Card Based Gaming Systems Technical Standards

Version 1.0

April 2017

Trim Ref 17/59605

Tasmanian Liquor and Gaming Commission

Tasmanian Government

Contents

1 Introduction

1.1 Objective

1.1.1 The objective of this technical standard is to ensure that Card Based Gaming Systems (CBGS) and related equipment, operated in Tasmania, are designed to:

- ensure the integrity and fairness of the system;
- ensure the security and auditability of the system and associated equipment;
- be auditable; and
- minimise the potential for harm from gambling.

1.1.2 To ensure, to the greatest extent reasonably possible, the integrity of gaming and security of player funds, card based gaming in Tasmania should only be offered in gaming venues via the Licensed Operator. This does not prevent Licensed Operators from obtaining CBGS from third parties.

1.1.3 The types of cards used must be approved by the Commission and examples that may be used include Mag-stripe, Watermark, Smart Cards and Optical Cards however, the card may only be linked to the membership, player account and player loyalty systems if approved. The card cannot be linked to other systems such as EFTPOS or other external financial facilities.

1.1.4 The offering of card based gaming requires three separate elements to be approved:

- The Terms and Conditions for card use - these are the basis of the contract between the player and the Licensed Operator.
- CBGS - this is the hardware and software, within the supplier's control, that deliver the system to the player and includes the various components required to issue/validate/report various card based functions and redemption of player funds. This document describes the principles that apply to the functionality of computer systems used to supply and monitor card based gaming services, and the communications interface which connects these systems to other computer equipment.
- Internal Controls - this is the Licensed Operator's documented system of procedures for operating the system and ensuring security of the system and players' funds and entitlements. This document does not cover internal controls, but in describing CBGS 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 CBGS that may be approved from the Commission's viewpoint, bearing in mind the overarching object in the relevant gaming legislation and other adopted technical standards.

1.2.2 "Card based gaming" is a generic term that encompasses a variety of combinations and permutations. In its simplest form it can be no more than a "licence to gamble" i.e. a player inserts their player card into the EGM in order to start gaming or collecting credits

after inserting money into the EGM. In its advanced form, it can take the form of a smart card that incorporates a "gaming purse" which enables players to set their own parameters on the card. Those parameters enable the player to set a range of limits, including length of play per session, money played per session, either hourly, daily, weekly or monthly limits, predetermine what will happen with wins etc.

1.2.3 The focus of this document is on system and game integrity, player protection and harm minimisation. It is not meant to mandate the most sophisticated solution for every application, but rather to indicate the level of functionality expected of the system for the particular application being run. Attempting to mandate the technical aspects of the security and audit requirements would tend to have the undesirable effect of stifling innovation and lessening the integrity of the security and audit functions. Rather, the onus is on system suppliers to demonstrate that their product meets the regulatory objectives outlined in this document.

1.2.4 For each proposed product, the supplier will be required to demonstrate to the Commission that the system provides effective protection of player funds and entitlements, can be easily audited and incorporates appropriate functionality to enable players to better understand and manage their gaming behaviour.

1.2.5 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 will play an integral part in the testing of the CBGS.

1.2.6 It should also be noted that compliance with this document does not exempt the supplier and Licensed Operator from compliance with other laws (eg. laws relating to privacy, consumer protection, prohibited content, copyright and electronic cash transactions).

1.3 Associated Documentation

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

- Gaming Control Act 1993
- Australian/New Zealand Gaming Machine National Standard and Tasmanian Appendix
- Tasmanian Liquor and Gaming Commission Mandatory Code of Practice
- Tasmanian Liquor and Gaming Commission Casino Licence Rules
- Tasmanian Liquor and Gaming Commission Gaming Operator Licence Rules
- Tasmanian Liquor and Gaming Commission Licensed Premises Gaming Licence Rules
- Tasmanian Liquor and Gaming Commission Premium Player Program Rules
- ePayments Code 2011
- 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

1.4 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 Card Based Gaming Minimum Technical Requirements as a basis for the development of this technical standard.

