TECHNICAL STANDARDS FOR CLIENT-SERVER SYSTEMS (SINGAPORE)

Version 1.0

With effect from 20 January 2011

Total number of pages: 24 (inclusive of cover page)

Technical Standards for Client-Server Systems (Singapore)

Whilst every effort has been made to ensure that the information contained in this document is accurate as at the date of issue, the Authority makes no warranty or representation whatsoever with regards to the information in this document. The Authority assumes no responsibility or liability for any consequences (financial or otherwise) suffered directly or indirectly by persons who have entered into commercial activities upon reliance on any information in this document.

The information in this document is subject to change from time to time to adapt to the continual development and evolution of the gaming industry in Singapore. The Authority reserves the right to change its policies and to amend, modify or supplement any information in this document.

This document does not in any way bind the Authority to grant any approval for or exemption from any matter for which approval is required under any written law in Singapore.

This document shall not affect any regulatory requirements of any other competent authority in Singapore.

Persons who may be in doubt about how the information in this document may affect them or their commercial activities are advised to seek independent legal advice or any other professional advice they may deem appropriate.

Technical Standards for Client-Server Systems (Singapore)

TABLE OF CONTENTS

PREFACE

The purpose of this document is to establish the requirements for the design and operation of client-server systems within the Singapore jurisdiction and to guide certification and testing bodies on the areas for technical compliance on such equipment.

A Client-Server System (CSS) can be defined as either a Server Based Game (SBG) system or a Server Supported Game (SSG) system; both of which are combination of a central server, client terminals and all interface elements that function collectively for the purpose of linking the client terminals with the central server.

A Server Based Game (SBG) system is a type of gaming equipment comprised of server and client terminals, and together they form a single integrated system where the server portion of the game determines or helps to determine the outcomes of the individual games conducted on the client terminals and the client terminals cannot operate independently from the system.

A Server Supported Game (SSG) system is a type of gaming equipment comprised of a collection of client terminals connected to a server for the purpose of downloading control programs, configuration changes and other software resources to the client terminals on an on-demand or scheduled basis. The client terminals connected to the server are capable of operating independently from the system once the downloading process has been completed. The outcome of the game is determined by the individual client terminals connected to the server and not by the server itself.

Unless otherwise stated, the requirements in this document apply to client-server systems in general, and not specific to either SBG or SSG.

The intent of this document is to ensure that gaming on client-server systems occur in a manner that is:-

a. Honest;
b. Secure;
c. Reliable; and
d. Auditable.

It is not the intent of this document to:-

a. Mandate a single solution or method to realise an objective;
b. Limit technology application to gaming equipment;
c. Limit creativity and variety of choice;
d. Limit any supplier or manufacturer of equipment; and
e. Preclude research and development into new technologies or innovative ideas.

As far as possible, this document stipulates what the minimum technical requirements for client-server systems are instead of how these standards should be met, and does not mandate a particular solution or method as the means to realise these standards.

Technical Standards for Client-Server Systems (Singapore)

The Casino Regulatory Authority of Singapore (the "Authority") is the regulatory authority that supervises and regulates the activities of casinos in Singapore. Casino operators are required to be licensed by law and the gaming equipment deployed on the casino floor must comply with these technical standards as part of their licensing requirements.

Where applicable, the provisions in the Casino Control Act (Cap. 33A) and its subsidiary legislations shall take precedence over these technical standards.

This document would be reviewed on an ongoing basis to take into account the evolution of technologies utilised in client-server systems and the development of other casino related technologies that may require technical regulation.

Comments on this document can be forwarded to:-

Casino Regulatory Authority of Singapore
Gaming Technology and ICT Systems Division
460 Alexandra Road, #12-01
Singapore 119963
Website: http://www.cra.gov.sg

1. INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this technical standard is to:-

a. Create technical standards that would ensure that the operation of Client-Server Systems (CSS) in casinos in Singapore is secure, reliable, auditable and operated appropriately;

b. Establish the minimum integrity standards for CSS;

c. Construct technical standards that are technology neutral wherever feasible; and

d. Construct technical standards that do not specify or approve any particular method or algorithm. The intent being to allow a wide range of methods to be used to conform to these standards as long as the methods are secure, reliable and consistent with the best practices of the day for the relevant technologies.

