Department of Justice and Attorney-General

Office of Liquor and Gaming Regulation

Card based gaming minimum technical requirements

Version 1.3.2

Queensland Government

The information contained herein is subject to change without notice. The copyright owner shall not be liable for technical or other errors or omissions contained herein. The reader/user accepts all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this information.

For further information, please contact the Office of Liquor and Gaming Regulation on 13 QGOV (13 74 68) or visit www.business.qld.gov.au/industry/liquor-gaming

1 Contents

2 Introduction

2.1 Copyright

2.1.1 This document is the property of the Queensland Office of Liquor and Gaming Regulation (OLGR). Copying, making extracts or use of the document, without prior permission, is prohibited.

2.2 Perspective

2.2.1 In April 2000, the Queensland Government released its *Policy Direction for Gambling in Queensland*. The *Policy Direction* reflects the Government's response to growing concern over the growth of gambling in the community and in particular the growth in gaming machines. The Government is committed to ensuring an appropriate balance in the provision of gambling services. On the one hand, acknowledging the value that this form of entertainment provides to individuals while recognising the social and economic costs of gambling.

2.2.2 In this regard, all gambling legislation was amended in late 2000 to incorporate an overarching community protection objective to provide that, on balance, the State and community as a whole benefit from the conduct of gambling. The balance is achieved through a system of regulation and control designed to protect players and the community through –

1. ensuring the integrity and fairness of games; and
2. ensuring the probity of those involved in the conduct of gambling; and
3. minimising the potential for harm from gambling.

2.2.3 The introduction of new technologies such as card based gaming has the potential to provide many benefits to gaming venues such as reduced cash handling and security costs however, it also has the potential to impact adversely on a player's gaming behaviour. Consequently, whenever new technologies are incorporated in gaming machine technology, they should also enhance the capacity of the player to better understand and manage their gambling behaviour.

2.2.4 To ensure to, the greatest extent reasonably possible, the integrity of gaming and security of player funds, card based gaming in Queensland should only be offered in clubs and hotels via the clubs and hotels licensed monitoring operator (LMO) and in casinos by the casino operator. This does not prevent LMOs or casino operators from obtaining card based gaming systems from third parties.

2.2.5 The types of cards that may be used include Mag-stripe, Water mark, 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.

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

- The card based game rules - these are the basis of the contract between the player and the provider. This document is not a guide to drafting rules although it does touch upon some elements of consumer/player protection.

- The Card Based Gaming System (CBGS) - this is the hardware and software, within the provider'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, the communications interface which connects these systems to other computer equipment.
- Internal Controls - this is the provider'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.

2.3 Scope and Purpose

2.3.1 The scope and purpose of this document is to describe guidelines for the functionality of Card Based Gaming Systems (CBGS) that may be approved from the regulator's viewpoint bearing in mind the overarching object in the relevant gaming legislation.

2.3.2 "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 must insert their player card into the gaming machine in order to start gaming by inserting money into the gaming machine. 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.

2.3.3 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 providers to demonstrate that their product meets the regulatory objectives outlined in this document.

2.3.4 For each proposed product, the provider will be required to demonstrate to OLGR 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.

2.3.5 The process for the approval of the proposed product will be determined by OLGR in consultation with the provider. It is expected that approved evaluators will play an integral part in the testing of the CBGS.

2.3.6 It should also be noted that compliance with this document does not exempt the provider and gaming venue operator from compliance with other laws (eg. laws relating to privacy, consumer protection, prohibited content, copyright and electronic cash transactions).

2.4 Further Reading

2.4.1 Potential Providers, third party suppliers and system developers should also familiarise themselves with the following:

- Australian/New Zealand Gaming Machine National Standard. (http://olgr.qld.gov.au/industry/gamingServices/gaming_machine_equipment/index.shtml)
- Electronic Funds Transfer (EFT) Code of Conduct (http://www.asic.gov.au)
- Financial Transactions Act 1988 (Cth) (http://www.comlaw.gov.au/)
- Privacy Act 1988 (Cth) (http://www.privacy.gov.au)

2.4.2 Queensland Responsible Gambling Code of Practice and Implementation Resource Manual (http://www.olgr.qld.gov.au/responsibleGambling/)

2.4.3 ISO/IEC 17799:2000 Information Technology – Code of practice for information security management

3 Player Protection and Harm Minimisation

3.1 Introduction

3.1.1 This section discusses the principles that apply to card based gaming systems to -

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

3.2 General Requirements

3.2.1 Gaming may only occur if the player is using a card with the venue's gaming provider.

3.2.2 Once issued by a gaming provider, each registered and anonymous card must have a unique identifier, to enable identification of the appropriate card and account details/balances by the CBGS.

