transserv\Deliverables\Deliverables_ final\ATE\Tesztelesi_eredmenyek_20120206 alkönyvtár (benne 28 jegyzőkönyv)	1.0.0
Teszt lefedettség elemzés	SMTR_teszt_lefedettseg_v1.00_20120206	1.00
Teszt mélység elemzés	SMTR_teszt_melyseg_v1.0	1.00

2.4 Az értékelési folyamat tanúsítási szempontú ellenőrzése

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

- az értékelési folyamtok módszertani szempontú ellenőrzésével;
- különböző szakértői megbeszéléseken való részvétellel;
- az értékelői teszteléseken való részvétellel.

3 Megfelelőségi nyilatkozatok

3.1 Módszertani megfelelőség

A felhasznált Biztonsági előirányzat a Common Criteria (CC) 3.1 revision 3 verzió alapján készült.

Az Értékelési jelentés a KIB 28-as Ajánlásában szereplő MIBÉTS módszertan (mely megfelel a Common Criteria (CC) 3.1 revision 2. verziónak) alapján készültek.

A felhasznált Biztonsági előirányzat megfelel a CC 2. részének, megfelel a CC 3. részének, és megfelel a MIBÉTS kiemelt garanciaszint (a CC EAL4 értékelési garanciaszint) követelményeinek.

A megfeleltetés elemzést alátámasztja a rendszer szoftverbiztonsági értékelése.

4 Biztonsági követelményeknek való megfelelés

Az alábbiakban bemutatásra kerül az elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményeknek történő megfeleltetés eredménye.

Azo-nosító	NHH ajánlás követelménye	Határozat (teljesíti/ támogatja/ környezettől várja el)	Feltétel
Általános biztonsági követelmények			
MA: Menedzselés (Management)			
MA1	Rendszer- és biztonságkezelés		
	[MA1.1]	támogatja	1. számú feltétel
	[MA1.2]	támogatja	1. számú feltétel
	[MA1.3]	támogatja	1. számú feltétel
	[MA1.4]	környezet	2. számú feltétel
SO: Rendszerek és működésük (Systems and Operations)			
SO1	Üzemeltetés menedzselése [SO1.1]	támogatja	3. számú feltétel
SO2	A folyamatos szolgáltatás biztosítása		
	[SO2.1] csak minősítettre	támogatja	4. számú feltétel
	[SO2.2] csak minősítettre	környezet	4. számú feltétel
	[SO2.3] csak minősítettre	környezet	4. számú feltétel
SO3	Időszinkronizáció [SO3.1]	környezet	5. számú feltétel
IA: Azonosítás és hitelesítés (Identification and Authentication)			
IA1	A felhasználó hitelesítése		
	[IA1.1]	támogatja	6. számú feltétel
	[IA1.2]	támogatja	6. számú feltétel
	[IA1.3]	támogatja	7. számú feltétel
	[IA1.4]	támogatja	1. számú feltétel
	[IA1.5]	környezet	6. számú feltétel
IA2	A hitelesítési hiba kezelése [IA2.1]	környezet	8. számú feltétel
IA3	A titkok ellenőrzése [IA3.1]	környezet	9. számú feltétel
SA: Rendszer-hozzáférés ellenőrzés (System Access control)			
SA1	Rendszer-hozzáférés ellenőrzés		
	[SA1.1]	támogatja	6. számú feltétel
	[SA1.2]	környezet	6. számú feltétel
KM: Kulcs kezelés (Key Management)			
KM1	Kulcselőállítás [KM1.1]	N/A	
	[KM1.2] - [KM1.3]	környezet	9. számú feltétel
KM2	Kulcselosztás [KM2.1]	támogatja	9. számú feltétel
KM3	Kulcshasználat		
	[KM3.1]	támogatja	8. számú feltétel
	[KM3.2]	támogatja	10. számú feltétel
	[KM3.3]	támogatja	11. számú feltétel
KM4	Kulcscsere [KM4.1] - [KM4.2]	támogatja	9. számú feltétel
KM5	Kulcs megsemmisítése [KM5.1] - [KM5.4]	környezet	12. számú feltétel
KM6	Kulcs tárolása, mentése és helyreállítása [KM6.1]	támogatja	13. számú feltétel
	[KM6.2]	támogatja	9. számú feltétel
	[KM6.3]	támogatja	13. számú feltétel
	[KM6.4]	támogatja	13. számú feltétel
	[KM6.5]	támogatja	13. számú feltétel
KM7	Kulcs archiválása [KM7.1]	teljesíti	
AA: Naplózás (Accounting and Auditing)			
AA1	Napló adatok generálása [AA1.1]	támogatja	14. és 15. számú feltételek

