GAMING STANDARDS ASSOCIATION
48377 Fremont Blvd, Suite 117 Fremont, CA 94538 USA
Tel: +1 510.492.4060 Fax: +1 510.492.4001 www.gamingstandards.com

GSA Protocols: How and Why they are Important and Relevant to Lotteries and Lottery Operations

By Marc McDermott, Technical Director, Gaming Standards Association (GSA)

As posted at PGRI - Public Gaming Research Institute in 2008

GSA Part 2 of a 3 part series

In part one of this series, we discussed the GSA organization and its mission statement – the development of standards for the gaming industry. We also discussed some of the advantages of open communications and looked at some of the benefits it provides for lottery operators. In part 2, we will dig deeper into GSA and its protocols to see, in more specific terms, what benefits GSA protocols offer and how they apply to lotteries and lottery operations.

GSA protocols address the three fundamental "A"s: Authentication, Accountability, and Agility. These three concepts are at the heart of the protocols. It is because of a concentration on the three "A"s that the GSA protocols can provide the gaming industry with the communications technology capable of supporting it for the foreseeable future.

To see exactly how this works let's start with the first "A": **Authentication**.

Authentication, in this sense, is the ability to ensure that the software on the floor, or in the games, is exactly what was approved to be there and is free of tampering. This concept applies to large, casino style, lotteries and, even more so, to wide area lotteries where small numbers of gaming terminals are in numerous, small, and in many times remote, locations. It is these small, remote operations where: the surveillance is limited or non existent, the proprietor of the location containing the terminals is the least sophisticated in gaming and the ability of the lottery operator to physically check the terminals is seriously limited, that the highest level of risk occurs. To address this concern as well as to address the requirements of the larger operations, GSA included the GAT functionality in the G2S protocol.

Gaming Authentication Terminal or GAT, provides a means of verifying the software in a gaming terminal from the back offices of a large casino operation or from the lottery offices for any type of location. GAT is not a software package and requires no third party equipment to be installed or used. GAT is simply a set of commands that have been incorporated in the G2S protocol that, if supported by the terminals and the querying system, can provide a powerful authentication capability that exceeds, from a security aspect, all but a very thorough on-site inspection.

GAMING STANDARDS ASSOCIATION
48377 Fremont Blvd, Suite 117 Fremont, CA 94538 USA
Tel: +1 510.492.4060 Fax: +1 510.492.4001 www.gamingstandards.com

The G2S GAT, while much more sophisticated then the original GAT, still follows the same basic principles for validating software on a gaming terminal. GAT allows an operator to command a gaming terminal to run a hash over its internal software and to return the answer to the querying terminal. The operator compares the returned hash answer to the hash answer on file and, if it matches, the software in the terminal is correct and unchanged from when it was originally approved and installed.

As an additional security measure, and to prevent an attacker from learning the hash answer and returning it, the G2S GAT supports several different hashing functions including CRCs, MD5 and several variants of the SHA hash algorithm. The algorithm type that the terminal is supposed to run is sent with the command to run the verification. Each verification algorithm will return a different hash value. In this way multiple hash values may be checked and verified to be correct. Beyond that, the G2S GAT also allows a “salt” and/or “seed” value to be sent with the command to verify the terminal’s software. These values are used to add a starting value to a hash algorithm or to adjust the initial components of the hash algorithm. The result is a hash answer that is completely dependant on the seed or salt value issued as indicated in figure #1. The seed or salt values can be determined immediately prior to the verification so that the likelihood that someone would know them and be able to fake a correct answer is extremely remote. The result is an extremely high confidence level validation of the terminal’s software.

Because the GAT capability is based on sending specific commands to, and receiving information from, a gaming terminal, the GAT function can be conducted from anywhere there is a secure connection to the terminal. In a G2S network, for example, all the data is encrypted using TLS/SSL encryption. A security certificate is supplied specifically by the venue operator or the lottery operator and is required to be able to communicate on the network. Without the certificate, information cannot be encrypted or decrypted and so no intelligence can be gained from the information. So, from inside the gaming venue, communication from the GAT server to the terminal targeted for software validation requires that both the GAT server and the gaming terminal each contain a security certificate. Also required is that both the server and the terminal have implemented the G2S GAT protocol. Once these security and protocol requirements have been met, the GAT commands are sent, the results are received and compared to the master file and the basic verification is complete. As mentioned above, additional hash functions may be used, provided they are supported by the terminals, and seed/salt values may be used in further GAT verification commands if the operator feels it is necessary. Additionally, this function may be automated so that many machines may be instructed to authenticate software simultaneously.

GAT operation from a remote location is basically the same as from the gaming operation back-of-house offices except that additional security measures, such as firewalls and VPN (Virtual Private Network) connections, are established between the lottery offices and the venue where the targeted terminals are located. The basic layout for both the back of house and remote GAT connections are described in Figure 2. Note that the Figure 2 is intended to convey basic function and does not include all the network equipment necessary.

