Trusted Transaction

Trusted Transaction™ (TR) server is a product designed to digitally timestamp, record and verify transactions.

- It has a high-performance transaction engine processing up to 2,000 TPS[1].
- It operates 24/7/365 in a fully automated way, without operator intervention.
- For higher performance and redundancy, multiple TR servers and multiple HSM (hardware security modules) can be deployed.
- **Typical lottery configurations include:**

  two TR servers, each with two HSMs, one Trusted Audit™ (TA) system and one Trusted Monitor™ (TM) system in a primary site and the same or reduced configuration in a backup site.

- TR server logs in real time[2] all transactions locally; in addition, it logs transactions to one or more remote systems: TA system or ICS, etc.

TR can be deployed together with Trusted Draw (TD – RNG server for draw games) and Trusted Play (TP - RNG server for instant win games and interactive games).

While all the functions are described in context of gaming systems, TR can be deployed for any transactional environment where transaction data integrity verification is required, e.g. personal records, medical records, financial transactions, etc.

Trusted Audit

TA system combines transactions from multiple TR servers and allows viewing transactions from all TR servers. In addition to viewing/verifying single transactions, it automatically verifies signatures for every transaction and creates an extract of all transactions logged. Depending on configuration, the extract can be in one or more .CSV files. For each business day, a separate set of extract files are created. These files can be either imported from TA server, or they can be automatically exported by TA server using FTP or sFTP.

[1] TR supports two types of logging: optimized and non-optimized. In optimized mode, response time is ~20 msec and TR supports up to 2,000 TPS. The transaction is actually signed and logged up to 250-350 msec after TR response. In non-optimized mode, TR supports up to 1,000 TPS. The response time is ~200 msec, transaction is signed and logged before TR responds to gaming system.

[2] Logging to remote system may be delayed up to 300 milliseconds after the transaction is logged locally. In the case of a network interruption, logging is automatically resumed without operator's intervention. Logging to remote system is either in clear or encrypted, using AES and many other standard encryption protocols.

Viewing of transactions

Transactions can be viewed directly from TR system, but is limited to local transactions. When viewed from a TA system, all transactions from all TR systems are available. To view specific transactions, a TR transaction identifier (URI – Universal Record Identifier,) assigned by TR system, is used. On TA or TM systems, either URI can be used or a transaction ID from a gaming system could be used (not currently implemented). TR server supports URI access on the same business day or for previous days. TA and TM system supports access by URI and gaming system transaction ID[3] on the next business day, for a previous day or any days before.

Transactions can be viewed via TM user interface (search by a transaction ID via a browser) or using a XML-RPC request[4]. TR server or TA system will locate a transaction, verify the transaction signature, and provide transaction extract in the form of two records: comma separated field description record and comma separated values of the record. Both TR servers and TA systems are configured with descriptions of each type of record. New records' layouts can be easily configured.

System Interface

Gaming system interface to TR is via S2S standard XML-RPC protocol[5]. As a part of request, gaming system (client) provides user data in a form of ASCII ';' separated string of fields. TR Server provides a transaction URI and URI handle. These can be used to access transactions; URI will always provide an access to the record, URI together with URI handle allows for much faster access to the record.

Proposed TR Deployment for Draw Verification using ICS system

1) All active wagers, cancellations and other critical transactions are sent to TR server for time stamping. If Trusted Draw (TD) is used and TD RNG is performing a draw, hash of all valid wagers[6] is also included in a draw request.
2) The gaming system records the draw URI.
3) ICS system then obtains verified and decoded draw information from either TD RNG or TA system (using either XML-RPC request or export/import of decoded transactions from TA).
4) At this stage ICS system should verify if the winning numbers are the same as those used by gaming system, and if hash of wagers is correct.
   a) If draw numbers are incorrect or the hash of wagers is incorrect, the issue should be investigated.

[3] Access by gaming system record identifier is not currently supported. A lookup function can be implemented on gaming system or on TA / TM.
[4] For example, XML-RPC request is used by Lottomatica to verify instant win transactions.
[5] Other standard or proprietary protocols can be implemented.
[6] This hash needs to be calculated in a way that ICS system can verify it.

b) If hash of wagers is incorrect, TA system should export all decoded transactions to ICS system for reconciliation[7].

