Szrek2Solutions

Trusted Transactions™

by Szrek2Solutions

SMART TECH 2006

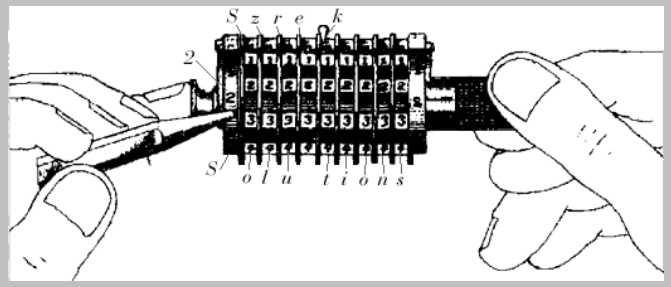
Las Vegas, March 1st

Szrek2Solutions
60 Spencer Ave, East Greenwich
RI 02818 / tel. 1(401)398-0395
website: www.szrek.com
e-mail: info@szrek.com

Szrek2Solutions, LLC

Lead technology experts for innovative and secure gaming

- Szrek2Solutions LLC started in 2003, founders: Irena & Walter Szrek
  - –Founders & Principals each have 25 years lottery experience
  - –Walter Szrek - system architect, senior technical consultant
  - –Irena Szrek - software director, project and product manager
- International gaming products & service company
  - –Secure software systems solutions
  - –Data security & system integrity, RNG-s
  - –Product development and implementation
  - –Lottery systems and solutions consulting
- Szrek2Solutions Accomplishments
  - –Invented & patented RUN+A™ RNG method
  - –Developed Trusted Draw™ - tamper evident electronic draw system w/audit
  - –Developed Trusted Play™ - secure bet server for instant games (many platforms)
  - –Launched Trusted Play Sep 05 - to supply instants bets over Internet for Danish Lottery
  - –Added Trusted Transactions™ to Trusted Products™ family – to be launched in May 06



Szrek2Solutions

Trusted Transactions™ (TT)

Unique method of securing lottery transactions before a draw

- to ensure bet integrity
- protect from any potential alteration of bet data participating in the draw.
- at a precise time before the draw
- with no or minimal changes to the on-line system
- utilizing proven technology of digital time-stamping, but
- generating time-stamp in minimum time
- allowing for remote audit of transactions integrity any time
- employing standard NIST-certified tamper proof HSM

Legacy Methods

- Securing a tape with all transactions before the draw (physically)
- Writing all transactions to CD-ROM and securing it before the draw (physically)

Newer Systems

- Real time computing of one way hash of transactions and time-stamping before the draw
  - advantages for fast paced games (5 min Keno)
  - but requires
    - tight integration with lottery system, ICS
    - retesting with software changes

Time-Stamping - background

Time-stamping is a process of digitally signing data together with time

- traditional signature is not as strong - can be made after the draw
- typical time-stamping of large files takes too long to perform after sales / before draw
- to solve the problem time-stamping is done in real time (during sales)
- but that becomes technically difficult – some transactions impact past transactions (cancellations) and signature
- It requires complex modifications to lottery system and ICS, retest with software changes

