

Trusted Draw™ and Trusted Play™ White Paper.

What are Trusted Draw™ and Trusted Play™?

Trusted Draw™ and Trusted Play™ are two innovating products offered by Szrek2Solutions. They provide a tamper proof system for computerized draws and for computerized 'instantaneous winner' games. They are based on a patented method of unpredictable auditable random numbers. This method allows both to generate random game elements, such as a draw or a play data, and to audit these game elements. The products use state of the art cryptographic methods used in digital signatures generation. Trusted Draw™ and Trusted Play™ provide ultimate computerized draw and play security and verifiable integrity at a low cost.

The major difference between currently used technologies and the approach used by Trusted Draw™ and Trusted Play™ is the way system security is ensured. In the legacy approach, software, data bases, physical environment, proprietary algorithms, secret information and game elements need to be kept secure to ensure system integrity. In Trusted Draw™ and Trusted Play™ audit of the game elements and information used for their generation is sufficient to determine system integrity. In addition, audit can be done by a 3-rd party without exposing any secret information. There is no proprietary information or secret algorithms used. The audit can be done at any time after the game element was generated, even few years after. Trusted Draw™ and Trusted Play™ are using cryptographic hardware for game elements generation. The same cryptographic technology is used for verification, with no special hardware required.

In recent years new types of instantaneous games have been introduced into the lottery market – games with on-line generation of instant bets. These games are provided by traditional channel, such as Extra game implemented by Illinois Lottery, or via Internet channel, where instant type games are played. These types of games have bets generated via on-line system, where it is determined whether bets are winning or losing by bet processing software, rather than by a later drawing. This creates a new paradigm that requires new security measures to prove system integrity. Bet generation where ticket is an instant winner should require the same level of security as a traditional lottery draw. In traditional lottery games, after the draw drawing machines could be audited to prove that they worked correctly.

Similar issue appears in relation to on-line games with frequent draws. A very different type of drawing machine was introduced; when the frequency of draws was increased to tens or even hundreds per day (as for a Club Keno game) computer software is used to generate draws.

What are currently used security measures for draws?

Currently most common techniques used by Lotteries, to ensure draw security, are physical security and a physical draw machine audit. Physical security relates to limited access to a drawing machine and verifying that the drawing machine is intact (e.g. weighting of balls). Similar system security is implemented for the computerized drawings: machines are physically locked in separate rooms with constant monitoring; winning numbers are locally logged to the file and could be later compared with the actual results logged and statistically analyzed.

What are the drawbacks of security of the computerized draws?

Current approaches to security of computerized draws have drawbacks: draw elements are either somewhat predictable or if they are truly random, they are not auditable. The main protection against the fraud is a physical security and frequent inspections, which are costly and may not always be effective. As a result security could be circumvented by a skilled and dishonest programmer with access to the system. If an insider exchanged lines of code and was able to obtain winning bets, then replaced back the changed code, there would not be a clear proof that such a fraud took place, providing it was done smartly.

It is not to say that such a fraud is easy to do, but it is possible and not easily detectible. With the use of Trusted Draw™ a fraud in generating draw numbers will be detected by standard audit procedure. It will not be possible by anyone to generate draw numbers without detection, hence removing risk of a fraud.

What are the security requirements for computerized draws?

The new requirements are based on the understanding that one needs unpredictable and verifiable results and verifiable draw methodology. Verifiable methodology ensures that even if a sophisticated insider

(e.g. malicious programmer) is able to get an undetected access to the system to alter the draw results, any such change would either be detected or would not affect security and integrity of the draw results.

What should be the requirements for the computerized instantaneous winner type games?

As for the draw procedures the requirements are based on the understanding that one needs unpredictable and verifiable results and verifiable methodology. We need guarantee that even if a malicious programmer is able to get an access to the system and modify any data or software, any change to the play outcome would either be detected or would not affect security and integrity of the play.

Are these security requirements cost effective and feasible?

