GLI® GAMING LABORATORIES INTERNATIONAL®

GAT - GAMING AUTHENTICATION

Empowering Regulators with GAT – The Future of Gaming Software Verification

By Thorsten Toms
Client Solutions Executive

GLI/KOBETRON TOOLS

PURPOSE

This white paper details the Game Authentication Terminal (GAT) standard and supplies information on its implementation. This white paper would likely be found most useful by regulators responsible for the verification of gaming software. Given that jurisdictions, resources, and needs vary widely, it is by necessity generic in nature.
Please contact your Client Solutions Executive (CSE) with any questions. If they cannot answer them, they will put you in contact with the appropriate subject-matter expert.

GAMING STANDARDS ASSOCIATION

The Gaming Authentication Terminal (GAT) is a set of standards issued by the Gaming Standards Association (GSA). GAT is not a GLI Standard. GLI, along with most gaming manufacturers and some regulators, is a member of the GSA. A full list of current members is available on the GSA website.

What is the purpose of the GSA? In general, a standards organization is a body whose primary function is developing, promulgating, revising, interpreting, or otherwise contributing to the usefulness of technical standards for those who employ them. Such an organization works to create uniformity across supplier, producers, consumers, government agencies, and other relevant parties regarding terminology, product specifications, protocols, and more.
As a Gaming Standards Association, the GSA is the standards organization for the gaming industry.

The GSA has issued standards for land-based gaming, online gaming, and standards pertaining to the regulation of gaming. At the time of this writing, GSA's regulation-specific standards include:

- GAT – Game Authentication Terminal
- CDI – Certification Database Interface
- RRI – Regulatory Reporting Interface
- NGI – Network GAT Interface
- TGR – Trusted GAT Results

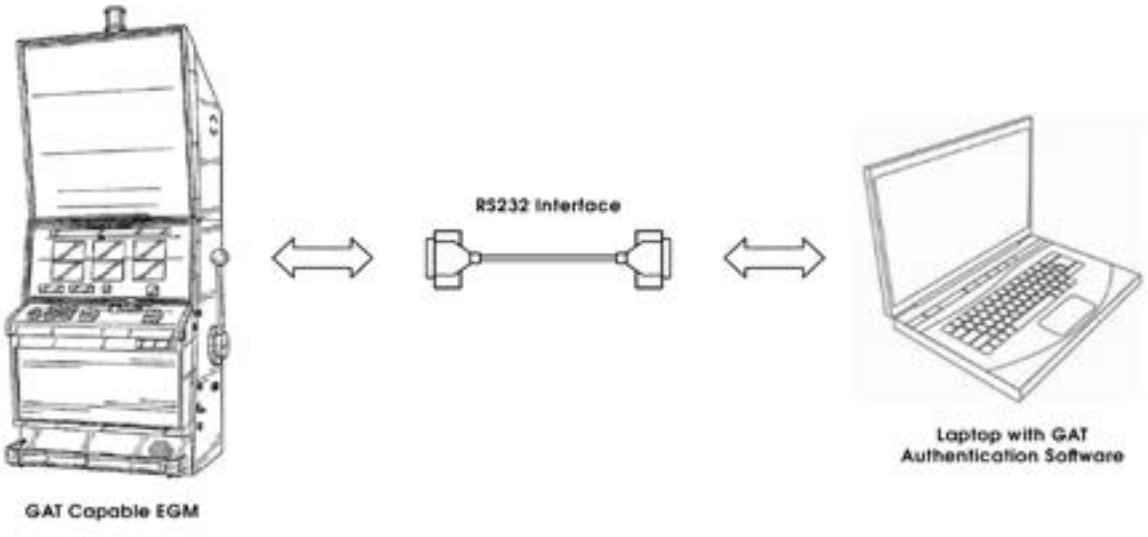
Notice that there are three GSA regulatory standards related to GAT. This white paper addresses implementing the GAT – Game Authentication Terminal, not the Network GAT Interface.

