Szrek2Solutions

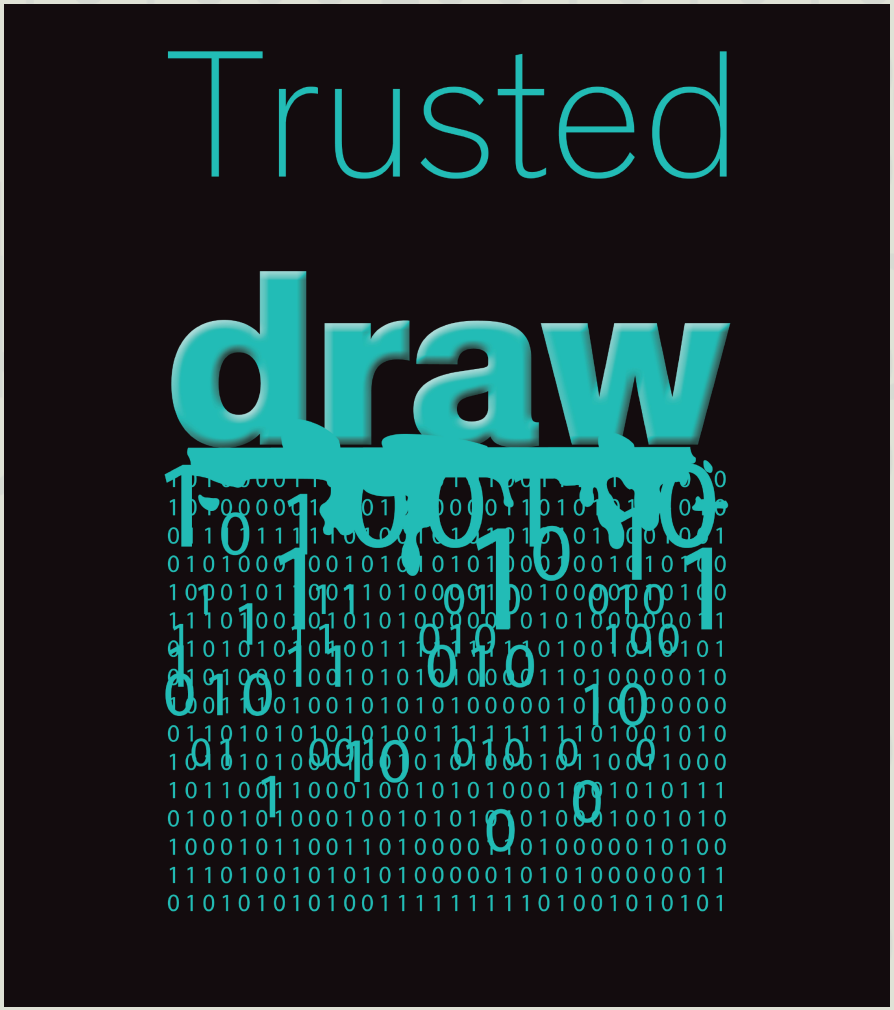
When I Play I Trust

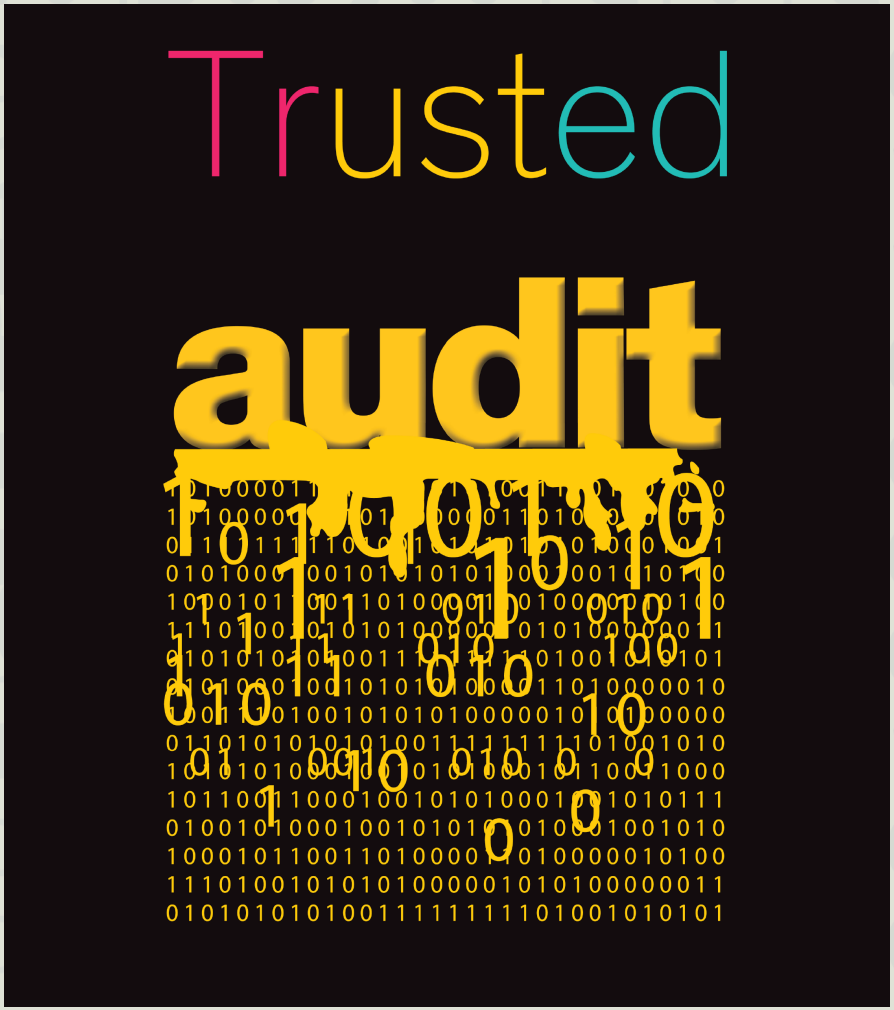
Trusted Draw™ and Trusted Audit™

Protecting RNG Integrity

Szrek2Solutions
When I Play I Trust

RNG PRODUCTS





Szrek2Solutions
When I Play I Trust

SUPERIOR SECURITY & FRAUD DETECTION

- Security of Traditional RNGs is based on prevention
- Prevention is not sufficient for security

PREVENTION

+

EARLY DETECTION = **SECURITY**

+

QUICK REACTION

Szrek2Solutions
When I Play I Trust

SZREK RNG - PREVENTION

- Preventive hardware security
- Preventive secure software and process
- System: secure computing environment
  - Protected area: no write, modify, delete privileges

    logs, executables, reports, configurations

  - Access security: 2+ users needed to perform a draw
  - Access only via GUI for users and administrators