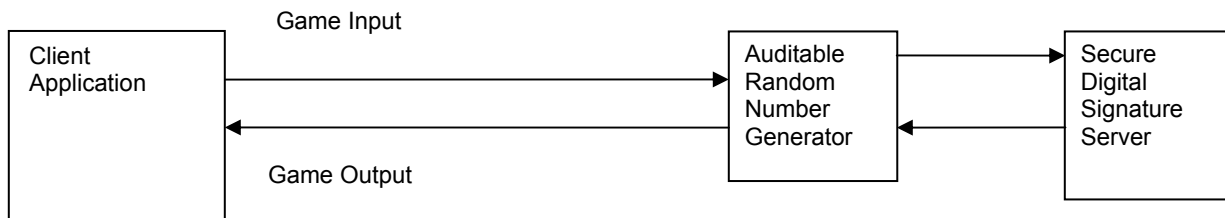
Recent developments in cryptographic hardware and software techniques allow approaching this problem in a novel, cost effective way. One can generate auditable, non-repeatable and unpredictable random numbers. Not only the random numbers are not predictable and auditable but also any input provided for their generation such as game and draw numbers or user ids are also auditable. On the basis of random numbers, draw numbers or instant play outcomes can be generated. Later the draw numbers or instantaneous winner bets can be audited. Audit can be provided any time, even repeated a few years later.

Examples of Gaming Applications that need to be audited

Following is a sample list of different applications that could be audited using Trusted Draw™ and Trusted Play™ methodology:

- Computerized draws.
- Instantaneous winner bets for the lottery add-on games can be generated according to a desired distribution.
- Any computerized games that are a game of chance, such as instant games, card games, games with spinning wheels, with throwing dice, and alike.
- Instant games played over the Internet or mobile phone channel can be generated according to desired distribution.
- Casino games played over the Internet or mobile phone channel can be generated according to desired distribution.
- In Casino on computerized machines winning could be generated in real time according to the desired distribution.
- Draw the winning numbers for progressive Jackpot games.
- Video Lottery plays could be generated in real time according to desired distribution.

How to make the draws and instantaneous bets auditable?



The client application prepares input data. This input data contains information such as game and draw number, terminal id and anything else that may be needed for the later audit. To generate a random number input data is sent to a Secure Digital Signature Server¹. Secure Digital Signature Server “stamps” the

¹ Secure Digital Signature Server is a tamper evident or tamper proof device providing a digital signature for the input data and some additional information, such as serial number provided by the server. The device generates 2 keys: one to digitally sign the data, called private key, and another for signature verification, called public key. Private key is kept secret and not accessible, it is never exposed, not even during its generation. With the public key anyone can independently verify the provided data and the digital signature. The device can be deployed in non-secure environments. Szrek2Solutions is working with two different server providers: nCipher (<http://www.ncipher.com>), and SPYRUS (<http://www.spyrus.com>).

input data and generates a unique digital signature. The string constituting the digital signature can now be converted into one or more random numbers using more traditional methods such as retrieving bits directly from signature (e.g. taking the first 32 bits of digital signature, using pseudorandom generator, encryption, etc). These random numbers are not predictable, as one cannot predict the digital signature; however they are auditable, since one can verify the signature with the public key, recreate from the signature random numbers and check them. These random numbers can now be used to generate draws or to generate a play outcome for instantaneous winner type games. The gaming or drawing system needs to log the digital signature and game element, and make it available to auditor. In addition the method of generating the input data for the digital signature, the method of generating the random number using the signature and the method of generating game element, draw or play outcome, from the random number has to be provided to the auditor.

How to audit game elements generated using Trusted Draw™ and Trusted Play™?

To verify game elements the corresponding steps to their creation are executed on the audit system: digital signature input data is recreated, digital signature is verified, random number is recreated and game element is recreated. By comparing now a game element with actual game element used in the system one can verify the process and game elements. Audit system is an independent system. It may be part of an ICS (Internal Control System) or a PC based independent system. Integrating Trusted Draw™ or Trusted Play™ in the ICS may have an additional advantage of verification of the whole game process on the daily basis with the minimal incremental cost to the audit process.

Current security measures vs. Trusted Draw™ and Trusted Play™

Product Features	Legacy Solution	Trusted Draw™ and Trusted Play™
Generates instantaneous game results with the desired distribution	YES	YES
Generates random draw results with good statistical properties	YES	YES
Audit can always fully determine that the game elements are compromised	NO	YES
Allows to verify integrity and security of game elements generated in a non-secure environment	NO	YES
Resilient to the sophisticated insider attack	NO	YES
Single journal file could be provided for the audit, so it could be easily processed on the audit system (ICS)	NO	YES
All information leading to the game element outcome could be published	NO	YES
3 rd party can be used for independent verification of the game elements (by players as well as a lottery providers)	NO	YES
Reliance on the publicly available/scrutinized methodology and not on internal secrets that could be exposed.	NO	YES
No possibility to access or to compromise sensitive data by the internal or external user or the auditor	NO	YES
Low cost of audit	NO	YES
Tamper proof /tamper evident security	NO	YES