GAT DEFINITION

As defined in the standard itself, GAT is:

> *GAT defines a communications protocol used, between a master and an EGM, to authenticate software and firmware components within the EGM. Typically, a portable PC or a laptop is used for the role of the master. EGMs and other devices can be used for the role of the EGM.*
>
> *The GAT communication protocol is simple in order to reduce complexity of design, implementation, testing and usage. Due to the simplicity of this protocol, a standard layered approach is not necessary. Only the physical layer and the application layer command set are specified.*
>
> *The GAT protocol and associated calculations are to be run on a properly functioning EGM. Any attempt to use GAT while an EGM is in an error state, tilted, or otherwise malfunctioning is beyond the scope of this standard.*
>
> *The GAT protocol and associated calculations are designed for the purposes of verifying software content on an EGM. Any attempt to use GAT for any other purpose, such as verifying jackpots, game history recall, and so forth, is beyond the scope of this standard.*

Simply put, GAT is a way for a computer used by a regulator to connect an interface cable to an EGM and authenticate the software on that EGM.



This connection allows the regulator to verify that the software signatures on the EGM match the signatures generated by GLI when the software was evaluated and certified for the jurisdiction.

EGMS AND SOFTWARE SIGNATURES

A modern slot machine (EGM) is very much like a home computer in that it runs on an operating system that hosts application software. The operating system of an EGM may even be the same as the one on your home computer, as most EGMs run on Windows or Unix. However, unlike the software on your home computer, the application software on an EGM consists of the games it presents to patrons and the additional software required to operate, present, and regulate those games.

The change in slot machines from electro-mechanical devices to digital EGMs began in the 1980s and fundamentally changed the industry. This change allowed exponential growth and development of the slot machine industry. However, it brought its own security challenges. Since EGMs were computers, they were susceptible to malicious attacks. Hackers could and did subvert the software on EGMs to steal from casinos.

Many of these attacks were the result of criminals who were able to change the software on the EGM without the manufacturer, operator, or regulator knowing that there had been an alteration. To address this issue, manufacturers, test labs, and regulators worked together to create a system that ensures that the software on the EGM is ***exactly*** the same as the software tested by GLI and approved by the regulator.
This is done using software signatures. Today, a manufacturer submits its hardware and software to a GLI test lab. GLI verifies that the software meets the regulatory requirements for the jurisdiction(s) that manufacturer would like to operate the EGMS in. Once that process is complete, GLI certifies that the EGM and associated software meets the jurisdictional requirements.

As part of the certification process, GLI generates signatures. These signatures are generated by running an analysis on the complied source code that is the application software being certified and supplies a secure signature based on compiled code. **Any change in the software results in a different signature.**

This means that regulators can verify the signature of software on an EGM on the casino floor and check it against the signature issued by GLI. If the signatures match, the regulator can be confident that the software they are inspecting is the same as what GLI certified.
As detailed below, this signature verification can be a cumbersome and time-consuming process, especially when testing multiple EGMs.

VERIFYING SIGNATURES

There are a variety of ways to generate signatures. One method is SHA-1. Secure hash algorithms (SHA) are cryptographic functions designed to keep data secure. They work by transforming incoming data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions.

The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data.

Let's break down the "A" in SHA (which stands for algorithm) with a simple example. An algorithm is just a formula; for example, f(x)=x+1 is an algorithm. If x is equal to 3, then f(x) is equal to 4 (x+1). If x is 72, then f(x) is 73. Algorithms can be simple like this, but they can also be complicated, like the example to the right.

Another self-evident but important characteristic of algorithms is that they work the same for everyone. Regardless of who completes the calculation or what equipment is used, f(x)=x+1 will give the same result for everyone if the same value of x is entered. This holds true for signatures; if the same signature-generating algorithm is used, the same input value will result in the same signature.

The "H" in SHA stands for hash and denotes a special kind of algorithm that always results in an output of the same length. For example, SHA-1 always returns a result that is 40 characters long, regardless of the length of the input. The SHA hash is also a cryptographic one. This means that you cannot easily reverse the hash result to determine the original input. This property of the hash algorithms used in calculating SHA is what makes them secure.
Using signatures is how regulators make sure the software they are checking is the software the manufacturer sent to GLI and the software that was certified.

SOFTWARE VERIFICATION

SOFTWARE DELIVERY AND VERIFICATION

Gaming software is delivered across a variety of mediums. These include old technology, like EPROMs (Erasable Programmable Read-Only Memory) and compact discs, to newer ones, such as flash drives and electronic delivery. As you know, gaming software is highly regulated, with shipping notifications and other requirements varying between jurisdictions. Most jurisdictions require that the software have its signature verified upon delivery. This makes sure that the correct, unaltered software requested by the operator and approved for shipment by the regulator is what was delivered.

