Trusted Draw™- Breakthrough Security Concept

While in recent years Lotteries have been introducing electronic draw systems, there has been growing controversy among the public whether electronic draws are secure. Szrek2Solutions has taken action and introduced its Trusted Draw™ secure electronic draw system. This latest generation of electronic draw machine employs a breakthrough methodology to ensure secure generation of draw results and provides capability for verification. With a cryptographic processor as its ‘electronic heart‘, Trusted Draw is the only system available that can conclusively detect fraud in draw number generation. Even the most untraceable types of fraud can be detected; e.g. insider fraud resulting from access to the drawing machine or conspiracy among draw personnel.

Evidence of Correct Operation

Trusted Draw provides a unique method of random number generation with an unmatched level of security. What is unique is that the number generation process itself creates **evidence of correct operation**. This evidence provides proof of draw integrity that can be readily verified by a security officer or an auditor, demonstrated to the public; for example, by publication on the Internet, or offered as evidence in a legal proceeding as proof of draw integrity. Evidence of correct operation addresses the controversy associated with electronic drawing, as the drawing is now transparent and fully auditable.

Chain of Trust in Legacy Solutions

With other electronic drawing machines, the integrity of the draw results is assumed and confidence in the results is based more on trust than on any actual evidence: trust that draw results are being approved because the drawing system has been certified; trust that certification has uncovered any defects or hidden features in the drawing system; trust that only the system and components certified have been used in the draw; trust that the system certified has not been tampered with or modified; trust that security has been properly enforced; trust that operating personnel have been honest; trust that the drawing has been conducted at the time indicated and not earlier, etc., etc. An approach that relied this much on trust would not be acceptable in many areas of the modern business world; for example, the finance and securities industries. It is surprising that trust is relied upon so much in winner determination in today’s lottery industry.

Trusted Draw - Unique Proof of Integrity

Trusted Draw eliminates the chain of indirect reasoning based on trust, and proves the integrity of the draw directly, without the need to trust the integrity of other elements: physical security, draw system hardware and software, draw personnel, etc. While good practices such as code reviews, configuration control, equipment certification, enforcement of physical security and other procedures are still needed as preventative security measures, with Trusted Draw these measures are no longer the sole source of confidence in system integrity. For every draw Trusted Draw produces an audit trail - evidence of correct operation - which cannot be falsified, even if an attacker has unlimited access to the system software, firmware, or hardware. No other existing drawing system provides this level of security and confidence in the integrity of draw.

Mathematic Verification

The evidence of correct operation produced by Trusted Draw contains draw data and its digital signature. This information is readily verifiable mathematically, using standard cryptographic methods, allowing for the detection of fraud or error in winning numbers or the draw process. This verification can be performed at an auditor’s office, security office, or other location, and can be repeated any number of times any time after the draw - even years later.

Trusted Draw™ - Advantages

Trusted Draw uses a patented method[1] of number generation known as **RUN+A**, which stands for **Random Unpredictable Numbers with Audit**. RUN+A enables the random number generator (RNG) to produce random outcomes in a way that allows for verification of the random number generation process: audit of the random numbers themselves, of the RNG matrix, of the exact time of number generation and of the hardware producing the RNG seed.

There are many important advantages of using the RUN+A method for RNG:

1. Capability to audit winning numbers.
2. Ability to audit the time of random number generation.
3. Capability to audit that the numbers were generated from the correct range/game matrix.
4. RNG Hardware verification.
5. Ability to run verification audit at any time after the draw, also remotely.
6. Proof to the public that draws are transparent and honest.
7. Fraud detection serving as a deterrent to fraud. The certainty of detection all but eliminates the financial incentive for fraud.

The Trusted Draw RNG protects the entire drawing process from dishonest employees (i.e., lottery, drawing machine vendor, TV station employees) and other personnel involved in the drawing process or with the drawing system.

Trusted Draw™ - Inner Workings

The key element of RUN+A is the digital signature of the draw data. Digital signature is performed by a certified, tamper-evident, cryptographic processor. Since a digital signature is unpredictable yet can be verified, using it as a seed for a proven standard random algorithm provides both the necessary unbiased and unpredictable results and a means for their certification - by recreating the random numbers and verifying the integrity of the draw process. In other words, RUN+A allows for the realization of a seemingly impossible task – the generation of unpredictable random numbers in a way that can later be used to prove that the numbers generated were the unique and unpredictable numbers that should have been generated. The digital signature itself becomes part of the evidence of correct operation verifying the random number generation process.

SPYRUS LYNKS II HSM (hardware security module) cryptographic processor is used in Trusted Draw for secure random numbers generation. The LYNKS II card performs cryptographic operations and is FIPS 140-2 level 2 certified (tamper evident); it is used for high security applications by the US military and National Security Agency. Over 400,000 LYNKS cards manufactured. Trusted Draw uses following features of the LYNKS HSM:

1. RSA signatures – it is an approved signature standard in the US and other countries. These signatures guarantee that draw integrity can be verified for many years
2. LYNKS II card generates a private/public key pair such that the private key is never accessible outside the card. This, and the fact that the card is tamper evident, guarantees that the random numbers derived from the signature cannot be altered without detection.
3. LYNKS II card uses a sequencer technique which allows for accounting for each signature/draw, detection of missing or extra draws and replay attacks (numbers generated earlier and presented later).
4. LYNKS card has a battery backed up real time clock (RTC), which cannot be altered without detection. At the time of digital signing, this clock value is signed. This enables accounting and verification of the actual time of number generation.

[1] “METHOD OF GENERATING UNPREDICTABLE AND AUDITABLE RANDOM NUMBERS”- US patent no 6,934,846