1.2 Scope

1.2.1 The scope of these technical standards covers the minimum standards required in the operation of the CSS so that security, reliability and integrity of the CSS is achieved.

1.2.2 The scope of this technical standard does not cover:-

a. Requirements that are not related to gaming (such as health and safety); and

b. Components or sub-systems that involve the delivery and/or display of media contents which are solely marketing or promotional in nature and shall not affect the play of game(s) on the client terminals.

1.3 Terminology

1.3.1 The following terminologies used in this document are to be interpreted as follow:-

a. Shall: The guideline defined is a mandatory requirement, and therefore must be complied with;

b. Should: The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented; and

c. May: The guideline defined is an optional requirement. The implementation of this guideline is determined by the operator's environmental requirements.

1.4 Definition of Terms

Authority/ The CRA	The Casino Regulatory Authority of Singapore
Client-Server System	A client-server system (CSS) can be defined as either a Server Based Game (SBG) system or a Server Supported Game (SSG) system. Both of which are combination of a central server, client terminals and all interface elements that function collectively for the purpose of linking the client terminals with the central server.
Server Based Game System	A Server Based Game (SBG) system is a type of gaming equipment comprised of server and client terminals, and together they form a single integrated system where the server portion of the game determines or helps to determine the outcomes of the individual games conducted on the client terminals and the client terminals cannot operate independently from the system.
Server Supported Game System	A Server Supported Game (SSG) system is a type of gaming equipment comprised of a collection of client terminals connected to a server for the purpose of downloading control programs, configuration changes and other software resources to the client terminals on an on-demand or scheduled basis. The client terminals connected to the server are capable of operating independently from the system once the downloading process has been completed. The outcome of the game is determined by the individual client terminals connected to the server and not by the server itself.
Client Terminal	The client terminal is a component of the CSS which interfaces directly with the players to facilitate playing of CSS games. This does not include any portable gaming devices.
Control Program	The software that operates the client terminals functions, including the paytable(s) and the executables of the game. The Control Program can run independently from the CSS in a SSG setup or run off directly from the server in a SBG setup to perform the client terminal functions.
Download Package	A data file that is downloaded to a client terminal by a server. The package may contain control program and configurations changes or similar.
Download Data Library	A controlled library that resides at the CSS server. It contains the complete game program, the server side of the critical components of a game program and/or other download packages.
Idle State	A machine state of the Client Terminal when the terminal is idle in maintenance mode; or there is no activity, no credits and no errors on the client terminal.

Nearline storage	Nearline storage is not immediately available, but can be made online quickly without human intervention. This includes optical jukeboxes, automated tape libraries, as well as spin-down massive array of idle disk (MAID) technologies.
Offline storage	Offline storage is not immediately available, and requires some human intervention to bring online. This can include universal serial bus (USB) memory sticks, compact disc or Digital Video Disc (CD/DVD) optical media, shelf-resident tape cartridges, or other removable media.
Online storage	Online storage is immediately available for access. This includes dynamic random access memory (DRAM) and always-on spinning disk, regardless of rotational speed.
TITO	Ticket In - Ticket Out - a type of cashless wagering transaction with use of tickets or vouchers.
Tilt Condition	A tilt condition has occurred when the device detects an internal error, malfunction, attempted cheating or other specific events (see Section 2.12 of Technical Standards for Electronic Gaming Machines). Further play is disallowed until the event is resolved.

1.5 Testing

1.5.1 Testing of CSS by recognised testing laboratories shall be aimed at determining compliance with the technical requirements provided in this document. Areas of non-compliance shall be reported in the test/certification report. Where, in the opinion of the testing or certification laboratory, the technical requirements spelt out in this document are insufficient, inappropriate or not pertinent to the design of the subject CSS, the laboratory shall seek direction and further clarification from the Authority before proceeding to testing/certification.

1.5.2 This set of technical standards for the CSS should be read in conjunction with the Technical Standards for Electronic Gaming Machines (Singapore). It is a comprehensive set of standards that covers the requirements pertaining to the design and operation of gaming machines within the Singapore jurisdiction. All standards that apply to gaming machines shall be applicable, where possible, to the client terminals in the CSS.

