Department of **Employment, Economic Development and Innovation**

Office of Liquor Gaming and Regulation
Client-Server System Gaming - Principle

Version 0.03 Draft

Toward Q
Tomorrow's Queensland

Queensland Government

OLGR – Technical Unit is independently certified to ISO 9001:2008 by SAI Global Ltd

Contents

1 General

1.1 Introduction

This Principles document has been created to facilitate the introduction of Client-Server Systems (CSS) gaming technology into Queensland. It is likely that this document would be used in conjunction with other established electronic gaming machine standards to provide comprehensive coverage. This document should be referred to in conjunction with the Remotely Upgradeable EGMs document which was published in 2005-2006 to generate industry discussion on how best CSS gaming technology can be potentially adopted in Queensland. The Remotely Upgradeable EGMs document is a higher level document which contemplates potential infrastructure and security to facilitate CSS gaming technology. This CSS Principles document is more specific in providing guidance around the equipment itself and attempts to fill the gaps where other established standards may not offer sufficient coverage to cater for the technology or provide a certain level of exemption for some conventional requirements where the nature of the technology may question their relevancy.

This draft document is now published on the OLGR website to stimulate industry comment and feedback. Please email any comments/feedback to notify@treasury.qld.gov.au.

1.2 Definitions

This document addresses regulatory requirements for Client-Server Systems (CSS) which are to be used for server based gaming. Server based gaming can be defined as either a System Based Game (SBG) or a System Supported Game (SSG). Both of which can be defined as the combination of a Central Server (CS), Player Terminals and communication network for linking the Player Terminals (clients) with the server. The communication network may be totally contained within a single venue (LAN) and/or over a wide area network (WAN) whereby a server in one location supports client Player Terminals in multiple sites.

1.2.1 A System is defined in this context as one or more computers which are linked to and involved in the control of multiple gaming devices.

1.2.2 "System Based Game" (SBG)

A gaming device comprised of a server or system part and client stations that together, form a single integrated device where the system portion of the game determines or helps to determine the outcomes of the individual games conducted on the client stations and the client stations cannot operate independently from the system.

1.2.3 "System Supported Game" (SSG)

A gaming device comprised of a collection of conventional gaming devices or client stations connected to a system for the purpose of downloading control programs, configuration changes and other software resources to the conventional gaming device or client station on an intermittent basis. The client stations connected to the system are capable of operating independently from the system once the downloading process has been completed. In a system supported game, game outcome is determined by the

conventional gaming devices or client stations connected to the system and not by the system itself.

1.2.4 Many of the requirements in this document will apply just to System Based Games.

1.2.5 Standard multi-terminal gaming devices such as MTGMs are covered in other Standards and are not addressed by this Standard unless the central server provides SBG or SSG functionality.

1.3 Configurations

There are a number of different configurations for client / server gaming systems. The following defines the two fundamental configurations.

1.3.1 "Central Based Server"

All of the components of the server are held in the secure computer room of the operator. Communication to the client stations would be through a dedicated wide area network for remote operations or local area network (LAN) within a venue.

1.3.2 "Venue Based Server"

Some or all of the components of the server are held in each venue. Communication with the client stations occurs within that venue from the server equipment through a LAN.

2 Hardware

2.1 Client Terminal Hardware

2.1.1 As a general rule, client terminals must meet all of the EGM hardware relevant requirements of other established Standards.

Program Storage / Chain of Trust

2.1.2 For client terminals in SBG and SSG that use writeable program storage, e.g. execution from hard disk or writeable Flash, there must be a non-modifiable within the gaming device, physical storage device, such as an EPROM or non-writeable Flash, which executes the first bootstrap on device restart / power-up.

2.1.3 This bootstrap must verify the next layer(s) of software that is to operate via a cryptographically secure algorithm.

2.1.4 This bootstrap must be socketed so that it can be removed and verified.

2.2 Critical Memory

Typical SBG configurations will store much, if not all critical memory in a database on the Server. This may be an acceptable configuration provided that a number of requirements are met that are specified elsewhere in this document.

2.2.1 If a Client terminal completes a monetary / security transaction before the transaction is committed in the server database, the client terminal must have local critical memory meeting all of the relevant requirements of other established Standards.

2.2.2 Examples of these kinds of monetary / security transactions are:

a) A banknote is stacked.
b) Coins are accepted.
c) A cashless transaction is conducted and completed with an external cashless support system connected directly to the client station.
d) Security events.

