STANDARD SERIES

GLI-16:

Cashless Systems in Casinos

Version: 2.0

Release Date: April 20, 2007

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International**, **Inc.** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, Inc. will provide a certificate of compliance along with an appropriate *Gaming Labs Certified*™ mark evidencing the certification to this Standard.

Cashless Systems in Casinos

GLI-16 Revision 2.0

Date Released: April 20, 2007 Version V2.0, *Final*
Date Released: June 30, 2006 Version V1.3, *Released for comment*
Date Released: February 7, 2002 *Final* Version V1.2
Date Released: December 7, 2001 *Draft* for Comment V1.1
Date Created: August 27, 2001 *Draft* for Comment V1.0

REVISION HISTORY

REV 2.0

Rev 1.3 *Final* was renamed to **Rev2.0** *Final* for document control purpose.

REV 1.3

1.1.1 Removed the disclaimer indicating that SmartCards are not authorized for use and are not addressed within this standard. See the new 3.2.7 rule.
3.1.4 Clarified meter requirements pertain to EGD and System. Added meters should be labeled in accordance to their function, they should be stored in units equal to the denom or dollars and cents and specified the required meters.
3.2.7 New section added which permits the use of Smart Cards provided the system validates the amount and player account information. Noted that Smart Card"technology implementation will be evaluated on a case-by-case basis.
3.2.8 Added a new rule requiring that the game or the interface element display to the player information stating that cashless transactions are unavailable when communications between the host and the client are lost.
3.2.9 Added a rule requiring encryption on all communication between the interface element and the backend system.
3.4.1 (c) Changed requirements regarding liability report.
3.6 Software Verification – this section was added to require that each component used in the Cashless System, that would affect the integrity of the system, have the ability to be verified by a third party verification tool.

REV 1.2

General grammatical changes.
1.3.4 Changed the reference to 'regulations' to 'standards'
2.3.2(g) Moved from 2.4.1(d) to here since this rule requires a connectivity manual since this is actually a Hardware requirement.
2.4.1(d) Moved to 2.3.2. This rule is now RESERVED.
2.6.2 Removed the reference to the firmware that is 'subsequently placed in the field' since this is a submission requirement.
3.1.1 Clarified that this section applies to gaming devices of a cashless environment.

3.1.3 Added clarification so the gaming device has the ability to recall the last 25 transactions.
3.1.3(d) Added to the requirement to provide audit trails for cashless transactions that included the players account to be either an account number or a unique transaction number to authenticate.
3.1.4(b) Removed the requirement that the meters be currency based
3.1.4(b)(i) Removed the reference to currency based because of the 3.1.4(b) change.
3.1.4(b)(ii) Removed the reference to currency based because of the 3.1.4(b) change.
3.1.4 NOTE Removed because of the 3.1.4(b) change.
3.1.5(d) Changed this section (transaction confirmation) to accommodate 3.1.3(d)
3.1.6(b)(i) Removed this section because it's now combined with 3.1.6(b)
3.1.6 Note removed this section because it's now combined with 3.1.6(b)
3.1.8 Modified the rule to specify on gaming machines an indication for non-participation in addition to the previous requirement for games that are participating.
3.2.4 Changed the security levels requirement to refer to the number of users since there will most likely be more than one.
3.2.6 Changed the diagnostic tests on a gaming device to report the activity to the system.
3.3.1 Central system audit trails was changed to be able to provide the 'pending' transactions in addition to the 'completed' transactions.
3.4.1(b) Removed the requirement for the system to produce an employee cashless account summary since this would be an Internal Control, not a technical standard.
3.5.1 Added an example to the security for the transactions to clarify a PIN or other means (ie. Fingerprint recognition). Also removed reference to 'currency based' because of the change to 3.1.4(b)

