Office of Liquor and Gaming Regulation

Card-Based Gaming Minimum Technical Requirements

Version 1.4.1

Queensland Government

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

Contents

1 Introduction

1.1 Objective

The objective of this technical standard is to ensure that card-based gaming systems (CBGSs) and related equipment operated in Queensland are designed to:

- meet the requirements of Queensland's regulatory framework
- ensure the integrity and fairness of the system
- ensure the security and auditability of the system and associated equipment
- be auditable
- minimise the potential for harm from gambling.

1.2 Scope and purpose

This document is applicable to all gaming providers who conduct (or intend to conduct) operations in Queensland. This document describes the requirements that apply to the technical evaluation of CBGSs submitted for evaluation in Queensland.

A CBGS is any system that facilitates the electronic transfer of credits to and from a player account for the purposes of gambling via a player, member, loyalty or other type of card.

The focus of this document is on system and game integrity, player protection and harm minimisation and to advise the industry of the Office of Liquor and Gaming Regulation's (OLGR's) technical requirements for CBGSs that are designed to:

- protect the security of player funds and entitlements
- promote responsible gaming
- protect the privacy of player details
- ensure requirements are consistently applied
- achieve a high standard of integrity, security and consistency of CBGSs used for gaming in Queensland.

OLGR reserves the right to undertake further evaluation to be satisfied that a CBGS allows the operator to meet their legislative requirements including, but not limited to, matters relating to taxation.

Compliance with this document does not exempt the provider and gaming venue operator from compliance with other laws (e.g. laws relating to privacy, consumer protection, prohibited content, copyright and electronic cash transactions).

1.3 Policy

All CBGS products intended to be used within Queensland licensed premises must be submitted for evaluation and approval under the *Gaming Machine Act 1991* and, where applicable, the *Casino Control Act 1982*.

Card-based gaming in Queensland must only be offered in clubs and hotels via the club's or hotel's licensed monitoring operator (LMO) as defined in the Gaming Machine Act and in casinos by the casino operator. This does not prevent LMOs or casino operators from obtaining a CBGS from a third party.

The card may only be linked to a premises' membership, player account and player loyalty systems if approved by OLGR. Cards issued for card based gaming must only be linked to systems approved for card based gaming and cannot be linked to other systems such as EFTPOS.

1.4 Definitions

Term	Description
Anonymous account/card	One of two player card types available for gaming purposes in CBGSs; requires no registration
Approved evaluator	A licensed testing facility operator approved by OLGR
Betting terminal (BT)	Any device in the CBGS that accepts bets from registered or anonymous cards/accounts (e.g. electronic gaming machines and fully automated table games can be BTs)
Cash terminal Cash redemption terminal (CRT)	Refers to any electronic device (either automated or operator driven) that at a minimum allows a player to add or remove cash funds from their account. Refer to OLGR's CRT Minimum Technical Requirement for accepted functionality and details.
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 BT is enabled using a player card. The session ends when the card is removed or when a time period elapses.
Gaming provider	Licensed monitoring operator as defined under the Gaming Machine Act and licensed casino operators under the Casino Control Act
Inactive account	Applies to both registered and anonymous accounts—accounts are considered to be inactive when there has been no transactions on the account for 12 months
Registered account/card	One of two player card types available in CBGSs; can only be obtained by player registration and has higher CBGS limits than anonymous cards
System provider	The CBGS developer who provides support to the gaming provider in terms of features and bug fixes. A system provider can also be the gaming provider.
Pre-commitment	A harm minimisation feature to help players manage their spending behaviour by being able to set limits, such as: maximum spend, maximum session times etc.
Transaction	The transfer of money/credits to or from an account

1.5 Further reading

CBGS providers, third-party suppliers and system developers should also familiarise themselves with the following legislation, codes, standards and requirements:

- Australian/New Zealand Gaming Machine National Standard. (https://www.business.qld.gov.au/industry/liquor-gaming/gaming/technical-services/electronic-gaming-equipment)
- Electronic Funds Transfer (EFT) Code of Conduct (http://www.asic.gov.au)
- *Financial Transactions Act 1988* (Cwlth) (https://www.legislation.gov.au/)
- *Privacy Act 1988* (Cwlth) (https://www.oaic.gov.au/)
- Queensland Responsible Gambling Code of Practice and Implementation Resource Manual (https://www.business.qld.gov.au/industry/liquor-gaming/gaming/gambling-awareness-campaigns)
- ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls
- OLGR Cash Redemption Terminals Minimum Technical Requirements (https://publications.qld.gov.au/dataset/cash-redemption-terminal-minimum-technical-requirements)
- OLGR's Queensland responsible code of practice (https://publications.qld.gov.au/dataset/responsible-gambling-code-of-practice-and-resource-manuals/).

