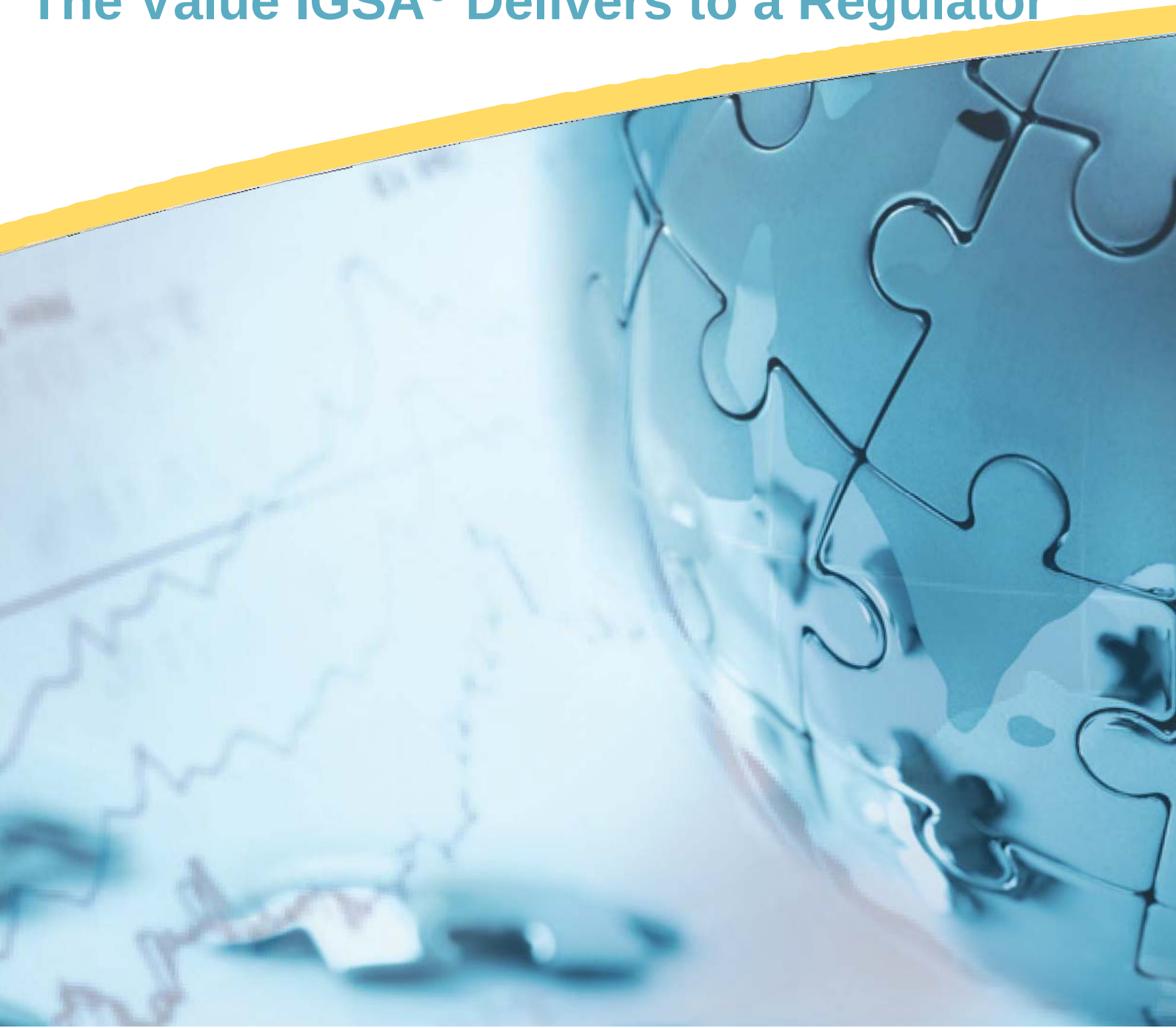
A Regulator's Guide to IGSA Standards

The Value IGSA® Delivers to a Regulator



A Regulator's Guide to IGSA Standards: The Value IGSA Delivers to a Regulator

Released20/09/01, by Gaming Standards Association® (GSA®), dba IGSA.