REV 1.1

*Several changes were made based on the TAM Conference held in Golden, Colorado on November 8 & 9 of 2001, where many regulators attended and supplied their comments.
1.1.1 Added further clarification on the definition of Cashless Systems.
1.3.4 Excluded Smart Card technology as being covered by this standard.
2.3.3 Removed reference to Section 6.2 since it doesn't exist.
3.1.1 Clarified that the Gaming Device/Card Reader requirements apply to those elements that the player interfaces directly.
3.1.2 Replaced the word 'had' with 'allows' to better clarify.
3.1.3 Clarified the last 25 transactions 'transmitted' to the host system. In addition, added the ability to have a 100-event log if a gaming device has promotional or host bonusing features enabled simultaneously with cashless features.
3.1.3(d) Added 'The player's account number' to be included with the transaction log.
3.1.4(b) Changed the rule to require the accounting meters to be currency based to avoid confusion.
3.1.4 NOTE This was removed because of the above change (3.1.4(b)). Added a new note that requires 'all accounting meters as mandated in GLI-11, as well as credit meter displays at the device, must be maintained in units. All currency based meters must be at least 10 digits, 8 digits dedicated to dollar value, and 2 digits dedicated to pennies.'
3.1.5 Transaction report was removed and replaced with Transaction Confirmation requirement that may use a display, a receipt of any method of notification at game centric level.
3.1.6 Restructured this area to include two subsections (host system and gaming device error conditions), Also, throughout this rule, removed the requirement to display to the patron for a transaction failure since this is covered in 3.1.5
3.17 Was "Diagnostic Tests on a Cashless Gaming Device" which was moved to 3.2.6. 3.17 is now the 'Full Transfer of all Transactions' rule.

3.2.1 Added requirement for the game and host to be secure enough so failure events can be identified and logged.
3.2.2 Added clarification that would require security of the patron information to be guaranteed at all times.
3.2.6 Added 'Diagnostic Tests on a Cashless Gaming Device' rule here. Was rule 3.17.
3.3.1(a) removed requirement that referenced GLI-11 device standards for the system log requirements. This was an error.
3.5.1 Indicated 'Currency Based' throughout this rule in conjunction with 3.1.4(b) change, above.
3.5.2 Same as 3.5.1, above.
3.5.6 Removed the requirement to display the transfer amount in the appropriate format since it will only be in terms of currency now with the 3.1.4(b) rule change.

Table of Contents

CHAPTER 1

1.0 OVERVIEW - STANDARDS FOR CASHLESS SYSTEMS IN CASINOS

1.1 Introduction

1.1.1 Cashless Systems Defined. Cashless systems allow players to play gaming devices through the use of a magnetic strip player card, which accesses a player's account at the host system in the casino. Funds may be added to this player cashless account via a cashier station or any supporting gaming machine (through the insertion of coins, ticket/vouchers, bills, and coupons). The account value can be reduced either through debit transactions, in smaller amounts at a gaming device or by cashing out at a cashier's cage. A Cashless system is characterized as a host system whereby a player maintains an electronic account on the Casino's host database. Usually a casino issues a patron a unique magnetic card and Personal Identification Number (PIN) in conjunction with a cashless account on the system's database, although any method of uniquely identifying patrons could be implemented. All monetary transactions between a supporting gaming machine and the host must be secured either by card insertion into a magnetic card reader attached to the host and PIN entry or by other protected means. After the player's identity is confirmed, the device may present transfer options to the patron on the LCD/VFD display of the card reader, which requires selection using a keypad/touchscreen before occurring. Such options would include how many credits they wish to "withdraw" and placed on the machine they are playing. Some systems may move either a predefined amount or the player's entire balance to the machine for play. Once play is complete the player may have the option to move some of the credits back to the player's account or cash out some credits. Other systems may require that the entire credit value be transferred back to the system.

It should be noted here, at the outset, that some readers may have heard the term "EFT," which stands for "Electronic Funds Transfer". While this term has been used in the gaming industry as a description for Cashless gaming, it is important to note that this document does not contemplate nor request opinions on transferring money from a credit card account or bank account (ATM) for use in gaming. The "account" as described here is an account set up at the local casino for the purpose of play at that casino. Players, casinos, and the system described here cannot access the banking system for any transaction contemplated.