3.2.3 The player must be issued with a registered or anonymous card that is embossed with the Gambling Helpline telephone number.

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

3.2.5 Funds from a player account associated with a registered or anonymous card may only be used with a gaming provider if the card is issued by that gaming provider.

3.2.6 The player must select the amount to be transferred from their player account or balance on the card to the credit meter on the gaming machine. The amount cannot over-ride any regulatory limits. Note: In the case of clubs and hotels, the maximum amount that may be credited to the credit meter is MAXCR (refer Appendix A).

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

3.2.8 Details of card verification attempts must be logged.

3.2.9 A list of all registered and anonymous cards (current or otherwise) and accounts (active or otherwise) must be maintained by the gaming provider.

3.2.10 A gaming provider must be able to return the balance of the player's account (subject to there being no other claims on the account).

3.2.11 The CBGS may have a provision to allow the purchases of other non-gaming products such as meals and beverages.

3.3 Registered Card

3.3.1 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.

3.3.2 The gaming provider may only register a player for a registered card if the gaming provider 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.

3.3.3 On request from a player or club or hotel the relevant gaming provider must exclude the player from being able to bet by means of deactivation of the player's registered card. Any such exclusion may only be lifted on application by the player in accordance with the provisions contained in the applicable gaming law.

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

3.3.5 Upon issuing a registered card and pre-commitment is enabled in the venue, a player must be provided with the following information:

- all terms and conditions regarding the operation of the card based gaming system;
- gaming machine player information;
- mechanisms available via the CBGS to manage their gaming behaviour;
- contact points for people unable to control their gaming machine behaviour; and
- exclusion mechanisms available via the CBGS and by the venue.

3.3.6 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.

3.3.7 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. 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.

3.4 Anonymous Card

3.4.1 Instead of a registered card, a player may request and be issued an anonymous 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.

3.4.2 The gaming provider or its authorised agent at the gaming venue may issue a player an anonymous card if the gaming provider or its agent at the venue is satisfied that the player is at least 18 years of age.

3.4.3 Players issued with an anonymous card are not permitted to participate in any player loyalty/reward scheme offered by the venue and/or gaming provider.

3.5 Pre-commitment functionality

3.5.1 If Pre-commitment has been implemented and is enabled in the system, the player must be capable of setting the following limits:

- The maximum account balance into the player account or on to the card (MAXBAL), and
- The maximum amount that a player can spend (MAXSPEND), and
- 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 gaming provider, 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.

3.5.2 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.

3.5.3 Increases to previously set player limits may only occur on request by the player and shall take effect no sooner then the next business day of the gaming provider.

3.5.4 Decreases to previously set player limits must take effect immediately on request by the player. The new limit must be implemented at the gaming venue immediately. Where the card is a multi-venue card, the decrease is to take effect within one hour of the initial request made by the player.

3.6 Player Funds Maintenance

The following principles apply to the maintenance of player funds:

3.6.1 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.

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

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

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

3.6.5 Inactive registered accounts holding moneys in the system must be protected against forms of illicit access or removal. Balances in accounts not activated for 12 months must be remitted by cheque in the name of the owner of the account to the registered address of the owner, or directly into a financial institution account in the name of the owner nominated by the owner.

3.6.6 Inactive anonymous accounts holding moneys in the system and are inactive for 12 months must be remitted by cheque to OLGR.

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

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

3.7 Player activity statements

3.7.1 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 to, as far as is reasonably possible, to reconcile the statement against their own records of deposits and withdrawals since the last issued statement.

