BULLETPROOF

a GLI® company

Assessment Report

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

Document Details	
Client	Szrek2Solutions
Title	Independent Review of Security and Non-repudiation of the Szrek2Solutions Electronic Draw System (EDS)
Author	Thomas Bierbach
Bulletproof Tester(s)	Thomas Bierbach
Reviewed By	Wade Dauphinee, Director, Governance Risk & Compliance Greg Doucette, VP Solutions Delivery & GRC Danielle Boudreau, Technical Writer
Approved By	Greg Doucette, VP Solutions Delivery & GRC
Classification	none

Distribution List
Irena Szrek, Szrek2Solutions Walter Szrek, Szrek2Solutions

Table of Contents

Initially published and distributed on July 10, 2018.

1 GENERAL INFORMATION

1.1 Client Information

Organization	Szrek2Solutions
Address	60 Spencer Avenue, East Greenwich, RI 02818 U.S.A.
Phone	+1 (401) 398-0395
Contact	Irena Szrek
Email	irena@szrek.com
Authorized by	Irena Szrek

1.2 Project Details

Szrek2Solutions has requested that Bulletproof conduct an independent review of the Szrek2Solutions proprietary electronic draw system platform, primarily the key components of “Trusted Draw” and “Trusted Audit,” to assess and verify its concepts and controls of integrity and security in an independent assessment report.

The primary focus of this assessment was the technical aspects of the electronic draw solution, the auditable RNG method and the implementation of chain of trust and non-repudiation concepts within the Szrek2Solutions Trusted RNG platform.

Applicable Legislation / Standards

The following internationally-recognized standards or best practice frameworks were used as guidelines to establish baseline criteria for the review.

Standard	Focus
World Lottery Association: Security Controls Standard (WLA SCS:2016)	The WLA Security Control Standard (WLA-SCS) is designed to help Lottery and Gaming Industry Organizations achieve levels of control that are in accordance with both generally accepted information security and quality practices as well as specific industry requirements. The new WLA SCS:2016 provides requirements specifically for electronic draws systems and the control objective and controls were used as guidance.
Industry Best Practice in securing electronic draw systems.	Driven by fraud cases in the industry over the past years, the best practices for security in electronic draws have significantly evolved and continue to improve. The current key global industry best practice concepts have been used as baseline and guidance in this assessment.

Key Dates

Request Date	April 25th, 2018
Assessment Start Date	June 19th, 2018
Assessment Completion Date	June 22nd, 2018
Draft Report Issue Date	June 29th, 2018
Final Report Issue Date	July 10th, 2018
Last Revision Date	August 31st, 2018

Assessment Team

Thomas Bierbach	Certified Information Systems Auditor, Accredited WLA Assessor, Engagement Manager
Wade Dauphinee	Senior Technical Assessor and Quality Assurance
Paul Leger	Senior Technical Assessor and Quality Assurance
Greg Doucette	Executive Sponsor, Quality Assurance

2 EXECUTIVE SUMMARY

2.1 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.

2.2 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.

2.3 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 operation: 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.

3 SCOPE, APPROACH & METHODOLOGIES

3.1 Scope

The scope of the review was based on two of the four focus areas of the Bulletproof ADM and EDS review methodology as outlined below. The primary focus was on the technical aspects of the solution and the auditable RNG method and the implementation of chain of trust and non-repudiation concepts within the Szrek2Solutions Trusted Draw and Trusted Audit platforms.

Focus Area 1 - The ADM / EDS / RNG Solution and Implementation

- ADM /RNG technology solution and implementation, server and networking aspects (networked vs air-gapped solutions, control balance).
- ADM /RNG concepts of game parameter code (game set) SW component and RNG interaction, process and data flow analysis.
- RNG technology, HW/SW, seeding concepts and processes.
- RNG certification, independent code review and SW validation policies and procedures.
- ADM / RNG development and build process and change management controls, code protection of the ADM / RNG and game parameter code.

Focus Area 2 - ADM / EDS / RNG Integrity & Auditability – Chain of Trust / Chain of Custody

- ADM / RNG operational process integrity, proof of integrity (that the RNG outcomes were not manipulated), logging and result non-repudiation and auditability for prevention or detection of RNG attacks/tampering based on chain of trust / chain of custody concepts.

