Gaming Machine Monitoring System Technical Standard

Ver1.0

8 February 2019

Tasmanian Liquor and Gaming Commission

Tasmania

Table of Contents

1 Introduction

1.1 Objective

1.1.1 The objective of this standard is to ensure that Gaming Machine Monitoring Systems (GMMS) operated in Tasmania, are designed to:

- ensure the integrity of transactions and fairness of the GMMS;
- ensure the security and audit capacity of the GMMS and connected gaming machine equipment;
- ensure the GMMS accurately monitors, records and reports information and events gathered from connected gaming machine equipment;
- ensure GMMS compliance with supported gaming machine protocol communication requirements;
- ensure games connected to the GMMS comply with Tasmanian legislation and Commission adopted technical standards;
- ensure the GMMS has interface capability with respect to other gaming related systems;
- ensure the GMMS correctly calculates gross profit and tax payable;
- ensure the GMMS correctly awards player entitlements; and
- minimise the potential for harm from gambling and provide support for consumer protection measures.

1.1.2 To ensure, to the greatest extent reasonably possible, the integrity of gaming, a GMMS used in Tasmania must only be operated in gaming venues by the licensed operator. This does not prevent licensed operators from obtaining a system from an external supplier authorised under the *Gaming Control Act 1993*.

1.1.3 The supply of a GMMS requires the approval of the hardware and software, within the supplier's control, that deliver the system and the approval of internal controls - the licensed operator's documented system of procedures for operating the system and ensuring security of the system. This document does not cover internal controls, but in describing GMMS requirements, assumes that effective internal controls are in place.

1.2 Scope and Purpose

1.2.1 The scope and purpose of this document is to describe guidelines for the functionality of a GMMS that may be approved from the Commission's viewpoint, bearing in mind the overarching object in the relevant gaming legislation and other adopted standards.

1.2.2 The process for the approval of the proposed product will be determined by the Commission, in consultation with the supplier. It is expected that Accredited Testing Facilities (ATF) will play an integral part in the testing of the GMMS to ensure compliance with regulatory requirements.

1.2.3 It should also be noted that compliance with this document does not exempt the supplier and licensed operator from compliance with other laws (e.g. laws relating to privacy, consumer protection, prohibited content, copyright, electrical safety and electronic cash transactions).

1.2.4 This document does not seek to mandate use of any specific gaming machine communication protocol, however, it is expected that any supplied GMMS must comply with this Standard and operate in accordance with supported gaming machine communication protocol specifications.

1.3 Dispensations

1.3.1 In special circumstances, gaming equipment which does not fully comply with all the requirements specified in this standard, may be considered for approval provided GMMS gaming equipment operates in a manner that is suitable in respect of:

- fairness;
- security;
- integrity; and
- consumer protection.

Approval of any such equipment will be at the sole discretion of the Commission.

1.4 Associated Documentation

1.4.1 Potential Suppliers, third party suppliers and system developers should also familiarise themselves with the following to ensure the GMMS suitability:

- Gaming Control Act 1993
- Australian/New Zealand Gaming Machine National Standard 2016
- Tasmanian Appendix (V10.08) to the Australian/New Zealand Gaming Machine National Standard 2016
- QCOM 3 Interface SpecificationV3.0.*x*
- QCOM Gaming Machine Communication Protocol V1.6.*x*
- GSA G2S - Game to System Communication Protocol
- GSA S2S - System To System Communication Protocol
- ASP 2000B Gaming Machine Communication Protocol
- TLGC Card Based Gaming Systems Technical Standard V1.0
- TLGC Table Gaming Management System Technical Standard V1.0
- TLGC Responsible Gambling Mandatory Code of Practice
- TLGC Casino Licence Rules
- TLGC Premium Player Program Rules
- TLGC Gaming Operator Licence Rules
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- Privacy Act 1988
- ISO/IEC 27002:2013 Information Technology – Security Techniques - Code of practice for information security controls

1.5 Copyright

The Tasmanian Liquor and Gaming Commission wishes to provide its acknowledgement and thanks to the Queensland Office of Liquor and Gaming Regulation (QOLGR) for granting it permission to use its Queensland Gaming Minimum Technical Requirements as a basis for the development of this technical standard.

This document is the property of the State of Tasmania (Department of Treasury and Finance). Copying, making extracts or use of the document, without prior permissions, is prohibited. Additionally, all material that has been sourced from the QOLGR technical standards continues to be remain the property of the State of Queensland. Accordingly, Queensland sourced requirements in this document remain subject to copyright laws applicable to that jurisdiction.