Patents

NOTE: The user's attention is called to the possibility that compliance with this [standard/specification] may require use of an invention covered by patent rights. By publication of this [standard/specification], GSA takes no position with respect to the validity of any such patent rights or their impact on this [standard/specification]. Similarly, GSA takes no position with respect to the terms or conditions under which such rights may be made available from the holder of any such rights. Contact GSA for further information.

GSA Intellectual Property

IGSA Contact Information

E-mail: sec@igsa.org

WWW: http://www.igsa.org

Table of Contents

1 How the IGSA GAT and G2S Standards Benefit Regulatory Authorities

1.1 What Regulators Focus On

Regulatory Authorities world-wide are asked to provide oversight of increasingly complex gaming technology. In many cases the oversight responsibilities of these Authorities span all gaming verticals from land-based to online to lotteries, in the many shapes and sizes that they come in.

As part of their oversight mandate, Authorities seek to

- Keep gaming fair
- Keep gaming free of crime
- Protect vulnerable individuals

IGSA standards are most beneficial in helping Authorities ensure that gaming is fair and legal and helps prevent susceptible players from self-harm.

IGSA Standards support Authorities by providing:

- data which cannot be accessed easily or at all without the standards to enable better oversight.
- increased levels of transparency providing regulatory authorities with actionable information.
- means to perform regulatory tasks using technology and automation to augment and support regulatory agents.

This document seeks to explain how this is achieved without delving into the technical details. Its goal is to spark thought, to generate questions and to start a dialogue. IGSA's Regulatory Committee[1] is an existing forum where ideas and issues are shared amongst its members, however, IGSA staff is available to meet with individual Authorities to discuss and think through current issues, to explore existing solutions and to identify potential new ones.

1.2 Keeping Gaming Fair

Within the context of IGSA Standards, keeping gaming fair means that gaming devices must utilize software that has been approved by the Regulatory Authority and must operate within the

[1] The Regulatory Committee is open only to Regulatory Authorities and is a trusted space where regulators can discuss issues openly and without any industry participation. Limited IGSA staff help facilitate and take notes and act as a conduit to the other IGSA Technical Committees, kept at arms-length, whenever the Regulatory Committee seeks their input. Please contact IGSA at sec@igsa.org for more information about this important resource.

parameters specified by the pertinent gaming jurisdiction.

Today, many Regulatory Authorities rely on tamper-proof tape, on data provided by operators, or on physical audits, to ensure that gaming devices[2] and online gaming software meet requirements. While these processes do in fact help ensure that gaming is being provided fairly, they have a series of drawbacks and limitations that can be eliminated. Specifically, these methods can be improved upon by using the Game to System (G2S) and Game Authentication Terminal (GAT) IGSA standards.

Authorities rely on third-party certified laboratories to test operating systems, random number generators and game software, ensuring that they meet the regulations for their jurisdiction. Third-party laboratories publish their test results and if found to comply with those regulations, Authorities approve the gaming software to be deployed. Copies of that originally tested and approved gaming software version are made by its supplier and distributed to various gaming entities. The same process is used for other gaming device software, and firmware, including those used in bill acceptors, printers, and other peripheral equipment.

How do Authorities ensure that only the approved version of gaming device software and firmware is being used?

1.2.1 Are Approved Versions of Software Running in the Field?

The Game to System (G2S) protocol standard provides access to data residing on gaming devices which the older SAS protocol cannot access[3]. That data can be of significant value as regulatory authorities work to keep gaming fair.

Regulatory Authorities wanting to verify the version of gaming software and firmware being used by licensees generally use one of two methods to perform that task. The first is to rely on information provided by operators from their casino management system (CMS) which, in most cases, is manually entered. The second is to have regulatory agents physically inspect each gaming device.