2 Submissions

2.1 General

2.1.1 A proposal to introduce a CBGS into a licensed premises must, at a minimum, include the following elements:

- the terms and conditions (or equivalent) for card use that are the basis of the contract between the player and the gaming provider
- the CBGS—the hardware and software, within the gaming provider's control, that delivers the system to the player and includes the various components required to issue/validate/report various card based functions and redemption of player funds
- internal controls—the gaming provider's documented system of procedures for operating the system and ensuring security of the system and players funds and entitlements (the gaming provider must have a security policy covered in its internal controls and accounting procedures).

2.1.2 Refer to the OLGR Submission Requirements (Gaming) document (https://publications.qld.gov.au/dataset/submission-requirements-gaming) for specific requirements relating to software, hardware, source code and systems submissions.

3 System requirements

3.1 General requirements

3.1.1 The system must provide effective protection of player funds and entitlements that can be easily audited.

3.1.2 To prevent player credit theft from occurring, any registered credit displayed by the betting terminal prior to a player's card being inserted must not be able to be removed by the insertion of a player's card.

3.1.3 The system must not, under any scenario, be susceptible to:

- loss of credits
- incorrectly transferring credits to another account.

3.1.4 The system must automatically deal with credit left on a betting terminal in the above scenario in a manner acceptable to the OLGR.

3.2 Transfer of player funds

3.2.1 The player must be able to select the amount to be transferred from their player account or balance on the card to the betting terminal (**MAXTRF**). The amount cannot override any regulatory limits. Refer to Appendix A—Queensland limits for card-based gaming systems.

3.2.2 The system must only transfer credits to a betting terminal using cleared funds from a registered or anonymous player's account. No cash advance or credit play gaming is allowed.

3.2.3 Funds from an 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.

3.2.4 The system must not accept a request to transfer credits to a betting terminal that would cause a player's account or balance on the card to become negative.

3.2.5 The system may have a provision to allow the purchase of other non-gaming related products, such as meals and beverages, even if limits have been reached.

3.3 Card or account balance requirements

3.3.1 The system must enforce a maximum balance limit on a card or player's registered or anonymous accounts—**MAXBAL** (maximum balance). Refer to Appendix A—Queensland limits for card-based gaming systems.

3.3.2 The system must be able to display the balance of the card or player's registered or anonymous account (subject to there being no other claims on the account) from the betting terminal.

3.3.3 The system may have a provision to allow for a 'soft' **MAXBAL** limit: Removing a player's card from a betting terminal that would credit and exceed the **MAXBAL** must first remove and transfer all credits from the betting terminal to a player's card, or a player's registered or anonymous account. The system must then suspend the player's card, or a player's registered or anonymous account for gaming, until the balance is reduced to a value equal to or less than the **MAXBAL**.

3.3.4 A player's balance that exceeded the **MAXBAL** limit can be decreased and therefore enabled by attending a point-of-sale terminal, cashier or CRT.

3.4 Registered card

3.4.1 A player may apply for a registered card with a **MINTRCASHIERTIME** expiry date from the date of the last transaction performed on the card. (Refer to Appendix A—Queensland limits for card-based gaming systems.)

3.4.2 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, age (at least 18 years old) and the person is not an excluded person.

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

3.4.4 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.

3.4.5 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.

3.4.6 On request from a player, 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.

3.4.7 A registered card may be used at other venues that utilise the same gaming provider—that is, a multi-venue card.

3.5 Anonymous card

3.5.1 Instead of a registered card, an eligible player may request an 'anonymous card' (if available) that is valid for play for a period of **MINTRCASHIERTIME** from the date of the last transaction performed on the card. (Refer to Appendix A—Queensland limits for card-based gaming systems)

3.5.2 An anonymous card must only be issued if the gaming provider or its agent at the venue is satisfied that the player is at least 18 years of age and not subject to an exclusion order.

