A LEAP FORWARD IN INSTANT TICKET SECURITY

IGT's NextGen technology is a breakthrough that takes security further than previously possible — by harnessing the blockchain to create **unalterable instants game-creation and audit files.**

Ensuring game integrity has always been core to the lottery industry. And for instant tickets, which represented about two-thirds of total retail U.S. lottery sales in 2022, security is critical not only for programming games and preventing unauthorized game reconstructions, but also for enabling authorized game reconstructions when required — for example, to validate damaged physical tickets that are presented as prize winners.

In all of these instances, lotteries can now benefit from a new, state-of-the art patented system for secure predetermined instants game generation, developed by IGT.

This proprietary system, known as NextGen, harnesses **modern digital-security technology** to improve on the legacy security processes that have been commonly used throughout the industry for the past two decades.

Among its advantages, IGT's NextGen platform maintains **an unalterable forensic blockchain** of an instant game to help prevent the possibility of security breaches. A blockchain is associated with each instant game's unique database and protects not only the entire **game development process** but also the **reconstruction process.**

Benefits of NextGen Security vs. Industry Legacy	IGT NextGen	Industry Legacy
Encrypts Genesis/Shuffle Seed	✓	✓
Ciphertext Decryption Seed Managed by at least one "Trusted Party"	✓	✓
Enables Multiple Parties to Manage and Approve a Game Reconstruction	✓	✗
Forensic Audit Trail Maintained in an Unalterable Blockchain	✓	✗
Forensic record of both Game Generation as well as Ticket Reconstruction	✓	✗
Enables audit of distribution or arrangement of Winning and Losing Tickets in the Development Phase	✓	✗
Database Architecture for secure storage of all Game Elements	✓	✗

And rather than rely on just one trusted party for the security of game reconstruction, as has been the norm in the industry, IGT's proprietary system can optionally allow lotteries to ensure that **multiple trusted parties** must agree and participate before a game reconstruction can occur.

Keith Cash, IGT Vice President Global Instant Ticket Services, shared more about this innovative technology, now being used to generate secure instant games for IGT customers worldwide.

PGRI: How did the new game security system come about?

Keith Cash: Over the past few years, IGT invested several million dollars in developing a next-generation platform for programming instant games that is revolutionary in many ways.

To begin with, it takes more of a data-based approach, as opposed to traditional game programming, and this approach has given us vast means to innovate to add value for customers and players. For example, we are now using this advanced platform to create our Infinity Instants™ games, a whole new category of instants in which virtually all elements of the ticket can be enhanced. But that's just one of its applications.

When we created the NextGen game-programming process, it also allowed us to develop a new and superior security process that harnesses the advantages of blockchain technology and **can be used for all of IGT's instant products.**

How does the use of the blockchain increase instant game security?

Our NextGen technology uses a game database to store all of the basic elements required to generate a given game, including the prize structure, the game art, and the rules (see Figure 1). NextGen maintains a separate blockchain for each game database, logging every access or modification. You cannot create a game or reconstruct a game without touching this associated database, which leaves a permanent and visible record — or signature — in the blockchain.

When anybody accesses the database, for example, to program or to audit the game, each action is logged automatically by the user's name, Internet Protocol (IP) address, and computer identifier, with this information stored in a game-specific blockchain. By virtue of how blocks in the chain are generated, the previous blocks **cannot be altered.** Now the entire record of the game – any action made when a game is generated, accessed, or recreated — shows up in that blockchain. And we can share that blockchain with our customers, so they can always see the life of their game.