Both methods have shortcomings. With the former, the data provided by operators may not be accurate or up to date and with the latter, a significant amount of labor and time is required to physically inspect each gaming device.

A much more accurate and automated way to perform this task is to use the G2S protocol. G2S supports providing an inventory of every piece of software running within a gaming device and the peripheral equipment. Regulatory authorities can utilize their own computer to interrogate each gaming device over a network to collect that information and to verify that the software is compliant.

This G2S capability is especially useful when gaming device or peripheral equipment software has been revoked by the regulatory authority or considered obsolete for some reason. For example, note acceptor software might have to be updated to deal with a new type of counterfeit bill. The ability to quickly and easily collect software information from the gaming devices ensures compliance and reduces risk.

See Appendix 1 for a discussion on G2S implementation methods that minimize cost and operational disruption.

[2] The term gaming devices should be understood to mean physical devices such as Electronic Gaming Machines, Video Lottery Terminals, etc. and Electronic Table games.

[3] For a more detailed fact-based comparison of SAS and G2S features and functions, please refer to the IGSA article found at https://www.gamingstandards.com/sites/default/files/documents/gsa-game-to-system-protocol_0.pdf

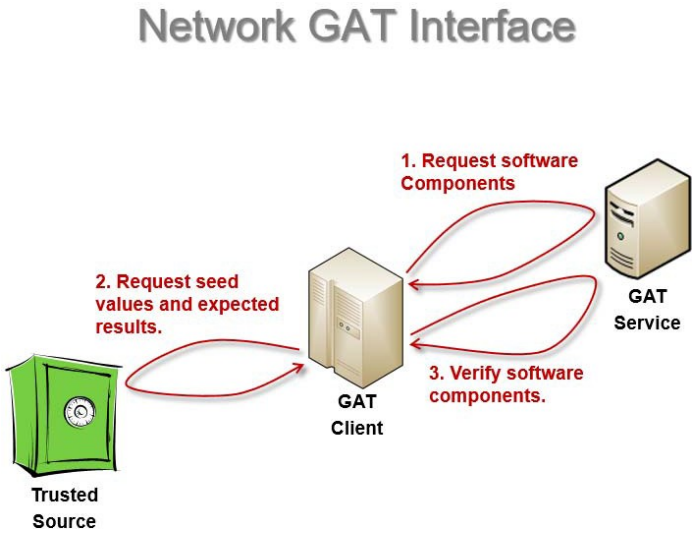
1.2.2 Has the Gaming Device Software been Hacked?

Ensuring that approved versions of gaming device software are being used within gaming sites is one aspect of ensuring that gaming is occurring in a fair manner. The other part of this is to ensure that the gaming device software is the authentic software as tested by accredited testing labs and approved by the Regulatory Authority.

In the past, Regulatory Authorities relied on tools such as Gaming Laboratories International's Verify+. This tool, the latest generation authentication device (very useful Kobetron tools), performs the software authentication process flawlessly. However, it requires being physically at the gaming device, the use of special adapters and removal of software storage devices.

IGSA developed the Game Authentication Terminal (GAT) protocol to help streamline the software validation process. Instead of requiring purpose-built tools, GAT runs on an ordinary laptop. Instead of having to remove software storage devices, GAT requires the laptop to be connected to a serial (GAT) port inside the gaming device. The software then executes the authentication process and provides a result which should match the value created by the certification laboratory.

While this GAT process improved the authentication process, it still requires regulatory agents to be physically at each gaming device, to open that device, connect a cable and remain at the device while the authentication process runs. Testing several tens if not hundreds of gaming devices in this manner, is a time-consuming undertaking.



To further streamline the process, IGSA developed the Networked GAT Interface (NGI). NGI supports executing the GAT authentication process over a network. NGI allows a Regulatory Authority to use its own computer to request a GAT verification to occur on one or more gaming devices over a network. The regulator's computer can be connected over a network directly to the gaming devices or to a GAT Server at the gaming site, which then connects to the gaming devices.