NOTE: *"Smart Card" technology implementation will be evaluated on a case-by-case basis.*

1.1.2 Phases of Certification. The approval of a Cashless System shall be certified in two phases:

a) Initial laboratory testing where the laboratory will test the integrity of the system in conjunction with EGDs, in a laboratory setting with the equipment assembled; and
b) With on-site certification where the communications and set-up are tested on the casino floor prior to implementation.

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 RESERVED

1.3 Purpose of Standard

1.3.1 General Statement. The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying the Cashless System operation.
b) To only test those criteria which impact the credibility and integrity of gaming from both the revenue collection and game play point of view.

c) To create a standard that will insure that Cashless Systems in Casinos are fair, secure, and able to be audited and operated correctly.

d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to set their public policy with respect to gaming.

e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.

f) To construct a standard that can be easily changed or modified to allow for new technology.

g) To construct a standard that does not specify any particular technology, method, or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

1.3.2 No Limitation of Technology. One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes, and incorporate new minimum standards for the new technology.

1.3.3 Scope of Standard. This standard will only govern Cashless System requirements necessary to achieve certification when interfaced to electronic gaming devices (EGD), for the purpose of communicating mandatory security events and electronic meters. This infers that all relevant monetary transactions at the EGD level are handled through:

a) Credit Issuance. Electronic transfer through a secure communication protocol.

b) Credit Redemption. Electronic transfer through a secure communication protocol.

1.3.4 Exceptions to Standard. This standard does not govern Bonus or Promotional System requirements for any other form of electronic transaction.

Please refer to GLI-17 for Bonusing System and GLI-18 for Promotional System standards.

1.4 Other Documents That May Apply

1.4.1 General Statement. This standard covers the minimal requirements for Cashless Systems and all associated components. The following other standards may apply:

a) Gaming Devices in Casinos (GLI-11);
b) On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos (GLI-13); and
c) Individual Gaming Board Minimum Internal Control Procedures.

CHAPTER 2

2.0 SUBMISSION REQUIREMENTS

2.1 Introduction

2.1.1 General Statement. This chapter shall govern the types of information that are, or may be, required to be submitted by the submitting party in order to have equipment tested to this Standard. Where the information has not been submitted or is not otherwise in the possession of the test laboratory, the submitting party shall be asked to supply additional information. Failure to supply the information can result in denial, in whole or in part, of the submission and may lead to testing delays.

2.1.2 Previous Submission. Where the testing laboratory has been previously supplied with the information 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 at the testing laboratory. Every effort shall be made to reduce the redundancy of submission information.

2.2 Prototype (Full Submission) Submissions

2.2.1 General Statement. A Prototype (full submission) submission is a first-time submission of a particular piece of hardware or software that has not previously been reviewed by the test laboratory. For modifications of previous submissions, including required changes to previously submitted Prototype (full submission) certification, whether certified or pending certification, see 'Submissions of Modifications (partial submissions) to a Previously Certified Item,' Section 2.7.

***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. Regular upgrades normally preclude testing at the manufacturers' facility except in the case of prototype submissions.*

2.2.2 Submission Letter Requirements. Each submission shall include a request letter, on company letterhead, dated within one (1) week of the date the submission is received by the test laboratory. The letter should include the following:

a) The jurisdiction(s) for which you are requesting certification;
b) The 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.

2.3 System Hardware Submission Requirements – Prototype (Full Submission) Certification

2.3.1 Presentation of Equipment to the Test Laboratory; Identical Equipment. Each item of gaming equipment supplied by a manufacturer to the field 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, see also 'Submissions of Modifications (partial submissions) to a Previously Certified Item,' Section 2.7.