AA2	A napló adatok garantált rendelkezésre állása [AA2.1] - [AA2.2]	környezet	14. számú feltétel
AA3	Naplózási paraméterek [AA3.1]	támogatja	15. számú feltétel
AA4	A napló választható áttekintése [AA4.1] -[AA4.2]	környezet	14. számú feltétel
AA5	Korlátozott naplómegtekintés [AA5.1] - [AA5.2]	környezet	14. számú feltétel
AA6	Riasztás generálása [AA6.1]	környezet	14. számú feltétel
AA7	A napló adatok sértetlenségének garantálása [AA7.1]	környezet	14. számú feltétel
AA8	A napló időbejegyzéseinek garantálása [AA8.1]	támogatja	5. számú feltétel
AR: Archiválás (Archiving)			
AR1	Archív adatok generálása [AR1.1]-[AR1.2] [AR1.3] [AR1.4]	környezet támogatja támogatja	14. számú feltétel 5. számú feltétel 14. számú feltétel
AR2	Szelektálható keresés [AR2.1]	környezet	14. számú feltétel
AR3	Az archivált adatok sértetlensége [AR3.1]	környezet	14. számú feltétel
BK: Mentés és helyreállítás (Backup and Recovery)			
BK1	Mentés generálása [BK1.1] - [BK1.3]	környezet	16. számú feltétel
BK2	A mentési információ sértetlensége és bizalmassága [BK2.1] [BK2.2] [BK2.3]	 környezet támogatja környezet	 16. számú feltétel 16. számú feltétel 16. számú feltétel
BK3	Helyreállítás [BK3.1] - [BK3.2]	környezet	16. számú feltétel
GE: Általános követelmények (General)			
GE1	A szolgáltatások által létrehozott üzenetek védelme [GE1.1]	teljesíti	
GE2	Az archiválás szolgáltatást igénybe vevők regisztrációja [GE2.1]-[GE2.4]	teljesíti	
Biztonsági követelmények az Archiválási szolgáltató szolgáltatásaira			
IN: A befogadással kapcsolatos funkciók követelményei (Ingest)			
IN1	Archiválásra benyújtott információk fogadása [IN1.1] [IN1.2]	 teljesíti teljesíti	
IN2	Archiválásra benyújtott információk ellenőrzése [IN2.1] [IN2.2] [IN2.3] [IN2.4] [IN2.5] [IN2.6]	 teljesíti teljesíti teljesíti teljesíti támogatja teljesíti	 17. számú feltétel
IN3	A megőrzési időtartam kezelése, befejezése [IN3.1]	teljesíti	
IN4	Archiválással kapcsolatosan benyújtott információk visszaigazolása [IN4.1] [IN4.2] [IN4.3] [IN4.4] [IN4.5] [IN4.6]	 teljesíti teljesíti teljesíti teljesíti teljesíti teljesíti	
IN5	A hozzáférési jogosultságok kezelése [IN5.1]	teljesíti	
IN6	A befogadás funkciócsoport naplózása [IN6.1]	teljesíti	
LA: A megőrzéssel kapcsolatos funkciók követelményei (Longterm Archiving)			
LA1	Az archivált elektronikus adatok rendelkezésre állásának megőrzése [LA1.1]- [LA1.2]	környezet	4. és 14. számú feltételek
LA2	Az archivált elektronikus adatok sértetlenségének megőrzése [LA2.1]- [LA2.2]	környezet	4. és 14. számú feltételek