NGI eliminates the need for regulatory agents to carry purpose-built tools or laptops and to have physical access to the gaming device. The Regulatory Authority can have a GAT Client software application created that, depending on its level of sophistication, could automatically query a random selection of gaming devices to perform the GAT authentication and compare the results with the expected value.

While NGI is a significant improvement over plain GAT, IGSA recognized that many Regulatory Authorities wanted to utilize both the software inventory and software authentication capabilities of its standards. To achieve this, IGSA created G2S GAT.

G2S GAT essentially imbeds the GAT functionality into the G2S protocol effectively marrying the two capabilities — providing a full software inventory and full GAT authentication. Just as with NGI, the Regulatory Authority can use its own computer as a G2S Host and connect to gaming devices remotely over a secure Virtual Private Network (VPN). This then allows them to remotely collect the information they need to ensure that gaming devices are running authentic software and that gaming devices and peripheral equipment are running the approved versions of software.

1.2.3 Is Accurate Meter Information Being Reported?

While it has several different names, Gross Gaming Revenue (GGR), Gross Gaming Yield (GGY), Gross Gaming Earning (GGE) and others; the calculations that determine gaming entity profitability and amount of tax owed is dependent on gaming device meter information.

Ensuring that meter information is correct is tackled in a manual fashion. Gaming devices are tested when connected to systems to ensure accurate reporting, financial reports are audited to ensure accuracy, etc. These time-tested processes provide a measure of assurance that the meter information being reported is accurate. But there may be a better way.

G2S as a networked protocol allows a gaming device to connect to multiple systems. One of those systems could be a Regulatory Monitoring System that collects meter and event data separate from the operator's CMS. This system can subscribe to any information generated by the gaming device in real-time or on a periodic basis, allowing the Authority to have an independent data feed of this data.

The Regulatory Monitoring System could perform both the GAT authentication as well as the Meter collection functions. Additionally, it could also report certain events that may be of interest to Authorities such as when an Electronic Gaming Device is RAM cleared.

2 How RRI benefits Regulatory Authorities

2.1 Regulatory Reporting

Regulatory Authorities oversee gaming activities by means of the data that is reported to them from gaming licensees. This data is used to achieve the regulatory objectives identified in section 1.1. In the absence of a common standard, each gaming jurisdiction is creating its own solution for how data should be reported. The type of data, the reporting frequency, and the format within which this data should be reported are different across existing gaming jurisdictions. These differences will most likely continue to grow, not only as new jurisdictions allow gaming, but also as existing jurisdictions allow new types of gaming and as requirements are reviewed and changes identified.

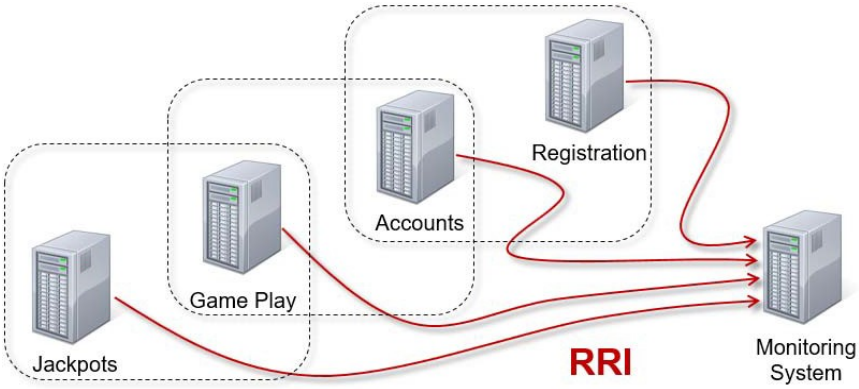
These different reporting requirements result in duplication of effort and an inability to accurately share and compare data. This potentially places an undue burden on licensees seeking to operate in multiple jurisdictions having to essentially 'recreate the wheel'.

IGSA identified the need for a single reporting standard that could be applied to all types of gaming activity, implemented by large and small operators and system suppliers alike, and which accommodated the various frequency of data collection required by each jurisdiction.

