

Trusted Play+™ Overview

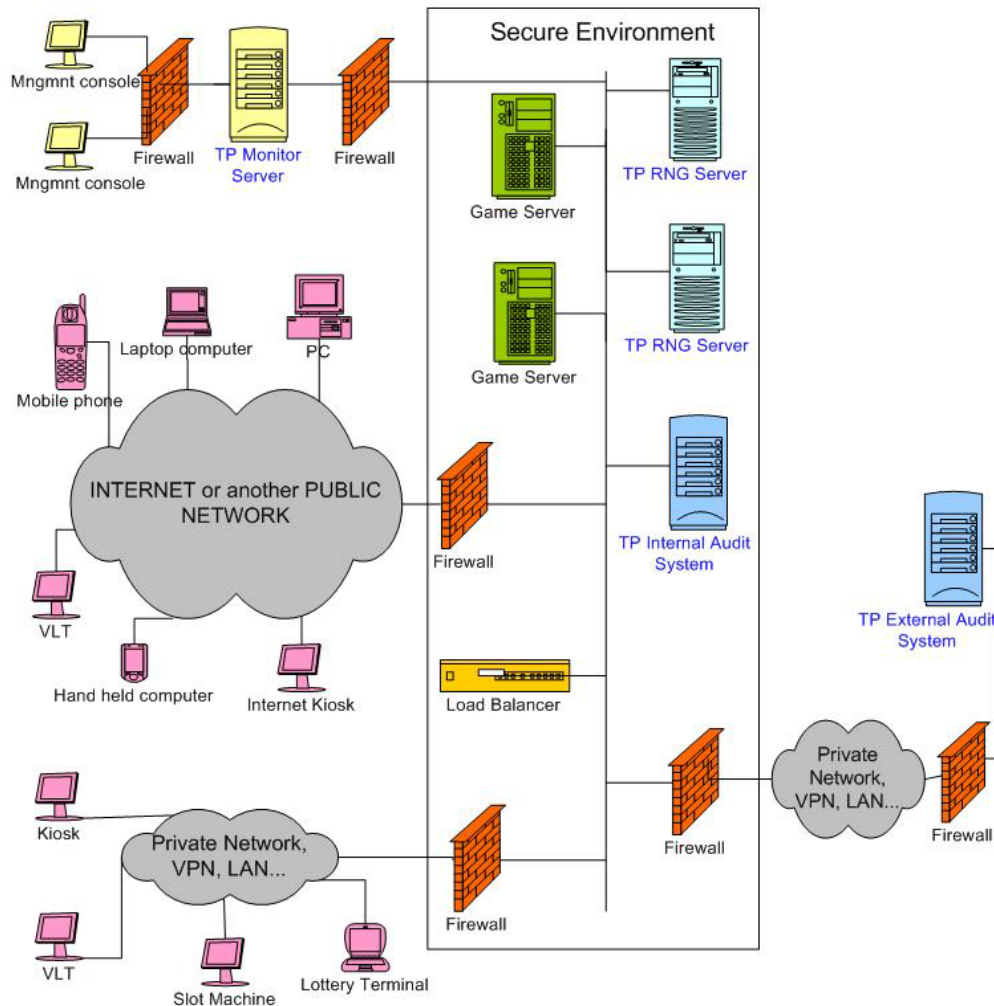
Abstract

Trusted Play+™ - innovative random number server generating instant and interactive game outcomes and draw results in a secure way, providing fraud protection through its Trusted Audit system. Audit detects any potential fraud against the system, including hard to detect insider attacks. Audit also offers internal control functions such as bet integrity verification and winner selection verification. Random Number Generation (RNG) and Audit processes and results can be monitored via system monitoring tool, Trusted Monitor.

Trusted Play+ Highlights:

- ♦ On one system platform merged functionality of Trusted Draw™ (TD) and Trusted Play™ (TP)
- ♦ Supports wide variety of on-line, instant (fixed odds, fixed pool, probability) and interactive games on variety of gaming platforms (traditional on-line, 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/TD Server and TP/TD 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 or draw generation system on the market; based on patented RUN+A method utilizing digital signature
- ♦ Audit mathematically proves integrity of the generation process and certifies that there was no fraud
- ♦ Audit also proves bet integrity - it proves that bets were not modified after the draw
- ♦ Audit verifies draw information, optionally performs independent winner selection and prize calculations and compares results with game server results
- ♦ System monitoring tool provides web browser based view of the system from outside of secure environment to monitor RNG and audit process and results.
- ♦ Easy integration with 3-rd party monitoring tools such as Tivoli, BigBrother, etc.

Trusted Play+ Architecture



<p>TP Monitor provides view into TP System from outside secure environment; monitors status, progress, reports; supports access for external management systems.</p>
<p>Game Server communicates with variety of Access Point Devices . Game Server verifies requests from Access Points. Game Server requests random numbers (wager and draw outcomes) from TP RNG Server, authorizes transactions and provides the results to Access Point Devices. At the end of every business day Game Server provides bet data file to TP Audit Systems for verification. It also provides bet files before a draw.</p>
<p>TP RNG Server provides random numbers to Game Servers and logs audit/ verification information locally and to remote audit systems. Each TP RNG Server can process up to 700 bet/draw outcomes per second.</p>
<p>TP Internal Audit System receives all audit/verification log files from TP RNG Servers and bet data files from Game Servers. It automatically merges and verifies TP RNG log and Game Servers' files - every bet and draw is verified for their win and payout status/outcome. With built-in reporting system all transactions and any integrity issues can be traced back.</p>
<p>TP External Audit System provides the same functionality as TP Internal Audit System. It is "owned" by an independent organization</p>
<p>Load Balancer balances connections from Game Servers to TP RNG Servers. Another Load Balancer may be used to balance incoming transactions from Access Point Devices to Game Servers.</p>
<p>Access Point Devices devices such as PCs, mobile phones, VLTs, Lottery terminals, slot machines used to access Game Server.</p>

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/TD RNG server and
2. An optional, fully automated TP/TD 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:
 - 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 algorithms. RNG itself has been certified for gaming applications.

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

² LYNKS HSM from SPYRUS is NIST 140-1 level 2 certified and in process of 140-2 level 3 certification.

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/TD RNG and TP/TD Audit systems does not require any operator intervention. Systems run 24/7/365 and automatically recover from network and system problems. TP/TD RNG server provides random numbers to the Game Servers and logs, in real time, evidence of correct operation locally and on the redundant TP/TD Audit systems. Each Audit system verifies and automatically merges and compares information from Game Servers and 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 1000 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 Hrafnelsson, 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 Denmark by Dansk Tipstjeneste (currently Danske Spil), 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 Danske Spil.

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

Szrek2Solutions and its products have a successful record with customers and will offer references upon request.