LA3	Az archivált elektronikus adatok bizalmasságának megőrzése [LA3.1] [LA3.2] [LA3.3]	 támogatja N/A N/A	18. számú feltétel
LA4	Az archivált elektronikus adatok hitelességének és letagadhatatlanságának megőrzése [LA4.1] [LA4.2] [LA4.3]	 támogatja teljesíti teljesíti	16. számú feltétel
LA5	Az archivált elektronikus adatok értelmezhetőségének a fenntartása [LA5.1]	teljesíti	
LA6	Az archivált információk törlése [LA6.1]	támogatja	19. számú feltétel
LA7	A megőrzés funkciócsoport naplózása [LA7.1]	támogatja	20. számú feltétel
DS: A kibocsátással kapcsolatos funkciók követelményei (Dissemination)			
DS1	Adat kérések teljesítése [DS1.1]-[DS1.2]	 teljesíti	
DS2	Igazolás kérések teljesítése [DS2.1]-[DS2.8]	 teljesíti	
DS3	Szolgáltató-váltás előkészítése [DS3.1]	teljesíti	
DS4	A kibocsátás funkciócsoport naplózása [DS4.1]	teljesíti	

5 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]

6 Javaslat a Tanúsítvány szövegezésére

6.1 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 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 Nemzeti Akkreditáló Testület 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.

6.2 Javaslat a Tanúsítvány mellékleteire

Javasoljuk, hogy a Tanúsítvány mellékleteiben a következők szerepeljenek:

- Az SMTR 1.0 legfontosabb tulajdonságainak összefoglalása, lásd az alábbi fejezetet:

  1.3 A tanúsítás tárgya, biztonsági környezete és határai

- A biztonságos felhasználás feltételei, lásd az alábbi fejezetet:

  5 A biztonságos felhasználás feltételei

- A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások, lásd az alábbi fejezetet:

  2.1 Az alkalmazott tanúsítási és értékelési módszer

- A tanúsítási eljárás egyéb jellemzői:
  - A tanúsításhoz figyelembe vett fejlesztői dokumentumok
  - A tanúsításhoz figyelembe vett, fejlesztőtől független dokumentumok
  - A követelményeknek való megfelelés vizsgálat garancia szintje

7 Rövidítések

Az alábbiakban meghatározzuk a jelen tanúsítási jelentésben használt betűszavak jelentését.

AO	archiválási tisztviselő
CEM	Common Evaluation Methodology (Közös értékelési módszertan)
DB	Database (adatbázis)
DBMS	DataBase Management System (Adatbázis-kezelő rendszer)
DLL	Dynamic-Link Library (Dinamikus csatolású könyvtár)
EAL	Evaluation Assurance Level (értékelési garanciaszint)
EO	külső (NAV) tisztviselő
ETSI	European Telecommunication Standard Institute
ETSI TS	ETSI Technical Specification
GSA	játékszerver adminisztrátor
HSM	Hardvare Security Module
IIS	Internet Information Services
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
KIB	Közigazgatási Informatikai Bizottság
MIBÉTS	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
OS	Operating System
PIN	Personal Identification Number
RSA	Rivest, Shamir, and Adleman (az RSA algoritmus)
SO	biztonsági tisztviselő
SSL	Secure Sockets Layer
SSO	felsőszintű biztonsági tisztviselő
TCP	Transmission Control Protocol
TO	token tisztviselő
TOE	Target of Evaluation (az értékelés tárgya)
TSA	Time Stamping Authority
WCF	Windows Communication Foundation