1.6 Consistency of Interpretation

1.6.1 The Authority recognises that the technical standards may be subject to different interpretations by manufacturers, casino operators and testing/certification laboratories. As such, any feedback where different interpretations may be applied to the technical standards provided in this document should be directed to the Authority for clarification when it arises.

2. SYSTEM COMPONENTS REQUIREMENTS

This section outlines the system component requirements of the CSS which includes requirements for the server, client and the system as a whole.

2.1 System

2.1.1 The CSS may exist as a collection of servers for load balancing, redundancy or functionality reasons.

(Section 2.1.2 through 2.1.3 only applies to SSG)

2.1.2 For a SSG system, the server shall not participate in any determination of a game outcome.

2.1.3 The server shall facilitate the downloading of control programs and other software resources to the connected client terminals. Such download process shall be conducted on an on-demand or scheduled basis.

(Section 2.1.4 only applies to SBG)

2.1.4 For a SBG system, the server shall interface with the connected client terminals to ensure that the following data are minimally displayed on the terminals accurately:-

a. credits;

b. game result components, e.g. balls, cards or reel stop positions;

c. actual game results; and

d. updates to the credit meter for winning games.

Redundancy

2.1.5 The CSS shall have component redundancy and modularity to prevent the loss or corruption of critical data due to any component failures during its operations. Critical data shall minimally include audit logs, transactional logs and system databases.

Backup

2.1.6 All backup of the CSS data shall be carried out in such a way that no single failure of any portion of the system would cause the loss or corruption of data.

2.1.7 There shall be a mean to back-up the data to a device that can be removed for the purpose of storage at another secured location.

2.1.8 In the event of a system failure, it shall be possible for the database to be reloaded from the last backup point such that all data up to the minute of failure are fully recovered.

2.2 Server

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

Critical Memory *(Section 2.2.2 only applies to SBG)*

2.2.2 All critical memory shall be stored in a database on the server, and the database shall satisfy the following mandatory requirements :-

a. The redundancy requirements of Section 2.1.5 shall be met;

b. There shall be an internal check within the database such that errors in the database are identified and flagged promptly;

c. The system shall automatically halt should the database encounter any errors; and

d. There shall be methods to recover the database should the database encounter any error.

Random Number Generator (RNG) *(Section 2.2.3 through 2.2.4 only applies to SBG)*

2.2.3 All RNGs which reside on the server shall meet all of the requirements of Section 3.4 of the Technical Standards for Electronic Gaming Machines.

2.2.4 If there are more than one RNG in use, there shall be means to identify the RNG that has been used for the respective client terminals or games.

2.3 Client

2.3.1 As a general rule, where applicable, the client terminals shall meet all of the EGM requirements in the Technical Standards for Electronic Gaming Machines.

3. SECURITY

This section outlines the security requirements of the CSS, which includes logical access protection, database security, software verifications and client management security.

3.1 Logical & Physical Access

3.1.1 All servers and their logging devices shall reside in a secure area with logical intrusion protection against unauthorised access.

3.1.2 Logical access to the CSS shall be logged automatically on the servers and/or their logging device. The logged data shall not be accessible to the same individual(s) who has/have gained logical access, and shall meet the requirements in Section 6.

3.1.3 If the servers are located on the casino floor, the server hardware (inclusive of its logic area) shall be protected from forced illegal entry. There shall be retention of evidence for any sign of illegal entry.

3.1.4 CSS shall be configured such that system administrator level access may not be achieved without the presence and participation of at least two individuals.

3.1.5 The CSS setup or configuration menu(s) should only be made accessible through system administrator level or above.

3.2 Server Database Security

3.2.1 There shall be no means for any unauthorised users of the CSS to create, modify and delete any database record in the server manually (including the use of customized scripts).

3.2.2 Authorised manual reconciliations of database records in the server shall be logged automatically and meet the requirements in Section 6.

3.3 Software Verification

CSS Software Third-Party Verification

3.3.1 Each software component of the CSS shall have a method to be verified via a third-party verification procedure.

3.3.2 The third-party verification process shall be able to verify all critical files including executables, data, operating system files and other files resident on the CSS, which may affect the game outcome or operation.