2 General Requirements

2.0.1 The GMMS must perform the following functions:

- monitor and maintain the security of connected gaming machines and associated equipment;
- monitor and maintain compliant operation of machines and connected jackpot systems;
- maintain accurate gaming machine operating records such as fills, hand pays, game meters, jackpot meters and other significant events in a secure and auditable fashion;
- provide accurate reporting of gaming machine game and jackpot events and performance;
- provide the capability to interface with related gaming systems;
- ensure compliance with adopted gaming machine communication protocol requirements;
- provide precise calculations of tax payable; and
- provide support for consumer protection measures.

3 Validation and Security Requirements

3.0.1 The GMMS must be configured to only permit the live operation of compliant game configurations.

3.0.2 The GMMS must be able to securely interface with all gaming machines, jackpot systems and other gaming equipment operating in conjunction with gaming machine games.

3.0.3 The GMMS must have high levels of security with different access levels and all meter edits and changes to software must be securely logged and reportable.

3.0.4 An approved GMMS change control system and/or joint password control arrangements must be in place.

3.0.5 The GMMS must not permit the operation of games where a loss of communication would adversely impact on the system's ability to control, record and monitor significant game and jackpot events (*for example, linked jackpot games must not be permitted to operate if the system cannot control, monitor or record operation during an outage*).

3.0.6 The GMMS must be able to turn off any variable game features for player classes if the system is unable to verify a player is of the appropriate class (*for example, if the monitoring system was temporarily inoperable or a feature must be limited to a class of player*).

3.0.7 The GMMS must have the capacity to enforce compulsory gaming machine software authentication via an approved validation method. The system must not use static hashing techniques to perform gaming machine software authentication, however, one of the following methods is acceptable:

- Use of a short term (daily) seed to calculate a game software set hash result;
- Use of a randomly selected seed against a large pool of seeds to calculate a game software set hash result; or
- Use of another gaming machine game software authentication method that provides equivalent levels of authentication to those stated above, for each gaming machine connected to the GMMS.

3.0.8 The GMMS must not permit the live operation of games unless the authentication of the gaming machine software has been successfully completed.

3.0.9 The GMMS must successfully authenticate gaming machine software if the logic area is accessed, before it permits the game to enable for live operation.

3.0.10 The GMMS must be fully or partly capable (*in conjunction with surrounding manual processes*) of verifying that integrity-based game configurations (*such as, but not limited to denomination, variation, maximum limit configurations and machine caps*) operate in an approved manner.

3.0.11 The GMMS must have the capacity to detect and act upon unauthorised game configurations (for example *the GMMS must be capable of verifying that intended configurations on the system reconcile with those manually configured on the machine*) and automatically disable a game where verification has failed.

3.0.12 The GMMS may support multiple gaming machine communication protocols, however, games must not be operated in a live capacity unless they are able to be monitored in accordance with this standard and protocol requirements.

4 Registered Play

4.0.1 The GMMS must have the capability of operating or interfacing with registered card play systems. *Refer to TLGC Card Based Gaming Systems Technical Standard for specific card based requirements.*

4.0.2 The GMMS must have the capability of interfacing and supporting the operation of mandatory and voluntary pre-commitment systems.

5 Hardware/Software

5.1 Minimum Requirements

5.1.1 To ensure reliable performance, the GMMS must meet all minimum hardware and software specifications.

5.2 Approval

5.2.1 All hardware and software used by the GMMS to conduct gaming must be considered suitable for approval pursuant to section 81 of the *Gaming Control Act 1993*.

5.3 Requirement for Encryption

5.3.1 Where sensitive data is being passed over communication lines, such data must be encrypted. Examples of sensitive data that require encryption are passwords and encryption keys, including any information that if made public could compromise the security of the GMMS.

5.3.2 Sensitive data must be encrypted on an end-to-end basis (*for example the data must never appear on a LAN or WAN in an un-encrypted form*). This includes sensitive data transmitted between computer systems within a casino operator's premises.

5.3.3 Sensitive data transmitted between systems within a single secure data centre need not be encrypted.

5.3.4 Sensitive data transmitted between GMMS infrastructure located within separate secure data centres need not be encrypted if the communications path is physically secure and cannot be accessed by unauthorised people.

5.3.5 Encryption systems are to be demonstrably secure. Only published, public, encryption algorithms and protocols may be used and must have a demonstrated track record against attacks and history of reliable performance.

5.4 Requirement for Time of Day Adjustments

5.4.1 The GMMS must be capable of automatically adjusting time settings as required to accommodate the commencement and conclusion of daylight saving time.

5.4.2 Automatic time change adjustments made to the GMMS must not adversely impact upon EGM meter and significant event reporting.

6 Central Site Requirements

6.0.1 This section stipulates requirements for the GMMS, including reporting, data recovery and software version controls.