  - Multiple user roles and restricted privileges

Szrek2Solutions
When I Play I Trust

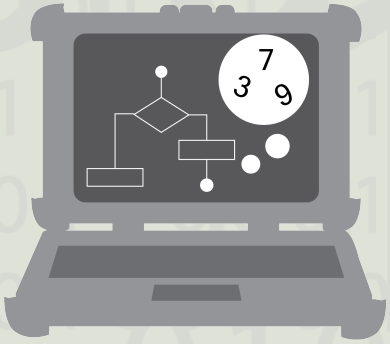
SZREK RNG - FRAUD DETECTION

- Detect any and all manipulations to the RNG and DRAW DATA
  - 100% detection of fraud
  - Proof of the integrity of all insiders
    - Draw team
    - Vendors
    - Certification agency
    - Operators
    - Subcontractors
  - No dependence on Chain of Trust
  - Proof is admissible evidence in court

→ QUICK REACTION

Szrek2Solutions
When I Play I Trust

SZREK RNG - SECURITY INNOVATION



- Our patented RNG method combines established technologies:
  - Digital signatures (private key, public key)
  - Certified cryptographic tamperproof hardware
  - Generation of random numbers from RNG seeds

- We use digital signatures as RNG seeds
  - Guarantees verifiability and unpredictability of generated random numbers

