TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft., mint a Nemzeti Média- és Hírközlési Hatóság adatbázisában nyilvántartott tanúsító szervezet és a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

tanúsítja,

hogy az

SMTR Tranzakció-kezelő és Archiváló szerver v1.1.1

valamint az

Webgam-Universum játékszerver v1.0.715.092

összetevőiből álló

/a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény által meghatározott/

központi szerverben alkalmazott, játéklogikákat kiszolgáló

véletlenszám-generátor

informatikai alkalmazás

megfelel

a

statisztikai és megjósolhatatlansági követelményeket kielégítő, az 1. számú mellékletben részletezett hibrid véletlenszám-generálási modellből levezett elvárásoknak az ISO/IEC 19790 Level1 szinten.

Készült: a WSG Szerver Üzemeltető Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T- RNG-001-2012**.
A tanúsítás kelte: 2012. augusztus 28.
A tanúsítvány érvényességi ideje: visszavonásig érvényes.
Melléklet: tulajdonságok, követelmények, feltételek, egyéb jellemzők; összesen 6 oldalon.

PH.

Endrődi Zsolt Tanúsítási igazgató	dr. Szabó István Ügyvezető igazgató

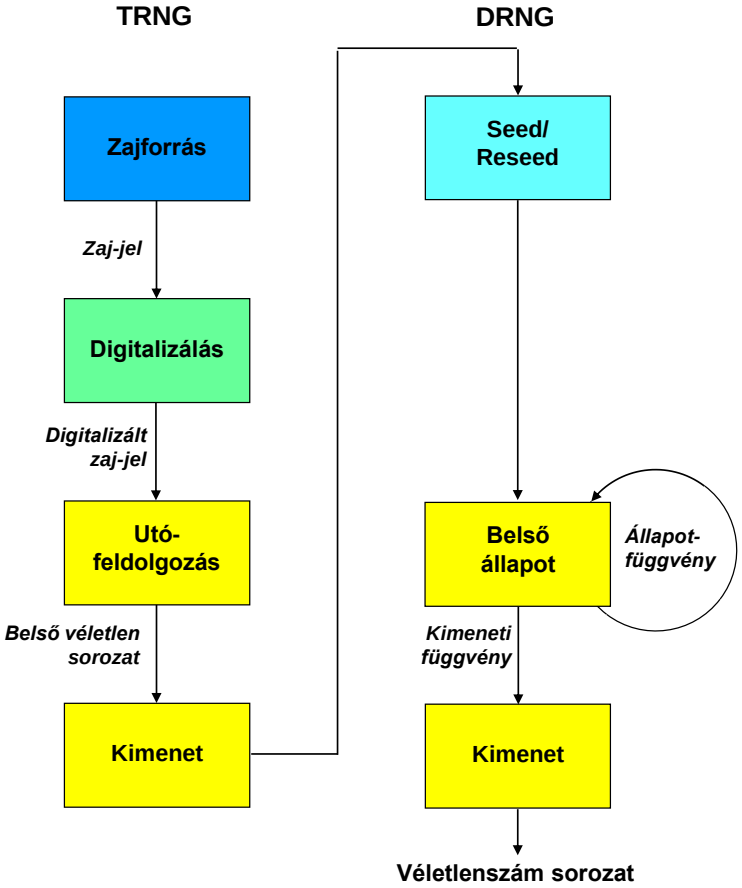
1. számú melléklet

A tanúsított termék legfontosabb tulajdonságainak összefoglalása

A tanúsított véletlenszám-generátor egy fizikai és egy determinisztikus véletlenszám-generátor komponensekből összeállított ún. hibrid modell, melyre vonatkozó (kriptográfiai és egyéb területeken) nemzetközi szinten elfogadott követelmény-rendszer az alábbi BSI[1] dokumentációkban szereplő elvárásokon alapul:

- A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators - Version 3.1 - 25.09.2001, BSI [AIS[2]31],
  mely a TRNG[3] (valódi, fizikai) véletlenszám-generálás követelményeit részletezi; valamint
- Functionality classes and evaluation methodology for deterministic random number generators - Version 1 – 2.12.1999, BSI [AIS20],
  mely a DRNG[4] (determinisztikus, algoritmikus) véletlenszám-generálás követelményeit részletezi.

