BULLETPROOF

a GLI company

Independent Review of Security and Non-repudiation of the Szrek2Solutions Electronic Draw System (EDS)

Prepared for:

Szrek2Solutions

60 Spencer Avenue,

East Greenwich, RI 02818 U.S.A.

Project Code:

PS07156 Issue

Date:

July 10th, 2018

EXECUTIVE SUMMARY

1.1 Background

Security and integrity with respect to the operation of Electronic Draw Systems (EDS) and the use of Random Number Generators (RNG) is a widely discussed topic at present in the lottery and gaming industry for a number of reasons. Some EDS operators, such as lotteries, are faced with the challenge to evolve traditional ball draw systems to electronic and automated draw systems as technology progresses, while others that have already implemented electronic and automated draw systems for their draw based game operations are faced with the challenge to keep current systems aligned with technology development and increasingly critical security and integrity requirements.

The most prevalent reason that electronic draw systems are currently under heightened scrutiny is recent cases of fraud in the lottery industry involving the tampering with electronic draw systems or the RNGs within, as well as integrity issues with RNG hardware or software. These security and integrity issues raise the need for bringing current RNG technology concepts to the levels required to address prevalent gaps, as the industry is considering the fraud and integrity risks around electronic draw systems and RNGs in particular. Primarily, these gaps are the lack of transparency in the electronic draws process and the lack of using effective methods to provide true proof of the authenticity, integrity and origin of RNG output and subsequent draws results.

This is typically exacerbated in the industry by overemphasis of physical security around electronic draws and the use of pseudo-audit functionality concepts. Both factors can create a false sense of security and integrity and false trust in the draw outcome, as RNG systems without non-repudiation and conclusive audit capability may not be able to detect existing problems. Further, the inner workings of an electronic draw system and RNGs can be complex and are often not entirely understood by stakeholders, while great reliance was put on only the certification of randomness and distribution of RNG results. These factors can cause real security gaps in EDS and RNG solutions to be overlooked and critical risks to remain unmitigated. As a result, we may not know how many and which electronic draws were in fact subject to integrity problems or potential fraud. Conversely however, systems that meet the highest standards of security and integrity are often overlooked as well, as their technology is not understood.

1.2 System Overview

As a key vendor in the industry, Szrek2Solutions has asked Bulletproof to evaluate its electronic draw system solution by conducting a technical review of the system components and its patented RNG method (https://patents.google.com/patent/US6934846), which is based on utilizing digital signatures as RNG seeds, deploying an external secured Hardware Security Module (HSM) for digital signing.

The Szrek2Solutions electronic draw system solution (Trusted Draw) is a software and hardware based solution operating on the key integrity concepts of auditability, the ability to reconstruct draw results and providing true, irrefutable proof of integrity through non-repudiation in the random

number generation.

The Trusted Draw system achieves non-repudiation in its random number generation process by using a cryptographic digital signature as the seed for a software RNG algorithm. This seed is generated by a NIST certified, tamperproof hardware device, a hardware security module (HSM).

A critical characteristic of the digital signature is that it is unpredictable through its creation by a hardware security module (HSM) while it is verifiable by use of a public key and a standard algorithm. This verification occurs within Trusted Draw prior to the actual draw and further on a separate and independent audit system (Trusted Audit) and allows the detection of faults (hardware or software) as well as any attacks on the digital signature or the result data.

The initial step in the random number generation process is the verification that the RNG HSM device generates a correct RNG seed. Any further steps, and thus the actual draw, can only be initiated if no device error is detected, in which case an alternate HW device would have to be used.

In the next step, the verified RNG seed in form of a digital signature is saved in a draw Signature File (along with other digitally signed system and game specific data) for use in the draw's result verification. The Signature File is transferred to the independent audit system (Trusted Audit), either manually in an air gapped system setup or via network in a connected system. A key security and integrity measure in this methodology is the fact that the draw Signature File is tamper evident. It cannot be altered or manipulated without detection through the verification and audit steps and thus provides a reliable mechanism to detect attempts of attack or compromise, but also to identify malfunction of the hardware or software or a configuration error.

The independent audit system (Trusted Audit) is the third step and link in the chain of custody. It reads the Signature File and conducts two primary functions; a) the verification of the RNG seed (the digital signature generated by the hardware security module) and b) the reconstruction of the draw results by using the Signature File data including the signature seed with the same public algorithm. Comparison of the results enables the detection of configuration errors, system errors in the RNG system and any and all integrity issues as described above.

Using this methodology, the audit system is capable of reproducing historical draw results. This allows for verification of the authenticity of all historical draw results and for detection of any potential faults or fraud attempts which, without this verification, may remain undetected.

The capability to detect hardware faults, software problems and fraud attempts, and to reproduce or verify the draw results, are key integrity factors in the Szrek2Solutions EDS. In Bulletproof's experience, primarily protective security measures have been the focus in EDS solutions in the industry so far, lacking reproducibility and conclusive verifiability of the draw results.

Detailed process descriptions of the technology and methodology can be found in section 4, Detailed Observations, Technical Descriptions and Process Mapping.

1.3 Evaluation Summary Result

While assessing the above technology solution, Bulletproof has directed the key focus on verifying the

measures and controls that address the identified key risks in EDS operating: attacks on and tampering with RNG and draw results, the substitution of RNG results or hardware/software as well as RNG hardware deterioration and faults. These key risks and vulnerabilities are detailed in Appendix A: The Key Vulnerabilities of Electronic Draw Systems.

Bulletproof has evaluated and tracked the random number generation process and data flow within the Trusted Draw and Trusted Audit systems and was able to verify the existence and effectiveness of the measures and controls that address all identified vulnerabilities and risks outlined above.

The assessed electronic draw system, Trusted Draw, utilizes cryptographic hardware and algorithms in its methodology to provide proof of integrity through non-repudiation in the generation of random numbers. It creates unpredictable, unmodifiable data which is independently verifiable. Hardware as well as software faults and attacks against the RNG and its components are conclusively detectable.

The use of the independent Trusted Audit system completes the chain of trust in random number generation through validation and independent audit of the draw results. It verifies the seed for the random number generation and the supplied result data. Then it recreates the draw results and thus provides conclusive proof of integrity and non-repudiation in the random number and draw result generation process.

It should be noted that while the Trusted Draw system alone provides secure random number generation on the basis of non-repudiation and auditability, only its use in conjunction with the Trusted Audit system will provide end to end, conclusive proof of integrity of the draws process. This proof of integrity is equally conclusive when performed in an air gapped configuration or in a connected system configuration.

Transparency in the EDS and RNG process through auditability, proof of integrity by non-repudiation and effective fraud prevention and detection are the current key industry security and integrity best practices for electronic draw systems. Bulletproof concludes that the assessed Szrek2Solutions Trusted Draw and Trusted Audit system provides conclusive auditability and proof of integrity and thus meets or exceeds the current industry best practices for EDS and RNG technology and all relevant security standard requirements at the current time.

This document consists of the executive summary of the Independent Review of Security and Non- repudiation of the Szrek2Solutions Electronic Draw System (EDS) performed by Bulletproof.

For the redacted version of this review, please go to:

https://szrek.com/wp-content/uploads/2019/09/Bulletproof-EDS-Review-Redacted1.pdf

For the full document, please contact helena@szrek.com