2.2.3 If some or all of the Critical Memory for a client device is stored in a server database:

a) The redundancy requirements of 2.3.1 must be met.
b) There must be an internal check within the database such that errors in the database are identified and flagged.
c) The system must automatically halt should this type of error occur.
d) There must be procedures in place for recovering the database should such an error occur.

2.3 Server Hardware

Redundancy

2.3.1 A SBG server shall have sufficient redundancy and modularity to accommodate a component failure to prevent the loss of critical data in the SBG operations.

2.3.2 There shall be redundant copies of each audit log and system database, where applicable, on a SBG or SSG Server with open support for backups and restoration. This includes a server that has support for failover redundancy.

2.3.3 Backup must occur with a frequency such that it is always possible to restore data following the failure of a single media device.

2.3.4 There must be a means to back-up the data to a device that can be removed for the purpose of storage at another location.

Multiple Servers

2.3.5 A SBG or SSG may in fact be a collection of servers for load balancing, redundancy or functionality reasons. For example, there might be two or more game servers, a finance server, monitoring server, download server, etc.

2.3.6 The server system as a whole, which may be a collection of such servers, must meet the full requirements of this specification but not necessarily each server. For example, a download server in a SBG configuration may not have to meet the redundancy requirements of Sections 2.3.1 - 2.3.3 but the system as a whole must.

2.3.7 If there are to be multiple servers, there must be a means to determine which Server was controlling a client terminal for each game played and monetary transaction.

Venue Based Server Hardware

2.3.8 Venue Based Server hardware must meet the jurisdiction’s physical security requirements that apply to EGMs in that Jurisdiction.

2.3.9 The server equipment must be located in a secure area with access only by properly authorised persons.

3 Software

3.1 General

3.1.1 For a System Based Game system, the Game Server shall generate and transmit to the Player Terminals control, configuration and information data, depending upon the actual implementation, examples are:

a) credit movement,
b) random numbers,
c) game result components, e.g. balls, cards or reel stop positions,
d) actual game results,
e) updates to the credit meter for winning games or
f) downloading control programs and other software resources to the Player Terminals.

3.1.2 For a System Supported Game system, the Game Server will not participate in the game determination process i.e. the purpose shall be that of downloading control programs and other software resources to the conventional gaming device or client station on an intermittent basis.

CSS Software Verification

3.1.3 Each component of the CSS must have a method to be verified via a third-party verification procedure.

3.1.4 In addition, the CSS shall have the ability to:

3.1.4.1 Authenticate all critical files including, but not limited to, executables, data, operating system files and other files, which may affect the game outcome or operation, which reside on the medium.

3.1.4.2 Employ a third-party industry standard secure hashing algorithm. The algorithm shall use a key or seed of sufficient length and complexity. The manufacturer should be prepared to demonstrate the algorithm choice to both the testing laboratory and jurisdiction.

3.1.4.3 The third-party verification process shall not include any process or security software provided by the operating system manufacturer. A secondary check may use commercially available software by the operating system manufacturer as part of the secondary verification. Rationale: there must be an independent algorithm for which source code is available.

3.1.4.4 The CSS Server must be capable of verifying that all control programs are authentic copies of approved games.

Copy Protection

3.1.5 Copy protection to prevent unauthorized proliferation or modification of software, for servers or clients, may be implemented provided that:

a) the method of copy protection is fully documented and provided to the Regulator's representative, e.g. ATF, who will verify that the protection works as described; and
b) any device(s) involved in enforcing the copy protection can be individually verified by the methodology described in Section 3.1.7.

Virus Protection

3.1.6 All servers and client devices should have adequate virus protection, where applicable.

Verification of devices that cannot be interrogated

3.1.7 Program devices that cannot be interrogated, such as Smart cards, may be used provided they are able to be verified by the following methodology:

a) A challenge is sent by the peer device, such as a hashing seed, to which the device must respond with a checksum of its entire program space using the challenge value.
b) The challenge mechanism and means of loading the software into the device is verified by a Testing Laboratory and approved by the regulator.

3.1.8 Such devices, where examination of the source code by a test laboratory shows that there can be no affect on approved game or monetary outcome, shall not be subject to these requirements.

3.2 Server Software

Intrusion Protection

3.2.1 All servers shall have sufficient logical intrusion protection against unauthorized access.

3.2.2 An audit log detailing all logical accesses to the servers must be maintained.

Configuration Access Requirements

3.2.3 The CSS interface element setup/configuration menu(s) must not be available unless using an authorized access method that is secure.