If TD RNG is not used for drawing, a similar technique can be used. Instead of draw numbers, a 'draw signature' should be requested by the gaming system. In the request, the gaming system should provide a hash of all valid wagers. TR system will digitally sign the draw. ICS should verify the bets similarly to when TD RNG was providing the draw service.

Information signed (and verified)

TR server timestamps the following information:

1. **User data**: critical transaction data. Data has to be provided as ASCII string with fields separated with ';'
2. **NTP**: synchronized clock time of TR Server
3. **Built in RTC (Real Time Clock) on HSM**: the clock is protected by HSM and cannot be changed[8]. This clock can prove actual signing time even if the clock on the TR Server was manipulated.
4. **Sequencer**: HSM controls a built-in sequencer, so that every generated signature is accounted for; this ensures that no transactions or signatures can be inserted.
5. **One or more transactions:** transactions are signed in real time, however under high volume many transactions can be signed together.
6. TR control information (e.g. URI)

If there is a need for independent verification of data and digital signatures, S2S will provide the format of the signed data.

Architecture

Attached drawing presents a typical architecture of Trusted Transaction, with a primary and a backup data center.

- **Primary data center:** two Trusted Transaction servers, a Trusted Audit system, and Trusted Monitor system in the primary data center
- **Backup data center:** Single TR and TA system
- *In addition, a test environment is included where TR and TA servers can coexist on a single system.*

[7] Szrek developed a simple technology for reconciliation of digitally signed transactions by TR and transactions received in a different format by ICS system from the gaming system. This method of reconciliation of individual transactions can be implemented on ICS system.
[8] RTC suffers from a small drift. This drift is 'constant' and conformance of the RTC and actual time is easily verifiable

TR systems are connected to the gaming system and TA systems are connected to the ICS. Depending on the requirements, different system configurations can be used. TM allows viewing transactions from all TR and TA and to verify single transactions. TR allows viewing transactions from one system or from other TR systems. When a request is made to view a transaction from another system, TR automatically routes viewing requests to TR servers that issued the transaction and reroutes the response to the client.

Sample configuration

TR can operate on the same system as Trusted Draw / Trusted Play RNG products. All TR, TD, TP, TA and TM systems operate on Windows 2012 R2 or later. TR server and TD RNG servers are equipped with one or two[9] HSMs (LYNKS II USB cards).

For cost efficiency TR, TA and TM systems can be virtualized.

Disk sizing

Disk sizes should be configured according to expected transaction volume requirements. When a single transaction is signed, each transaction is 1-1.5 KB. Under high volume, transactions are signed in batches. Each additional transaction signed in a batch carries an overhead of length of user data plus 16-24 bytes. In optimized mode, there are four batches per second.

TR requires approx. 200 MB, plus OS overheard, plus transaction storage. We normally configure it for minimum 70 GB. Size needs to be adjusted to expected volume requirements.

TA requires disk space to store transactions from all TR servers. Each verified and decoded transaction is ~0.5 KB (verification overhead) plus actual length of user data. We normally configure it for minimum 70 GB. Size needs to be adjusted to expected volume requirements.

Trusted Monitor does not require extra disk space.

Other Server Elements

We suggest using the same basic Windows server class hardware and the same maintenance as for online system. Each system should have at the minimum 8GB of memory and a single dual processor and single or dual LAN.

[9] Two cards are used for redundancy; however, our experience reflects that these cards are very reliable.

Test and staging systems

For test systems, we recommend using the same hardware, with smaller disks. TR and TD RNG can use a single LYNKS HSM. For staging environment, we recommend using exactly the same configuration as for production.

HSM

S2S configures two LYNKS HSMs on each TR server (TR server and TD / TP RNG server can be located on the same hardware box). HSM provides time stamping functionality for TR and RNG seeding for TD/ TP RNG.

For security reasons, TD RNG needs to use LYNKS HSMs or another time stamping device with an incorruptible sequencer controlled by the HSM. TR server can be programmed to time stamping devices that do not support the sequencer. TA and TM do not need access to time stamping devices.

LYNKS HSM hardware (physical security), roles, services, authentication and design are certified to FIPS 140-2 level 3. LYNKS HSM overall certification is FIPS 140-2 level 2.[10]

[10] Certification on US government NIST web site: (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt679.pdf).

TR Schematic