Szrek2Solutions

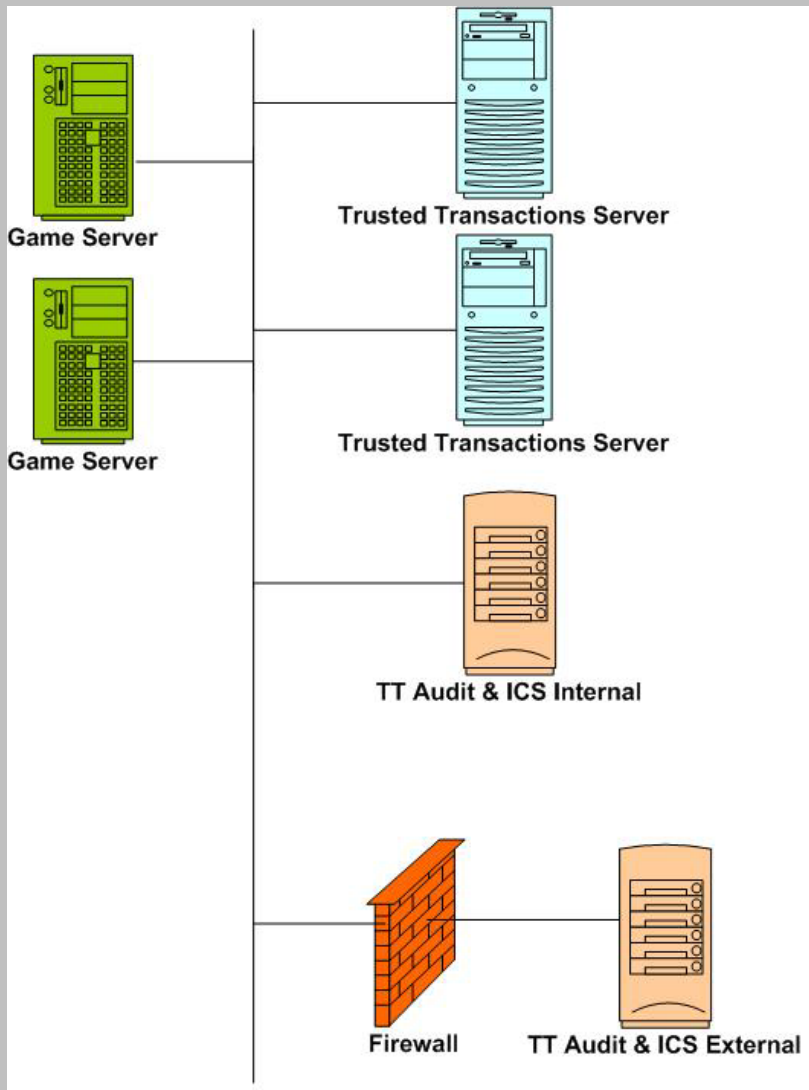
Trusted Transactions™

TT solves a technical challenge of time-stamping of large files in a short time:

- provides rapid time-stamping of bet data (<1 min)
- creates proof of bet content which can be verified after the draw
- TT time-stamp proof is incorruptible and provable to 3-rd party any time (minutes, years)
- TT time-stamp can be verified remotely preserving security
- designed to work with legacy and newer systems
- addresses both fast pace and regular games
- TT time-stamp can be integrated with electronic draw

Trusted Transactions™ Functionality

- consists of TT Server and TT Audit
- TT Server: obtains file with all bets participating in a draw (remote log, file transfer); performs time-stamping and sends time-stamp to TT Audit
- TT Audit – verifies the time-stamp; optionally TT Audit can perform ICS functions (e.g. winner selection and comparison)
- audit can be performed remotely by a 3-rd party
- employs standard NIST certified HSM
- both TT Server and Audit are high performance systems, automated (work w/o operator intervention)
- TT systems are robust, recover form error conditions, use redundant HSM-s