Server Programming

3.2.4 There shall be no means available for an Operator to conduct programming on the server in any configuration. In specific, the Operator should not be able to perform SQL statements to modify the database.

System Failure

3.2.5 The CSS shall be designed to protect the integrity of pertinent data in the event of a failure. Audit logs, system databases, and any other pertinent data must be stored using reasonable protection methods.

3.2.6 If hard disk drives are used as storage media, data integrity must be assured in the event of a disk failure.

3.2.7 The method used must also provide open support for backups and restoration. Refer also to Sections 2.3.1 - 2.3.3.

Recovery Requirements

3.2.8 In the event of a catastrophic failure when the CSS cannot be restarted in any other way, it shall be possible to reload the database from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information, where applicable:

a) Significant events.
b) Auditing information.
c) Game play.

d) Account balance updates.
e) Specific site information such as game configuration, security accounts, etc.

Self Monitoring

3.2.9 The CSS must implement self-monitoring of all critical Interface Elements (e.g. Central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of the condition, provided the condition is not catastrophic. Self monitoring that is implemented by off the shelf components may be acceptable if it adequately addresses these requirements – see 3.2.11.

3.2.10 The CSS shall be able to perform this operation with a frequency of at least once in every 24-hour period.

3.2.11 The design and implementation of self-monitoring schemes will be reviewed on a case-by-case basis by testing laboratory(s) to which the CSS is submitted.

3.2.12 Additionally, all critical interface elements will be reviewed on a case per case basis and may require further action by the system depending upon the severity of the failure.

Server Information Display

3.2.13 The Server that supports a System Based Game must be able to provide a complete play history for the most recent game played and at least 4 games prior to the most recent game for each client station connected to the system based game as per other established Standards.

3.2.14 The display must meet the relevant requirements of other established Standards e.g. Last Play Information Required.

3.2.15 Gaming devices offering games with a variable number of intermediate play steps per game must meet the relevant requirements of other established Standards e.g. Game Sequences.

3.2.16 The requirement to display game recall applies to all game programs currently installed on the server portion of the System Based Game.

3.2.17 The Server that supports a System Based Game must be able to provide a complete transaction history for transactions with a cashless wagering system to include the most recent and the previous thirty-four transactions prior to the most recent transaction for each client station and the previous 99 transactions for the overall gaming device, that incremented any of the cashless in-or out meters.

3.2.18 The capability to interrogate transaction history must be available at the client or conventional gaming device for the transaction history specifically associated with the particular client station initiating the history information request.

3.2.19 Refer also to Section 5.2.

RNG

3.2.20 In the event the CSS has the ability to determine the game result or to download Random Values to the Client Terminal, the Random Number Generator shall meet all of the relevant requirements of other established Standards.

3.2.21 There may be one or more of such RNGs in the server but each must meet these requirements.

3.2.22 If there are more than one RNG in use, there must be a means to identify which RNG has been used for each client terminal / game.

3.3 Downloads

3.3.1 This section outlines the requirements of the CSS for downloading Download Packages, which may be software, games and other configuration data, to Player Terminals, if the Game Server provides the functionality of downloading control programs and other software resources, whether for a System Based Game system or a System Supported Game system.

3.3.2 All packages that are to be downloaded to Player Terminals must have a means of being signed by, at least, the Regulator or testing laboratory.

3.3.2.1 The signing algorithm must be cryptographically secure.

3.3.2.2 The Player Terminal must verify the correct signing when a package is downloaded.

3.3.2.3 If the signature is not correct, the Player Terminal must reject the package and also cause a security event to be logged at the Server.

Foreground vs. Background Downloads

3.3.3 The download process must function in the background i.e. must not interfere with normal game play or other operation.

3.3.4 All download packages which are sent to the client device must be initially stored at the device e.g. on a hard disk.

3.3.5 A separate activation process must be executed later to use the downloaded package e.g. to replace the active software, add a new game or execute other authorised instructions in the downloaded package.

3.3.6 Activation can only occur when the client terminal is in an idle state – refer to Sections 3.3.8 - 3.3.10.

3.3.7 Background downloads may use commercial software upgrade provided the packages delivered by the commercial software can be verified to have been accurately delivered from the server to the client(s) by external means e.g. secure hash verification.