Specifically within the scope were the validation of the concepts of non-repudiation, proof of integrity, chains of custody, and chains of trust, and the documentation of the processes and description of the technology. The technology description and analysis is focused on the RNG and verification processes. The scope also included other points such as:

- Risks which the system protects against;
- How is it assured that the produced results originate from the RNG?
- What is the assurance that the methodology guarantees RNG fault and fraud detection?
- What is the assurance that the RNG is not at risk of any interference with the software, processes, or otherwise?
- Are there residual or other risks, depending on how the RNG is implemented?

3.2 Engagement Approach (Audit Process) & Assessment Methodology

Bulletproof utilized a proven approach and methodology in conducting the assessment within defined key focus areas. These focus areas map to the required aspects and objectives for the assessment and cover the detail controls, which form the basis of the assessment report frame.

The review methodology for the risk-based review consists of the four stages of planning, assessment, analysis and reporting, which delivers a purposeful, quality assessment product. The standard audit stages applied are described below.

The review was conducted at Bulletproof offices in Moncton, NB, together with Szrek2Solution and was primarily based on technical interviews with the principal solutions architect(s) and the observation and documentation of system processes and data flows in a real-time system setup.

Following this approach, Bulletproof conducted the review in several stages.

Stage 1 – Planning

Bulletproof's planning for the Szrek2Solutions electronic draw system review included the following steps:

a. Development of working papers, checklists and review protocols, mapping and base-lining relevant control references;

b. Planning of the onsite review together with the principals of Szrek2Solutions regarding electronic draw system operations. We established project timelines, assigned resources, identified key focus areas and developed a schedule of interviews and meetings.

Stage 2 – Assessment

Bulletproof conducted a technical assessment together with Szrek2Solutions which began with a desk top review of Szrek2Solutions' electronic draw system and RNG operational concepts and methods. This review allowed Bulletproof to assess the established electronic draw system technical processes.

The objectives of this stage were to:

- Review the electronic draws and electronic draw system control framework;
- Collect necessary information for optimizing the review to focus on critical risk areas;
- Specifically consider the key focus areas of the chain of trust, chain of custody and non-repudiation concepts.

The assessment phase included the following steps:

a. Documentation review:

   Bulletproof performed a review of critical electronic draw system technical documents and records, including the following elements:

   - Review of the Szrek2Solutions RNG Methodology and RNG Non-repudiation;
   - Review of security and integrity controls and procedures.

b. Identification of the specific core RNG processes and mapping of the security and integrity controls which provided the opportunity to:

   - Observe the technology solution operation and the security and integrity controls implementation and effectiveness;
   - Verify the implementation and operation of the chain of trust and non-repudiation concepts within the solution as key areas of focus.

Stage 3 – Analysis

Bulletproof analyzed the results obtained during the assessment phase to obtain an evaluation of the state and maturity of Szrek2Solution's electronic draw system in operations and to validate the Szrek2Solutions RNG methodology and chain of trust and non-repudiation concepts.

a. Completed analysis and evaluation:

   Where necessary, Bulletproof completed further evaluation of the observations from the assessment phase and validated the risk analysis of the findings.

b. Developed the assessment results with evaluation of the observations of the technology solution and validation of the core security and integrity concepts and methodologies.

Stage 4 – Reporting

Bulletproof's reporting phase includes the following steps:

a. Develop draft report:

   Bulletproof documented the technical process mapping and observations and the results from the review and analysis of the security and integrity processes.

b. Client review of draft report.

c. Complete and submit final report.

3.3 Risk Evaluation Methodology

Bulletproof uses this risk methodology in risk assessments to determine risk values by evaluating the criteria of likelihood and impact of the risk event occurring. A detailed description of our risk methodology has been provided in Appendix D.

Sections 4 and 5 removed

For the full report, please contact
Helena Pereira at helena@szrek.com

6 Appendix A: The Key Vulnerabilities of Electronic Draw Systems

The following key vulnerabilities are widely recognised as being at the core of EDS security and integrity issues. Szrek2 Solutions lists these vulnerabilities as the key risks the Trusted Draw and Trusted Audit platforms address. Bulletproof validates these to be the key risks in electronic draws operation while the Szrek2Solutions methodology addresses further vectors of attack beyond those listed.