3.5.3 Play using an anonymous card will not contribute toward any player loyalty / reward scheme offered by the venue or gaming provider.

3.5.4 An anonymous card may only be used at the venue that issued it.

3.6 Card information

3.6.1 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.

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

3.7 Pre-commitment functionality

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

- maximum amount that a player can spend (**MAXSPEND**)
- total time spent on game play on a single gaming day (**MAXSESS**).

3.7.2 If the CBGS utilises cashless functionality, the following other limits must also be available:

- maximum account balance into the player account or on to the card (**MAXBAL**)
- 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 maximum credit input limit by the betting terminal.

3.7.3 If the player who enrols for pre-commitment has not selected any of the above limits, refer to the default limits for pre-commitment in

3.7.4 Appendix B—Pre-commitment default values.

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

3.7.6 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 1 hour of the initial request made by the player.

3.7.7 Upon issuing a registered card where 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 CBGS
- gaming machine player information on how to use the CBGS
- mechanisms available via the CBGS to manage their gaming behaviour
- contact points for people unable to control their gaming machine behaviour
- exclusion mechanisms available via the CBGS and from the venue.

3.8 Player funds maintenance

3.8.1 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.

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

3.8.3 Positive player identification, including any personal identification number (PIN) entry, may be made for registered cards before withdrawal of moneys held by the system.

3.8.4 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. Alternatively, a player can attend the venue to collect their funds.

3.8.5 Account balances for inactive anonymous accounts must be paid to OLGR within **14 days** of the account becoming inactive.

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

3.8.7 Adjustments to accounting on the system must be subject to strict security control and audit trail.

3.8.8 Inactive accounts holding moneys in the system must be protected against forms of illicit access or removal.

3.9 Account transaction statements

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

3.9.2 Account transaction 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 and transactions performed over a specified period.

3.10 Privacy of player information

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

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

4 Hardware

4.1 Cards or card readers

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

4.1.2 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.

4.1.3 If keypads for PINs are to be used at the betting terminal to authenticate a registered card, they are to be located as part of the betting terminal or in a position that is in close proximity to the betting terminal and is secured in a safe manner.

4.1.4 If PIN entry is used, 3 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 or on the betting terminal. An event must be recorded and the account disabled until manually re-enabled.

4.1.5 All accounts relating to the disabled registered card are to be suspended until cleared by the devices that control the card accounts.

4.1.6 Other secure methods of validating a registered card may be acceptable, at the discretion of the Chief Executive of OLGR or Commissioner for Liquor and Gaming.

4.2 Requirement for encryption

4.2.1 Where sensitive data is being passed over communication lines, it 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 unencrypted form). This includes sensitive data transmitted between computer systems within a gaming provider's premises.

4.2.3 Encryption systems are to be demonstrably secure. Only publicly published encryption algorithms and protocols may be used and must have a demonstrated track record against attacks and history of reliable performance. Industry standard best practice encryption and authentication techniques must be used.

5 CBGS host requirements

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

5.1 System documentation

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

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

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

5.2 Reporting capabilities

5.2.1 The system must be able to fulfil its tasks in providing reports to regulators to verify:

- the financial activity of all gaming conducted on the CBGS
- the activity on the player's account/card in the case of disputes
- the correct operation of the CBGS.

5.2.2 The core set of reports a CBGS host must be capable of producing are: daily, weekly, monthly and yearly financial summary reports that total all funds in, funds out, turnover, and total wins for the system.

5.3 System backup

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

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

5.3.3 The retention period for backups must be aligned to the applicable legislative requirement for retention of records.

5.4 Self-audit

5.4.1 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.

5.5 Accounting of master resets

5.5.1 The CBGS must be able to identify and properly handle failures or resets on other computer systems that affect game outcome, win amount or metering.

5.5.2 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.

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

5.6 Recordable events

5.6.1 The CBGS must keep records of the following events:

- player registration, card or player's account creation and deactivation
- changes to player's registration, card or account details (e.g. address)
- changes made by gaming providers to gaming parameters (e.g. deposit)
- all transactions made on a player's account
- large transfers 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
- 3 consecutive bad PIN entries.