Download Activation

3.3.8 Prior to activation of a downloaded package by the client terminal, e.g. updated software, the software must be successfully authenticated, as defined within Sections 3.1.3 - 3.1.4 CSS Software Verification.

3.3.9 Verification of the client terminal Operating System is required only before activation of new software and not after every restart.

3.3.10 Activation of a downloaded package shall not be permitted until the Player Terminal is in an Idle State in accordance with the requirements of the Jurisdiction.

3.3.11 Any download activation that leads to changes of configuration that affects the player, e.g. a change of games, must provide notification to the player of the change(s) as required by the Regulator.

Game Data Upload

3.3.12 If the activation of the downloaded package leads to the irretrievable clearing of Game Data, the Game Data must be uploaded and securely stored on the CSS Server or connected CMS.

3.3.13 If stored on the CSS Server, it must be maintained for a minimum of 24-hours and archived after that time; or be permanently maintained in log or script file.

3.3.14 If this method is used, the process of activation of the new Control Program to the Player Terminal must ensure that all critical areas of memory are overwritten by a default value as per other established Standards.

Download Data File Library

3.3.15 The Download Data File Library refers to the formal storage of all approved data files / packages that may be downloaded to Player Terminals including control and game software, peripheral firmware, configuration data, etc.

3.3.16 Where applicable, the CSS Download Data Library shall only be written to, with secure access that is controlled by the regulator, in which case the manufacturer and/or operator will be able to access the Download Data File Library, provided that this access does not permit adding or deleting Download Data Files; or the Download Data File Library shall only be written to using a method that is acceptable by the Regulator.

3.3.17 It must not be possible to delete a game or software from the Download Library if they are currently in use anywhere in a venue under the control of the download server.

3.3.18 Any changes that are made to the Download Data File Library, including the addition, changing or deletion of Game Programs, must be stored in an audit log, which shall include:

a) Time and Date of the access and/or event;
b) Log In Name;
c) Download Data File ID Numbers added, changed, or deleted;
d) The Player Terminal(s) to which the Download Data File was downloaded and, if applicable, the file(s) it replaced; and
e) Changes to the Player Terminal configuration settings and what were the changes.

3.3.19 Once a record is stored in the Audit log there must be no means whereby it can be altered or deleted or other records inserted before it.

Download of Player Terminal Data Files and Control Programs

3.3.20 The CSS and/or Player Terminal shall provide the ability to conduct an independent integrity check of the Player Terminal, from a third-party outside source. The verification program used for the integrity check may be embedded within the CSS Server and/or Player Terminal software or have an interface port that is used to authenticate the media with the verification program that will not permit the alteration of the program (read only).

3.3.21 The CCS Server and/or Player Terminal shall authenticate all critical files including, but not limited to, executables, data, operating system files and other files, which may affect the game outcome or operation, which reside on the medium.

3.3.22 The CSS Server and/or Player Terminal shall use algorithm(s) that meet the requirements of Section 0.

3.3.23 For a SSG, the Player Terminal software must be checked in its entirety by the CSS and/or Player Terminal after the player terminal has been powered up.

3.3.24 In the event of a failed authentication after the player terminal has been powered up, the Player Terminal should immediately enter an Error Condition with the appropriate audio and visual indicator, and record the details, including time and date of the error in a log.

3.3.25 This error shall require operator intervention.

3.3.26 The Player Terminal shall display specific error information and shall not clear until either the file authenticates properly, following the operator intervention, or the medium is replaced or corrected, and the device's memory is cleared, the Player Terminal is restarted, and all files authenticate correctly.

Control Program

3.3.27 This section details the minimum technical standards that shall be met, where applicable, when downloading the Player Terminal Control Program from the CSS to the Player Terminal,

3.3.28 The download process must not adversely affect the Player Terminal operation:

3.3.29 The Player Terminal must have a method to monitor and report to the CSS all external door access during a foreground program download process and/or activation process.

3.4 Player Terminal Software

Game Variations/Paytable/Denomination Configuration Changes

This section refers to download packages that execute configuration changes but not new versions of software. Examples are commands to change to a new game variation (with their associated paytable) that is included within the running software but is not currently active or different tokenisation denomination.