2.3.2 Inventory of Equipment to the Test Laboratory. Each submission of hardware shall contain the following:

a) Server, Database, Front End Controller, Data Collector, and Ancillary Stations to include but not limited to: Jackpot/Fill functionality; Surveillance/Security monitor functionality; EGD Management functionality; and Accounting/Reporting Functionality;
b) Monitors, keyboards, mouse, printers, etc., to support the items listed above;
c) Minimum of seven interface element devices with corresponding power connectors (if separate from harness), keypads, displays, and card reader (or equivalent if an alternative media is used);
d) Minimum of one wiring harness for each EGD type desired for operational approval with system where specific harnessing is required;
e) Minimum of two of each type magnetic cards (or equivalent if an alternative media is used) used in the system, if applicable;
f) Un-interruptible Power Supply (UPS) for critical components; and
g) If not included in the user manuals, a connectivity manual for all unique electronic gaming devices capable of being interfaced with system to include device model numbers and compatibility list, if applicable; wiring diagrams depicting connection points to devices, power, etc.; and identification by part number or some other scheme, any unique wiring harnesses, ancillary boards required for communication of a particular device.

***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.*

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

a) If applicable, all UL, CSA, EC, AS3100, etc. or equivalent certification. This certification information may be supplied at a later date;
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 specialized 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 specialized equipment and/or software and all appropriate operation and user manuals for the equipment and/or software shall be included with the submission.

NOTE: *Commercially available products are not required for submission unless omission will impact testing and proper operation of the system.*

2.4 System Software Submission Requirements – Prototype (Full Submission) Certification

2.4.1 General Statement. Each submission of software shall contain the following:

a) Two sets of all EPROMs, CD-ROMs, or other storage media which contain identical contents. This includes all program executables, system component firmware, bin files, etc. Where the test laboratory already has tested a software component, resubmission may not be necessary;
b) Source Code, a Link Map, and Symbol Table for all primary software executables. In addition, if requested, explanation of all non-volatile RAM on any system device with the non-volatile RAM locations described;

c) 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;
d) RESERVED;
e) 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;
f) If not included in the user manuals, a list of all supported communication protocols specifying version, if applicable;
g) If utilizing 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 for the intended application, rules for selection of algorithm coefficients or "seeds", and means of setting the algorithm coefficients or "seeds"; and
h) If completed by the manufacturer, provide a system test plan and results to detail electronic gaming devices and software versions tested with.

2.5 Software Programming Requirements and Compilation

2.5.1 ***General Statement***. The following items shall be contained within all submitted source code or related modules:

a) Module name;
b) Brief description of module function; and
c) Edit History, including who modified it, when, and why.

2.5.2 ***Source Code Commented***. All source code submitted shall be commented in an informative and useful manner.

2.5.3 Source Code Completeness. All source code submitted shall be correct, complete, and able to be compiled.

2.6 Program Identification

2.6.1 Software Requirements. On the primary system software components submitted and subsequently placed in the field, each program shall be uniquely identified and either display version information at all times or utilize a user accessible function.

2.6.2 Firmware Requirements. On the system firmware submitted, each program shall be uniquely identified, displaying:

a) Program ID ;
b) Manufacturer;
c) Version number;
d) Type and size of medium (requirement can be met by manufacturer stamp) ; and
e) Location of installation in interface element device, if potentially confusing.

NOTE*: For EPROM based firmware, the identification label shall be placed over the UV window to avoid erasing or alterating the program.*

2.7 Submissions of Modifications (Partial Submissions) to a Previously Certified Item

2.7.1 General Statement. For any update submission (e.g., a revision to an existing hardware or software that is currently under review, certified, or has been reviewed and not certified), the following information shall be required to process the submission in addition to the requirements set forth in 'Submission Letter Requirements', Section 2.2.2. All modifications require re-testing, examination, and re-certification by the test laboratory.

2.7.2 Modification of Hardware. Each hardware submission shall:

a) Identify the individual items being submitted (including part number);
b) Supply a complete set of schematics, diagrams, and data sheets, etc., describing the modification along with the reason for the change(s); and
c) Provide the updated or new hardware with a description and the method of connection to the original system or hardware components.

2.7.3 Modification of System Software Functions or to Correct Software Error. The submitter should use the same requirements as in the 'Software Submission Requirements – Prototype (Full Submission) Certification' Section listed above, except where the documentation has not changed. In this case, a resubmission of identical documents is not required. However, the submission must include a description of the software change(s) and modules affected and new source code for the entire program, if applicable.