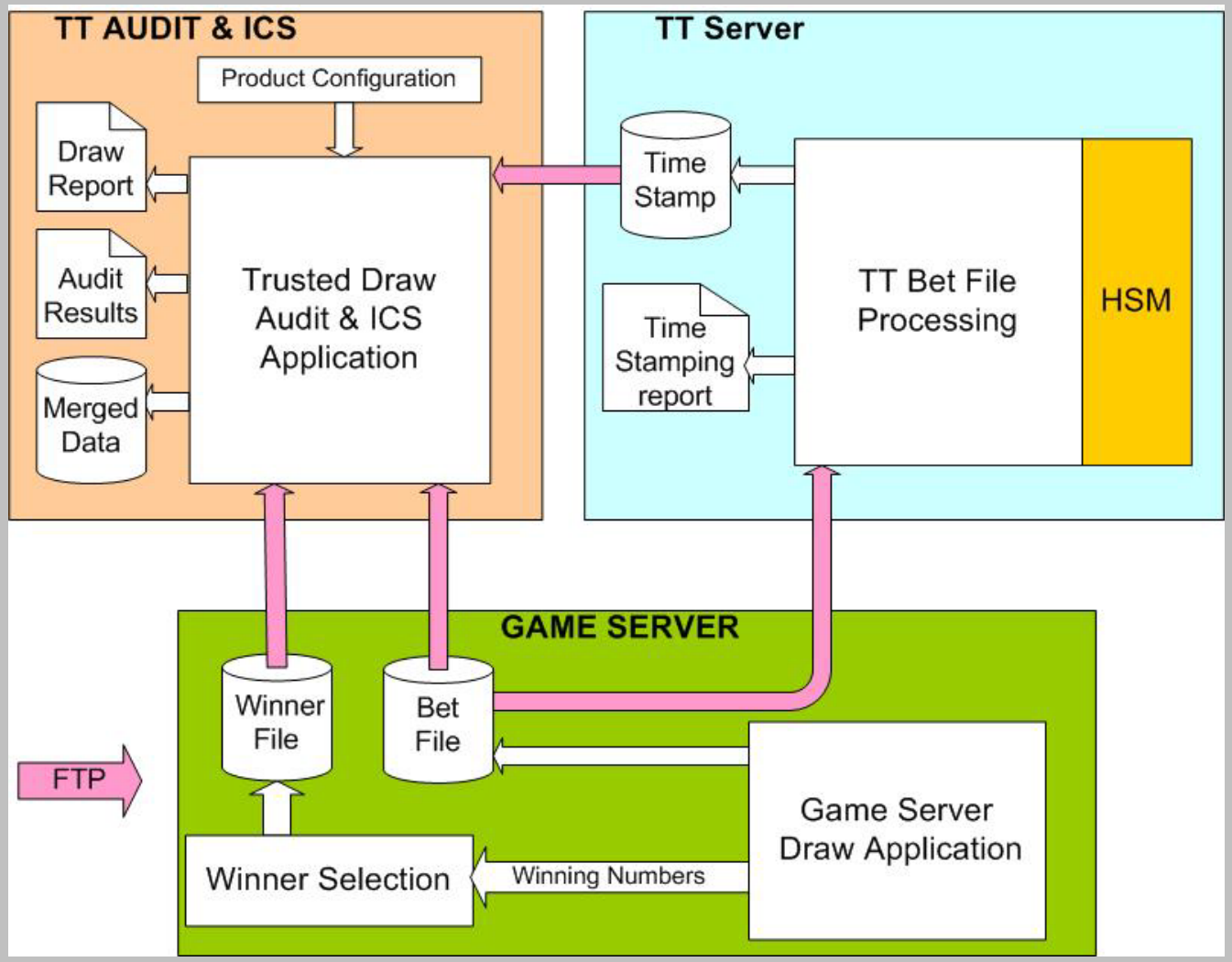
Game Server provides bet file to Trusted Transactions Server. This is done either by FTP or real time logging. It also transfers files with all bets and winners to TT Audit & ICS for verification.

Trusted Transactions Server - receives bets from Game Server. TT timestamps the file with bets and sends the timestamp and optionally the file with bets to TT Audit & ICS Systems.