3.4.1 Player Terminal Control Programs that offer multiple game variations, (with their associated paytable) and/or denominations that can be configured via the CSS Server must comply with jurisdictional Regulatory provisions and:

3.4.1.1 All game variations /(with their associated paytable) that are available meet the local theoretical return to player requirements;

3.4.1.2 All game software, which includes game variations (with the associated paytable) and denominations has been previously approved by the Regulator;

3.4.1.3 The CSS and/or Player Terminal maintains the Amounts Bet and Amounts Won meters within Critical Memory for each of the game variations that are available;

3.4.1.4 The CSS and/or Player Terminal maintains the Master Accounting meters in dollars and cents;

3.4.1.5 The Player Terminal is in an Idle State when the update to operational game variations (with their associated paytables) and/or denominations occurs, refer to Sections 3.3.8 - 3.3.10; and

3.4.1.6 The change will not cause inaccurate crediting or payment (i.e., Player Terminals using coin hoppers and coin acceptors with a fixed denomination.)

Player Terminal Critical Memory Clear

3.4.2 The process of clearing Critical Memory on the Player Terminals via the CSS must utilise a secure method that would require Regulatory Control.

3.5 Game Development Kit (GDK)

3.5.1 Should the CSS provide a game development kit to enable offline development of games, especially for use by other game suppliers, the GDK and full documentation must be included in the formal submission material.

3.5.2 It may be acceptable for the accuracy of games implementation to be verified by a testing laboratory using a special version of the GDK. In this instance, source code for

that version of the GDK must be submitted along with documentation on how to use it to create a range of results.

3.5.3 The Player Information Display (PID) data must be downloaded with each game.

4 Artwork

4.1 Game Specific Artwork

For SSG and SBG systems which provide game changing capabilities, the artwork available to the player must:

4.1.1 meet the relevant requirements of other established Standards;

4.1.2 always be consistent with the game(s) currently available to the player.

5 Banknote Acceptance

5.1 Critical memory

5.1.1 If a Client Terminal Banknote acceptor stacks bills before they are confirmed to be stored in the Server database, the Client Terminal must have the appropriate critical memory storage to retain these transactions in case of failure of the link to the server – Refer to Section 2.2.1.

5.1.2 There must be a means to view the financial transactions in the critical memory, including stacked banknotes, at the client terminal should the link between it and the server be broken.

5.2 Banknote recall

5.2.1 A SBG system with client terminals that use a bill validator and stores banknote input information in the server database, shall have the ability to display at a server terminal or device the following information required for the last five (5) items accepted by the bill validator (i.e. Banknotes, etc.)

5.2.2 Total monetary value of all items accepted;

5.2.3 Total number of all items accepted; and

5.2.4 A breakdown of the bills accepted:

5.2.5 For bills, the game shall report the number of bills accepted for each bill denomination;

5.2.6 For all other notes, the game shall have a separate meter that reports the number of items accepted, not including bills.

5.3 Banknote Recall Log

The banknote recall log may be combined or maintained separately by item type. If combined, the type of item accepted shall be recorded with the respective timestamp.

6 SUBMISSION REQUIREMENTS

6.1 Introduction

6.1.1 The submission requirements of this section are additional to those that would apply to the client stations as described in other established Standards.

Previous Submission

6.1.2 Where the Jurisdiction or its licensed testing laboratory has been previously supplied with the information or equipment on a previous submission, duplicate documentation is not required, provided that the previous information is referred to by the submitting party, and those documents are easily located. Every effort shall be made to reduce the redundancy of submission information.

Prototype (Full Submission) Submissions

6.1.3 A Prototype (full submission) submission is a first time submission of a CSS that has not previously been reviewed by the Jurisdiction or its licensed test laboratory.

NOTE: Due to abnormal component complexity and/or excessive cost it is sometimes necessary for on-site testing of a system at the manufacturer's facility.

6.2 Submission Letter Requirements

6.2.1 Each submission shall include a request letter, on company letterhead. The letter should include the following:

a) The jurisdiction(s) for which you are requesting certification;
b) The CSS items requested for certification. In the case of software, the submitting party shall include ID numbers and revision levels, if applicable. In the case of proprietary hardware, the submitting party shall indicate the manufacturer, model, and part and revision numbers of the associated components of hardware; and
c) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.
d) If a wireless network solution is desired, then the design and scope of the wireless solution needs to be reviewed for security considerations.

6.3 Submission Requirements – Prototype (Full Submission) Certification

Hardware

6.3.1 Each item of equipment supplied by a manufacturer that is to operate in a remote venue shall be functionally identical to the specimen tested and certified. For example, an interface element supplied as a certified device shall not have different internal wiring, components, firmware, circuit boards, circuit board track cuts or circuit board patch wires from the certified specimen, unless that change is also certified.

