Szrek2Solutions

Trusted Play™ (TP) is a high-performance random number server that generates instant and interactive game outcomes for a variety of channels, ensuring security by detecting any potential RNG fault or fraud. It is offered in a redundant configuration with a minimum of two independent TP RNG servers and a Trusted Audit verification system.

The TP system is typically used for on-line real time applications for internet and mobile betting, interactive TV betting, Video Lottery, casino betting, and on-line lottery systems.

Game Support

TP server provides certified and auditable random numbers for a variety of games:

1. *Fixed pool.* Generation without replacement. After a random number is generated, the outcome is removed from the pool and the next generation uses a depleted pool of outcomes. The pool can be increased when a defined level is reached. Numbers are chosen randomly for games such as: *Instant tickets, Probability game, Card games, Slot machines, Monitor games, Progressive Jackpot games.*
2. *Fixed Distribution.* Generation with replacement. Numbers are chosen in a random fashion with a desired distribution. All outcomes are possible for each generation. This type of generation can be used for applications such as: *Instant tickets, 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 replacement, for games such as numbers, joker, bingo, keno, lotto, second chance draws, and raffle games.

RNG - Unpredictable and Auditable Random Numbers

Szrek2Solutions' patented RNG methodology [1] provides unpredictable and verifiable random numbers. Any attempt to defraud the system is detectable even if the attacker has full access to the system, hardware, and software. During random number generation an irrefutable audit trail is created to prove the system integrity:

1. Digital Signatures: the system uses digital signatures/timestamps as RNG seeds. For generating digital signatures NIST certified Hardware Security Modules are used. All random numbers are derived from these digital signatures.
2. 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.

---

[1] US patent no 6 934 846 and several international patents.

3. 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.
4. The time of generation - each random number is time-stamped at generation.
5. Generation hardware – the hardware used to generate the specific random numbers is verified.
6. Each random number generation is accounted for.
7. Game data integrity: players' and transactions' information is digitally signed to prove integrity.

This audit trail, which includes digital signatures used as RNG seeds, is secured in the form of blockchain and serves as a mathematical proof of the integrity of the RNG process.

The TP implementation utilizes only standard elements - certified and industry proven cryptographic hardware and software. TP does not use any proprietary algorithms. The 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 HSMs (Hardware Security Modules) are used for random number generation: if one fails, another one will be used. For each generated random number, the RNG seed is verified in real time to avoid "bad" random numbers caused by the hardware failures. For every random number generation (RNG transaction), the Game Server is assured of the TP RNG system integrity. Each TP RNG system logs the secured audit trail in real time to multiple Trusted Audit systems. In case of a network failure or systems being off-line, once the systems are back up, the 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. Trusted Audit systems verify and automatically merge and compare information from Game Servers and TP RNG systems. Status of all servers, system services and individual

game outcomes can be viewed with a Trusted Monitor™, a web browser-based monitoring system. The TP system ensures high performance of the RNG – a single server supports on average 1500 transactions per second. Multiple TP RNG servers can be used in production for higher performance. Trusted Audit is often integrated with the Lottery's ICS (Internal Control System) for verification of the RNG outcomes.

Ease of Deployment and 100% Availability

The TP system is designed to be easy to integrate with a client via industry standard interfaces and is simple to deploy.

After initial deployment, the TP system does not require changes: games can be changed and added dynamically, without stopping the system. Customers using the TP product have included Danske Spil and Lottomatica, where these systems run 24/7/365 and have been available 100% of the time over 12-15 years of operation. The TP system used by IGT for eInstants is servicing multiple US lotteries over many years, with new lotteries being added in real time with no changes to the Trusted Play and Trusted Audit systems.

Support

Szrek2Solutions provides full Trusted Play documentation and training for Operations staff. After system installation, Szrek2Solutions offers on-going warranty support for any problems and questions, including 24/7 emergency support and problem resolution.