

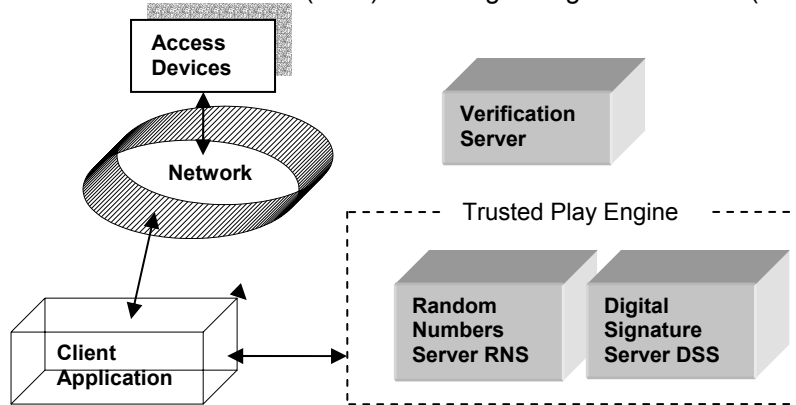
Trusted Play™ Technical Spec

Executive Summary

Trusted Play™ is a secure and auditable system that generates outcomes for instant win games played over a variety of channels (such as on-line, internet, mobile, and VLT). Trusted Play detects tampering with instant win game outcomes by state of the art cryptographic hardware and software. The main advantage of using Trusted Play over any other system is that it produces unpredictable random game outcomes that can be audited. Trusted Play ensures required statistical distribution and provides an audit trail. Audit of the game data certifies the integrity of the system, even years after the game is played. Trusted Play uses FIPS-140-1 level 2 certified hardware. No other bet generation system has a tamper detection solution as effective and conclusive as Trusted Play.

System Components

Trusted Play™ system consists of Trusted Play Engine and Verification Server. The Trusted Play Engine includes a Random Numbers Server (RNS) and a Digital Signature Server (DSS).



- Client Application provides input data elements required for play number generation.
- RNS resides on a separate device. RNS communicates with the Client Application and DSS. RNS generates game data, and logs audit information.
- DSS is a secure tamper evident Hardware Security Module (HSM) - a plug-in card on the RNS.
- DSS utilizes a private key for digital data signature; it ensures that the digital signature is always unique, even for the same data.
- Verification Server is an independent system; it stores a public key for digital signature verification.
- Verification Server receives logged audit data over the Network or via storage media such as tape or disk. This functionality may be provided by an already existing audit system.

System Highlights

Trusted Play Engine code resides on a dedicated machine and communicates via LAN with Clients Application using socket or SOAP interface. Trusted Play engine supports redundancy and high reliability:

- No single-point-of-failure
- Capability to connect to multiple Trusted Play™ engines from a single client computer
- Two LAN connections supported
- Multiple DSS supported
- Logging of audit data to multiple files.

Trusted Play supports API's for standard games generation and verification:

- Set of unordered numbers from a range of N to M, where N and M are numbers between 1 and 2,000,000,000 (Numbers, Joker, Bingo, Cards, etc). Generation is with or without repetitions.
- Set of N out of M ordered numbers with no repeats (Lotto, Keno, e.g. N=6, M=49 for Lotto 6 / 49)
- Table based winners distributions:
 - Based on the probability of occurrence of each entry - Class III games.
 - Based on the fixed pool representing desired outcomes – Class II games.

Verification and Analysis

Verification of Trusted Play™ system generated play data is usually done on a separate verification server (PC). Client may optionally integrate audit functionality into an existing audit system or ICS.

Verification Server provides statistical analysis of play data:

- Analysis and simulation of actual play data
- Statistical analysis of simulated data:
 - Analysis of the frequency of the individual numbers generated
 - Analysis of correlation between different sets of numbers generated

Trusted Play™ Application Flow

Play numbers generation:

1. Client Application prepares verifiable input data and requests play data from RNS.
2. RNS prepares input data for digital signing.
3. Input data is passed to the DSS.
4. DSS generates input data digital signature using private key.
5. RNS uses digital signature to generate game outcomes. No secret keys or proprietary algorithms used.
6. Input data and digital signature are logged by the RNS.
7. Game elements are passed back to Client Application.

Play numbers audit:

1. Verification Server reads input data and digital signature.
2. Verifies input data.
3. Verifies the digital signature using public key.
4. Recreates random numbers using digital signature.

Digital Signature Server

Trusted Play™ works with LYNKS Privacy Card – a plug-in HSM by SPYRUS, world's largest producer of PC Card based security tokens. LYNKS Privacy Card is a tamper evident device. It keeps its private key in the CMOS memory inaccessible externally. LYNKS Privacy Card is FIPS 140-1 level 2 certified.

Technical Specifications – Hardware

Trusted Play Engine:

- PC desktop or laptop, as requested or provided by the client
 - Recommended speed min 2.4 GHz
 - Memory - 512 Mbytes
 - Disk space - minimum 5 Giga Bytes required for logging
- Cryptographic hardware:
 - 2 PC Card Readers LYNKS HSM, Model no RD300 PC400 PCMCIA 2.0 compliant interface
 - 2 LYNKS HSM from SPYRUS

Verification Server:

- PC desktop or laptop, as requested or provided by the client

Architecture Diagram