6.3.2 A minimum specification for equipment that is to be located in an Operator's premises must be provided.

6.3.3 Each submission of a CSS System shall contain the following: '

a) Server(s), Database(s), Front End Controller(s), and Ancillary Stations to include but not limited to: Cashier Booth functionality; System Configuration Parameters functionality; and Accounting/Reporting Functionality;
b) Monitors, keyboards, mouse, printers, etc., to support the items listed above;
c) Un-interruptible Power Supply (UPS), network cabling, hubs, switches and any wireless components that may be installed at a venue; and

d) Minimum of two of each type magnetic cards (or equivalent if an alternative media is used) used in the system, if applicable.

NOTE: In an effort to reduce system submission size, monitor and data switches may be used. Additionally, separate software may be housed in the same unit, as long as the functionality is not impaired and the software is identical to the field version.

6.3.4 Each submission of a CSS system must include at least two fully configured Client terminals.

6.3.5 An inventory of all equipment submitted must be provided.

Accompanying Documentation.

6.3.6 All accompanying technical documents, manuals, and schematics shall be submitted. In addition, the following items shall be provided:

a) If applicable, all external laboratory compliance certification. This certification information may be supplied at a later date but not before a recommendation for approval can be given;
b) Any other proprietary equipment that may be used in the field in conjunction with the Submission, if necessary to test the requirements set forth;
c) Accompanying software, see also, 'System Software Submission Requirements – Prototype (Full Submission) Certification,' Section 2.4; and
d) If the submitting party has specialised equipment and/or software which is needed by the test laboratory to test submitted system, such as load/game simulators or test data files, then the specialised equipment and/or software and all appropriate operation and user manuals for the equipment and/or software shall be included with the submission.

System Software

6.3.7 Software submitted with a CSS system, whether it be for Clients of the Server, shall contain the following:

a) Two sets of all PSDs, CD-ROMs, or other storage media which contain identical contents. This includes all program executables, system component firmware, bin files, etc., unless other arrangements are made in advance of the submission. Where the test laboratory already has tested a software component, resubmission may not be necessary;
b) Source Code for all primary software executables. In addition, if requested, explanation of all non-volatile critical memory on any system device with the non-volatile critical memory locations described;
c) A means of conducting independent compilation and verification of all CSS software;
d) All user manuals in both hard and soft copy format to include a general overview of the system from a component level, software and hardware setup and integration, and system block diagrams and flow charts for the communication program, if required;
e) If not included in the user manuals, a connectivity manual for all associated peripheral devices or remote sales or monitoring units;
f) If not included in the user manuals, provide example reports for each standard report capable of being generated on the system with a formula summary detailing all reporting calculations including data types involved, mathematical operations performed, and field limit;

g) If not included in the user manuals, a list of all supported communication protocols, including all message formats, specifying the version, if applicable; and
h) If utilising a software verification algorithm, provide a description of the algorithm, theoretical basis of the algorithm, results of any analyses or tests to demonstrate that the algorithm is suitable or the intended application, rules for selection of algorithm coefficients or "seeds", and means of setting the algorithm coefficients or "seeds."

6.3.8 Provide details of all off the shelf software that is used in the CSS including the name, function summary, supplier(s), version etc.

Games

6.3.9 Provide a list of each game that is to be included in the submission including game name, variations, characteristics (e.g. tokenisation), versions etc.

6.3.10 For each Game submitted, provide the game and artwork information as required in other established Standards.

6.3.11 If not provided in other documentation, documentation of how games interface with the CSS server in SBG configurations.

6.3.12 Provide a means for the Jurisdiction and/or its approved testing facility to create a range of game outcomes during the testing process.

6.4 Update Submissions

6.4.1 The same submission principles for hardware, software and games espoused in other established Standards are to apply.

6.4.2 The submission must advise if there have been changes to system software that could affect previously approved games operating in the CSS.