2.1.1 Why Are There So Many Different Reports?

The *Regulatory Reporting Interface* (RRI) identifies and defines an exhaustive list of data elements which are generated by gaming activity and which Authorities around the world require[4]. This is essentially a data dictionary, that lists and defines each data element including its length, its type (string, number, etc.), whether it is required and how many instances of it can be reported.

RRI is the mechanism by which the data elements are reported by the source systems, from land-based, online (casino games, sports betting, e-sports) or lotteries, to the regulatory systems and at which frequency (real-time, near-real-time, or periodically).



This diagram shows how the individual system components that comprise an online gaming system utilize RRI to send information to a Regulatory Monitoring System.

[4] The European Commission mandated that a pan-European reporting standard for online gaming be created. The European Committee for Standardization (CEN) is working on creating that standard. GSA Europe is a liaison organization to CEN and has donated the RRI standard to this effort. GSA Europe has been acting as Co-project Lead to create this standard which is slated for release in 2021.

RRI is flexible and extensible. Flexible in that each Authority can specify the reporting frequency, specify which data elements they want, and which they do not, and specify the order in which data elements are to be reported. Extensible in that additional data elements can be added without breaking compatibility, and sub-elements can be added by individual jurisdictions where they may be required.

RRI solves the problem of not being able to compare data, provides Authorities with a single simple means to get data from systems managing all types of gaming activity, and eliminates the need for gaming system suppliers to create custom reporting systems for each jurisdiction they operate in.

2.1.2 Who's doing what and where?

RRI, through its standardized defined data elements and single data transmission methodology also helps protect vulnerable individuals. Many jurisdictions espouse strong Responsible Gaming strategies and require operators to implement measures to responsibly provide gaming entertainment. From Know Your Customer (KYC) to Limits Setting and ultimately Exclusions, Authorities in partnership with the industry are doing their best. However, sharing information across gaming companies and across gaming verticals is challenging within a single jurisdiction. That challenge is compounded when trying to implement solutions that cross jurisdictional boundaries.

RRI solves that data sharing problem. Regardless of the gaming vertical and regardless of the gaming jurisdiction, if the RRI standard is embraced and implemented, data, *in the same standard format and same standard definition*, can be shared and compared. That data becomes actionable because a player's activity can be tracked across verticals and across jurisdictions.

In of itself, RRI is not a Responsible Gaming standard. However, RRI becomes the underpinning for solutions that can provide greater transparency and greater aid to those susceptible players.

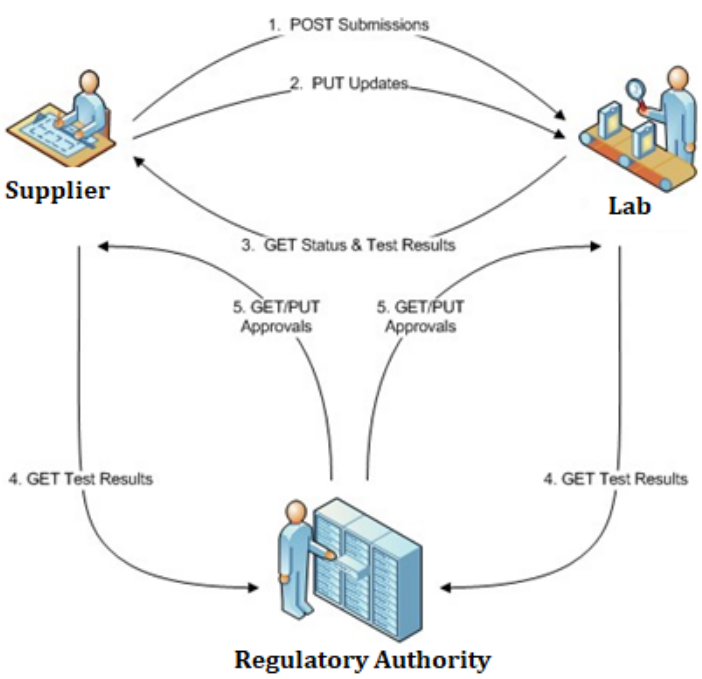
3 How CDI benefits Regulatory Authorities