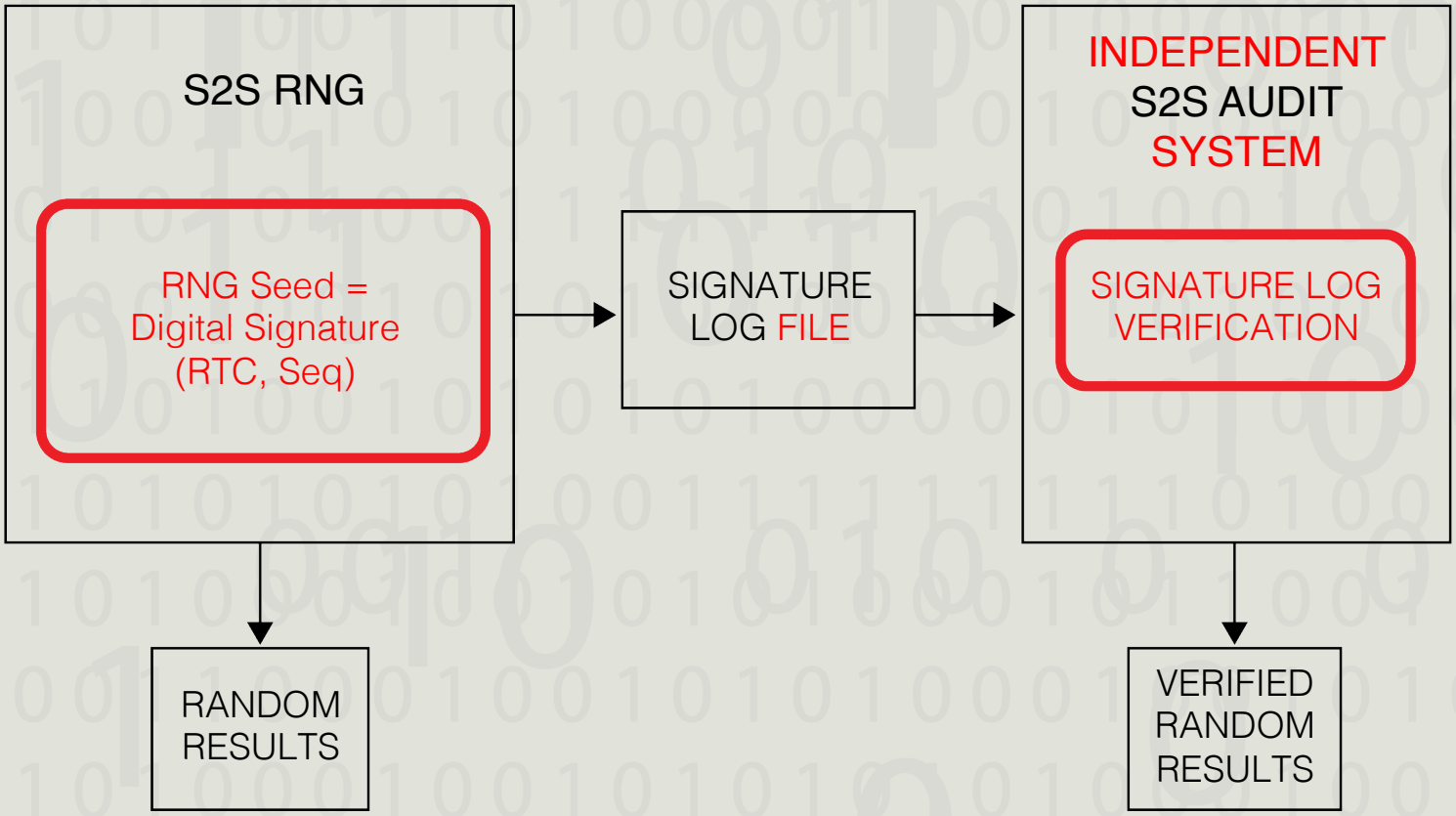
Szrek2Solutions
When I Play I Trust

HARDWARE SECURITY MODULE (HSM)

- Szrek RNG uses certified HSM (FIPS 140-2 level 2)
- HSM does not allow changes in the RNG seeds (digital signatures)
- Each time a random number is generated, a tamper-proof record is written to the signature log

Szrek2Solutions
When I Play I Trust

FUTURE-PROOF AUDIT CAPABILITY



Szrek2Solutions
When I Play I Trust

WHY SZREK RNG SECURITY WORKS

- No attack on Szrek RNG will succeed: fraud is detected even when the RNG system is compromised
- Possible attacks on RNG

MANIPULATION	CONSEQUENCE
Alteration of signature	Verification would fail
Manipulation of signed data	No advantage, signature cannot be predicted
Attack on signing process	Not effective, signing key is secured by HSM
Manipulation of draw time	Not effective, draw time is protected by HSM

Szrek2Solutions
When I Play I Trust

FUTURE-PROOF AUDIT CAPABILITY

- The signature log of the RNG allows for a systemic independent audit to be performed any time after the draw
- An independent Audit system reproduces the draw and proves the integrity of all generated and signed data
  - Drawn numbers
  - Draw time
  - Each and every use of RNG
  - Draw device used
  - Game matrix
  - Associated transaction data (e.g. that an instant win belongs to a specific player, that bets were not modified after the draw, etc.)

Szrek2Solutions
When I Play I Trust

FUTURE-PROOF AUDIT CAPABILITY

- Electronic proof of integrity that the RNG outcomes were not manipulated
- Proof independent of the RNG system which was possibly compromised
- Proof available anytime, immediately after the draw and years later, for every draw
- Proof verified by an independent audit - separate audit system
- Systemic audit – mathematical verification of signature log - manual or automated
- Can be integrated with ICS (for connected system)

Szrek2Solutions
When I Play I Trust

SECURITY BENEFITS of Trusted Draw + Trusted Audit

- Preventive measures, as built into Traditional RNGs, are designed to protect against ***known*** – but not unknown - vectors of attack
  - Some of these vectors of attack are very difficult to protect against even when anticipated
- Traditional RNGs are dependent on a ***chain of trust,*** requiring absolute trust in the:
    - computing environment
    - procedures
    - personnel with access to the system
    - RNG provider
    - RNG and OS maintenance personnel
    - certification authority, etc.
  - The chain is only as strong as its weakest link
- With the Szrek system, our RNG audit detects all attacks – known and unknown - so that you can react immediately

Szrek2Solutions
When I Play I Trust

THREATS FOR TRADITIONAL SYSTEMS

- Substitution of software
  - Hidden code installed on the RNG system
  - Self-destructive root-kit
- Substitution of hardware
- Substitution of time of draw
- Phishing
- Hardware deterioration
- Situations where integrity proof is needed

VECTORS OF ATTACK – Substitution of software

Source of attack: Hidden code installed on the RNG system (DLL, scripts, executables, etc.)