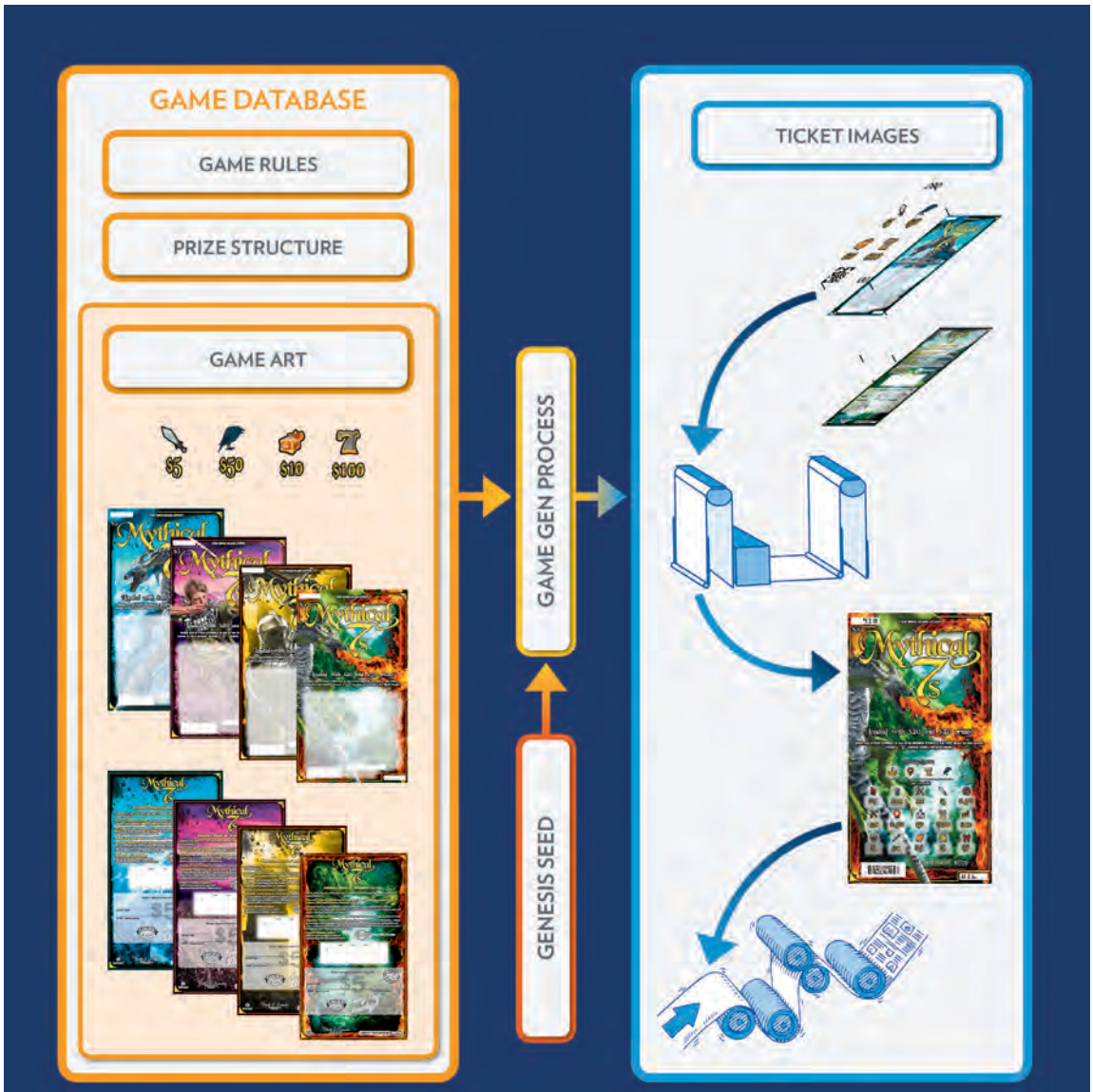


FIGURE 1: An end-to-end illustration of IGT's secure game generation process

In an ongoing process over the past couple of years, **we have already migrated about 98% of all IGT instant games over to NextGen security.** This system not only increases transparency but gives us and our customers a checkpoint to monitor their games' security.

What's the process for preventing unauthorized reconstructions?

The game database generation process also includes what we call the **Genesis Seed,** which creates the unique arrangement of winning and non-winning tickets for the game being created. For live games, the Genesis Seed is created by a True Random Number Generator (TRNG), which ensures that the live-game production Genesis Seed is truly random and therefore unpredictable. This is similar in concept to the "shuffle seed" in legacy security systems, but with another important differentiator: IGT's proprietary technology supports **multiple levels of encryption** of the Genesis Seed.

At the foundational level, we encrypt the Genesis Seed with what's called a One-Time Pad (OTP), the only form of encryption that's been mathematically proven to be unbreakable, and that action is recorded in the blockchain.