3.7.2 Account statements must also 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). Refer Appendix C – Account Statement sample.

3.8 Player Loyalty Systems

3.8.1 For operations regarding Player Loyalty Systems please refer to the "Guidelines for Player Loyalty Programs", which can be found under the Advertising and Promotions guideline section at the OLGR's Responsible Gaming Code of Practice website: *http://www.olgr.qld.gov.au/responsibleGambling/gamblingProviders/codeOfPractice/index.shtml*

3.9 Privacy of Player Information

3.9.1 Any information obtained by a gaming provider in respect to player registration or account establishment must not breach any relevant privacy legislation.

3.9.2 CBGS operators must respect all statutory obligations for privacy requirements at both state and federal level.

4 Hardware

4.1 Card/Card Readers

4.1.1 Each registered or anonymous card must be uniquely identified within the system.

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

4.1.3 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 gaming machine or via a remote device providing there is adequate security arrangements in place to guarantee the integrity of the authentication.

4.1.4 If keypads for PINs are to be used at the gaming machine 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 is secured in a safe manner.

4.1.5 If PIN entry is used, three consecutive invalid pin numbers entered should 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.

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

4.1.7 Other secure methods of validating a registered card may be acceptable, at the discretion of the Chief Executive.

4.2 Requirement for Encryption

4.2.1 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.

4.2.2 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 gaming provider's premises.

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

4.2.4 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.

4.2.5 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. OLGR recommends that current best practice encryption algorithms should be used.

5 Central Site Requirements

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

5.2 System Documentation

5.2.1 The gaming provider must have a security policy covered in the control system.

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

5.2.3 The CBGS system provider must provide adequate documentation to the gaming provider to configure, maintain and troubleshoot the CBGS without needing the system provider's guidance.

5.3 CBGS Reporting Capabilities

5.3.1 There are three main areas in which a system must be able to fulfil its tasks in providing reports to regulators:

- The regulator 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 regulator in the case of disputes.
- The correct operation of the CBGS system must be able to be verified by the regulator.

5.3.2 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.

5.4 System Backup

5.4.1 There must be a method to backup all player information data with sufficient frequency to allow recovery in the event of an interruption.

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

5.5 Self Audit

5.5.1 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.

5.6 Data Recovery

5.6.1 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).

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

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

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

5.7 Software Verification

5.7.1 The CBGS provider and/or its suppliers must provide a method to the approved evaluator to enable verification of the software.

5.8 Source Code

5.8.1 Source code submissions should comply with the section for Source Code Submissions in the OLGR Submission Requirements document.

5.9 Accounting of Master Resets

5.9.1 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.

5.9.2 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.

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

5.10 Recordable Events

5.10.1 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 gaming providers to gaming parameters (eg max bet, loss and deposit),
- all transactions made on a players account.
- large transfer of funds as per AUSTRAC requirements,
- player exclusion (including exclusion, requests to lift exclusion, and actual lifting of exclusion),
- Adjustments to account balances.
- Reconciliation failures.
- Three consecutive bad PIN entry.

5.10.2 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.

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

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

5.11 Audit Trail

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

5.11.2 Events in the audit trail must be kept for a minimum period of 5 years.

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

6 Submission Requirements for Card Based Gaming Systems

The Submission requirements specify the type of information that may be required to be supplied when making submissions of card based gaming systems to OLGR.

6.1.1 Refer to the Submission Requirements document available at (http://olgr.qld.gov.au/industry/gamingServices/index.shtml) relating to all required submissions for Card Based Gaming Systems for software, hardware, and systems.