2.7.4 Software Submission - Modification to Existing or Create New System Functionality. For a system specific submission (e.g., new workstation software), the following information may be required to process the submission:

a) If new, a complete description of the function, including amendment manual and user documents, and new source code if applicable; and
b) If modifying, the submission must include a description of the software change(s), modules affected and new source code, if applicable.

2.8 System Security Submission Requirements

2.8.1 General Statement. Where a system requires the use of defined user roles with associated passwords or PIN numbers, a default list of all users and passwords or PIN numbers must be submitted including a method to access the database.

2.9 Joint Venture Submissions

2.9.1 General Statement. A system is considered a joint venture when two or more companies are involved in the manufacturing of one system. Due to the increasing amount of joint venture submissions (more than one supplier involved in a product submission) and to alleviate any confusion to the suppliers, our regulator clients and GLI has set forth the following procedures for such submissions:

a) One company will prepare and submit the entire submission, even if they are using parts from other suppliers, and must identify all part numbers of all components. This will be the primary contact for the submission.
b) The company submitting an approval request should do so on their letterhead. GLI will delegate an internal file number in this company's name and will bill this company for all costs incurred throughout the approval process.
c) The primary contact will be called when questions arise. However, GLI engineers will work with all parties involved while completing the review.
d) All suppliers who are part of the submission "group" may need to be licensed in the jurisdiction(s) where the submission is being approved. As a courtesy to the supplier, GLI may inquire as to who does not need to be licensed from the regulator client. It should be noted that licensing questions should be handled directly with the jurisdiction.
e) Upon completion, it is the primary contact company that will receive the approval letter, provided the submission meets the jurisdictional requirements. The primary contact company may then release copies of the approval letter to the associated manufacturer(s).

CHAPTER 3

3.0 CASHLESS DEVICE AND SYSTEM REQUIREMENTS

3.1 Gaming Device/Card Reader Requirements

3.1.1 ***General Statement***. The requirements throughout this section apply to gaming devices of the cashless environment. These requirements are in addition to the requirements set forth in GLI-11 Gaming Devices in Casinos and GLI-13 On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos.

3.1.2 ***Configuring Cashless Transactions on a Gaming Device***. Since a Cashless feature would impact the electronic accounting meters, any gaming device that allows Cashless gaming as a selectable feature must conform to the 'Configuration Settings' requirements outlined within GLI-11 Gaming Devices in Casinos, Section 3.13.4.

3.1.3 ***Audit Trails for Cashless Transactions***. Cashless Gaming Devices must have the ability to recall the last twenty-five (25) monetary transactions received from the host system and the last twenty-five (25) monetary transactions transmitted to the host system. However, if a gaming device has promotional or host-bonusing features, or both, enabled simultaneously with cashless features, a single 100-event log would suffice. The following information must be displayed:

a) The type of transaction (upload/download);

b) The transaction value;

c) The time and date; and

d) The player's account number or a unique Transaction Number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to).

3.1.4 Meter Requirements for Cashless Gaming Devices and Systems. Cashless gaming devices and cashless host systems must incorporate electronic accounting meters that conform to the following electronic metering requirements:

a) The operation of the mandatory electronic accounting meters, as mandated in GLI-11, must not be impacted directly for Cashless type transactions;

b) Specific Cashless electronic accounting meters shall exist which should increment to indicate:

i. electronic credits received from the central system---downloaded to game from host.

ii. electronic credits transmitted to the central system---uploaded from game to host.

c) Meters shall be labeled so they can be clearly understood in accordance with their function.

d) The following Cashless meter information shall stored in units equal to the denomination of the device or in dollars and cents:

i. Electronic Funds Transfer In* (EFT In). The machine must have a meter that accumulates the total value of cashable credits electronically transferred from an MCS to the machine when using EFT commands in the function of bonusing, promotions or cashless wagering.