We then take the OTP-encrypted version of the Genesis Seed — the ciphertext — and encrypt it again with the public key of the lottery's trusted third party. Again, this second-level encryption is recorded in the blockchain. And we can advance this security process *n* number of steps further by encrypting it with multiple trusted parties' public keys — as many as the lottery designates — so that no one individual can access the unencrypted — cleartext — Genesis Seed (see Figure 2).

Each "key" is a series of bits that are astronomically large (512 bits) – it runs to a decimal number with 154 zeros behind it. To provide some perspective on how big that number is, the estimated number of atoms in the Milky Way galaxy is a number with only 67 zeros behind it.

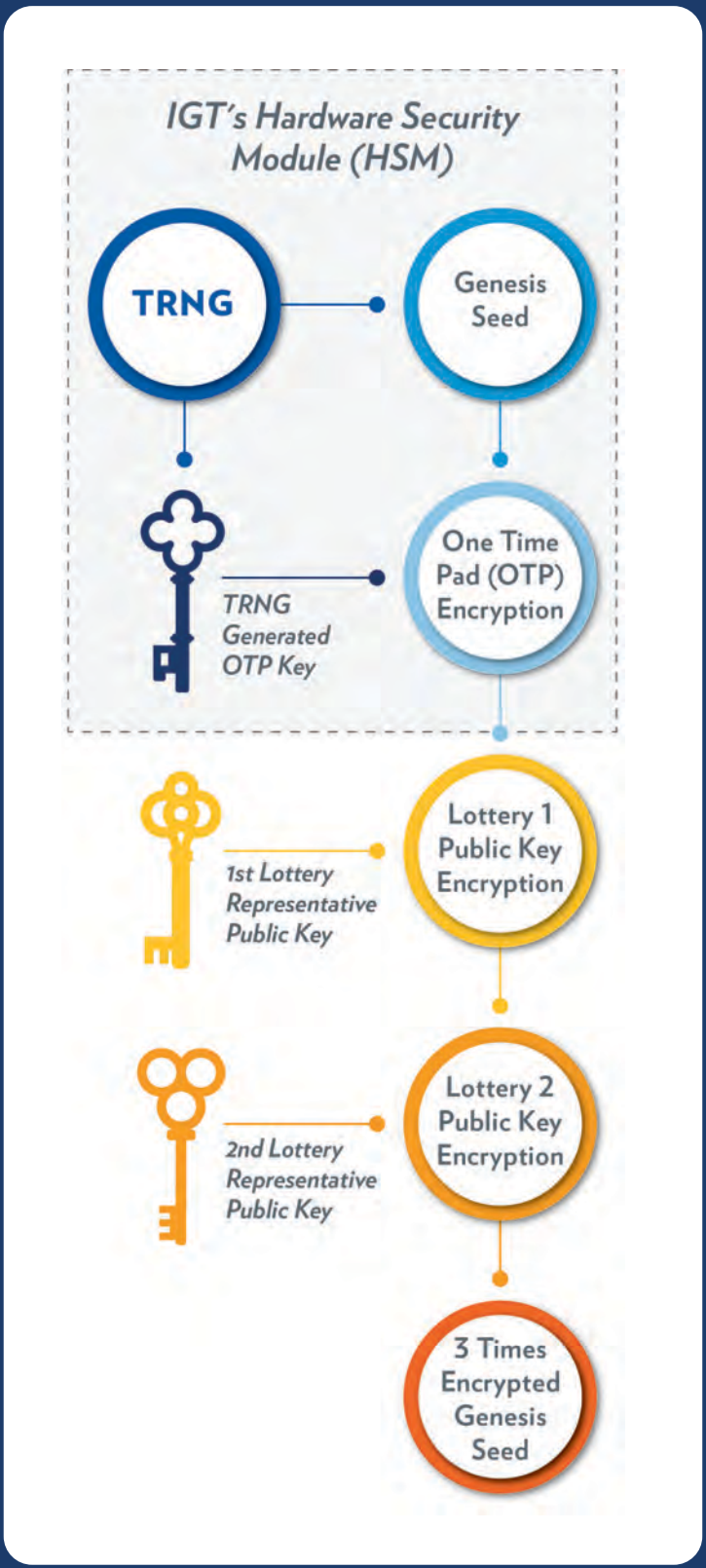


FIGURE 2: The difference between the live game and a test game is the Genesis Seed, which for the live game is created anew by a True Random Number Generator (TRNG) for live games.