2 Player Protection and Harm Minimisation

2.1 Overview

2.1.1 This section discusses the principles that apply to CBGS to:

- protect the security of player funds and entitlements;
- promote responsible gaming; and
- protect the privacy of player details.

2.2 General Requirements

2.2.1 Card based gaming may only occur if the player is using a card issued for use with the venue's card based gaming system.

2.2.2 Once issued for use, each registered and unregistered card must have a unique identifier, to enable identification of the appropriate card and account details/balances by the CBGS.

2.2.3 The player must be issued with a registered or unregistered card that has the Gambling Helpline number printed on it.

2.2.4 The CBGS can only transfer credits to an EGM from an issued registered or unregistered card using cleared funds from a player's account/balance on the card.

2.2.5 Funds from a player account associated with a registered or unregistered card may only be used with a Licensed Operator if the card is issued by that Licensed Operator.

2.2.6 A registered player must have the ability to select the amount to be transferred from their player account or balance on the card to the credit meter on the EGM. The amount cannot over-ride any regulatory limits. Note: The maximum amount that may be credited to the credit meter is MAXCR (refer Appendix A).

2.2.7 The CBGS must not accept a bet that would cause a player's account or balance on the card to become negative.

2.2.8 Details of card verification attempts must be logged.

2.2.9 A list of all registered and unregistered cards (current or otherwise) and accounts (active or otherwise) must be maintained by the Licensed Operator.

2.2.10 A Licensed Operator must be able to return the balance of the player's account (subject to there being no other claims on the account).

2.2.11 The CBGS may have a provision to allow the purchases of other non-gaming products such as meals and beverages. Any systems or equipment that a Licensed Operator wishes to interface with the approved CBGS to facilitate these products and services must be independently tested, certified and approved by the Commission.

2.3 Registered Card

2.3.1 A player may register for a registered card with a MINTRCASHIERTIME (refer Appendix A) expiry date from the date of the last transaction performed on the card.

2.3.2 The Licensed Operator may only register a player for a registered card if the Licensed Operator or its agent at the venue is satisfied of the player's identity, place of residence, player's age is at least 18 years and the person is not an "excluded" person.

Acceptable age identification includes the sighting of at least one of the following: -

- Current passport
- Current drivers licence
- Current document issued by a Commonwealth or State Department that contains the document holder's name, photograph and age

2.3.3 On request from a player, the relevant Licensed Operator must exclude the player from being able to bet by means of deactivation of the player's registered card. The player's registered card may only be reactivated upon the expiry or revocation of the player's exclusion from gaming. Any such exclusion may only be lifted on application by the player in accordance with the provisions contained in the *Gaming Control Act 1993*.

2.3.4 Multiple registered cards are not permissible for the same person.

2.3.5 Registered player account information must be maintained on a secure part of the system or card and may only be accessed by authorised personnel in accordance with the system of Internal Controls.

2.3.6 Where a player elects to have security on the use of their registered card, there must be a provision for a player to authenticate the use of the card at the start of each gaming session if the card inactive period (five minutes) has expired. The authentication methodology and other card security arrangements must be demonstrated to be sufficiently robust to prevent unauthorised access to a player's funds and account details.

2.4 Unregistered Card

2.4.1 Instead of a registered card, a player may request and be issued an unregistered card which is valid for play for a period of MINTRCASHIERTIME (refer Appendix A) from the date of the last transaction performed on the card.

2.4.2 The Licensed Operator or its authorised agent at the gaming venue may issue a player an unregistered card if the Licensed Operator or its agent at the venue is satisfied that the player is at least 18 years of age.

2.4.3 Players using an unregistered card are not permitted to participate in any player loyalty/reward scheme offered by the venue and/or Licensed Operator.

