Trusted Draw™ Family of Products

Szrek2Solutions (SZREK) designed its draw system, Trusted Draw™, to support various lottery principles, such as trust, growth and changing environments:

1. Ensure **trust**. Trusted Draw was designed and implemented to ensure transparency in generation of draw numbers. There are a few major elements enabling this trust:
    a. ***Physical security*** – enforced by lottery
    b. ***Secure system set up*** – enforced by a setup of Trusted Draw system by SZREK.
    c. ***Procedures enforcing security*** – enforced by the lottery procedures
    d. ***Audit system which will detect fraud if any of previous measures were broken*** – provided by Trusted Audit™ system by SZREK.
2. Provide **growth**
    a. ***Support for current and future games*** **-** Trusted Draw supports traditional games such as lotto, numbers, high frequency games, such as Keno or Bingo, and many innovative games, such as individual player games, various raffle games, raffle-combination games, etc.
    b. ***Future proof security*** – Trusted Audit detects integrity issues independent from Trusted Draw drawing solutions, versions, configurations, and environments.
    c. ***Migration path*** – Trusted Draw can be deployed initially in a simple configuration and allows migration to more complex environments.
3. Support **change** – Trusted Draw supports different drawing solutions to fit various environments.
    a. Enable secure draw in a **variety of environments**:
        i. ***Offline*** - stand-alone, portable draw system located in a secure location, such as a draw room; draws conducted manually
        ii. ***Remote*** – draw system located in a data center; draws invoked manually from remote location
        iii. ***Online*** – draw system located in a data center, connected to the gaming system; automated draws invoked by the gaming system
    b. Enable **monitoring** the draws remotely in real time
    c. Provide **portable drawing solution** which would enable local drawing during special events, e.g. during state fair or football game.
4. Integration with Animation Manager™ – Trusted Draw creates the file that is automatically processed by Animation Manager. Animation Manager automatically renders the animation with VOR (where numbers drawn are pronounced by the speaker). Animation Manager provides capability to upload rendered animation to social sites and TV broadcast stations.

Unpredictable and Verifiable Random Numbers

In 2003 SZREK designed and patented[1] a unique secure technology for generation of random numbers, which allows auditing of random numbers to ensure transparency of the draw process. The basic features of this certified technology are:

- use of tamper evident hardware for RNG seed generation,

[1] SZREK RNG technology was patented in the US, Canada, and other countries. US patent no 6,934,846

- generation of winning numbers in a way that provides mathematical proof[2],
- digital sealing[3] of wagers before the draw,
- accountability for each random number generated,
- capability to verify draw time[4],
- real time verification of RNG seed to detect any hardware problems, which could lead to faults,
- ability to audit draw outcomes any time after the draw - a second or years later,

The above features of draw systems from SZREK are truly unique and provide unmatched transparency in generation of draw numbers, ensuring verifiable integrity of not only the draw process but also wagers participating in the draw.

The RNG generation process involves generation of a so called RNG seed and from the seed a cryptographic strength random numbers (draw numbers) are generated. The random numbers are unpredictable and independent– the knowledge of any random numbers does not allow deducing any previous or future random number. The tamper evident hardware used by SZREK for generation of random numbers is LYNKS II HSM (Hardware Security Module) - a cryptographic processor from SPYRUS[6]. LYNKS II HSM is certified by NIST as a tamper evident device which allows detecting any attempt to expose a private key it contains. The private key is used to generate a digital signature and provides a public key used to verify the signature/seed. The seed is used to generate random numbers via mathematical functions and knowledge of the seed allows verification of any random number generated. Since the private (signing) key is unknown the seed and the outcome in unpredictable, however the public (verification) key is available so the verification of the outcome can be done. To further secure the seed and the generated random numbers other two features of LYNKS II are used – real time clock (RTC) and an internally controlled sequencer. The clock allows verification of the time when the random numbers were generated and the sequencer provides accountability of every generated random number. The use of sequencer also enforces that each digital signature is different.

---

[2] Actually generated numbers are mathematically proven. This methodology is accepted by US jurisdictional system as valid evidence.

[3] SHA1 or SHA256 of bets is digitally signed/ time stamped as a part of draw numbers generation. Any modification of bets after the draw can be detected

[4] Time of the draw is digitally signed. Two different clocks are signed: system time and real time clock safeguarded by HSM

[5] Trusted Draw RNG meets all randomness and certification requirements without the use of so called true or hardware RNG. Some lotteries require in their RFPs use of hardware RNG.

[6] SPYRUS is a leading supplier of authentication equipment for US government, NSA and US military http://www.spyrus.com/products/lynks_hardware.asp

Based on this technology SZREK developed its Trusted Draw™ product and a suite of related *trusted* products. These products have been deployed by lottery customers over the last 12 years. In order to respond to different customer requirements SZREK provided four different types of draw systems. They all use the same certified RNG engine platform and benefit from the audit functionality offered through the Trusted Audit™ system. To suit diverse customer needs they offer different interface to a draw/RNG client:

1. **Trusted Draw 360™ Offline**. The TD 360 offline system is a stand-alone, introductory draw system, not connected to a network and draws are conducted manually. Draw Manager and Draw Auditor log directly to a Trusted Draw system to manually conduct a draw via TD 360 GUI. All typical lottery draw games: lotto, numbers, joker, raffle, 2nd chance draws etc. are supported. TD 360 offline comes in a portable and stationary configuration; minimum configuration includes two TD 360 systems and optional Trusted Audit system. This is the least expensive draw system to buy, however the operational costs related to security and staffing requirements are the highest. Trusted Draw Offline is ideal for daily and weekly games and infrequent draws such as raffle draws or promotional draws and can be used for off-site draws e.g. at fairs without sacrificing security. SZREK provided these systems as a rental to Florida Lottery and Kansas Lottery, as a multiyear lease to Iowa Lottery, Texas Lottery, Oregon Lottery and multiple times as a draw service to South Carolina Educational Lottery (SCEL). For SCEL a Trusted Audit system was also provided.
2. **Trusted Draw Remote**. This solution is ideally suited for environments where draw needs to be invoked manually but a physical drawing system is located in a secure remote location, such as an on-line system computer room or a central drawing facility for many lotteries. Trusted Draw Remote comes in two flavors – draw via TD 360 GUI or draw via browser.

   (b) **Draw via TD 360 GUI** (TD 360™ Remote). Draw Manager and Draw Auditor log securely from the remote PC through GUI interface. They need to be collocated, if requested SZREK may develop functionality to not require collocation. Remote observer, in another location, may observe the draw, but observer is not required to conduct the draw. Draw Manager conducts a draw; draw Auditor monitors the draw. The Trusted Draw system is usually provided in a configuration with a redundant system, in a single site or in multiple sites (primary and backup data centers). The Trusted Draw Remote provides support for all typical lottery games. It was deployed to support numbers games, lotto games, raffle and 2nd chance draws. Corresponding Trusted Audit system provides support for verification and auditing of draw numbers and draw process. There might be one or more Trusted Audit system deployed. TD 360 Remote supports all Trusted Draw Online and TD 360 Offline functionality.

   (a) **Draw via Web browser** - Draw Manager and Draw Auditor log securely from their PC-s to a management console system called Trusted Monitor™ through a browser[9] interface. They do not have to be collocated; however, both need to be logged to perform the draw. Draw manager conducts a draw; draw auditor monitors the draw in real time. Both have the capability to print draw reports, which can be then signed. The Trusted Draw system is usually provided in a configuration with a redundant system, in a single site or in multiple sites (primary and backup data centers). The Trusted Draw Remote provides support for all typical lottery games. It was deployed to support 2, 3, 6 digits numbers games and lotto game. This system also supports raffle-combination[10] draws. Corresponding Trusted Audit system provides support for

verification and auditing of draw numbers, draw process, integrity of bets and integrity of winner selection. There might be one or more Trusted Audit system deployed. Trusted Audit systems do not need to be located in the same data centers. Such system was provided to lotteries in the UK, Pakistan and Russia. Trusted Draw Remote supports all Trusted Draw Online functionality. Trusted Draw Remote can be deployed to also interact with an ICS system. The Trusted Draw RNG, Trusted Monitor and optional Trusted Audit are deployed on Windows Servers.

3. **Trusted Draw Online.** This is the most economical and convenient system to use. Drawings are invoked directly by an on-line gaming system, communicating via a standard protocol XML-RPC. A physical drawing system is located in a secure remote location such as an on-line system computer room or a central drawing facility. In this case Lottery establishes directly how and when draws are generated with its online vendors. Since draw is invoked in an automated fashion and there are no operational procedures, a draw break may be as short as a fraction of a second. The system is easy to integrate to online gaming system via standard XML-RPC interface. Using a standard browser, Operations and draw auditor may follow in real time drawing from a remote location over the LAN or VPN. This system is ideally suited for all typical lottery draw games including high frequency draw games such as Keno or Bingo. This system can also support raffle-combination draws. Corresponding Trusted Audit system provides support for verification and auditing draw numbers, draw process, bets integrity and integrity of winner selection. There might be one or more audit systems deployed. Trusted Audit systems do not need to be located in the same data centers. Such drawing system was provided to lotteries in Denmark and Italy. Trusted Draw Online can be combined with Trusted Draw Remote, i.e. it can support remote draw functionality for some games. Trusted Draw Online can be installed to interact with an ICS system. Trusted Draw Online also supports Trusted Play™ functionality (generating outcomes for instant win games) and to Trusted Transactions™ (digitally signing bets in real time). The Trusted Draw, Trusted Monitor and optional Trusted Audit are deployed on PC servers.
4. **Trusted Draw Hybrid.** This is the most flexible and convenient system to use. It combines the features of TD 360 Remote and Trusted Draw Online. Drawings are invoked either directly by an on-line gaming system, communicating via a standard protocol XML-RPC or by a remote TD 360 GUI or customer provided GUI. A physical drawing system is located in a secure remote location such as an on-line system computer room or a central drawing facility. For Gaming System invoked draws Lottery establishes directly how and when draws are generated with its online vendors. Since draw is invoked in an automated fashion and there are no operational procedures, a draw break may be as short as a fraction of a second. The system is easy to integrate to online gaming system via the standard XML-RPC interface. Using a standard browser or another TD 360 Remote GUI, Operations and draw auditor may follow in real time drawing from a remote location over the LAN or VPN. This system is ideally suited for all typical lottery draw games including high frequency draw games such as Keno or Bingo. Corresponding Trusted Audit system provides support for verification and auditing draw numbers, draw process, bets integrity and integrity of winner selection. There might be one or more audit systems deployed. Trusted Audit systems need to be collocated, another observer might be in another location. If desired Szrek may provide a support for Draw Manager and Draw Auditor conducting draws in different locations.