The thoroughness and complexity of the GAT functionality shown in figure 2 is an indication of how important the verification process is to our member companies. GSA sees this capability as a fundamental requirement as it provides those responsible for the proper operation of the machines a

GAMING STANDARDS ASSOCIATION
48377 Fremont Blvd, Suite 117 Fremont, CA 94538 USA
Tel: +1 510.492.4060 Fax: +1 510.492.4001 www.gamingstandards.com

serious means to ensure themselves and their constituents that the games are being conducted in a fair and responsible way.

Serious authentication capability is not the only way GSA protocols assist those responsible for the integrity of the games.

Accountability is the second "A" in GSA's 3"A"s program.

Accountability is at least as important as authentication. However, there are many forms of accountability. The most obvious is the correct and proper reporting of information from the EGM to the back of house system. Basically, does the information get from the machine to the accounting system, is the information correct when it gets there and does the information provide a complete report of the machine's performance.

Another form of accountability is that of the government regulatory agency and the lottery operator to its constituents and patrons. This type of accountability is more in regards to the integrity of the games, and the integrity of the lottery operation. The fairness of the games, what software is actually installed, can a patron actually win, these issues are critical to the success of the lottery as they speak to the most basic concepts of the games and to the reason that the governing body is involved.

Fortunately, the GSA protocols assist in all areas of accountability. For the games themselves, GSA protocols provide meters for every function that the Committees responsible for the protocols can think of. We have reviewed meter requirements from numerous jurisdictions to make sure the protocols allow compliance with all of them. On the rare occasion where we find, or are told about, a meter we are missing, we include it in the next revision of the affected protocol. It is that simple and that straight forward.

GSA protocols also make sure the information gets from the game to the accounting system. We have a transport protocol that makes sure the messages get to the right place and are not tampered with. The key part is the industry standard SSL (Secure Socket Layer) encryption that keeps the information secure. Additionally, back at the message layer, all incoming messages are checked against rules (Schema validation) that dictate the format the messages must follow. Messages that do not conform to these rules, either by intentional tampering or unintentional bad data, are rejected, an error sent and the faulty message retried.

At this point, one of the most important innovations in the GSA protocols, and a serious departure in the way that lottery regulators receive their information today, comes into play. In GSA's G2S protocol, the regulators can get the information straight from the games themselves instead of from the Slot Management System (SMS). Figure 3 shows the current slot floor configuration. In this configuration, all the information flows from the games to the SMS and then to regulators either electronically or through reports. The regulatory functions are dependant on the information received from the SMS. In figure 4, the diagram shows that the regulators can get their information straight from the game using their own

GAMING STANDARDS ASSOCIATION
48377 Fremont Blvd, Suite 117 Fremont, CA 94538 USA
Tel: +1 510.492.4060 Fax: +1 510.492.4001 www.gamingstandards.com

G2S regulatory server. There is no SMS involved. This is where the true accountability for the regulator comes in.

The regulatory server can be designed by the regulatory agency or contracted from a machine manufacturer or other third party. It would be owned and controlled by the regulatory agency.

As mentioned earlier, accountability has many forms. Perhaps even more important than making sure the games are reporting properly is accountability regarding the integrity of the games. So far, we know that, from a regulatory point of view and from a lottery operator's point of view, we can use G2S and GAT to make sure the software on the games is proper. We are also sure that the games are reporting properly such that the revenue for the operator and the government (in some cases the same entity) is correctly distributed. However, for the networked games that are being introduced in the lottery and non-lottery gaming, the software on the games may change and may change often. There is no question that the lottery and the governing body that sanctions the lottery is still held accountable for the operation. The question, then, is how can one manage networked gaming such that the lottery benefits from the new technology, but does not get so caught up in the technology that the integrity of the games and patron confidence are adversely affected? GSA's protocols have the answer.

The G2S committee, in the development of the protocol, added the ability to authorize changes on the gaming terminal. These changes range from any type of configuration changes to complete downloads of new software. The changes are authorized by a list of "authorization" hosts. This list could be blank, such that changes may occur immediately, on demand, or there may be several hosts that must specifically authorize the changes to be made. If there are one or more entries in the authorization list, all must agree that a particular change is appropriate before the change can be made. If an authorization host fails to authorize a change within a specified authorization time, the change "times out" and is rejected.

In practice, an authorization host is a server or workstation that registers as an authorization host. The regulatory server monitoring the meters back in figure 4, could also be an authorization host. Additionally, using a secure connection to the regulatory server, the regulatory authorization may be made remotely, from the government offices much like the GAT functions.

The ability to authorize a change is not just important to the governing body. The slot director and other key personnel may want, or need, to have authorization capability to make sure that the changes are appropriate at a particular time. They too would have an authorization server and would register that server as an authorization host. In this configuration, changes could be authorized by the regulator and/or the operator hosts. However, if a change is requires authorization from both hosts, both must provide the authorization within the authorization time or the change will be rejected.

So with the proper use of the authorization capability, even the networked games can be managed to improve the patron's experience and still maintain the integrity of the lottery that both the operator and the regulating body have worked so hard to establish.

