

Trusted Play+™ Overview

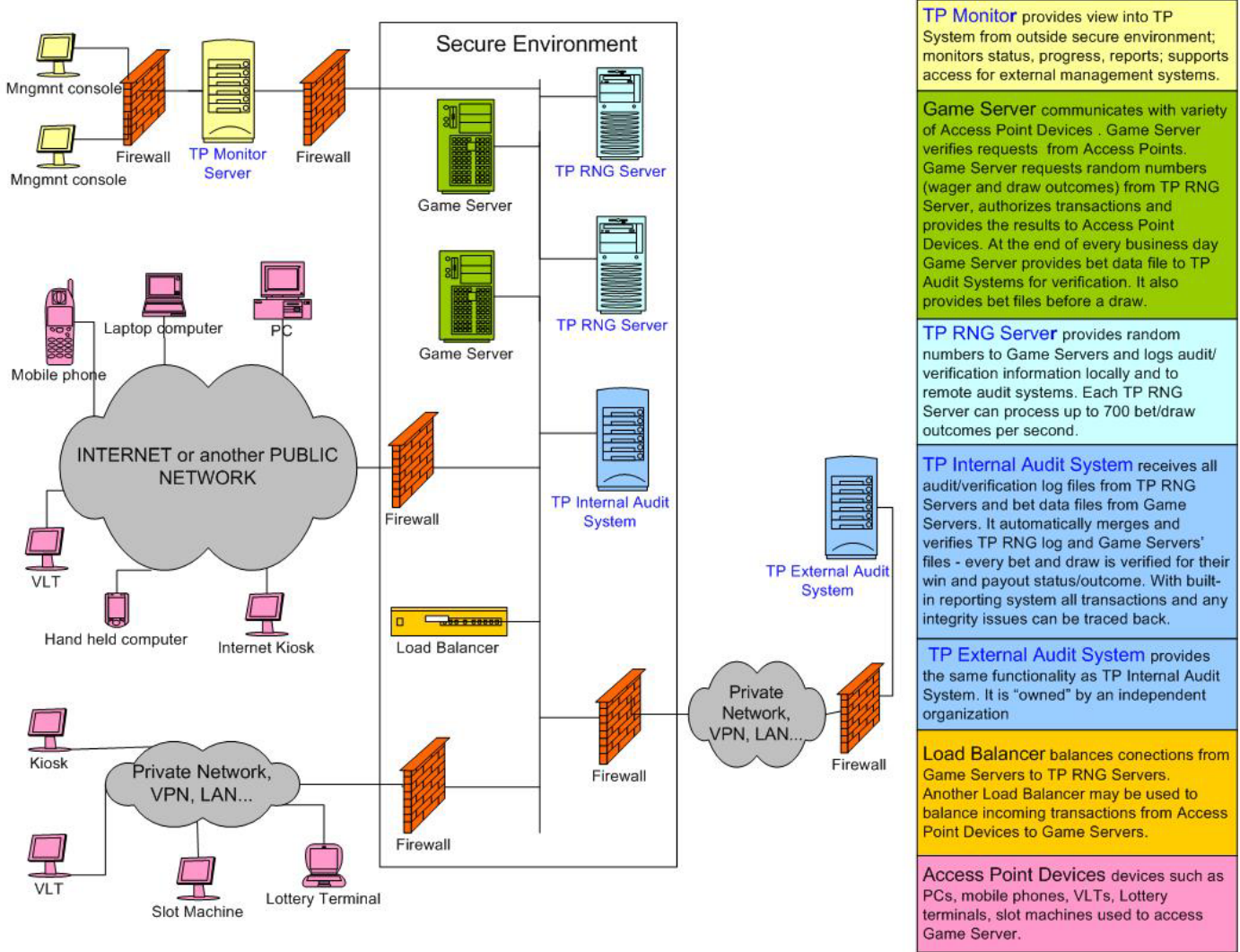
Abstract

Trusted Play+™ - innovative RNG server generating instant and interactive game outcomes and draw results in a secure way, providing fraud protection through its Trusted Play+ Audit system; audit detects any potential fraud against gaming system, including hard to detect insider attacks. Audit also offers internal control functions such as winner selection verification. RNG and Audit process and results can be monitored via Trusted Monitor.

