

Trusted Play™ (TP) - innovative RNG server generating instant and multiplayer game outcomes on variety of platforms and channels in a secure way, detecting any potential fraud against gaming system. It is a high performance redundant, highly scalable, distributed system. It consists of two independent TP RNG servers and optional automated Trusted Audit system. Typical use of TP system is for on-line real time applications for betting over the internet platform, for mobile betting, interactive TV betting, Video Lottery, casino betting and on-line lottery systems.

Game Support

TP server provides auditable random numbers for variety of games:

1. *Fixed pool.* After a random number is generated, the outcome is removed from the pool and next generation uses a reduced pool of outcomes. Numbers are chosen randomly for games such as: *Instant tickets, Probability game, Card games, Slot machines, Monitor games, Progressive Jackpot games.*
2. *Fixed Distribution.* Numbers are chosen in a random fashion with a desired distribution. On each generation all outcomes are possible. This type of generation can be used for application such as: *Instant ticket, Slot machines, Progressive Jackpot games and many other games*
3. *Integer random numbers.* A very general method for generation of integer random numbers with and without repetition, for games such as numbers, joker, bingo, keno, lotto, and second chance draws.
4. *Lotto.* A specialized method for lotto type games, providing full sequence of game selections.

RNG - Unpredictable and Auditable Random Numbers

Szrek2Solutions developed and patented RNG methodology¹ providing unpredictable and verifiable random numbers. Any attempt to defraud the system is detectable even if the attacker has a full access to the system, hardware and software. During random number generation an audit trail consisting of the following elements is created:

1. The generated random numbers - although unpredictable, the outcomes are proven to be the only outcomes that could have been generated and no other numbers are valid.
2. The game matrix and “pool” of game elements – verifying that the random numbers were created from a specific game matrix and were taken out of the complete “pool” of the available game elements
3. The time of generation - each random number is time-stamped at generation
4. Generation hardware – specific random numbers generation hardware is verified
5. Each random number generation is accounted for

This audit trail will serve as an irrefutable mathematical proof of integrity of the RNG process.

The TP implementation utilizes only standard elements - certified² and industry proven cryptographic hardware and software. TP does not use any proprietary algorithms. For random numbers generation RSA signature is used. RNG has been certified multiple times for gaming applications.

Three ‘R’ System - Robust, Reliable, Redundant

Each TP system is built in a redundant fashion to ensure it has no single point of failure. To recover from any disk failures RAID 1 disk set is configured on each TP system. Redundant HSM (Hardware Security Modules) are installed: if one fails, another will continue generating random numbers. For each generated random number RNG seed is verified in real time to avoid “bad” random numbers caused by the hardware failures. For every transaction Game Server verifies integrity of TP RNG system. Each TP RNG system logs audit trail in real time to multiple Trusted Audit systems. In case of the network failure or systems being off-line, once the systems are back up, remote log is automatically recovered.

Ease of Operation and High Performance

Day-to-day operation of TP RNG systems does not require any operator intervention. Systems run 24/7/365 and automatically recover from network and system problems. TP RNG server provides random numbers to the Game Servers and logs in real time audit trail to Trusted Audit systems, which verify and automatically merge and compare information from Game Servers and TP RNG systems. Auditors may view audited data with Trusted Monitor™ system. TP system ensures high performance of RNG - it can support average of 1500 transactions per second.

Ease of Integration and Installation

TP system is designed to be easy to integrate with a client via industry standard XML-RPC protocol. Real world examples are the best testimony: after Betware integrated Trusted Play into their internet platform, Stefan Hrafnkelsson, CEO of Betware stated “Trusted Play was easy and quick to integrate with and it supports better auditability than I have ever seen before”. After initial integration no update, modification or fix was needed. Once the system was fielded in Danske Spil (DS), there was not a single problem reported related to TP RNG System or Trusted Audit.

Support

Trusted Play system comes with a comprehensive documentation package, including Operator’s Guide and Q&A’s, and a customized training course for Operations staff. After system installation Szrek2Solutions offers on-going support for any problems and questions, including 24/7 emergency support and problem resolution.

¹ US patent no 6 934 846; several international patents applied for

² LYNKS II HSM from SPYRUS for RNG seed generation is NIST 140-2 level 2 certified with hardware and design certified to level 3.