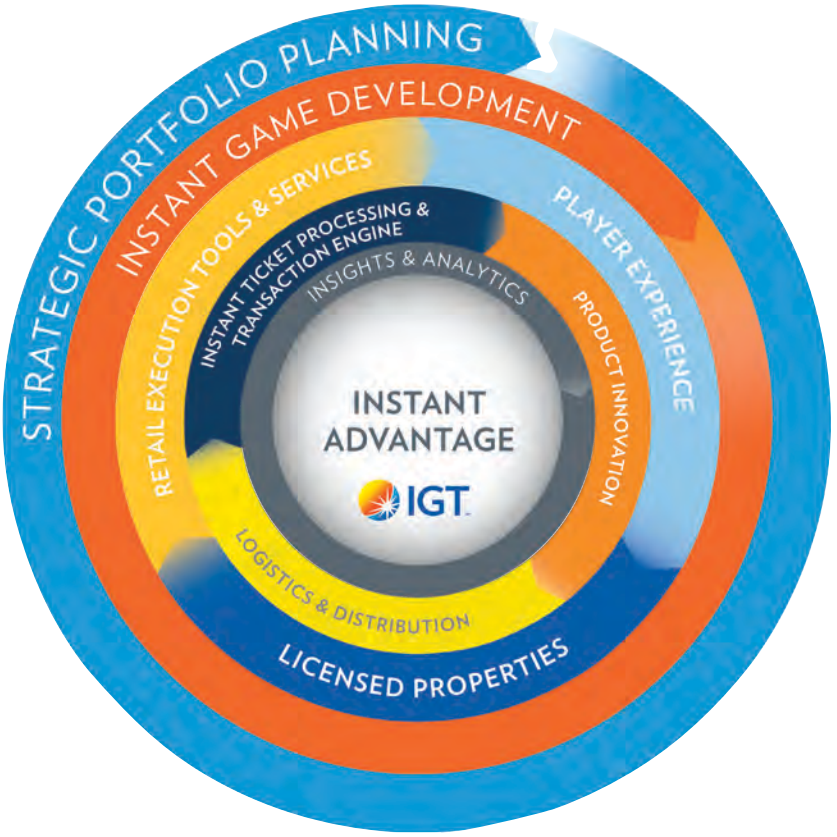
IGT's NextGen security system encrypts the Genesis Seed for a game with multiple trusted parties — as many as the lottery designates — so that no one individual can access the unencrypted (cleartext) version of the Genesis Seed.

The lottery and IGT can always read the blockchain, but to perform a reconstruction, the private key(s) from the trusted party(ies) are needed. And even after each private key is used to perform one level of decryption, the lottery is still transmitting an encrypted version of the Genesis Seed to us — if you recall, it was encrypted and secured with the One-Time Pad. We take that encrypted version, perform the final stage of decryption, and provide the lottery with the reconstruction.

Is this more involved or time-consuming than in the past?

Not at all, in fact one of the many advantages of the new system is that it's **more convenient for the lottery.** Each decryption can now happen in less than a second. Of course, this takes a lot of computing power, and to supply it, IGT also invested in a server farm of computers with an unbelievable amount of computational power. If you compare it to the computing power available when the U.S. landed on the moon, it's trillions and trillions of times greater. This investment is what makes the process secure, fast, and practical.

NextGen also removes the requirement that the trusted parties be present at a certain physical location to initiate a reconstruction. A lottery can even initiate the process at their own headquarters. This is something that other security systems can't enable, because in those legacy systems, once the shuffle seed is run through the trusted third party's private key, it reveals the unencrypted — cleartext — shuffle seed.



Given the significant investment required to create these advanced systems, what drives IGT to improve on the status quo?

Lotteries upgrade their technology periodically because they know technology is central to bringing new innovations and capabilities to the industry. We know this, too, and the NextGen system is a vivid illustration because it has resulted in security that is significantly higher than legacy solutions. It's an example of how we're harnessing our investments in new technology to deliver superior value and multiple benefits for customers.

We understand the lottery market and our customers' needs, and even after all these years in the lottery business and the instants business, we still see room for advancements and growth in this category. We don't like the status quo. That's what drives us to innovate. Over the past couple of years, our customers have seen us invest millions of dollars toward quality, service, and innovation – and security is just the most recent example.