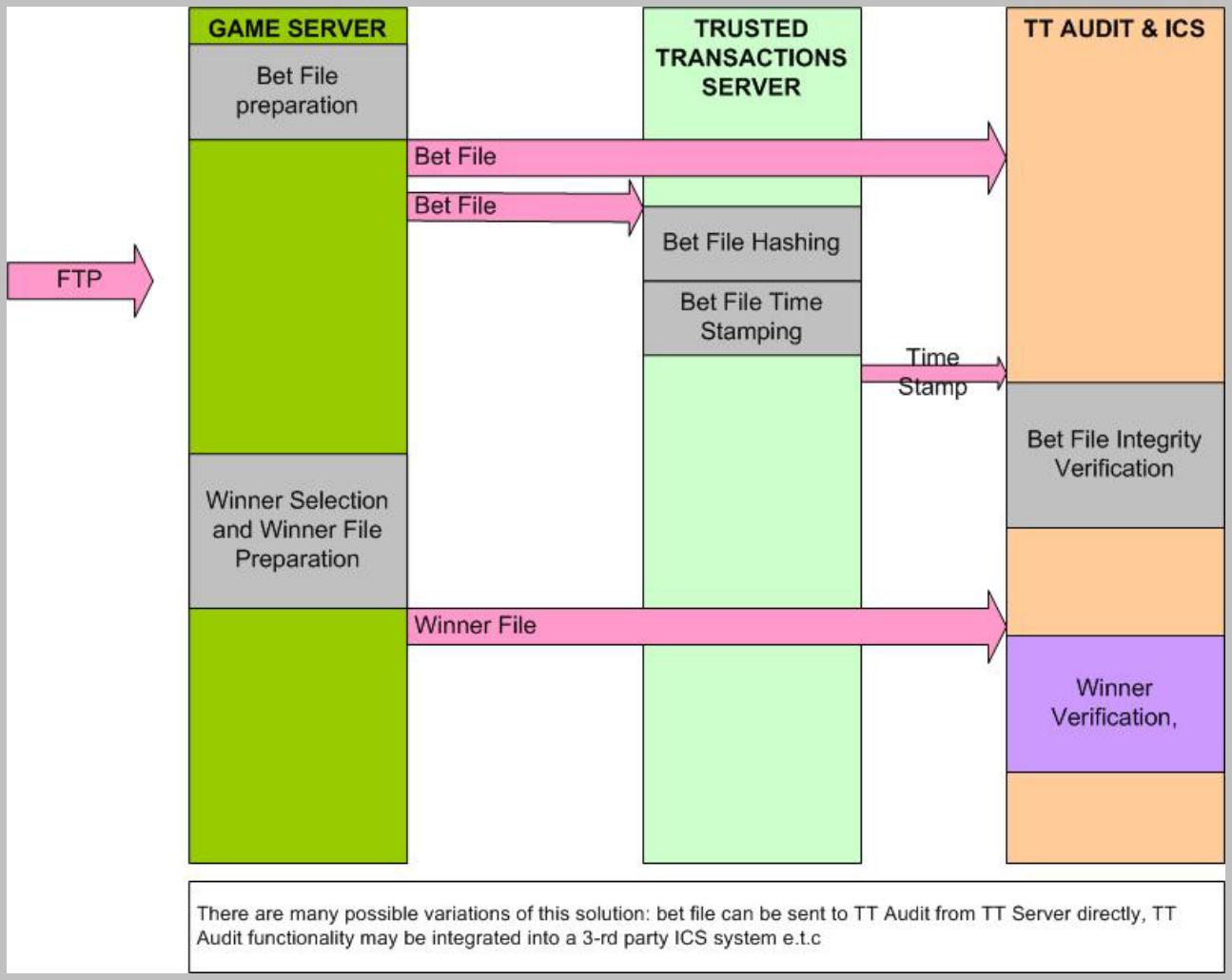
TT Audit & ICS External - TT audit verifies bet file and bet file time-stamp. Optional ICS verifies winners. System is separated by firewall. It is connected by VPN if located externally.

TT Audit & ICS Internal - optional audit and ICS system for internal use, same functionality as TT Audit External

Trusted Transactions Architecture



Trusted Transactions Functional Diagram



Trusted Transactions Flow

Security of TT System

TT system is designed with security as a main design goal:

- critical data and RTC protected by tamper evident cryptographic hardware
- digital signatures – 1024 bit RSA
- non-refutable time-stamp proves bet file integrity
  - detects modification of bet file
  - detects use of unauthorized hardware (HSM)
- logs all system activity
- read-only log folders and reports
- enhanced PC security
- fault tolerance is built into TT (hardware and software)