2.5 Pre-commitment Functionality

2.5.1 The CBGS must have the capacity to record and manage player loss limits together with the ability to;

- record time spent playing EGMs over multiple time periods;
- advise the player when limits are reached and require the player to manually acknowledge the event on the gaming machine (e.g. via the removal of their card or other method) before further participation is permitted;
- prevent unauthorised players and players who have reached their limits from participating in less restricted modes of play where changing game features by player type are available (e.g. less restricted EGM play for premium players);
- support feedback on player gaming activity to be displayed at the EGM, either on request or automatic display. This includes gambling time, player win/loss, turnover, progress towards player limits (loss and time as appropriate);
- display general dynamic warnings or other regulatory messages that are not necessarily related to player-specific information;
- disable game-play for a player that has reached limits or if a limit is set at zero; and
- allow the changing of pre-commitment limits. The lowering of limits should be effective immediately, however the system must not allow for limits to be increased unless the registered pre-commitment limit period has concluded for the player.

2.5.2 If pre-commitment has been implemented and is enabled in the system, the player must be able to set the following limits:

- The maximum account balance into the player account or onto the card (MAXBAL);
- The maximum amount that a player can spend (MAXSPEND);
- The total time spent on game play on a single gaming day (MAXSESS); and
- The maximum amount that may be transferred to the credit meter from the player account or balance on the card at any one time (MAXTRF) while respecting the MAXCR limit.

Note: *Limits set by the player must not override any maximum levels set by the Licensed Operator, game rules or regulatory requirements. The above are options which must be provided to the player. It is not mandatory for the player to select any of the above options but default limits (where stipulated as part of these requirements) will apply. The objective of the above is to assist players to better manage their gambling behaviour if they choose to do so.*

2.5.3 If the player has not selected any of the above limits, refer to the default limits for pre-commitment in Appendix B - Pre-Commitment Default Values.

2.6 Player Funds Maintenance

The following principles apply to the maintenance of player funds:

2.6.1 Player funds and entitlements, and the player's right to access their funds and entitlements must be preserved and secured against access by persons other than the player, unless otherwise authorised by the player in writing or to another party through relevant legislation.

2.6.2 Registered cards on the system must be secured against invalid access or update, other than by approved methods.

2.6.3 Positive player identification, including any Personal Identification Number (PIN) entry, must be made for a registered card before any withdrawal of moneys held by the CBGS.

2.6.4 All deposit, withdrawal, transfer or adjustment transactions are to be maintained in a system audit trail.

2.6.5 Inactive cards (accounts) holding moneys in the system must be protected against forms of illicit access or removal. A report must be provided to the Liquor and Gaming Branch detailing the balances on all cards (in accounts) not activated for 12 months, as at the end of that calendar month, and must be remitted to the Department of Treasury and Finance as Unclaimed Monies by the 7th day of the next month.

2.6.6 All transactions involving moneys are to be treated as vital information to be recovered by the CGBS in the event of a failure.

2.6.7 Adjustments to accounting on the CBGS must be subject to strict security control and audit trail.

2.7 Account Activity Statements

2.7.1 Account balances and account statements must be provided to the player on request by the player. Statements must include sufficient information to allow the player, as far as is reasonably possible, to reconcile the statement against their own records of deposits and withdrawals since the last issued statement.

2.7.2 Account statements must include details of the total amount of money bet on gaming. The data presented must be informative, showing at a minimum: Account balances, Wins, Turnover and Spend (Turnover – Wins).

2.7.3 Account statement information relating to Player Loyalty Program activity must as a minimum clearly identify expenditure for the period of the statement and differentiate points that have been accrued from gambling and non-gambling activities.

2.8 Player Loyalty Systems

2.8.1 For operations regarding Player Loyalty Systems, refer to the Commission's Rules which can be found on the Liquor and Gaming Branch's website.

2.8.2 Only registered cards are permitted to be linked to Player Loyalty Systems.

2.9 Privacy of Player Information

2.9.1 Any information obtained by a Licensed Operator in respect to player registration or account establishment must not breach any relevant privacy legislation.

2.9.2 CBGS operators must respect all statutory obligations for privacy requirements at both State and Federal level.

3 Hardware / Software

3.1 Card / Card Readers

3.1.1 Each registered or unregistered card must be uniquely identified within the system.

3.1.2 There must be a complete audit trail of all transactions conducted when using either a registered or unregistered card.