GAMING STANDARDS ASSOCIATION
48377 Fremont Blvd, Suite 117 Fremont, CA 94538 USA
Tel: +1 510.492.4060 Fax: +1 510.492.4001 www.gamingstandards.com

That brings us to the third "A" in the GSA equation: **Agility**.

Agility in business is the ability to change direction or business strategy quickly to take advantage of changes in the market. As the gaming business becomes more complex and more competitive, the ability to react quickly to changes in technology, and to the patron's changing views on what constitutes a "good" game, becomes critical. For example, in the last 7 to 10 years, average life expectancy of a slot program has gone from well over a year to around 3 or 4 months. Unfortunately, the cost of the programs has not been reduced accordingly. So, with the cost of the programs remaining high, and the life of the program getting shorter it becomes more important to buy the programs that will provide the most return on investment and the most enjoyment for the patrons. Unfortunately, no one has yet figured out which game will be successful prior to them hitting the casino floor (regardless of what your salesman tells you). The answer, then, is to develop the ability to quickly capitalize on the successful programs and minimize the exposure to unsuccessful programs. The result would be that a lottery operator could maximize revenue and, at the same time, provide the patrons with the games they want to play; a win, win situation.

GSA protocols are up to the task. G2S is the protocol that enables networked gaming. This protocol will allow an operator to download software or remotely change the configuration of the gaming terminals quickly. Currently, it is a time and labor intensive process to reconfigure and re-option a lottery terminal that is prone to errors due to 'finger trouble'. This limits the number of machines that may be reconfigured at any one time. With G2S, though, the changes can be pushed down to hundreds of terminals at the same time minimizing down time and labor costs, but more importantly, maximizing the operator's exposure of the games the patrons want to play. An operator can "test" a game with a limited number of machines, and, if successful, blast it out all over the floor in a very timely manner. Again, the operator benefits and so do the patrons.

The ability to remotely reconfigure games is even more important to lottery operators that have multiple small operations throughout a large area, such as a state or province. In these cases, it is not reasonable to manually reconfigure their terminals on a frequent basis. The result is that themes may grow old and revenue will suffer. To keep up with the latest patron preferences, and with the latest changes in a competing jurisdiction, the operator finds the ability to remotely reconfigure and download new programs essential to the success of the operation.

So agility is important for casino style as well as for distributed lottery operations as it allows operators to quickly adapt their game options to changes in the patron's desires. However, agility also applies to the lottery infrastructure, i.e. the system side of the lottery operation, as well.

Many lottery operations enter into long term contracts with lottery system providers as this provides stability in the lottery infrastructure and gives an aggressive pricing structure for the system. Additionally, these systems are all encompassing, and are very difficult and expensive to replace. This makes changing system vendors a difficult and inefficient choice. However, as G2S and S2S are changing the back-of-house in standard casino gaming, so are they changing the back of house operations in lotteries. Looking back one more time to figure 4, the servers connected to the G2S network can be

GAMING STANDARDS ASSOCIATION
48377 Fremont Blvd, Suite 117 Fremont, CA 94538 USA
Tel: +1 510.492.4060 Fax: +1 510.492.4001 www.gamingstandards.com

extended out to include other functions such as bonussing, player tracking, and accounting with each being an independent function acquired from a different manufacturer. The servers all talk G2S to the games and S2S to each other. Basically G2S, in its ability to support independent hosts for independent functions, has allowed the all encompassing lottery back-of-house system to be broken into its composite parts. Each of these parts may be provided by a single manufacturer or from multiple manufacturers.

From an agility standpoint, the capability to break a lottery system down into its component parts allows lottery operators to choose individual services based on the needs of the lottery instead of buying a single monolithic system because it has the best accounting module. Using the GSA protocols, the operator can select just the accounting module they like best and then select the player tracking module from a different vendor. Even more importantly, if a new accounting module or player tracking system is developed that provides a better solution for the lottery, changing is not difficult as only the affected module is changed. The lottery is better able to react to changes in the market and as a result is more profitable, more responsive to the desires and requirements of their constituents and more agile in its business stance.

Well that wraps up the three “A”s of GSA. Before closing, it is very important to understand GSA’s role in the networked gaming landscape. GSA develops protocols, not gaming applications. Your gaming manufacturers develop the applications. The functions discussed in this article are capabilities that the GSA protocols will support. It does not mean that your manufacturers have implemented these features in their products yet. That is where you lottery operators and government regulators come in. You pulling the technology in by specifying the particular functions you need for your operation will give the manufacturers the extra push they need to move this technology into the lottery realm. You can trust that the GSA will continue pushing from our side. All the major manufacturers are developing implementations for G2S and S2S. Applications are currently being approved for the traditional gaming market and these will be finding their way into lottery systems soon. Your pull will make it sooner.

If you have any questions or require any additional information regarding GSA you may visit GSA website at www.gamingstandards.com. Our standards are free for you to download at your convenience. There is also a means to send questions to GSA. If you do send a question, we will get back to you. You will also find information on being a member of the GSA. If you would like to get involved with the development of the standards either to assist in writing the protocols, establishing the direction of the protocols, or just to be involved in the latest developments, being a GSA member is the way to go. Thanks for following along and I hope you found the information useful.