3.3.3 The third-party verification process shall employ a third-party industry standard secure hashing algorithm. The hash value shall be of at least 160 bits such as SHA-1. The manufacturer shall be expected to demonstrate the algorithm of

choice and substantiate with its source code to both the testing laboratory and the CRA.

CSS Software Self Verification

3.3.4 The CSS shall be capable of verifying that all control programs and download packages contained on the servers and client terminals are authentic copies of software approved by the CRA. The CSS shall support the following verification methods in accordance with Section 3.3.5:-

a. scheduled at least once every 24 hours; and

b. on demand.

3.3.5 The method of self verification shall minimally use 128 bits of hash value for file signature comparison. If a mismatch is found during the comparison process, the execution of the software shall be prevented and the CSS shall provide a visual notification of the invalid program.

3.3.6 Any program software of the self verification mechanism shall reside on and securely load from media or partitions which are protected from alteration.

3.3.7 A report shall be available, which details the outcome of each automated execution of the mechanism and shall identify any invalid program software.

CSS's Verification of Client Terminal Data Files and Control Programs

3.3.8 The CSS shall provide the ability to initiate an independent integrity check of the client terminal. The CSS verification shall authenticate all critical files. Critical files shall minimally include executables, data, operating system files and other files, which may affect the game outcome or operation, and which resides on the client.

3.3.9 The CSS server and/or client terminal shall use algorithm(s) that meet the requirements of Section 3.3.5.

3.4 Client Management Security

3.4.1 The process of clearing critical memory on the client terminals via the CSS server shall utilise a secure method that satisfied all the requirements as per defined in Section 9.1.2.

3.4.2 Activity of clearing critical memory initiated by the server shall be logged automatically on the server and meet the requirements in Section 6.

4. ACCOUNTING

This section outlines the requirements of the CSS, concerning accounting information on the server and/or client terminals. These requirements addresses in a non-exhaustive manner, what kind of accounting information shall be handled; how accounting information shall be stored; and how transactions of accounting information shall be retained.

4.1 Meter Information

4.1.1 A complete set of meter information to include all meters required by Section 3.2 of the Technical Standards for Electronic Gaming Machines of all the client terminals shall be successfully communicated to a slot accounting system.

4.2 Banknote Recall

(Section 4.2.1 only applies to SBG)

4.2.1 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 and at the device the following information required for the last thirty-five (35) items accepted by the bill validator (i.e. Banknotes, Ticket/Vouchers, Coupons, etc.) per client terminal:-

a. Total monetary value of all items accepted;

b. Total number of all items accepted;

c. A breakdown of the bills accepted:

d. For bills, the game shall report the number of bills accepted for each bill denomination; and

e. For all other notes (Ticket/Vouchers and Coupons), the game shall have a separate meter that reports the number of items accepted, other than bills.

4.2.2 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.

(Section 4.2.3 through 4.2.4 only applies to SBG)

4.2.3 The client terminal shall have local buffer to store the financial transactions and security events, and meet all the requirements in Section 2.7 of the Technical Standards for Electronic Gaming Machines, if a client terminal has completed, but yet to commit and store the transactions into the server database. Financial transactions or security events include :-

a. A banknote is accepted;

b. Coins are accepted;

c. A cashless transaction is conducted and completed with an external cashless support system connected directly to the client terminal;

d. A Ticket In - Ticket Out (TITO) transaction is conducted and completed with an external ticket support system connected directly to the client terminal; and

e. Security events.

4.2.4 There shall be a mean to view the financial transactions and security events in the local buffer, including stacked banknotes, at the client terminal in case the link between it and the server is broken.

4.3 Transaction History

(Section 4.3.1 through 4.3.2 only applies to SBG)

4.3.1 For a SBG system, the server shall be able to provide a complete transactional history for transactions with a cashless wagering system and/or a TITO system to include the most recent thirty-five (35) transactions for each client terminal and the most recent one hundred (100) transactions for the server, that incremented any of the cashless in-or out meters.

4.3.2 The capability to view transaction history shall be available at the client terminal for the transaction history specifically associated with the particular client terminal initiating the history information request.

5. HISTORY RECALL

This section outlines the requirements of the CSS to display historical game replays on the server and client terminals.