5.6.2 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 → betting terminal, betting terminal → account)
- player ID
- location (i.e. venue ID)
- equipment ID
- for player–account transactions, including the final account balance.

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

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

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

5.6.6 Details of each registered card verification attempts that result in a failure must be logged.

5.7 Audit trail

5.7.1 The system must maintain an audit trail of all recordable events. (Refer section 5.6 Recordable events).

5.7.2 The system must maintain a complete audit trail of all transactions (deposit, withdrawal, transfer or adjustment) conducted when using either a registered or anonymous card.

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

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

6 Data recovery

6.1.1 The CBGS must be able to recover with no loss of data or state from unexpected restarts of any of its components.

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

6.1.3 All data must be stored via secure, fault-tolerant storage media and, at a minimum, a secondary copy on a separate device must be retained.

6.1.4 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).

Appendix A—Queensland limits for card-based gaming systems

QLD CBGS limits	Registered account default values	Anonymous account default values
MAXCR—The CBGS must not 'credit' the betting terminal that would cause the machine's credit meter to exceed this value	$199.99 (Clubs & Hotels) $9999.99 (Casinos)	$199.99 (Clubs & Hotels) $9999.99 (Casinos)
MINTRTIME—Minimum time a card is accepted in an betting terminal	12 Months	2 Days
MINTRCASHIERTIME— Default minimum expire time of a card	12 months	12 months
MAXBAL—Maximum account balance	$9999.99	$5000 (Clubs & Hotels[#]) $9999.99 (Casinos)
MAXTRF—Maximum credit value to transfer to a betting terminal (possible range: $20 to **MAXCR**)	$100	$100

[#] The venue may be able to set their own limits up to **MAXBAL**

Appendix B—Pre-commitment default values

Pre-commitment limits	Default values
MAXSPEND	Default of $100 with a maximum of **MAXBAL**
MAXSESS	Default of unlimited (displayed in HH:MM, e.g. 00:00)
If pre-commitment has been implemented in a Card Based Gaming System (Cashless System) then the following limits must also be available:	
MAXBAL	Maximum $9999.99 (Registered Accounts) Maximum $2000 (Anonymous Accounts)
MAXTRF	Default of maximum banknote denomination that is accepted by a betting terminal, while respecting **MAXCR**. (i.e. possible range: $20 to **MAXCR**)

Revision history

Version	What	Who	Date
1.4.1	• Redefined 'Gaming Session' as a result of NFC proposal. • Minor changes to 5.1.4	JA	14/01/2020
1.4	• Added 'Minimum' to document title. • Clarified soft-balance requirements. • Clarified disabled accounts to be re-enabled using CRTs. • Removed Account statement sample. Update to DJAG Template. • Updated requirements and URL links as per Industry and Internal feedback received. • Clarified Optional pre-commitment requirements. • Removed CSCOPE and Inactive funds entries in Appendix A. • Changed EGM references to Betting Terminals (BT). • Consolidated requirements that were of similar type e.g. submissions, general requirements. • Removed default pre-commitment limits. • Introduced mandatory encryption. • Introduced links to CRT MTRs and RGCOP. • Rearranged Introduction. • Revised Scope. • Updated ISO standard under Further Reading. • Renamed Player Protection and Harm Minimisation to System Requirements. • Renamed Glossary to Definitions and moved to Introduction. • Updated Glossary. • Updated 4.8.4 and 4.8.5. • Added 4.8.8. • Added 6.3.3 – Retention period of backups. • Moved (former) 4.1.1 to Policy section. • Moved (former) 4.4.1 to (new) 4.2.5. • Moved (former) 6.3.3 to (new) 7.1.4. • Moved blurb under System Requirements to Purpose. • Removed Perspective. • Removed blurb under Pre-commitment functionality. • Removed QIR from Revision History. • Added ability for players to attend the venue to collect their funds from registered accounts. • Added 'Terms and Conditions (or equivalent)' in section 3.1.1.1.	JA	18/06/2018
1.3.2	Updated to new JAG report document template	JG	19/07/2016

Version	What	Who	Date
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	14/03/2014
1.3	• 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	26/06/2013
1.2	Incorporate industry feedback	JA	Not Released
1.1	Updated to new DEEDI Report document template	RLL	20/08/2010
1.0	Initial release	LW	01/02/2005