3.1 Gaming Submission Tracking

Many Regulatory Authorities rely on certified third-party laboratories (Labs) to test gaming products, ensuring they meet the jurisdictional regulations. Suppliers submit their products directly to the Labs, provide the necessary equipment for testing to occur, instruct the Lab's staff on how the product works, if required, and then interact directly with the Lab staff to answer questions, discuss potential issues and address bugs throughout the testing process. In almost all cases, suppliers seek certification of their products for multiple jurisdictions. Labs, therefore, test the products to ensure compliance with the different jurisdictional requirements.

3.1.1 Electronic Submission, Tracking and Approvals

This process, while it has been functioning well for decades, can be improved by increasing Testing Transparency, Standardizing Test Result Documents and Reducing Duplicate Testing. The Certification Database Interface standard (CDI) delivers these improvements.



CDI addresses the data interchange needs of Authorities, Labs, and Suppliers. The initial release includes a standard interface for exchanging product testing information amongst Authorities, Labs, and Suppliers – for example, certification requests, product component information, pay table information, software signatures, associated documents, etc. This diagram illustrates the interactions.

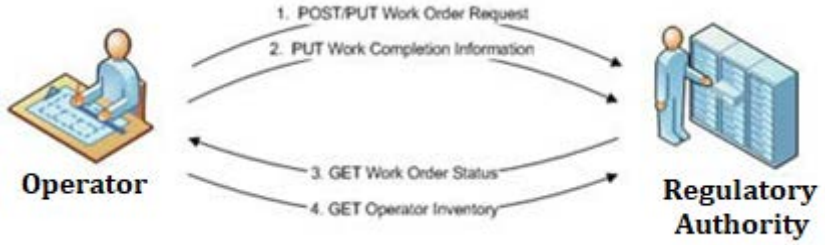
The process allows Suppliers to POST submission documents electronically to the Lab. If changes are required, Suppliers PUT those updates into the Labs repository. Suppliers can also GET testing results as they occur. Authorities can GET testing results from both Suppliers and Labs – allowing comparison - and PUT Approval documents sending them to the Supplier and Lab.

CDI provides both Authorities and Suppliers with more product testing transparency, through electronic on-demand information of the status of the testing, number of issues found, etc. It creates a single standard Testing Result document across all Labs eliminating some of the confusion that may be created by the different formats and content provided in those documents today. Finally, it also may reduce the number of times a product has to be tested and reduce the time needed to get a product tested for one jurisdiction to be certified for another jurisdiction. This may occur by eliminating the need to issue a Testing Result document per jurisdiction.

3.1.2 A more Streamlined Approval-to-Ship and Notification Process

The CDI may also be used to exchange information between Suppliers and Authorities when approval to ship gaming products are needed. The electronic CDI process eliminates the need for multiple forms, often specific to a jurisdiction, and creates a single standard means for communicating the required information to the Authority. The Authority can also electronically and on-demand, see the status of shipments that they're expecting.

This process can also be applied to situations where Operators must submit work orders which may be required when a gaming product is going to be moved, configurations changed, upgraded, etc.



A1 G2S Implementations Myths & Misinformation

Appendix 1

Dispelling the myths that the G2S protocol is costly and complex.

Myth 1 – G2S is too big, too complex, too difficult - it's not worth it!

The G2S protocol specification is large (well over 3,000 pages). There are several reasons why this is so:

- Functionality - G2S has much more functionality than its most common alternative SAS, and is fully extensible, allowing new features to be added;
- Audience – The document was created for developers and includes many hundreds of pages of sample code to help the developers; and
- Completeness – The document includes hundreds of diagrams and is written in a manner that ensures the reader understands the concepts.