7 Glossary

Term or Abbreviation	Description
Anonymous card	One of two player card types available in CBGS, requires no registration and has limits that are similar to Tickets.
Approved evaluator	A licensed testing facility operator approved by OLGR
CBGS	Card Based Gaming System
Cash Terminal	Refers to any electronic device (either automated or operator driven) that allows an account holder to add or remove cash funds from their account.
Casinos	Refers to gaming premises licensed under the Casino Control Act.
Clubs	Refers to a gaming venue with a Community club license in Queensland as defined in section 75 of the *Liquor Act 1992*.
Excluded Person	Refers to a person issued an exclusion notice or has received an exclusion direction under the Gaming Machine Act or Casino Control Act.
Gaming session	A session begins when a player card is inserted into an EGM. The session ends when the card is removed.
Gaming provider	Licensed Monitoring Operator as defined under the Gaming Machine Act and licensed casinos under the Casino Control Act.
Hotels	Refers to a gaming venue with a Commercial hotel license in Queensland as defined in section 59 of the *Liquor Act 1992*.
Registered card	One of two player card types available in CBGS (the other being anonymous cards), can only be obtained by player registration, account limits exceed Tickets.
Pre-commitment	A harm minimisation feature introduced as part of CBGS to help players manage their spending behaviour by being able to set limits such as: maximum spend, maximum session times etc.

8 Appendix A. QLD limits for CBGS

QLD CBGS Limits	Registered Account	Anonymous Account (Mirroring QLD TITO limits)
The CBGS must not "credit" the EGM that would cause the machine's credit meter to exceed this value **(MAXCR)**	$199.99 (Clubs & Hotels) $9999.99 (Casinos)	$199.99 (Clubs & Hotels) $9999.99 (Casinos)
Default minimum time a card is accepted in an EGM **(MINTRTIME)**	12 Months	2 Days
Default minimum expiry time of a Card **(MINTRCASHIERTIME)**	12 months	12 months
Maximum Account Balance **(MAXBAL*)**	$9999.99	$5000 (Clubs & Hotels#) $9999.99 (Casinos)
Default card scope **(CSCOPE)**	Operator Controlled Multi-Venue Card	Originating Venue only
Inactive funds sent to	Registered Patron	OLGR

*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 a cashier.

#The venue should be able to set their own limits up to MAXBAL

9 Appendix B. Pre-commitment default values.

Pre-commitment limits	Values
MAXBAL[1]	Maximum $9999.99 (Registered Accounts) Maximum $2000 (Anonymous Accounts)
MAXSPEND	Default of $100 with a maximum of MAXBAL
MAXSESS	Default of unlimited MAXSESS
MAXTRF[1]	Default of maximum banknote denomination that is accepted by an EGM, while respecting MAXCR. (i.e. possible range: $20 to MAXCR)

[1] – Only applies where pre-commitment has been implemented in a CBGS.

10 Appendix C. Account Statement sample

Account Statement for Mr. Ex. Ample for the Period 1/1/2013-7/1/2013

Date & Time	Card ID	EGM #	Turnover	Wins	Spend	Balance
Start of Week Balance						**$ 1,000.00**
1/01/2013 11:45 am	123456789	987654321	$1,300.00	$500.00	-$ 800.00	
1/01/2013 3:00 pm	123456789	987654322	$ 45.00	$500.00	$ 455.00	
End of Day Balance for 1/1/2013						**$ 655.00**
2/01/2013 10:45 am	123456789	987654321	$ 500.00	$ 20.00	-$ 480.00	
2/01/2013 11:00 am	123456789	10101234	$2,000.00	$ -	-$2,000.00	
End of Day Balance for 2/1/2013						**-$1,825.00**
End of Week Account Balance for Period 1/1/2013 to 7/1/2013						**-$1,825.00**

11 Revision History

Version	What	QIR	Who	Date
1.0 (Draft)	Initial release		LW	01-02-2005
1.1	Updated to new DEEDI Report document template		RLLARK	20/08/2010
1.2	Incorporate industry feedback	826	JA	Not Released.
1.3 draft	Remove mandatory requirements for Pre-commitment, addition of anonymous cards for CBGS and added QLD specific limits. Update to DJAG template Added Industry comment (2013)	-	JA	26/6/2013
1.3.1	Added Soft limit requirements for MAXBAL (refer: Appendix A) Clarified MAXTRF specifically for Pre-commitment (was MAXCR) Changed value of MAXCR to $199.99 to support $50 and $100 banknote denomination acceptance. Changed value of MAXBAL for Anonymous accounts to $5000	-	JA	14/3/2014
1.3.2	Updated to new JAG report document template		JG	19/7/2016