

Trusted Draw 360™ Overview

Trusted Draw 360™ is a modern, secure and cost effective draw proposition for any lottery or a game provider seeking a draw machine for a new game or planning to replace existing draw machines. Trusted Draw will support all current client lottery games and draw needs within a single system platform and be easily adapted to game changes or new games in the future, including add-on, instant win or promotional games. Trusted Draw uses a patented RNG method of generation of auditable random numbers with built in fraud detection. The Trusted Draw RNG has been certified by multiple independent labs. Trusted Draw has been used successfully by lotteries since 2005 in the US and internationally.

Trusted Draw has flexible configuration adaptable to clients needs. It is offered in an *offline* mode, *remote* mode or in *online* mode: in offline mode draw system is stand alone and is operated via a GUI, directly on the draw system. Remote mode allows triggering or observing draws securely from a remote console, while the actual draw system is placed in a secure site. Two staff persons need to log into the system to perform a draw, additional staff may witness the draw independently from a different console or location. In online mode Trusted Draw is securely connected to the lottery gaming system, which triggers draws and obtains automatically draw results. Remote and on-line mode can be combined to allow for variety of operational modes, e.g. to support frequent draws on-line and traditional or promotional draws in a TV studio.

An important feature of Trusted Draw is automation. It allows reducing to minimum complexity and human involvement, with associated with it inherent risks of error and fraud. In the off-line and remote mode draws are initiated with a single click, for all games with consecutive draws; there is no room for error as all game parameters are predefined and then certified, including if a lottery choses time window for the draw to be carried in. In the online mode draws are fully automated and draw parameters are predefined and executed, with no human participation during the draw.

Trusted Draw introduces high level of draw security, which ensures draw integrity – essential factor for all lotteries as the integrity of game provider is a critical element for the public and essential for successful games. In addition to standard preventive security measures such as dual log-in and protected console logs, Trusted Draw has integrity verification designed into the system. It guarantees detection of any and all attempts of draw fraud. This includes hard to discover insider fraud, which in other computerized draw systems can go undetected, due to limited audit capability. Traditional audit verifies syntax of logged draw data, Trusted Draw technology allows to verify draw data semantics – that the actual draw numbers and draw time were correct. Traditional audit relies on draw audit logs, which could be manipulated if draw system was compromised. Draw logs created by Trusted Draw system cannot be modified or created fraudulently without detection.

Trusted Draw comes optionally with Trusted Audit and Trusted Monitor systems, which allow verification and observing the draw: Trusted Audit provides mathematical verification of four critical draw factors, immediately following the draw or any time thereafter: (1) that the numbers presented at the draw were the actual rightful numbers generated by the system, (2) that the numbers presented at the draw were generated at the exact time indicated, (3) that the numbers presented at the draw were generated from the correct number range and (4) that the specific rightful hardware was used for draw generation. This verification can be done any time – immediately after the draw or years after.

Trusted Monitor allows real time monitoring of Trusted Draw and Trusted Audit systems. It is usually used with online draw system.

Additionally in online and remote mode Trusted Draw offers integration with ICS system - Trusted Audit can provide critical draw data to the lottery ICS system in real time for verification, to prove draw integrity.

Trusted Draw uses secure tamper evident hardware for random number generation. NIST certified LYNKS II hardware security modules (HSMs) from SPYRUS are used to generate digital signatures from which random numbers are derived according to Szrek2Solutions RNG patented generation method. Each RNG system may be optionally configured with Quantis hardware (True) RNG. This is done if lottery requires such device. Szrek2Solutions incorporated Quantis RNG preserving all security features and audit capabilities of Szrek2Solutions technology.

Supported Games

Trusted Draw was certified for various game types:

- (1) Lotto: any matrix such as regular lotto, bingo, keno, etc. Draw numbers can be sorted or unsorted
- (2) Numbers: any number of digits is supported, with and without repetitions
- (3) Table based games: probability of winning particular outcome is described by a distribution table:
 - Tables with pool depletion
 - Tables without pool depletion
- (4) High frequency games: e.g. 5-min Keno, electronic Bingo; Szrek2Solutions supports draws for the games designed for multiple players or individual players.
- (5) Raffle games:
 - Standard raffle games with N numbers drawn from a specific range with and without replacement.
 - Enhanced raffle games:
 - Raffle with cancelled tickets (i.e. incomplete range) and with multi draw support
 - Raffle with weighted odds for different raffle entries (e.g. for promotional games where chance of win is proportional to amount of sale),

For all raffle games numbers can be drawn with and without replacement, with support for multiple divisions, sorted and unsorted, game ranges can be provided manually via a console or via a file interface

- (6) Raffle-combination draws for lotto and number games. Trusted Draw system chooses a winning bet from the set of played wagers, each played combination has the same chance to be drawn. This type of game is ideally suited for lotto or joker games where lottery wants to guarantee a winner.
- (7) Second Chance: a winning bet is randomly selected from a set of wagers submitted for additional draw.

RNG certifications were performed by FORTE Technology, in Denmark, by La Sapienza University of Rome, Italy, University of Copenhagen, Denmark, and multiple certifications by GLI (Gaming Labs International), TST (Testing Labs), Eclipse Testing. Szrek2Solutions technology security was certified by Vigil Security.