5.1 Server Information Display

(Section 5.1.1 through 5.1.2 only applies to SBG)

5.1.1 The server that supports a SBG shall be able to display information and provide a complete play history for each individual client terminal as per Section 3.7 of the Technical Standards for Electronic Gaming Machines, with the exception of Section 3.7.4 of the Technical Standards for Electronic Gaming Machines.

5.1.2 Complete play history shall be retrievable on at least the last thirty-five (35) games for each individual client terminals.

6. LOGGING

This section outlines the logging requirements of the CSS. Logging applies minimally to application, security, event and gaming related logs. Unless otherwise stated, the requirements pertain to both the server and the client terminals.

6.1 Log Entries

6.1.1 CSS shall provide log entries for all system activities that minimally includes the following :-

a. Addition, removal or alteration of software component in the server or system portion of the device;

b. Logical access to the CSS;

c. Transaction logs;

d. Activities of clearing critical memory on client terminals;

e. Configuration changes of any components on the CSS;

f. System monitoring status; and

g. All manual reconciliations of database records.

6.1.2 Unless otherwise stated, each log entry shall minimally contain the following:-

a. Date and time of the action(s);

b. Identification of the component(s) affected;

c. If applicable, the identification of the individual performing action(s); and

d. If applicable, the reason for the action(s) performed and any pertinent validation information.

6.1.3 Log entries for logical access to CSS components shall minimally include the following:-

a. time;

b. date; and

c. identity of the individual accessing the secure area.

6.1.4 Log entries for changes made to the download data library on the CSS server, shall minimally include the following:-

a. time and date of the access and/or event;

b. log in Name/ID used;

c. download data file ID numbers added, modified, or deleted;

d. the client terminal(s) to which the download data file was downloaded and, if applicable, the file(s) it replaced; and

e. the changes made to the client terminal configuration settings.

6.2 Log Retention

6.2.1 All logged data shall be retained on the server or the client terminals and on the secondary logging device such that:-

a. Online search is possible for a minimum period of thirty (30) days; and

b. Data retrieval from online, nearline or offline storage is possible for a minimum period of five (5) years.

6.2.2 CSS shall detect and prevent any unauthorized changing of the logs.

6.3 Log Retrieval

6.3.1 CSS shall provide functions for an authorised user to access, export and print selected portions of information recorded in the logs as and when required.

7. DOWNLOADS

This section outlines the requirements of the CSS for downloading download packages, which may be software, games, media files (sound, graphics, video, image, etc.) and other configuration data, to client terminals, if the server provides the functionality of downloading control programs and other software resources. Unless otherwise stated, the requirements pertain to both the server and the client terminals.

7.1 Game Data Transfer

7.1.1 Prior to any software being added, removed or activated on the CSS that would result in the loss of accounting meter information, a complete set of meter information to include all meters required by Section 3.2 of the Technical Standards for Electronic Gaming Machines for all the client terminals as well as the server shall be successfully communicated to the slot accounting system.

7.2 Download Data Library in Server

7.2.1 All modifications to the download data library shall only be permitted to the authorised user and such activities shall be captured in the audit logs. There shall not be any methods available for unauthorised users, including the manufacturer, to override modifications made by the authorised user to the download data library unless otherwise approved by the CRA.

7.2.2 No game or software shall be deleted from the download data library if they are currently in use anywhere in a venue under the control of the server.

7.2.3 Any changes that are made to the download data library, including addition, modification or deletion of game programs, shall be logged which meet the requirements in Section 6.

7.3 Authorised Download Package

7.3.1 All packages that are to be downloaded to client terminals shall be digitally signed by the manufacturer, and approved by the CRA.

7.3.2 The digital signing shall be cryptographically strong enough to resist cryptanalysis.

7.3.3 The client terminal shall verify the correct signing when a package is downloaded from the server.

7.3.4 If the signature is not correct, the client terminal shall reject the package, and log such rejection as a security event at the server.

7.4 Loading of Download Package onto Client Terminal

7.4.1 The download process shall function in the background and it shall not interfere with normal game play or other operations.

7.4.2 Software downloaded to a client terminal shall be initially stored in a separate area or partition of memory, such that the software is segregated from the operating software to refrain from affecting the operation of the client terminal.