Software verification is usually accomplished using tools developed by an independent test lab. GLI's solution is a combination of software called Verify+ and Kobetron hardware machines. These work together to generate signatures from the software on the delivered medium and check that it matches the signature generated by the test lab.

Once the software has been tested and verified, it is available to be installed onto an EGM. Jurisdictions vary on the details of control of the tested software.

IN-MACHINE VERIFICATION

TRADITIONAL IN-MACHINE VERIFICATION

When the EGM software needs to be tested for any reason, the traditional method is to take the machine out of service, power it down, remove the software medium, and retest the same way as when the software was initially received. Then the signature can be verified again using Verify+ by Kobetron or the current Kobetron device (the Kobetron 4000 Pro as of this writing). This comes with some disadvantages with the primary one being that:

The EGM is out of service for a significant amount of time.

The steps to verify the EGM software in this way could include:

1.	Bring a slot technician and a regulator to the EGM with the required keys.
2.	Take the machine out of service.
3.	Power down the machine.
4.	Unlock the machine.
5.	Break and document breaking any seals.
6.	Remove the software.
7.	Get the software signature.
8.	Verify that the signature is correct.
9.	Reinstall the software.
10.	Reseal the machine.
11.	Power the machine back up.
12.	Test that the machine is operating properly.
13.	Put machine back into service.

Another complication is that there is no guarantee that the EGM will restart without any issues. Handling (removing, testing, and reinstalling) the game storage medium always carries the risk of damaging it. This method is especially cumbersome when many EGMs must be tested.

SIDE-BY-SIDE COMPARISONS

Verification with GAT compared to traditional verification:

	Traditional	GAT
1.	Bring a slot technician and a regulator to the EGM with the required keys.	YES
2.	Take the machine out of service.	YES (into test mode)
3.	Power down the machine.	NO
4.	Unlock the machine.	YES
5.	Open CPU door, break and document breaking any seals.	Plug in GAT cable and run GAT
6.	Remove the software.	NO
7.	Get the software signature.	YES
8.	Verify that the signature is correct.	YES
9.	Reinstall the software.	NO
10.	Reseal the machine.	NO
11.	Power the machine back up.	NO
12.	Test that the machine is operating properly.	NO
13.	Put machine back into service.	YES

Not only does GAT require fewer steps, but it eliminates unnecessary steps that are also some of the most time-consuming. Because the CPU door is not opened, there is no need to reseal it. Because the software is not removed, there is no chance of damaging it. Finally, by design, GAT can work on multiple machines simultaneously.

GAT PROCESS MANAGEMENT

MECHANICS

How does GAT achieve this efficiency? As detailed above, signatures are generated using an algorithm. Modern EGMs can generate signatures themselves because the ability to do so is built in; that is, they have the HASH generating algorithms built right into the software. When a regulator uses GAT, they are instructing the EGM to generate the signatures internally.

This is not an instantaneous process; it takes time to perform the complicated cryptological processes needed to generate signatures. But because the processing is going on inside the EGM, the regulator can initiate the GAT process using their laptop, move to the next machine, and initiate the process again and do so for an entire bank of machines, returning when appropriate to the first machine and upload the results.

SECURITY

Some regulators question if having the EGM test itself is truly a secure method of verification. Couldn't a competent hacker simply take over an EGM and program it to return the correct signatures? If you recall, the ability to generate the signatures is part of the software installed on the EGM, and that software was verified upon receipt. Given that software is independently tested externally before it's installation into the EGM regulators can be assured that GAT is secure. Additionally, by having policies in place that require all software be externally verified when taken out of service, manual signature checks can be done at any time.