7 Glossary

Reference	Definition
CSS	Client Server System
CSS Server	The 'host' computer that is the primary source of the system controls and information.
Control Program	The control program is the software that operates the Client Terminals functions, including the paytable(s) for the game. The Control Program can run independently of the CSS or may require information generated by the system to perform the Client Terminal functions.
Critical Memory	Critical memory is used to store all data that is considered vital to the continued operation of the client terminal.
Download Package	A data file that is downloaded to a Client Terminal by a Server whether it be a SBG or SSG. The package may contain new software, games, configurations changes or similar.
Firewall	Network security barrier. A firewall is a device that guards the entrance to a private network and keeps out unauthorized or unwanted traffic.
GDK	Game Development Kit
Game Program	The control program that resides at the CSS server and/or the client terminal
Download Data Library	A controlled library that resides at the CSS server that contains the complete game program, the server side critical components of a game program and/or other download packages.
Idle State	The Client Terminal is in an Idle State as defined by the Regulatory requirements – refer to Sections 3.3.8 - 3.3.10..
Client Terminal	An element within a CSS that is a client terminal. The Client Terminal in a Server-Supported configuration may function independently of the CSS Server upon a successful Control Program update or, requires Game Content, which is produced by the CSS Server, to function as in a Server-Based configuration.
Random Values	Where a Random Number Generator is stored on the CSS Server, and communicates random numbers to the Client Terminal(s) that are required for the Client Terminal to function, where the Client Terminal's Control Program is not independent of the CSS Server.
Server Based Game (SBG)	The combination of a server and client terminals in which the entire or integral portion of game content resides on the server. This system works collectively in a fashion in which the client terminal will not be capable of functioning when disconnected from the system.
Server Supported Game (SSG)	The combination of a server and client terminal(s) which together allow the transfer of the entire control program and game content to the client terminal(s) for the purpose of downloading control programs and other software resources to the conventional client terminal or client terminal on an intermittent basis. The client terminals connected to the system are capable of operating independently from the system once the downloading process has been completed. This configuration encompasses cases where the system may take control of peripheral devices or associated equipment typically considered part of a conventional client terminal such as a bill validator or a printer. In a System Supported Game, game

Reference	Definition
	outcome is determined by the client terminals connected to the system and not by the system itself. The client terminal is capable of functioning if disconnected from the system.

8 Communications

8.1 Introduction

This chapter refers to communications between the CSS Central Server(s) and the Player Terminals; Player Terminals to Player Terminals; Player Terminals to external Cashless systems, etc.

8.2 Communication Protocol

Each component of a CSS must function as indicated by the communication protocol implemented.

8.2.1 All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent tampering. Where it is necessary for data to be secure, Encryption or Authentication with secure seeds or algorithms is required.

8.2.2 If communicating with an existing CMS, the protocol used by that CMS must be fully implemented. It is acceptable to interface the Server to the CMS and have it emulate multiple stations on a CMS communications line.

8.3 Loss of Communications

For a System Based Game (SBG) loss of communications is defined as no communications between client and server for more than 20 seconds. Should that occur:

8.3.1 The Player Terminal, by definition, must be rendered unplayable. If a game is in progress, a mechanism must be provided to recover to the point of the game when communications was lost.

8.3.2 In the case of Player Terminals that have lost communications with the server, the client must provide a means, such as a hand pay, for patrons to cash out credits indicated on the system based gaming device at the time the communications was lost.

8.3.3 If the CSS provides the capability of transferring a player's session to another client terminal, the CSS must ensure that the meters balance for both the original and new destination terminals. At the least:

a) The credit meter on the original terminal must be set to zero.
b) The credit meter on the new terminal must be set to the balance on the original terminal.
c) An appropriate credit out meter must be incremented by the amount of the original credit meter maintained for the original terminal and an appropriate credit meter in must be incremented by the same amount for the destination terminal.

8.3.4 If the original terminal was in the middle of a game when the lost communications or disconnect occurred,

a) The new terminal must place the game in the same state as it had been on the original terminal.
b) Any credits played on the original terminal must update the credits played meter maintained for the original terminal.

c) Any credits won during the game must update the credits won meter maintained for the destination terminal.

8.4 System Security

Securing the Gaming Network.

Physical security.

8.4.1 All network components that make up the gaming intranet must be secured from unauthorised access.

8.4.2 The devices themselves must be password protected and hold an audit trail of configuration changes.

Unique network isolated to the gaming environment.

8.4.3 The gaming network must be isolated and insulated from non gaming networks.

8.4.4 The gaming network must be self contained either via a dedicated network infrastructure or via a secure VPN tunnel facility.

8.4.5 The network must be secured via an application layer “stateful” firewall and must not have the facility for alternate network paths.

Authentication.