By comparison, the SAS version 6.02 protocol is less than 200 pages. There are several reasons why:

- Functionality – SAS was developed in the 80's with limited functionality. In addition, it is not extensible. In fact, the protocol has, other than some minor repurposing of messages, not changed in decades;
- Audience – The document was created for developers that already understood how the protocol works and intended as a reference not a teaching document. The document is also is rather cryptic and only includes tables showing messages with no examples or any other development assistance.

Therefore, while the G2S document is indeed large, there are very valid reasons for this. Additionally, there is no requirement that all of the functionality supported by G2S must be implemented. In fact, it is quite the opposite.

G2S was designed to enhance interoperability between gaming devices and gaming systems. To do this a small core set of functions, in G2S-speak called 'classes', were identified which are required. This core set of classes includes the most basic requirements to allow a gaming device to talk to a gaming system. They are:

- Communications – How the gaming device communicates to one or more systems, such as sending and resending commands, point-to-point or multicast messages, data types and error codes;
- Cabinet – How the gaming device shares information about the features it supports, such as currencies, cash-out devices and error codes;
- Events – How the gaming device handles events, such as; listing supported events, sending an event notification, and configuring events;
- Meters – The meters supported by the gaming device such as, which meters are supported, how systems can subscribe to specific meters, and how meter consistency is ensured;

- Game Play – Information about the games loaded on a cabinet such as, game themes, paytables, and denominations;
- CommConfig – How the communications between the gaming device and gaming systems are configured to enable data flow; and
- OptionConfig – What gaming device options are supported and how they can be configured.

Beyond these core classes, all the other G2S classes are optional and only implemented if specific functionality is made available by a gaming supplier or required in a gaming jurisdiction.

Bottom line, no one is expected to implement *all* G2S, just the required core classes.

Myth 2 – No one has implemented G2S

Many gaming devices already support G2S and some can support both SAS and G2S simultaneously. The reason for this is that there are several gaming jurisdictions that mandate G2S be used. Those include all the Canadian provinces for the VLT market and Oregon and Illinois for the 'route' markets in North America. Austria, Greece and Finland all mandate that G2S be used. In some cases, Casino Operators have mandated that G2S be used. The Aria and The Cosmopolitan in Las Vegas are examples of this. Gaming suppliers selling games into those markets and to those operators must support G2S.

Bottom line, a quick review of gaming suppliers with gaming devices in those locations illustrates that many of the largest suppliers already supply gaming devices that support G2S, contrary to what some might say.

Myth 3 – A Casino Operator must replace their CMS if they implement G2S

G2S is a network-ready, encrypted, communication protocol that uses the same technology as a computer or laptop plugged into a network. This is commonly referred to as a TCP/IP network. SAS on the other hand is an unencrypted serial protocol that uses an older antiquated style of communication. Some may remember connecting printers directly to a computer using a parallel or serial cable.

Since they use completely different communication types, they also use completely different physical connection types to the gaming device. G2S uses the network connector known as an RJ-45 connector which is the same as the cable used to connect a computer to a network wall plate or router. SAS uses a serial connector known as a DB-25 which is a 25-pin male and female type connector. SAS also requires the use of a Slot Machine Interface Board (SMIB). The SMIB computer board acts as a translator between the gaming device which is 'talking' SAS and the gaming system which is 'talking' some other potentially proprietary language. Modern SMIBs utilize the same TCP/IP networks that G2S uses.

So, a gaming device that is capable of supporting both G2S and SAS simultaneously, (and as already explained in Myth 2, these do exist), can connect to one gaming system using SAS and other gaming systems[5] using G2S. Ideally gaming system suppliers will start to provide G2S systems as this will provide access to data which the gaming devices generate today but which older protocols like SAS cannot use.

Bottom line, the operator does not have to replace their CMS which is connected to gaming devices via SMIBs. That connection can continue to exist as it does today and function alongside the secondary G2S connection.

[5] G2S allows a gaming device to connect to multiple systems, like how a printer is accessed and shared on a network by multiple computers. This means that Authorities could have their own Monitoring System connected to the gaming device in parallel with the CMS.