CHECKLIST

1. Regulation and policy review:
   a. Review all applicable regulations, technical standards, and policies for anything that precludes the use of GAT.
   b. Identify any of the above that require updating.
   c. Note that GAT does not constitute a third-party signature verification. If your regulations require this, they must be changed to allow GAT.
2. Determine the required level of verification for your jurisdiction:
   a. Some jurisdictions require only system files.
   b. Some jurisdictions require system and personality files be verified.
   c. Some jurisdictions require verification for progressive controls, kiosks, and other non-EGM software.
   d. It is important to have your technical standards (or other regulations) detail what exactly needs verification.
3. Update and author regulations.
   a. Change any language that precludes the use of GAT as is necessary.
      i. If this requires an ordinance change, be aware of the time restraints implicit in changing a gaming ordinance.
      ii. Buy-in from all stakeholders is necessary for successful regulation updates.

GAT PROCESS MANAGEMENT (CONT.)

b. Pick a date for becoming a GAT jurisdiction.
   i. Even if the regulator is not yet utilizing GAT, having this date in place will assure that incoming EGMs are GAT capable for when the regulator does begin using GAT.

c. Add language that requires manufacturers to EGMs that meet the GAT standard.
   i. Sample language: "Effective on January 1, XXXX, the XYZ jurisdiction reserves the right to utilize the Gaming Standards Association's Gaming Authentication Terminal system to test controlled software. As such, all EGMs and associated software delivered to XYZ must be GAT compatible unless a waiver is received in advance from the Regulator."

4. Inform all stakeholders of the impending change.

   a. Determine if you are one of the rare jurisdictions that require a non-standard seed be incorporated in your signatures. If so, contact your CSE to initiate a discussion on the time and cost considerations resulting from using a non-standard seed.
   b. Inform GLI.
   c. Inform operations.
   d. Inform all manufacturers.
   e. Set reasonable expectations.
      i. Depending on how old your EGMs are and the rate of replacement, it may be years before an entire existing slot floor is GAT compliant.
      ii. GAT is a complement to, not a replacement for, traditional verification.

5. Update and author SOPs.
   a. Update shipping notification processes to require GAT and have manufacturers positively acknowledge that their delivery is GAT compliant.
   b. Update regulators EGM SOPs.
      i. Author internal SOPs that address the use of GAT.
         1. New EGM verification.
         2. Post-move EGM verification.
         3. Jackpot verification.
         4. Random verification.
         5. Any other cases where GAT use is anticipated.
      ii. Update SOPs and other applicable documents to incorporate GAT into process.
         1. Software receiving and verification.
         2. Turn over to operations.
         3. Others as applicable.

6. Get all the required hardware:

   a. RS-232 cables and adaptors.
   b. Laptops with Verify+.

7. Get training:

   a. Train everyone on the new processes.
   b. Be patient with yourself!

GAT

SLOT DATABASE – IRIS

Successful EGM software regulation implementation is predicated on having a database that is an accurate reflection of the regulated slot floor. Knowing what software is on each EGM is just as important as knowing that the software is approved for your jurisdiction.

While GAT will provide signatures and Verify+ and Kobetron (if properly updated from the central GLI data repository) will verify the status of the software, they only do so on EGMs being tested. They will not advise in real time if the all software on your floor is compliant (not revoked or obsolete) until you manually check it. If you are not already using IRIS as your database to track the status of your software, implementing GAT might be an opportune time to do so.

CONTACT YOUR CSE

Given that implementing GAT requires a significant effort in rewriting regulations and policies, some jurisdictions use the opportunity to streamline the software verification and delivery process. Jurisdictions vary, and this white paper is by necessity, generic. Contact your CSE to have one of our subject-matter experts speak with you about the specifics of GAT in your jurisdiction and the possibilities of increased efficiencies as part of the GAT implementation process.

ABOUT GLI

For more than 30 years, Gaming Laboratories International (GLI®) has been the world leader in testing for the global gaming industry. Compliance is the heart of what GLI does for suppliers, regulators, and operators. In more than 480 jurisdictions across 6 continents worldwide, companies turn to GLI for help with their compliance challenges in the areas of land-based gaming, iGaming, lottery, and cybersecurity. GLI's compliance offerings consist of five overarching categories that help clients wherever they are on their journey: policy and legislation consultancy, regulatory compliance, technical compliance, end-to-end testing, and full lifecycle compliance, and our cybersecurity services protect operators, regulators, and suppliers across each compliance category.

FOR MORE INFORMATION

For more information on the services offered by GLI please visit www.gaminglabs.com.

GLI® ILLUMINATING YOUR PATH **TO GREATNESS**

gaminglabs.com | +1.732.942-3999