Trusted Play+ Highlights:

- ♦ On one system platform merges functionality of Trusted Draw™ and Trusted Play™
- ♦ Supports wide variety of on-line, instant and interactive games (class II and III) and gaming platforms (Internet, mobile, VLT, slots)
- ♦ Randomly generated outcomes are unpredictable yet can be audited – outcomes, time, and hardware
- ♦ Uses NIST certified cryptographic hardware and software to generate and verify random outcomes
- ♦ Has undergone extensive tests proving desired statistical properties; RNG has been certified
- ♦ Robust, reliable, secure, persistent, high-performance with no single point of failure
- ♦ Easy and fast to integrate with gaming system via standard XML_RPC interface
- ♦ Has capability to log game and draw outcomes in real time to multiple audit systems
- ♦ TP Server and TP Audit are fully automated: run 24/7/365, no operator intervention is required for day switch or recovery from system or network problems
- ♦ RNG verification feature is unique— not available in any other bet generation system on the market
- ♦ Audit mathematically proves integrity of the generation process and certifies that there was no fraud
- ♦ Audit verifies draw information, optionally performs independent winner selection / prize calculations and verifies results with game server results.
- ♦ System monitoring tool provides view into the system from outside of secure environment to monitor RNG and audit process and results.

Trusted Play+ Architecture



Product Description

Trusted Play+ (TP+) System is a secure RNG and audit system for instant games and on-line game draw results on variety of platforms and channels provided by Szrek2Solutions. It is a high performance redundant, highly scalable, distributed system. It consists of two independent systems:

1. Fully automated TP RNG server and
2. An optional, fully automated TP Audit system.

Typical use of TP+ system is for on-line real time applications for betting and generating draw outcomes 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 will use a reduced pool of outcomes. Numbers are chosen in random fashion for games such as:
 - a. *Instant tickets* - winning/non winning share is randomly chosen out of the fixed pool of outcomes
 - b. *Probability games* – every ticket is a potential winner. Players’ scratching determines the winning
 - c. *Card games* for single player and multiple parties games
 - d. *Slot machines* with a pool of fixed outcomes
 - e. *Monitor games* for simulated car and horse racing. This generation mode allows generating random, non-repetitive outcomes with different odds.
 - f. *Draws* for such games as lotto, keno, bingo, Power Ball’s Multiplier etc.
 - g. *Progressive Jackpot games*
2. *Biased distributions.* 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:
 - a. *Instant tickets*
 - b. *Slot machines*
 - c. *Progressive Jackpot games*
 - d. *Many other games*
3. *Integer random numbers.* A very general method for generation of integer random numbers with and without repetition. This method is designed for numbers games drawings such as 3 digits, 4 digits, joker, bingo, keno, lotto, second chance draws etc.
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 evidence of correct operation 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 evidence will serve as an irrefutable mathematical proof of integrity of the RNG process.

The TP+ implementation merges functionality of Trusted Draw and Trusted Play products on a single platform, providing auditing for the games and draws. TP+ utilizes only standard elements - certified² and industry proven cryptographic hardware and software; TP+ does not use any proprietary

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

² LYNKS HSM from SPYRUS for RNG seed generation is NIST 140-2 level 3 certified.

algorithms. Security of the generated random numbers is equivalent to the security of 1024 bit RSA signatures. RNG itself has been certified 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. Multiple TP+ systems are installed. They work in distributed fashion or one can be a "primary" while other TP+ systems will be activated upon request by the Game Server. Each TP RNG system logs redundantly evidence of correct operation. This proof is logged in real time locally and to multiple TP 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 and TP Audit 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, evidence of correct operation locally and on the redundant TP Audit systems. Each TP Audit system verifies and automatically merges and compares information from Game Servers and TP RNG systems. In addition it can perform winner selection and prize calculations and have the results verified automatically with the ones from the Game Servers. The auditor may view audited data with TP+ provided reporting subsystem. Optionally a Trusted Monitor tool can be used to view system performance and results.

TP+ system is designed to ensure high performance of RNG. A single TP+ server can support average of 700 transactions per second. This can satisfy performance requirements of the biggest 'lotto-mania.'

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 Hrafinkelsson, 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 Dansk Tipstjeneste (DT), there was not a single problem reported related to TP RNG System or TP Audit System. Two TP RNG servers and three Audit Systems, one internal and two external, are used at DT.

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.

References

S2S and its products have a successful record with customers in Europe and will offer references upon request.