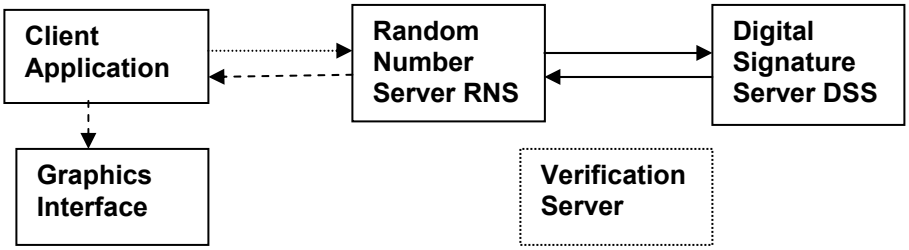
Trusted Draw™ Technical Spec

Executive Summary

Trusted Draw™ is a secure and auditable electronic drawing system for games of chance, with insider fraud detection. Trusted Draw is equipped with state of the art cryptographic hardware and software protecting against tampering with the system. The main advantage of using Trusted Draw™ over any other draw system is that it produces random unpredictable draw results that can be audited. Audit of the draw data proves the integrity of the draws, even years after the draws are held. Trusted Draw uses FIPS-140-1 level 2 certified hardware. No other drawing systems have a tamper detection solution as effective and conclusive as Trusted Draw.

System Components

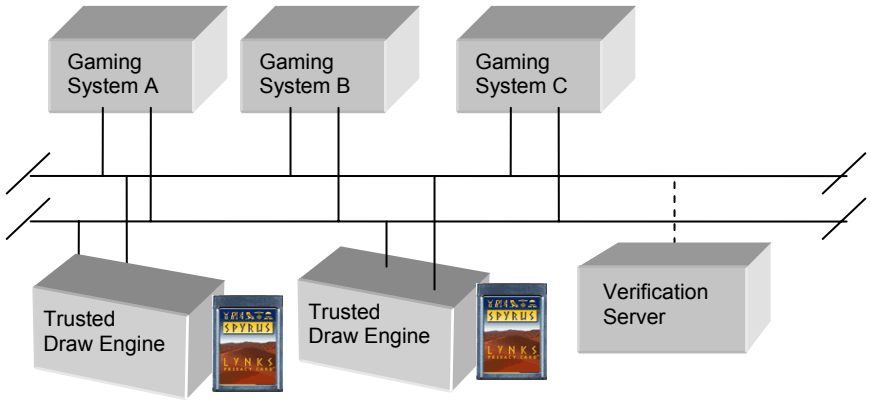
Trusted Draw™ system consists of a Random Number Server (RNS), a Digital Signature Server (DSS) with incorruptible RTC (Real Time Clock), a Verification Server and a Graphics Interface. DSS is a cryptographic tamper evident device – it combines user data with RTC to obtain digital signature. RNS uses elements of this signature for random numbers generation to produce draw data and logs relevant data for audit. The Verification Server uses logged data for auditing of the random number generation process and draw outcomes.



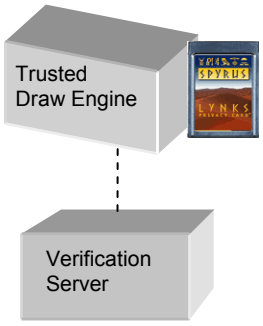
System Highlights

Trusted Draw™ engine operates in **stand-alone** or in **on-line (connected) mode** (see diagram below):

- Stand-alone mode – Trusted Draw™ generates draw data, Client Application reads the file with winning data. Drawing is triggered by:
  - Timer-based draw schedule, parameters: days of the week, start time, end time, frequency, game matrix, multiple schedules capability;
  - Operator request.
- On-line (connected) mode – Client Application requests the draw and Trusted Draw™ provides draw data. To communicate with Trusted Draw™ Client Application may use:
  - File exchange,
  - SOAP interface,
  - Custom connection.



On-line - connected mode



Stand-alone mode

Trusted Draw™ engine is **reliable** and **robust**; it is protected against single-point-of-failure by:
- Single Trusted Draw™ engine connects to multiple systems. Each of the systems may request draw data;
- Capability to connect to multiple Trusted Draw™ engines from a client system;
- Support for multiple LAN connections;
- Primary and backup logging to local or remote system;
- Redundant crypto processors.

Multiple API's for draw data generation and verification are supported to cover needs of all types of games:
- Numbers from the range 1 to N, where N is a number between 2 and 2,000,000,000 (Numbers game, Joker);
- N out of M, with or without replacement (Lotto, Keno, Bingo, Card Games … e.g. N=6, M=49 for Lotto 6/49);
- Table based distributions;
- Custom distributions for special applications.

Other optional interfaces:
- Built-in 'Bubbles Graphics' display allows for remote on-line draw viewing via Internet/Intranet or broadcast TV. Graphics are customized for customers and include logos, desired themes and advertising on the display;
- Customer provided graphical display;
- Logging of generated draw outcomes, input data, digital signature and request time required for audit.

Verification and Analysis

Audit of Trusted Draw™ generated draw data can be performed in two ways:
- Logged data audit on a separate PC-based Verification System;
- Optionally client may integrate audit functionality into an ICS (Internal Control System) system.

Statistical analysis of draw data:
- Built in capability to generate large data sets. These data sets could be analyzed with specialized packages like Diehard Battery of Tests or by independent testing organizations;
- Analysis of the frequency of the individual numbers generated;
- Analysis of correlation between different sets of numbers generated.

Digital Signature Server

Trusted Draw™ works with LYNKS Privacy Card, a plug-in Hardware Security Module (HSM), from SPYRUS, world's largest producer of PC Card based security tokens. LYNKS Card is a tamper evident device, complying with Federal Information Processing Standard (FIPS) 140-1 level 2. LYNKS Card firmware ensures integrity for gaming applications. http://www.spyrus.com/content/products/rosetta/HSM.asp

Technical Specifications

Security

- FIPS 140-1 level 2 tamper evident cryptographic hardware
- Client authentication
- Generated random numbers have cryptographic strength of 1024 bit RSA digital signatures
- Detection of modification of drawn data
- Detection of missing or superfluous draws
- Detection of change of the game matrix
- Detection of time attacks (before time draws)
- Detection of "fishing" attacks
- Detection of use of unauthorized HSM

Software

- OS: Microsoft XP Professional
- Language: C++.

Hardware

Trusted Draw™ engine:
- PC desktop or laptop, as requested or provided by the client
- Speed min 500 MHz
- Memory 512 Mbytes
- Disk space 50 Mbytes plus disk space required for the logging of draw data.
- PCMCIA 2.0 compliant interface
- One or two HSM-s per engine

Verification Server:
- PC desktop or laptop, as requested or provided by the client
- Verification subsystem resides on client's Internal Control System (ICS)