Trusted Transactions™ Overview

Summary

Trusted Transactions™ (TT) system from Szrek2Solutions offers a unique, time-efficient method of securing lottery transactions before a draw, at a precise time, to ensure bet integrity; protect from any potential alteration of bet data participating in the draw. TT utilizes a patent pending technology of digital time-stamping a file with lottery transactions just before the draw. To ensure highest level of security, Szrek2Solutions employs a NIST certified tamper proof cryptographic Hardware Security Module, which in addition to performing the time-stamping allows audit of the process.

Time-stamping

Time-stamping is a process of digitally signing data together with time. Why is time-stamping important? - standard digital signature provides a proof of the content of the data; it proves that the data corresponds to its signature. However a traditional signature could be made at any time, even after the draw. To ensure that draw data has not been altered before the draw, the time-stamping of the data is done – digital signature of the data together with time. Typically time-stamping of large files, such as lottery transaction files containing millions of bets, is time consuming. Szrek2Solutions solved the technical challenge of time-stamping large files in a very short time, which is critical for draw security applications. This technology used by S2S in TT system is also successfully developed for its Trusted Play and Trusted Draw products.

Time-stamping is not new to the lottery industry; it has been successfully employed by some lotteries (e.g. in Germany). However currently used approaches require complex modification of the lottery transaction processing system and of the Internal Control System (ICS). The approach proposed by S2S allows TT deployment with minimal or no changes to the current lottery transaction processing system, and with minimal or no changes to the existing ICS.

TT Functionality

TT system provides rapid time-stamping of bet data before the draw; it allows closing of sales in less than 5 minutes before the draw. TT time-stamping creates a proof of transaction file content which can be verified after the draw. It is a more secure solution than traditional preventive approaches, which are exposed to insider fraud. TT time-stamp proof is incorruptible and provable to a third party any time after the draw – one minute after or years after.

TT system consists of TT Server and TT Audit system. TT Server obtains a transaction file containing all bets participating in the draw (via file transfer or real time transaction logging); it performs time-stamping of the transaction file and sends the time-stamp to the TT Audit, which verifies the time-stamp; optionally TT Audit can perform internal control functions (ICS), such as winner verification.

Both TT Server and TT Audit systems can be deployed locally and remotely; time-stamp verification can be performed remotely by a third party (external TT Audit). TT Server and TT Audit use a Windows Server platform (hardware spec included below). For digital time-stamp TT employs NIST certified Hardware Security Module (HSM[1]). There is no special hardware required for the verification.

The HSM device is highly secure. It is tamper proof - safeguards cryptographic keys and the clock it contains (Real Time Clock –RTC). Private Key is protected and not readable by any external or internal, programmatic or non-programmatic means. Any attempt to change RTC would be detected, and it would also destroy the cryptographic keys. The signature schema used is a US standard 1024 bit RSA signature. It is generally viewed that these signatures allow protecting data for 20 years. If desired, S2S may deploy other signature standard or key length.

TT system can be also deployed with an optional ICS functionality providing automated winner selection and verification subsystem. In this case TT Audit system will perform winner selection and automatic comparison of winner selection outcomes generated independently on the Lottery system (Game Server) and on TT Audit system.

Both TT Server and TT Audit are high performance systems and work without any operator intervention.