3.1.3 If a registered card's account balance exceeds $100, a secure method to authenticate the registered card may be provided (e.g. PIN system). The secure method may be provided either at the EGM or via a remote device, providing there is adequate security arrangements in place to guarantee the integrity of the authentication.

3.1.4 If keypads for PINs are to be used at the EGM to authenticate a registered card, they are to be located into the cabinet sandwich or in the top box or installed in a position that is in close proximity to the EGM and are to be secured in a safe manner.

3.1.5 If PIN entry is used, three consecutive invalid PINs entered must result in the registered card being rejected, with an appropriate message being displayed to the player.

This message can be displayed either on the card reader/PIM LCD display or on the EGM. An event must be recorded and the account disabled until manually re-enabled.

3.1.6 All accounts relating to the registered card are to be suspended until cleared by the devices which control the card accounts.

3.1.7 Other secure methods of validating a registered card may be acceptable, at the discretion of the Commission.

3.2 Requirement for Encryption

3.2.1 Where sensitive data is being passed over communication lines, such data must be encrypted. Examples of sensitive data that require encryption are PINs, passwords, and encryption keys, including any information that if made public could compromise the security of the CBGS or a registered card.

3.2.2 Sensitive data must be encrypted on an end-to-end basis (i.e. 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 Licensed Operator's premises.

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

3.2.4 Sensitive data transmitted between systems that are located within separate secure data centres need not be encrypted if the communications path is physically secure and cannot be accessed by unauthorised people.

3.2.5 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.

4 Central Site Requirements

This section describes requirements for the central site (host), including reporting, data recovery and software version controls.

4.1 System Documentation

4.1.1 The Licensed Operator must have a security policy covered in its internal control and accounting procedures.

4.1.2 The system baseline network policy document defining the system network topology, which defines the communications which take place between devices in the system, must be maintained.

4.1.3 The CBGS supplier must provide adequate documentation to the Licensed Operator to configure, maintain and troubleshoot the CBGS without needing the system supplier's guidance.

4.2 CBGS Reporting Capabilities

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

- The Commission must be able to verify the financial activity of all gaming conducted on the CBGS.
- The activity on the player's account/card must be able to be verified by the Commission in the case of disputes.
- The correct operation of the CBGS must be able to be verified by the Commission.

4.2.2 The core set of reports a CBGS must be capable of producing are:

- A daily, weekly, monthly and yearly based financial summary report that totals all Funds In, Funds Out, Turnover, Total Wins for the system.

4.3 System Backup

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

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

4.4 Self Audit

4.4.1 The CBGS 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.

4.5 Data Recovery

4.5.1 In the event of a failure, the CBGS 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 (no time limit is specified).

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

4.5.3 The operator must have disaster recovery capability sufficient to ensure player entitlements and auditability up to the point of the disaster are protected.

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

4.6 Software Verification

4.6.1 The CBGS supplier and/or its suppliers must provide a method to the nominated Accredited Testing Facility to enable verification of the software.

4.7 Source Code

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

4.7.2 All source code central to the operation of the CBGS must be supplied to the Commission or representing Accredited Testing Facility where the supplier has the capability, right, and access to provide source code.

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

4.7.4 The Commission may also require that the CBGS suppliers have arrangements with closed source software vendors in place to allow appropriate access to source code by the Commission or representing Accredited Testing Facility for purpose of investigating software faults.

4.8 Accounting of Master Resets

4.8.1 The CBGS 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.

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

4.8.3 Adjustments to accounting on the CBGS are subject to strict security control and audit trail.

4.9 Recordable Events

4.9.1 The CBGS must keep records of the following events:

- Player registration, card or player's account creation and de-activation
- Changes to player's registration, card or account details (eg. address)
- Changes made by Licensed Operators to gaming parameters (eg max bet, loss and deposit)
- All transactions made on a players account
- Adjustments to account balances
- Reconciliation failures
- Three consecutive bad PIN entries

4.9.2 Transaction events must contain at least the following information:

- The amount of the transaction
- The date and time of the transaction
- The type of transfer (player->account, account->player, account->EGM, EGM->account)
- Player ID
- Location i.e. Venue ID
- Equipment ID
- For player <-> account transactions include the final account balance

4.9.3 The CBGS must be able to provide a means to view significant events including the ability to search for particular event types.