6.1 System Documentation

6.1.1 The licensed operator must have a security policy covered in its internal control and accounting procedures.

6.1.2 A GMMS baseline network policy document, defining the system network topology, configuration and the communications which take place between devices in the system, must be maintained.

6.1.3 The GMMS supplier must provide adequate documentation to the licensed operator to ensure day to day operation of GMMS without the system supplier's guidance.

6.1.4 The GMMS licensed operator must maintain documentation relating to the operation of any software audit control systems that are responsible for monitoring the approved state of GMMS gaming equipment.

6.2 General Reporting Capabilities

6.2.1 There are three main areas in which a system must be able to fulfil its tasks in providing reports to the Commission:

- It must be able to verify the financial activity and transactions of all gaming conducted on the GMMS.
- Gaming machine game significant event reporting must be obtainable from the GMMS.
- The GMMS must have the ability to generate regulatory reports as required.

6.3 Core Reporting Requirements

6.3.1 The core set of reports a GMMS must be capable of producing are as follows:

- A daily, weekly, monthly and yearly based financial summary report that totals all cash flow (*for example Funds In, Funds Out, Turnover, Total Wins*) for connected gaming machines.
- Gross profit reporting.
- Tax payable reporting.
- Levy payable reporting.
- Significant event reporting for all connected gaming machine games.
- Installed gaming machine and game configuration reporting.
- Gaming machine return to player reporting (minimum of three year performance reporting) for all connected gaming machine games.
- Individual performance reporting for multi-games and ante-bet game types (*for example the system must be able to separately record and report on meters for each player selectable multi-game, ante bet and non-ante-bet game).*
- Link and standalone jackpot performance reporting (*for example current jackpot configurations, current prize levels, overflow amounts, and win history for all connected gaming machine games*).
- Host and site controller significant event reporting.
- Gaming machine operating hours reporting.
- Gaming machine movement history reporting.
- Player information display usage reporting.
- Player information display tracking reporting.

6.3.2 The GMMS must allow for flexible reporting modules to support extensible reporting options, where required by the Commission.

6.3.3 Any alterations or adjustments to reports must be authorised by the Commission and the licensed operator must provide a written explanation for these changes.

6.3.4 There must be the ability to verify the integrity of reports to ensure reports remain certified and approved.

6.3.5 The GMMS must have the capacity to provide the Commission with efficient and seamless "read" access in a sufficient and secure manner in required locations. This

"read" access includes access to web based reporting systems that are able to facilitate the generation of reports for periods up to the close of the last trading day.

6.4 System Backup

6.4.1 There must be a method to backup all data with sufficient frequency to allow recovery in the event of an interruption and data must be backed up for a minimum period of seven years.

6.4.2 If there is sensitive information in the backup data then this must be protected from unauthorised access.

6.5 Data Recovery

6.5.1 The system must retain all data for a minimum of thirteen months.

6.5.2 In the event of a failure, the GMMS must be able to recover all critical information from the time of the last backup to the point in time at which the system failure occurred.

6.5.3 The system must be able to recover from unexpected restarts of its central computers or any of its other components.

6.5.4 The licensed operator must have disaster recovery capability sufficient to ensure player entitlements and records are accurate, up to the point of the disaster, are protected.

6.5.5 All data must be stored via secure, fault tolerant storage media and must have mirrored storage as a minimum.

7 Software Verification

7.0.1 The GMMS supplier and/or its suppliers must provide a method to the nominated ATF to enable verification of the software.

7.1 Source Code

7.1.1 All source code is to be properly commented and contain a change/revision history. If applicable, module descriptions or similar should also be supplied.

7.1.2 All source code central to the operation of the GMMS must be supplied to the Commission or representing ATF where the supplier has the capability, right, and access to provide source code.

7.1.3 Source code submissions must include all necessary hardware and/or software tools and instructions to enable the Commission or representing ATF to perform verification of source code with object code.

7.1.4 The Commission may also require that the GMMS suppliers have arrangements with closed source software vendors to allow appropriate access to source code by the Commission or the representing ATF for the purpose of investigating software faults.

8 Accounting of Master Resets

8.0.1 The GMMS must be able to identify and properly handle the situation when failures or resets have occurred on other computer systems that affect game outcome, win amount or metering.

8.0.2 The GMMS must be able to retrieve the last valid value of all important parameters stored within the system before the failure or reset occurred.

8.0.3 Adjustments to accounting on the GMMS are subject to strict security control and audit trail.

9 Recordable Events

9.0.1 The GMMS must be able to provide a means to record and view all significant events including the ability to search and report on particular event types.

9.0.2 The GMMS must be able to prioritise events correctly and take appropriate action where required (for example *log, alarm or disable connected machines where required by the Commission*).