OR

Self-destructive Root-kit / USB stick can be used to run a code and afterwards it can be removed or self-destruct

- Hidden code can later be removed or self-destruct
- Code could be used only once (conditional)
- Code can be encrypted and not detectable
- Software can be “hidden” during initial delivery (by vendor, certification party), inserted during the maintenance of the RNG application or OS, or inserted on a “hidden” drive/ USB by user with access to RNG at a later time

Szrek2Solutions
When I Play I Trust

VECTORS OF ATTACK - Substitution of software

Traditional systems fail

- Certification may not find hidden code because it runs only at certain times or is dependent on other conditional factors related to number generation
- Pre and post-testing will not detect the hidden code because such tests focus on analyzing the statistical distribution
- Verification of program checksums may fail – a different program may be running than the checksummed one, a verification tool may be corrupt
- Scanning of the system won't find the threat unless it looks for a specific attack
- Verification tests won't find hidden code: can only test for known problems, cannot predetermine all potential vectors of attack
- Post-mortem test: may not have a way to test for it

Szrek RNG – always creates a proof of integrity, immune to any manipulation

Szrek2Solutions
When I Play I Trust

VECTORS OF ATTACK - Substitution of hardware

- Source of attack: Hardware can be substituted in a fraudulent draw
  - This hardware may produce predictable results
- Traditional RNG: Unless there is a way to identify which hardware was actually used for a draw through background cycling, such a substitution may go unnoticed
- Szrek RNG Audit will identify hardware used. But Szrek RNG substitution does not provide predictable results, so no incentive to substitute.

Szrek2Solutions
When I Play I Trust

VECTORS OF ATTACK - Substitution of time of draw

- Source of attack: RNG System time change
  - Draw is generated and results are presented later as if the draw was performed at the correct time
- Traditional RNG –Offline system time cannot be verified. Time can be altered and draw results can be known earlier
- Szrek RNG – system keeps an independent, unmodifiable clock and the RNG will not perform a draw if the system time is more than a few hours off. Actual draw time is independently verifiable any time after the draw.

Szrek2Solutions
When I Play I Trust

VECTORS OF ATTACK - Phishing

- Source of attack: attempting by multiple RNG generations to obtain desired outcomes
- Traditional RNG will allow multiple generations
- Szrek RNG accounts for every random number generation, so it will detect such an attack

Szrek2Solutions
When I Play I Trust

Hardware: may deteriorate over time

- Traditional RNG: Verification of hardware integrity via statistical tests, may not always be accurate

- Szrek RNG detects failing hardware with 100% assurance and it will not use it to generate random numbers.

Szrek2Solutions
When I Play I Trust

INTEGRITY PROOF NEEDED

- Software problems ("border problems", "setup problems") were not detected causing undesired distributions
  - Tennessee – no repeats on 3,4 digit numbers
  - Arizona – 9 not occurring
  - California - draws from incomplete range
  - Australia – 5 minute keno – incorrect RNG seed initialization caused the same numbers to be drawn
- RI, Bulgaria, NC, Israel – same numbers drawn on consecutive/ near days causing distrust amongst customers
- Player perceptions (ex. of 'too similar' combinations of numbers, patterns on number combinations; 1, 2, 3, 4 or 1, 1, 1, 1)
- Szrek Audit system allows detection of "setup" problems and verification of the randomness of draw outcomes

Szrek2Solutions
When I Play I Trust

HOW TO ENSURE TRUE PROOF OF INTEGRITY

True Proof	False Proof
Digital signature of bets before draw -> bets cannot be manipulated	Digital signature of bets after draw -> bets can be manipulated
HSM generated digital signatures –> HSM is tamper proof	Computer embedded signatures -> computer can be broken into
Time stamping HSM -> HSM protects data and time	Standard HSM -> time can be manipulated
Digital signatures used as RNG seed -> Fraud always leaves trace, draw integrity verifiable any time	Digital signature of RNG seed or random numbers after generation -> Fraud may not leave a trace
Sequencer maintained by HSM -> accounts for every signature	Standard HSM / sequencer in software -> can phish for 'right' RNG outcome