4.9.4 The CBGS must be able to prioritise events (log, alarm or disable).

4.10 Audit Trail

4.10.1 The CBGS must maintain an audit trail of all recordable events (see above).

4.10.2 Events in the audit trail must be kept for a minimum period of seven years.

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

5 Glossary

Term or Abbreviation	Description
CBGS	Card Based Gaming System
Registered card	One of two player card types available for use with a CBGS (the other being unregistered cards), can only be obtained by player registration and has account limits in accordance with Appendix A
Unregistered card	One of two player card types available in CBGS, requires no registration and has limits in accordance with Appendix A
ATF	Accredited Testing Facility accredited by the Tasmanian Liquor and Gaming Commission
Casino	Refers to a premises issued with a Casino Licence under the *Gaming Control Act 1993*
Hotel	Refers to a premises issued with a Licensed Premises Gaming Licence under the *Gaming Control Act 1993* and a General Licence under the *Liquor Licensing Act 1990*
Club	Refers to a premises issued with a Licensed Premises Gaming Licence under the *Gaming Control Act 1993* and a Club Licence under the *Liquor Licensing Act 1990*
Excluded Person	Refers to a person who is excluded from gaming or wagering in accordance with Division 3 of Part 5 of the *Gaming Control Act 1993*
Gaming Session	A session begins when a player card is inserted into an EGM and the session ends when the card is removed and remains inactive for a period of five minutes
Licensed Operator	Refers to a casino operator or a gaming operator
Commission	Refers to the Tasmanian Liquor and Gaming Commission
EGM	Refers to Electronic Gaming Machine
Supplier	Refers to the supplier of the Card Based Gaming System

6 Appendix A. Limits for Card Based Gaming Systems

Card IT Limits	Registered Cardholders	Unregistered Cards
The CBGS must not "credit" the EGM with an amount that would cause the machine's credit meter to exceed this value **(MAXCR)**	$500 maximum	$500 maximum
Maximum Account Balance above which a card suspends **(MAXBAL)**	$9 999.99	$2 000
Expiry of a card (card locked) **(MINTRCASHIERTIME)**	12 months of inactivity	2 days of inactivity
Maximum size of payout that can be transferred to card - anything above this amount will generate a Cancel Credit **(MAXECT)**	$1 000	$1 000
Money transferred from the card to the EGM **(MAXTRF)**	$500 maximum	$500 maximum

**Removing a card from an EGM that would credit and exceed the MAXBAL limit, must first remove and transfer all credits from the EGM to the card/account. The system must then suspend the card/account until the balance is reduced to a value equal to or less than MAXBAL. This must be accomplished by attending the cashier.*

7 Appendix B. Pre-commitment Default Values

Pre-commitment limits	Values
MAXBAL	Maximum $9 999.99 (Registered Cards) Maximum $2 000 (Unregistered Cards)
MAXSPEND	Default limit as determined by the Commission with a maximum of MAXBAL
MAXSESS	Default limit as determined by the Commission
MAXTRF	Default of maximum banknote denomination that is accepted by an EGM, while respecting MAXCR. (i.e. possible range: $100 to MAXCR)

LIQUOR AND GAMING CONTACT DETAILS

Salamanca Building Parliament Square
4 Salamanca Place HOBART TAS 7000
Telephone: (03) 6166 4040 Facsimile: (03) 6173 0218

Level 3 Henty House 1 Civic Square LAUNCESTON TAS 7250
Telephone: (03) 6777 2777 Facsimile: (03) 6173 0218

GPO Box 1374 HOBART TAS 7001 Australia
Email: gaming@treasury.tas.gov.au Web: www.gaming.tas.gov.au

Tasmanian Government