ii. Cashless Account Transfer In* (AFT In). (A.K.A. WAT In-Wagering Account Transfer In) The machine must have a meter that accumulates the total value of cashable credits electronically transferred to the machine from a wagering account by means of an external connection between the machine and a cashless wagering system;

iii. Cashless Account Transfer Out* (AFT Out). (A.K.A. WAT Out-Wagering Account Transfer Out) The machine must have a meter that accumulates the total value of cashable credits electronically transferred from the machine to a wagering account by means of an external connection between the machine and a cashless wagering system;

3.1.5 ***Transaction Confirmation***. The gaming device or host card reader display must be capable of providing confirmation/denial of every cashless transaction initiated. This confirmation/denial must include:

a) The type of transaction (upload/download);

b) The transaction value;

c) The time and date (if printed confirmation);

d) The player's account number or a unique Transaction Number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to) [if printed confirmation]; and

e) A descriptive message as to why the transaction did not complete as initiated. This applies only to the denied transactions.

3.1.6 ***Error Conditions***. The following sections outline the Error Conditions that apply to the:

a) Host System. The following conditions must be monitored, and a message must be displayed to the patron at the host card reader for the following:
   i. invalid PIN or Player ID (Can Prompt for Re-entry up to maximum allowed); and
   ii. account unknown.

b) Gaming Device. Any credits on the gaming device that are attempted to be transferred to the host system that result in a communication failure for which this is the only available payout medium (the patron cannot cashout via hopper or ticket/voucher printer), must result in a hand-pay lockup or tilt on the gaming device.

3.1.7 ***Transfer of Transactions***. If a player initiates a cashless transaction and that transaction would exceed game configured limits (i.e. the credit limit, etc) then this transaction may only be processed provided that the patron is clearly notified that he has received or deposited less than requested to avoid patron disputes.

3.1.8 Identifying a Cashless Device. A patron should be able to identify each Cashless compatible machine by a means left to the discretion of the individual jurisdiction (e.g. remove display menu items that pertain to Cashless operation for gaming machines not participating; provide a host message indicating Cashless capability; or a specific sticker on gaming machines to indicate participation or non-participation).

3.2 Central System Security Requirements

3.2.1 General Statement. The rules within this section shall be implemented by the host system to allow for changing of any of the associated parameters or accessing any patron account. Additionally, the communication process used by the gaming device and the host system must be robust and stable enough to secure each cashless transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation.

3.2.2 Modification of Patron Information. An authorized, logged employee shall only change all player information. Security of this information (including patron PIN codes or equivalent patron identification) must be guaranteed at all times.

3.2.3 Balance Adjustments. Any adjustment to an account balance outside of the normal methodology would require a supervisor's approval with all changes being logged and/or reported indicating who, what, when, and the item value before and after the change, with the reason.

3.2.4 Security Levels. The number of users that have the requisite permission levels/login to adjust critical parameters are limited.

3.2.5 Prevention of Unauthorized Transactions. The following minimal controls shall be implemented by the host system to ensure that games are prevented from responding to commands for crediting outside of properly authorized Cashless transactions (hacking):

a) The network hubs are secured (either in a locked/monitored room or area) and no access is allowed on any node without valid login and password;
b) The number of stations where critical Cashless applications or associated databases could be accessed is limited; and
c) Procedures shall be in place on the system to identify and flag suspect player and employee accounts to prevent their unauthorized use to include:
    i. having a maximum number of incorrect PIN entries before account lockout;
    ii. flagging of "hot" accounts where cards have been stolen;
    iii. invalidating accounts and transferring balances into a new account; and
    iv. establishing limits for maximum Cashless activity in and out as a global or individual variable to preclude money laundering.

3.2.6 Diagnostic Tests on a Cashless Gaming Device. Controls must be in place for any diagnostic functionality available at the device such that all activity must be reported to the system that would reflect the specific account(s) and the individual(s) tasked to perform these diagnostics. This would allow all Cashless diagnostic activity that affect the gaming device's associated electronic meters to be audited by the local regulatory group.