7.4.3 A separate activation process shall 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.

7.5 Activation of Downloaded Package by Client Terminal

7.5.1 Prior to activation of a downloaded package by the client terminal, e.g. updated software, the software shall be successfully authenticated, as defined in Section 3.3.8 to 3.3.9.

7.5.2 Verification of the client terminal operating system is required only before activation of new software and not after every restart.

7.5.3 Activation of a downloaded package shall not be permitted until the client terminal is in an Idle State for at least 4 minutes.

7.5.4 No game play shall be allowed on the client terminal during the activation of a downloaded package.

7.5.5 Any download activation that leads to changes of configuration shall provide an on-screen notification.

8. ARTWORK

This section outlines the requirements of displays and static artwork associated with games played on the CSS. All displays, including reels, help screens, secondary displays, static artwork, top box features shall be accurate, comprehensive and non-misleading representations of the game played.

8.1 Artwork Available to Player

8.1.1 For CSS which provide game changing capabilities, the artwork available to the player shall:-

a. meet the requirements of Section 4 of the Technical Standards for Electronic Gaming Machines; and

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

9. COMMUNICATIONS

This chapter refers to communications between the components of CSS; and between the CSS to external systems such as cashless wagering systems, slots management systems (SMS), etc.

9.1 Communication Protocol

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

9.1.2 All protocols shall use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent tampering. All data shall be secured from the client terminals to the server. Encryption or authentication with secure seeds or algorithms is required.

9.1.3 When the CSS is communicating with an SMS, the protocol used by that SMS shall be fully supported by the CSS.

9.1.4 Each component of a CSS shall be able to synchronize its local date and time with the SMS intended for, within an accuracy of sixty (60) seconds so as to ensure that time stamping of all events and data is correct.

9.2 Authentication and Data Encryption

9.2.1 Network connections and gaming data between servers and client terminals within the gaming network shall be protected using industry proven encryption and authentication mechanisms.

9.2.2 The encryption keys shall conform to industry standard encryption and authentication structures.

9.2.3 Network authentication process shall have the capability to revoke and renew certificates used to authenticate the connections between servers and client terminals.

9.2.4 A documented industry-accepted frequency of revocation and renewal is required to ensure that the keys cannot be compromised via an external source.

9.2.5 A source shall authenticate the destination as trusted and vice versa, before data can be transmitted across the network.

9.3 Loss of Communications

(Section 9.3.1 through 9.3.2 only applies to SBG)

9.3.1 A client terminal shall render itself unplayable if communications from the server is lost. If a game is in progress, a mechanism shall be provided to recover to the point of the game when communications was lost.

9.3.2 Communication loss shall be logged by the system in accordance to Section 6.

Ability of Transferring Player's Session to Another Client Terminal *(Section 9.3.3 through 9.3.7 only applies to SBG)*

9.3.3 In the case of client terminals that have lost communications with the server, the CSS shall provide means for patrons to cash out the remaining credits at the time the communications was lost.

9.3.4 The player's session is allowed to continue on another gaming client terminal that has the exact game configurations including the settings for base game, denomination and return-to-player percentages that was played previously on the original terminal. The new terminal shall place the game in the same state as it had been on the original terminal prior to the game's disruption.

9.3.5 The CSS shall ensure that all on screen meter readings relating to the player's session prior to the disruption shall be ported over accurately to the new terminal. Further game play will be updating the machine meters of the new terminal.

9.3.6 The transfer of a player's session shall not affect the balancing of meter readings of the original and new terminals, stored on the SMS.

9.3.7 The transfer of the session shall be recorded by the system in accordance to Section 6.

9.4 Communication with External Systems

9.4.1 CSS may only communicate with systems or programs external to the CSS system through a secure interface. This interface shall not allow any external connection to directly access the internal components, software or data of the CSS. The interface shall:-

a. be based on a specific defined protocol or a specific set of defined commands and as a result of these commands, retrieve information for an external request;

b. place data in an area segregated from the CSS software that is available to external requests or systems; and

c. be capable of supplying requested information while isolating the external request or system from the CSS internal components, software or data.

Communication of SBG Server with SMS *(Section 9.4.2 only applies to SBG)*

9.4.2 SBG server shall be capable of communicating with the SMS that is implemented by the casino operator(s).