Myth 4 – A Casino Operator must have a networked casino floor to run G2S

While it is somewhat of an anachronism that there are casinos that still do not have a high-speed network on their casino floor, the fact of the matter is that there are some. Obviously, the cost to implement a network is not insubstantial. Therefore, this is often cited as a reason why G2S is not implemented.

As has been explained in Myth 3, there is no reason to replace the existing CMS to implement G2S. The CMS is in some jurisdictions referred to as 'the system of record', meaning that it is the system that must generate all the reports the operator is obligated to submit to authorities. It also means that it is the critical system which must be tested and certified by the authorities. If a casino does not have a high-speed network, sometimes referred to as an IP network, then they must be using an older style connectivity scheme to handle the CMS accounting and player tracking data.

A separate cost-effective solution is needed to support G2S connectivity. One that does not impact the current CMS solution used by the operator, but a solution that offers the operators and regulatory authorities independent access to the rich information that G2S offers.

That solution comes in the form of wireless connectivity. Wireless can mean WIFI or Cellular communication. Cellular or mobile data communication is sometimes referred to as GPRS.

Both communication technologies support data encryption methodologies that are identical to, and therefore equivalent to, encryption used on wired networks. Both support high-speed and reliable data throughput and both require little to no wiring. Certainly, the implementation costs are a fraction of the cost of putting in a wired high-speed network in an existing casino.

In this type of implementation, gaming devices are wired to local routers which then send the data wirelessly to local computer servers. The data is then distributed from there in the same fashion as CMS data is.

Some authorities still balk at the use of wireless technologies, even though as individuals many of them shop online and bank using a mobile phone. Further, online gaming is spreading worldwide, and it is conducted wirelessly via mobile devices, laptops, and cloud-based computing. GSA standards use the same encrypted technologies.

However, for those that still do not want to allow critical data, in other words 'system of record' data to be submitted wirelessly, then a wireless solution coexisting with a legacy wired CMS implementation would work.

Bottom line, not having a networked casino floor is no reason G2S cannot be implemented. Wireless solutions can provide the network connectivity required by G2S in a cost-effective way. It can still be used to allow authorities to connect their own monitoring systems to gaming devices. It can also allow operators to connect other systems which perform tasks, and provide access to information, that CMS systems using legacy communication protocols simply cannot.

Myth 5 – G2S requires replacement of all gaming devices and they must be replaced simultaneously

The idea that all gaming devices must be replaced and that they must be replaced all at one time, ties into Myth 3. As already described, there is no need to replace the CMS in order to take advantage of the benefits provided by G2S. Regulatory Authorities wishing to utilize G2S GAT and to implement G2S-based Monitoring Systems can do so working with operators in a phased-in approach. That approach would identify gaming devices that can be economically upgraded to support G2S and SAS first, creating a mandate that all new gaming devices purchased from a certain date support both G2S and SAS, and lastly agreeing to a timeframe over which older gaming devices (not upgradeable) can be removed from use.

For a gaming device to be able to use G2S, its motherboard must be capable of running an operating system that supports that protocol. Whether a cabinet needs to be replaced or not depends on several factors, but in most cases, cabinets should not need to be replaced. Those factors are:

- Operating System - Suppliers produce operating systems usually released to support new functionality required by game themes. Some suppliers create a single operating system which they use world-wide and which supports all communication protocols. Other suppliers produce different versions, per country or region and per communication protocol. Therefore, ideally the only thing that would need to be replaced within a gaming cabinet to support G2S is the operating system.

- Motherboard - Since it is not uncommon to find cabinets that are over ten years old still in use, it is possible that the motherboard inside the cabinet may need to be changed in order to support an operating system that runs G2S.

- Age – Gaming devices that were manufactured before a certain time or those that have become obsolete by their suppliers, may not have an upgrade path.

Bottom line, operators do not have to replace all their gaming devices. Understanding how many gaming devices fall into each of the factors above will identify the real cost of moving towards a G2S enabled floor. And a phased in approach that starts to deliver G2S-based value while managing operator expense is the best approach. The simultaneous replacement of all older non upgradable gaming devices is not required.