10 Audit Trail

10.0.1 The GMMS must automatically reconcile its total accounting meters collected and physical cash flow meters once every 24 hours. Any failure to reconcile must be recorded and investigated.

10.0.2 The GMMS must have the ability to record and produce a running audit trail accurately showing all transactions.

10.0.3 Events in the audit trail must be kept on the system for a minimum of thirteen months and backed up for a period of seven years.

10.0.4 The audit trail must be accessible only by authorised personnel.

10.0.5 The GMMS must record all gaming machine game meters and all meter edits must be fully auditable.

10.0.6 The GMMS must be able to manage, record and reconcile all linked jackpots connected to the monitored gaming machines as well as standalone jackpots. The system must be auditable and ensure that only approved jackpots are operated and that these reconcile. *Note: The preferred method is to have the system operate the jackpots to eliminate machines going standalone or not reconciling*.

10.0.7 Games supporting multi-meter functionality with individual game meters (*for example multi-game and ante-bet type games*) must be fully auditable.

11 Glossary

Term or Abbreviation	Description
Ante-bet Game	A game that offers a selectable ante bet option were player participation between bets causes a change to the resultant theoretical player return (RTP) of more than 0.20%.
ATF	Accredited Testing Facility approved by the Tasmanian Liquor and Gaming Commission and listed on the Roll of Recognised Manufacturers, Suppliers and Testers of gaming equipment under section 71 of the *Gaming Control Act 1993*.
Casino Operator	A holder of a casino licence granted and in force under section 13 or 28 of the *Gaming Control Act 1993*.
Commission	The Tasmanian Liquor and Gaming Commission (TLGC).
Communication Protocol	A communication specification that defines requirements for electronic gaming machines and monitoring systems.
EGM	Electronic gaming machine.
Fixed Jackpot	A jackpot where the winner is paid a fixed amount or casual merchandise, which was advertised in advance.
Gaming Operator	A holder of a gaming operator licence granted and in force under section 13 or 28 of the *Gaming Control Act 1993*.
GMMS	Gaming machine monitoring system.
Hash	A value that is generated from a hashing algorithm for the purpose of software authentication.
LAN	Local area network.
Licensed Operator	A casino operator or a gaming operator.
Linked Jackpot	A jackpot arrangement which links gaming machines within a single venue. Under this arrangement multiple gaming machines are pooled or linked together (managed by a jackpot controller or GMMS) to form a larger progressive jackpot.
Logic Area	A locked cabinet area (with its own locked door) that houses electronic components that have the potential to significantly influence the operation of the gaming machine.
Multi-game	A game that offers player selectable options to participate in more than one game on a single gaming machine.
Mystery Jackpot	A jackpot where the determination of the jackpot win is not related to the game outcome but instead by some non-game determined or externally determined random event.
PIN	Personal identification number.
Player Class	A category of player defined under loyalty or registered play arrangements.

Pre-commitment	A consumer protection measure whereby pre-set limits on time, frequency, or money spent gambling are registered by players prior to the start of play. Mandatory pre-commitment requires player registration of pre-set limits before permitting participation on gaming machines to prevent players spending more money than they have pre-committed for a period. Voluntary pre-commitment does not require mandatory participation, however, allows players to optionally register time, or money spent limits to track and inform them of their expenditure on gaming machines.
Progressive Jackpot	A progressive jackpot is an incremental prize that increases by the accumulation of contributions from the turnover of the specified game, from a pre-set base value. It is reset to a different value (generally a base value plus possible secondary or overflow amounts) when the progressive prize is won.
Seed	An input parameter used in conjunction with a hashing algorithm to generate a hash result for the purpose of software authentication.
Software Set	The combination of software components required for a gaming machine game's operation (*for example, a software set may consist of firmware, shell and game software components*).
Source Code	Is the set of instructions and statements written by a programmer using a computer programming language. This code is later translated into machine language by a compiler. Open source code refers to software for which source code is available. Closed source code refers to software provided by a third party, and where source code is not accessible under the terms of the software licence.
Stand Alone Jackpot	A jackpot where operation participation, maintenance and control of the jackpot, including selection of the jackpot win criteria, is performed by a single gaming machine.
Supplier	A person who provides the gaming machine monitoring system and is listed on the Roll of Recognised Manufacturers, Suppliers and Testers of gaming equipment under section 71 of the *Gaming Control Act 1993.*
WAN	Wide area network.
Wide Area Jackpot	A jackpot arrangement which links gaming machines in multiple venues. Under this arrangement multiple gaming machines are pooled or linked together (managed by a jackpot controller or GMMS) to form a larger progressive jackpot.

12 Version Control

Version	Date	Changes Made
1.0	8/2/2019	New standard created.