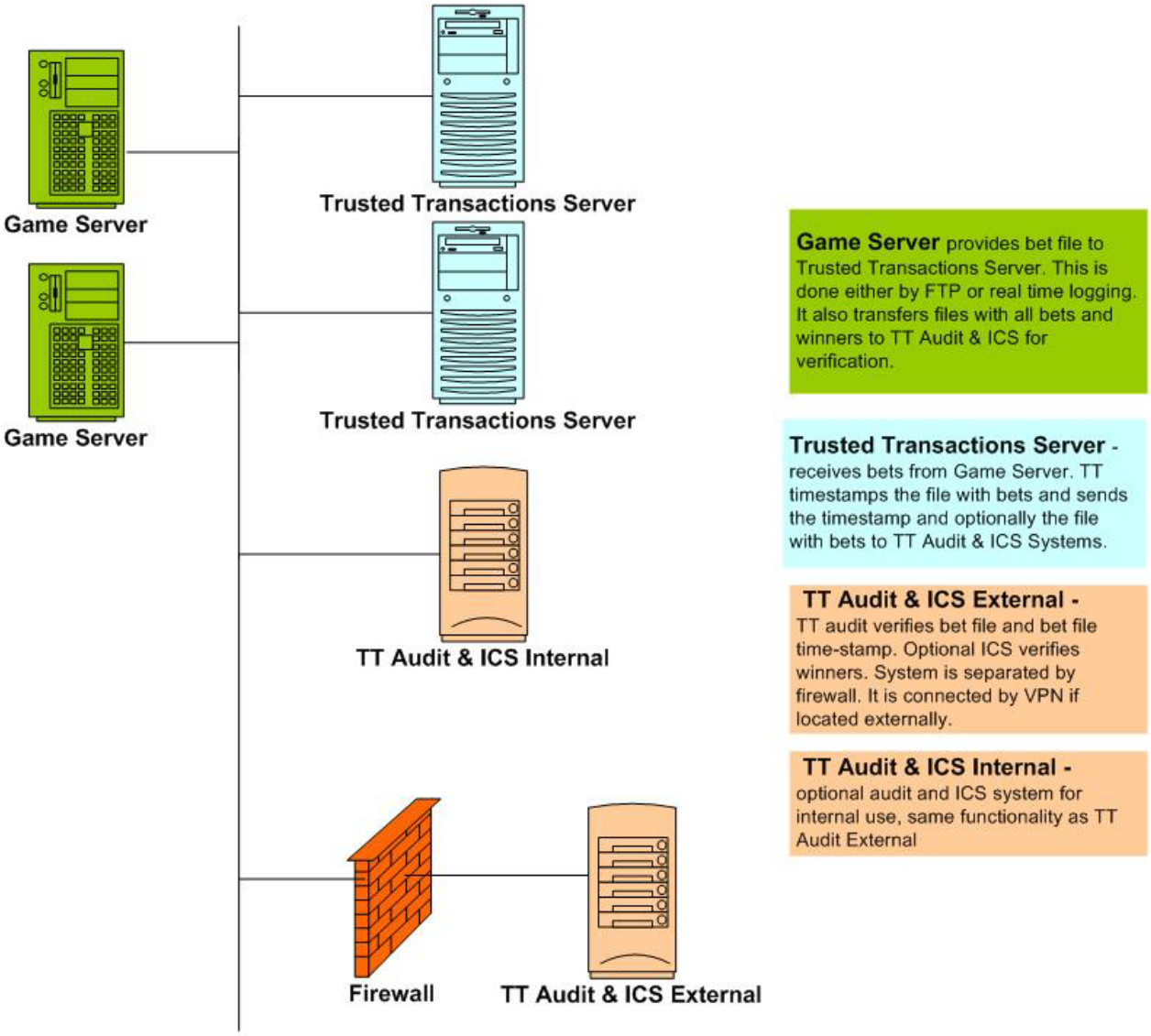
TT System Operation

TT system is designed to work in an automated fashion. Without operator intervention the system performs bet file time-stamp before the drawing, audits the time-stamp and optionally verifies winner selection. The system should recover from majority of error conditions such as system crash or network communication failure, without any operator involvement.

TT Architecture and Functionality

Following diagram presents a high level architecture of TT system:
TT system is distributed – it consists of multiple TT Servers available to process the bet file from the Game Server, to ensure that in case of one system being down another will process the file. An internal and external TT Audit system is offered – one can be used by the lottery staff, another by an auditor (a third party).
Description of the diagram components depicts also the general TT functionality.

[1] LYNKS I and LYNKS II cryptographic tokens from SPYRUS are used. This is a commercial product used by US military, NSA (National Security Agency) and for commercial application. There were over 400,000 of these HSM deployed.



Trusted Transactions Architecture

Security

TT has been designed with security as a main design goal. Following points summarize TT main internal security features:

- Critical data and an independent battery backed up Real Time Clock (RTC) protected by certified tamper evident cryptographic hardware. Cannot be manipulated programmatically
- Multiple user or client authentications required
- Digital signature has cryptographic strength of 1024 bit RSA digital signatures
- Non-refutable time-stamp proves draw data integrity; provides detection of:
  - Modification of draw data
  - Use of unauthorized hardware (HSM)
- Logging of all TT system activity (except operator passwords entry)
- Read-only log folders and draw report files

- Enhanced PC security
- One way hash protecting bet data integrity

TT System Fault Tolerance

Szrek2Solutions fully appreciates that one of the most important aspects of any live or "almost live" (short delay) application is that it simply cannot fail. With little or no time to correct problems, the system just has to work correctly.
Many elements of fault tolerance are built into the TT system:

- Redundant hardware:
    - Two or three TT systems
    - Two cryptographic HSM-s per system
- Re-entrant programs; programs can be restarted - there are no "states" precluding correct operation of any program if the program is aborted or fails for any reason.
- Data can be restored at any time, no internal states requiring "reversal" of any information.
- User entry robustness.
- Real time verification of cryptographic HSM. If verification fails or HSM comes back with an error another HSM is used for time-stamping.
- HSM is automatically tested when TT application is started, without waiting for the actual time-stamping.
- Reports and log files in read-only mode – unintentional operator mistakes are avoided.