A két modell (TRNG és DRNG/ előnyeit ötvözi az ún. hibrid modell, melyet az alábbi ábra mutat be:



[1] BSI: **B**undesamt für **S**icherheit in der **I**nformationstechnik
[2] AIS: **A**nwendungshinweise und Interpretatiionen zu CC und ITSEC im deutcschen **S**chema /Application Notes and Interpretation of the Scheme/
[3] TRNG: True Random Number Generator
[4] DRNG: Deterministic Random Number Generator or PRNG: Pseudo-random Number Generator

A hibrid modellt alkalmazó SMTR - Webgam-Universum központi szerverben az SMTR v1.1.1 tranzakciós szerverben lett implementálva a TRNG, míg a Webgam-Universum v1.0.715.092 játékszerverben valósították meg a determinisztikus véletlenszám-generátort, melyek együttműködve a központi szerverben az alábbi követelményeket teljesítik:

1.1. Megfelelő fizikai véletlenszám-generátor alkalmazása

Az SMTR v1.1.1 tranzakciós szerverben Common Criteria EAL4+ értékelési garanciaszinten tanúsított HSM[5] token került beépítésre, mely P2[6] tulajdonságot (és „magas” támadási potenciállal szembeni ellenállást) garantáló hardver eszköz.

1.2. Seed és reseed funkció biztosítása az erre jogosultak számára

Az 1.1. alatt meghatározott generátor a seed és reseed funkcióit kizárólag a központi szerveren regisztrált és aktív státuszú játékszerverek számára teszik elérhetővé. A hozzáférés-ellenőrzést az SMTR tranzakciós szerver végzi.

1.3. Valódi fizikai véletlenszám-generálás

A (seed és reseed) funkció jogosult meghívása esetén a tranzakciós szerveren az 1.1. alatti hardver eszközzel 2x128 véletlen bit kerül legenerálásra (teljesítve a legalább 100 bit entrópia elvárását).

1.4. Valódi fizikai véletlenszám exportálás

Az SMTR tranzakciós szerver a (seed és reseed) funkció jogosult meghívása esetén a TRNG által kimenetként generált biteket átadja a jogosult játékszerverek számára.

1.5. A DRNG seed és reseed funkciójának garantált meghívása

A Webgam-Universum játékszerver rendszeres időközönként meghívja a reseed funkciót a belső állapot értékének frissítéséhez.
Amennyiben a játékszerver elindításakor nem érhető el a seed funkció, akkor ezt riasztást kiváltó eseményként naplózza és a játékszerver leállításra kerül.

1.6. Védelem a hamis vagy lefigyelhető seed és reseed értékek ellen

A Webgam-Universum játékszerver - mivel külső forrásból (a tranzakciós szervertől) kapja a seed és reseed értékeket - védelmi mechanizmusokat alkalmaz a forrás hitelességének és a kapott értékek integritásának és bizalmasságának ellenőrzésére.

1.7. Continuous random test végrehajtása

A játékszerver a seed-értékekre egyszerű "continuous random test"-et végez. Amennyiben az egyszerű teszt nem az elvárt eredményt adja, akkor riasztást kiváltó eseményként naplóz és a játékszervert leállítja.

---

[5] HSM: Hardware Security Module

[6] P2: A P2 tulajdonság (a P1 elvárásokon túl) lényegében azt követeli meg, hogy a belső véletlen számokat gyakorlatilag ne lehessen meghatározni még akkor sem, ha az előzmények vagy a következő állapotok ismertek.
/Részletesen lásd [AIS31]: Requirements on P2-TRNGs: i) - xiii)./
A P1 tulajdonság lényegében azt követeli meg, hogy véletlen számok bizonyos statisztikai tesztek elvárásainak megfeleljenek.

1.8. A játékszerveren futó DRNG megfelelő szabadsági fokának biztosítása

A Webgam-Universum játékszerver a reseed funkció végrehajtása során a DRNG aktuális belső állapát a TRNG kimenetét képező reseed érték és a korábbi érték XOR művelettel létrehozott eredményével képezi. Ezzel biztosított a DRNG megfelelő szabadsági foka.

1.9. Szabványos determinisztikus véletlenszám generálás

A Webgam-Universum játékszerver egy K3[7] tulajdonságot biztosító, nemzetközi szabványon alapuló állapot és kimeneti függvényt valósít meg.

1.10. A véletlenszámok megfelelő felhasználása

A Webgam-Universum játékszerveren a DRNG kimeneteként megjelenő véletlenszám sorozatból olyan módon kerülnek generálásra a felhasználás igényeit kielégítő [0,n-1] intervallumba eső egész értékek, hogy mind az n lehetséges érték egyforma valószínűséggel kerül kiválasztásra, másrészt egyetlen véletlen bit sem kerül ismételt felhasználásra.