- **Draw time substitution**
  Altering of the time stamp for offline draws after the results are generated, meaning draw results can be known before they are published.
- **Substitution of numbers drawn**
  After the results are generated, an insider can substitute the winning numbers and this can go unnoticed if the RNG system does not provide verification methods and the results are not consistently verified.
- **Phishing or attempting multiple RNG generations**
  To obtain desired outcomes. Many RNGs allow for multiple generations and it may be impossible to know how many have occurred.
- **Inadequate RNG design & implementation**
  Gaps in the detection of software and hardware errors and malfunctions, the lack of software designed to check for errors and to detect hardware issues and malfunction.
- **Hardware substitution**
  Substitution of HW for alternative HW that produces predictable results. Such substitution may go unnoticed unless there is a way to identify the hardware used for each draw.
- **Software Substitution**
  Substitution of RNG or parameter SW during initial delivery, during maintenance, or later. Typical certification, pre-post testing, verification of program checksums, system scans, verification tests, and post-mortem testing may not find hidden code.
- **Hardware deterioration**
  Results in hardware not performing RNG functions safely or properly. RNGs may not have specific hardware verification tests in place.

Appendix B removed

For the full report, please contact
Helena Pereira at helena@szrek.com

8 Appendix C: Glossary of Terms

EDS	Electronic Draw System
ADS	Automated Draw Machine
RNG	Random Number Generator
HSM	Hardware Security Module
TD	Trusted Draw
TA	Trusted Audit
Non-repudiation	A service that provides proof of the integrity and origin of data. An authentication that can be asserted to be genuine with high assurance.
Digital signature	A mathematical scheme for presenting the authenticity of digital messages or documents.
XOR	Exclusive or or exclusive disjunction is a logical operation that outputs true only when inputs differ (one is true, the other is false). The XOR gate (sometimes EOR gate, or EXOR gate and pronounced as Exclusive OR gate) is a digital logic gate that gives a true (1 or HIGH) output when the number of true inputs is odd. An XOR gate implements an exclusive or; that is, a true output results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both".
Chain of Trust	In computer security, a chain of trust is established by validating each component of hardware and software from the end entity up to the root certificate. It is intended to ensure that only trusted software and hardware can be used while still retaining flexibility.
Chain of Custody	General: A process used to maintain and document the chronological history of the handling of electronic evidence. A chain of custody ensures that the data presented is “as originally acquired” and has not been altered prior to admission into evidence.

9 Appendix D: Risk Assessment Methodology

Risk IT Processes

Exhibit 1 represents the process by which Bulletproof conducts risk assessments of the findings identified during the course of our fieldwork.