8.4.6 Cryptographically secure authentication must be provided to authenticate source and destination of data across the network.

Data Encryption.

8.4.7 All gaming data traversing the network must be encrypted.

8.4.8 The encryption keys must conform to industry standard encryption and authentication structures.

Intrusion protection

8.4.9 Network connections between clients and servers within the gaming intranet must be protected using and industry accepted encryption and authentication structures.

8.4.10 In support of this infrastructure the network authentication process must have the capability to revoke and renew the Certificates used to authenticate the connections between the clients and servers.

8.4.11 An industry accepted frequency of revocation and renewal is required to ensure that the keys cannot be attacked via an external source.

8.5 Firewall Audit Logs

The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

8.5.1 all changes to configuration of the firewall;

8.5.2 all successful and unsuccessful connection attempts through the firewall; and

8.5.3 the source and destination IP Addresses, Port Numbers and MAC Addresses.

8.6 Wide Area Network Communications

Wide Area Network (WAN) communications within the CSS is permitted provided that:

8.6.1 the Jurisdiction(s) within which the CSS is to operate do not specifically prohibit the linking of multiple sites;

a) the communications over the WAN are secured from intrusion, interference and eavesdropping via techniques such as use of a Virtual Private Network (VPN), encryption, authentication etc; and
b) only functions documented in the communications protocol are used over the WAN. The protocol shall be submitted a part of the approval process for each jurisdiction. The protocol documentation may be in multiple parts e.g. delivery mechanism and message formats.

8.7 Access

Remote Access is defined as any access to the system outside of the submitted network architecture – note that approved WAN access as described in Section 8.6 is considered to be part of the Internal Network.

8.7.1 Remote Access, where permitted, shall authenticate all computer systems based on the authorized settings of the CSS or firewall application that establishes a connection with the CSS.

8.7.2 The security of Remote Access will be reviewed on a case-by-case basis, in conjunction with the current technology and approval from the local regulatory agency.

8.7.3 The following are additional requirements:

a) Only authorized remote user administration functionality may be used (examples of functionality that are unlikely to be authorized are adding users, changing permissions, etc.);
b) Only authorized access to any database such as information retrieval using existing functions is permitted; and
c) Only authorized access to the operating system is permitted.

8.8 Remote Access Auditing

The CSS Server must maintain an activity log either automatically or have the ability to manually enter the logs depicting all Remote Access information that includes the:

8.8.1 Log on Name;

8.8.2 Time and date the connection was made;

8.8.3 Duration of connection; and

8.8.4 Activity while logged in, including the specific areas accessed and changes that were made.

8.9 Wireless Communication

Should a wireless communication solution be adopted, then additional security precautions must be taken. The following principles must apply:

8.9.1 The wired LAN (Local Area Network) must be isolated from the wireless (WLAN) network through the layering of additional network security methods.

8.9.2 The following recommendations are to be considered minimum recommendations and not restrictions:

a) The wireless access point must be physically positioned in the building so that it is not easily accessible by unauthorized individuals.
b) The access point must not be placed directly onto the venue network unless a stand-alone stateful packet inspection firewall is employed.

c) Wireless network traffic must be secured with additional encryption and/or authentication codes.
d) The keys used to encrypt the communication through the wireless network must be stored in a secure location.

8.9.3 All wireless networks must be protected via an industry standard challenge / response authentication mechanism where authentication keys are refreshed randomly to avoid decryption.

8.10 Signature Checks

For Jurisdictions that mandate signature checks of gaming equipment from the CMS or its components, the following requirements apply:

8.10.1 In principle the entire program space of the gaming device should be included in the signature calculation. However, it is likely that the size of the programs would be prohibitive so the following must apply:

a) Off the shelf components need not be included in the signature checks.
b) For devices that have a secure boot chain and the signature calculation software is contained in an area of the initial boot, only the lowest level boot ROM(s) need to be calculated.
c) Otherwise, the lowest level boot ROM(s) should be included in a foreground signature check and the rest of the application software in a background check.

8.10.2 These requirements apply to the:

a) Client Terminals.
b) Venue based server equipment in the configuration defined in Section 1.3.2. In this case, a signature check request for a client terminal should lead to a combination of the result of the client and the server signatures.

9 Revision History

Version	Changes	QIR	Who	Release Date	Incept Date
0.02	Draft			DRAFT	
0.03	Updated to new DEEDI report document template		YS	20/8/2010	imm