1.11. A seed és reseed funkciók aktivizálásának megfelelő naplózása

A Webgam-Universum játékszerver naplózza a seed/reseed funkciók minden meghívását (akár sikeres, akár sikertelen). A naplóba nem kerül be a seed/reseed generált értéke.

[7] K3: Egy támadó számára gyakorlatilag lehetetlen meghatározni vagy kitalálni a véletlenszám-sorozatot megelőző vagy követő számokat, illetve meghatározni vagy kitalálni egy belső állapotot. A támadó támadási potenciáljára különböző feltételezések vonatkozhatnak.
/Részletesen lásd [AIS20]: Requirements on K3-DRNGs: i)-iv)./

2. számú melléklet

A Tanúsítvány érvényességi feltételei

Az elvégzett vizsgálatok alapján a tanúsítvány megfelelőségi állítása az alábbi feltételek betartása mellett érvényes:

F1. A véletlenszám-generátor informatikai alkalmazás megfelelőségi állításai kizárólag a tanúsított verziójú tranzakciós szerveren és játékszerveren futtatott komponensekre érvényesek.

F2. A különböző szerverkomponenseken megvalósított funkciók kommunikációja kerüljön értékelésre a hitelesség szempontjából a rendszerértékelés folyamán (ld. 1. számú melléklet, 1.6. elvárás).

F3. Érvényességi idő: A Tanúsítvány visszavonásig érvényes. Visszavonásra akkor kerülhet sor, ha

- a Tanúsítvány alapját képező Értékelési jelentésben leírt feltételek, illetve alapvető megállapítások valamelyike a továbbiakban nem áll fenn, a hivatkozott tanúsítványok, szabványok visszavonásra kerültek; vagy
- a jogszabályokban olyan módosított, vagy új elvárások jelennek meg, melyeknek a vizsgált termék már nem felel meg.

3. számú melléklet

A megfelelőségi tanúsítás során figyelembe vett dokumentumok

Mértékadó jogszabályok

1. Az 1991. évi XXXIV törvény a szerencsejáték szervezéséről (2012.05. módosítás mellett)
2. A nemzetgazdasági miniszter 14/2012. (VI. 28.) NGM rendelete a helyhez kötött szerver alapú pénznyerő automatákat és a nem helyhez kötött szerver alapú pénznyerő rendszereket üzemeltető központi szerver működtetésének személyi, pénzügyi, műszaki és informatikai feltételeinek, valamint a központi szerver működtetőjét megillető szolgáltatási díj meghatározásáról
3. A nemzetgazdasági miniszter 15/2012. (VI.28.) NGM rendelete az egyes szerencsejátékok engedélyezésével, lebonyolításával és ellenőrzésével kapcsolatos feladatok végrehajtásáról szóló 32/2005. (X.21.) PM rendelet módosításáról.

Figyelembe vett mértékadó szakmai dokumentumok

4. A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators - Version 3.1 - 25.09.2001 [AIS[8]31];
5. Functionality classes and evaluation methodology for deterministic random number generators - Version 1 – 2.12.1999 [AIS20]
6. ANSI X9.31 Appendix A.2.4 Using AES

Az értékelési folyamat során figyelembe vett további dokumentumok

7. Universum_RNG_ER_v1.00 számú Értékelési jelentés a véletlenszám generálásról és felhasználásról.
8. SMTR Tranzakció-kezelő és Archiváló szerver v1.01 - Biztonsági előirányzat HUNG-T-MIBÉTS-002-2012 Tanúsítvány (SMTR Tranzakció-kezelő és Archiváló szerver v1.1.1)
9. HUNG-TK-MIBÉTS-002/1-2012 Tanúsítvány karbantartási jegyzőkönyv (SMTR Tranzakció-kezelő és Archiváló szerver v1.1.1)
10. Webgam-Universum játékszerver – Biztonsági előirányzat 8117 (12.07.15)
11. HUNG-T-MIBÉTS-003-2012 sz. Tanúsítvány (Webgam-Universum játékszerver v1.0.715.092)
12. AT90SC25672RCT-USB MCU Security Target Lite /cible2006_30en.pdf/
13. Certification Report 2006/30 ATMEL Secure Microcontroller AT90SC25672RCT-USB rev. D /2006_30_en.pdf/

[8] AIS: **A**nwendungshinweise und Interpretatiionen zu CC und ITSEC im deutcschen **S**chemaApplication Notes and Interpretation of the Scheme / Application Notes and Interpretation of the Scheme/