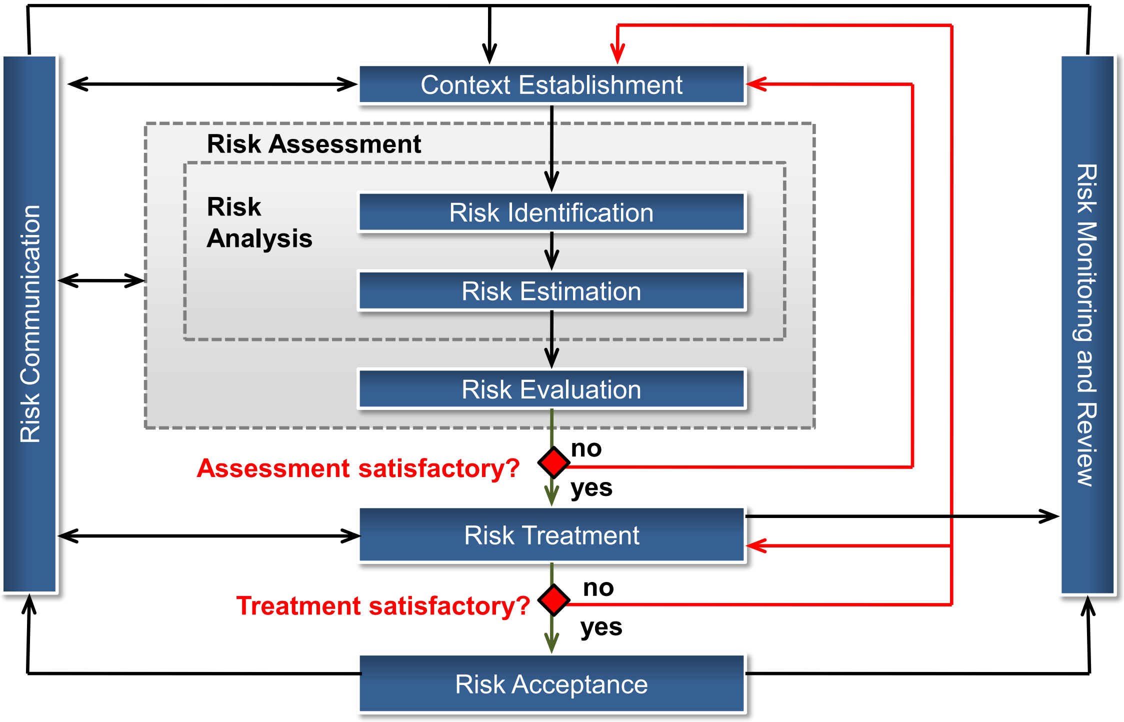

Exhibit 1

The various process blocks define the process flow.

Term	Definition
Risk management	Coordinated activities to direct and control an organization with regard to risk
Risk identification	Process to find, list and characterize elements of risk
Risk estimation	Activity to assign values to the probability and consequences of a risk
Risk analysis	Systematic use of information to identify sources and to estimate risk.
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk assessment	Overall process of risk analysis and risk evaluation.
Risk treatment	Process of selection and implementation of controls to modify risk
Risk acceptance	Decision to accept a risk
Risk communication	Exchange or sharing of information about risk between the decision-maker and other stakeholders

Bulletproof determines risk values by plotting against the criteria in the following heat map. The heat map in Exhibit 2 shows the criteria to be used in determining the risk associated with the findings of non-compliance to standards.

Likelihood Impact	Rare	Unlikely	Possible	Likely	Almost certain
Insignificant	🟩	🟩	🟩	🟨	🟨
Minor	🟩	🟩	🟨	🟨	🟨
Significant	🟩	🟨	🟨	🟨	🟥
Major	🟨	🟨	🟨	🟥	🟥
Severe	🟨	🟨	🟥	🟥	🟥

Exhibit 2

Risk was calculated by evaluating the impact on the organization and the likelihood of occurrence. Exhibit 3 describes the impact criteria.

Impact Areas	Impact Score				
	Insignificant	Minor	Significant	Major	Severe
Reputation & Image	One isolated negative news story	Short term (one to two months) adverse media attention due to negative news stories in one state	Short term (one to two months) negative media focus in all four states and minor concerns raised by stakeholders & customers	Prolonged negative media attention in all four states & sustained concerns from stakeholders & customers	Prolonged & highly negative media coverage. Stakeholder loss faith in company
Financial	Minimal impact on potential profits	$100,000 to $500,000 impact on potential profits	$500,000 to $1.0 million impact on potential profits	$1.0 to $3.0 million impact on potential profits	Over $3.0 million impact on potential profits.
Autonomy/ Shareholder	No damage to shareholder relations or structure	Minimal impact on relationship or minor change to company's decision making ability	Medium term damage to relationship and/or moderate changes to company's decision making ability or control	Long term damage to relationship and/or legislative criticism, questioning and debate	Irreparable damage to relationship and/or legislative inquiry or Ministerial intervention
Legal & Compliance	No impact on current or planned gaming initiatives	Misinterpretation of laws and regulations resulting in slight modification to	Stakeholders question company related to its compliance with laws/ regulations results in short term delays in initiatives	Stakeholders believe company may not be compliant with laws/ regulations resulting in delays	It is determined company breached laws/ regulations resulting in legal action/staff fired

		plans but no significant delay.		in current and planned gaming initiatives.	

Exhibit 3

Exhibit 4 describes the criteria used to calculate the likelihood of the risk occurring.

Likelihood		
Descriptor	**Likelihood / Frequency**	**Frequency of Occurrence**
Almost Certain	The risk is expected to occur in most circumstances.	Greater than 95% likelihood of occurrence or more than once per year.
Likely	The risk will probably occur in most circumstances.	60% to 95% likelihood of occurrence or more than once per year.
Possible	The risk may occur at some time.	30% to 60% likelihood of occurrence or once every three years.
Unlikely	The risk is not expected, but it could occur at some time.	5% to 30% likelihood of occurrence or once every ten years.
Rare	The risk may only be realized in exceptional circumstances.	Less than 5% likelihood of occurrence or less than every 30 years.

Exhibit 4