3.2.7 Smart Card Technology. It is permissible for systems to allow player's to access their accounts using "Smart Card" technology where the account information, including the current balance, is maintained in the host system's database. Some "Smart Cards" have the ability to maintain a player account balance. This method of technology is only permissible when host system validates that the amount on the card is in agreement with the amount stored within the system's database

NOTE: *"Smart Card" technology implementation will be evaluated on a case-by-case basis.*

3.2.8 Loss of Communication If communication between the Cashless accounting system and the gaming device is lost, the game or interface element must display a message to the player that cashless transfers cannot currently be processed.

3.2.9 Encryption All data transmitted to and from the gaming device must employ some form of encryption. This does not apply to communication between the gaming device and the interface element

3.3 Central System Audit Trails

3.3.1 General Statement. The central system shall have the ability to produce logs for all pending and completed Cashless transactions. These logs shall:

a) RESERVED
b) Be capable of being filtered by:
   i. machine number
   ii. patron account; and
   iii. time/date.

3.4 Financial and Player Reports

3.4.1 General Statement. The system shall have the ability to produce the following financial and player reports:

a) Patron Account Summary and Detail Reports. These reports shall be immediately available to a patron upon request. These reports shall include beginning and ending account balance, transaction information depicting gaming machine number, amount, and date/time.
b) RESERVED;
c) Liability Report. This report is to include previous days ending value (today's starting value) of outstanding Cashless liability, Total Cashless-in and Total Cashless out and the current day's ending Cashless liability.
d) Cashless Meter Reconciliation Summary and Detail Reports. These reports will reconcile each participating gaming device's Cashless meter(s) against the host system's Cashless activity.

e) Cashier Summary and Detail Reports. To include patron account, buy-ins and cash-out, amount of transaction, date and time of transaction.

3.5 Player Accounts

3.5.1 ***General Statement***. All monetary transactions between a supporting gaming machine and the host must be secured either by card insertion into a magnetic card reader attached to the host and PIN entry or by other protected means (e.g. finger-print recognition). After the player's identity is confirmed, the device may present transfer options to the patron on the LCD/VFD display of the card reader, which requires selection using a keypad/touchscreen before occurring. Such options would include how many credits the player wishes to "withdraw" and be placed on the machine. Some systems may move the entire player's balance to the machine for play. Once play is complete the player may have the option to move some of the credits back to the account or cash out. Other systems may require that the entire currency value of the credit balance be transferred back to the system.

3.5.2 ***Adding Money to a Players Account***. Money may be added to this account via a cashier station or any system-controlled kiosk, assuming that such kiosk has been approved. Money may also be added by any supporting gaming device (through credits won, the insertion of coins, ticket/vouchers, bills, coupons, etc.)

3.5.3 ***Removing Money from a Players Account***. Money may be removed from this account either through downloading of credits (currency based) to the gaming device or by cashing out at a cashier's cage.

3.5.4 ***Movement of Money***. Players may also be afforded the option of moving some of their system credit to the gaming device they are playing through "withdrawal" from the player's account, which is maintained by the system. When they are finished playing, they can "deposit" their balance from the machine onto their player account. Cashless gaming transactions are entirely electronic.

3.5.5 Personal Identification Number. Usually a casino issues a patron a unique magnetic card and personal identification number (PIN) in conjunction with an account on the system's database, although any method of uniquely identifying patrons could be implemented.

3.5.6 Account Balance. Current account balance information should be available on demand from any participating gaming device via the associated card reader (or equivalent) after confirmation of patron identity and be presented, in terms of currency, to the patron.

3.6 Software Verification

3.6.1 General Statement. Each component within the System, that would affect the integrity of the System, must have the ability to allow for an independent integrity check of the component's software that is critical to its operation, from an outside source. This must be accomplished by being authenticated by a third-party device, which may be embedded within the component's software (see NOTE within this section, below) or having an interface port for a third-party device to authenticate the media. This integrity check will provide a means for field testing the software to identify and validate the program. The test laboratory, prior to system and/or component approval, shall approve the integrity check method.

NOTE: If the authentication program is contained within the software, the manufacturer must receive written approval from the test laboratory prior to submission.