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

Office of Liquor Gaming and Regulation
Electronic Seal Minimum Requirements

Version 1.1

Toward Tomorrow's Queensland

Queensland Government

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

Contents

1 Introduction

Policy

This document is released to the public for discussion and comment before becoming policy.

Purpose

This document proposes the minimum requirements and methods for the implementation of an "Electronic Seal" for use with sealed computer devices such as Electronic Gaming Machines (EGMs), Jackpot Triggering Devices and any computer controlled devices where a high degree of physical security is required.

Applicability

These requirements may require some cost to be implemented initially and thus should only be enforced where appropriate. It is proposed any Device would be eligible to meet these requirements which is responsible for items such as jackpots which could exceed the value of $60,000 for any single prize and where the Device is located in an insecure remote area such as the premises of a club/hotel. These requirements would also be applicable to Devices that have remote upgrade capability (ie. where the Device's software can be upgraded without accessing its physical program storage devices).

Abbreviations & Glossary

Device	Refers to the device being sealed for which these requirements apply. Usually this is an EGM or a Jackpot Triggering Device.
EGM	Electronic Gaming Machine.
MAC	Message Authentication Code
PSD	Program Storage Device
UPS	Un-interruptable Power Supply

2 Backgound

In the area of sealing, the main objective is to protect the integrity of the Device's program and NV-RAM data from unauthorised alteration. In EGMs, two existing methods are used to achieve this goal, the physical sealing of the EGM's processor cabinet and the power off processor door monitoring of this cabinet.

Physical seals suffer from the drawback that they have to be regularly physically inspected to ensure the integrity of the Device. In theory the device can only be trusted while the device's seal is currently being inspected.

The second method currently in use is the power off door monitoring of the EGM's security cabinet. This method has the one disadvantage in that the Device does not report the access until after the access has taken place.

The Electronic Seal methodology defined in this document is an improvement on the power off door monitoring method. It allows secure remote detection of access to the EGM's sealed cabinet

and eliminates the need for regular inspections or even the presence of a physical seal. Note however, physical seals also remain a part of this method as an additional physical deterrent to tampering or opening the secured cabinet, especially if locks are not used.

These technical requirements will also assist in the introduction of new applications that require greater security, such as remote downloads and message authentication (eg. of jackpot events).

3 Overview

The new Electronic Seal works in the same way a physical seal operates, in that when access is obtained, something is irrecoverably destroyed in the process. In the case of a physical seal, the seal is destroyed, in the case of the Electronic Seal, a private encryption key is destroyed.

The Electronic Seal's private encryption key stored by the Device in a special area of NV-RAM.

The Device must monitor for access to the sealed/locked compartment with or without mains power connected, similar the existing power off door monitoring except for the following additional behaviour:-

Upon any detected access to the sealed compartment of the Device, the Device must automatically and immediately erase or destroy the private encryption key. This must occur without destroying any other NV-RAM data except for the private encryption key. The irrecoverable loss of the Device's private key means it will no longer be able to successfully authenticate itself to parent devices, thus ensuring evidence of the access cannot be covered up. The same key once erased is not recoverable, except by chance, which would be highly improbable.

The Electronic Seal may be verified remotely at any time (the Device must be connected to a network or have some method of communication). To do this, the device would send a message upon request (usually containing some form of a random data and the date and time) which contains a MAC generated from the Device's private key. The message can then be authenticated using the Device's public key stored in a database in the host system. If the MAC authenticates on the message then the Electronic Seal may be assumed to be intact. If the MAC fails then it must be assumed the device's security cabinet has been accessed and the device will have to be recommissioned. In simple cases of legitimate cabinet access, the Device will simply report the access as normal, which also will indicate the Device needs to be recommissioned with a new private key.

The Device may also use its private key to sign important messages such as large jackpot hit events.

4 Software Requirements

- a public key encryption algorithm (Recommend RSA, Patent has now expired and there are plenty of libraries implementing RSA available).
- a digital signature (one-way hash) algorithm (Recommend MD5, strong, readily available)
- a strong RNG algorithm for the generation of the private key.
- a strong random number seeding methodology.

5 Hardware Requirements

Sealable compartment.

The Device must have a physically sealable or lockable compartment which houses the Program Storage Devices (PSDs), the CPU, NV-RAM and encryption keys. The compartment must only have one door and the compartment must not be able to be removed from the overall Device without having to first open the door. Ideally, the compartment should have no holes or line of sight via any ventilation holes to the interior of the compartment.

The compartment must carry a warning label that states “No Unauthorised Access” or the equivalent.

Sealed compartment access detection circuit.

The Device must be able to detect access to the internals of the secure compartment of the Device. The detection mechanism must operate with or without power applied to the Device. Using a rechargeable battery to power the detection circuitry is acceptable so long as if the battery fails with mains power connected, the Device immediately assumes it has been accessed. The detection circuit must be able to operate without mains power for at least 3 months.

The detection circuit/switch must be highly resistant to hot-wiring or mechanical tampering from all areas external to the compartment, as this is the weakest point of the Electronic Seal. Careful consideration must be given to the routing of cables and the locations of sensors. For example, use a single pole double throw switch and put sensors on both the normally on and normally off sides. Combine this with light sensitive switches. Be creative, the harder the circuit is to defeat, the higher the money/prizes the Device will be approved for.

The circuit must be easily testable on the Device prior sealing.

Special NV-RAM reserved for private key.

A special NV-RAM to store the device’s private key, 2-8k bytes should be sufficient. Copying the key to other areas of NV-RAM must be avoided. Copying the key to volatile RAM for use is acceptable.

The private encryption key must be stored securely only in the device’s NV-RAM and must not be able to be compromised without first destroying it or causing significant permanent, un-concealable physical damage to the Device. In assessing this requirement a cost/benefit analysis will be applied.

If power is disrupted in any way to the monitoring circuit (even a spike causing a reset or watchdog timeout) or access to the sealed compartment of the Device is detected, then the private key is to be destroyed immediately. Thus must take no longer than 10 milliseconds.

If the Device does not run off an U.P.S. then an additional mini CPU may be required to implement these requirements (For example, a PIC which performs the cabinet door monitoring, key storage, transfers and erasures).

To avoid unnecessary and costly Device recommissioning, ensure the circuit is highly immune to ESD and EMF.

Communications.

The device needs a method of communication such as a network for remote seal authentication. A VDU could be used to verify the Electronic Seal locally on the Device.

6 Typical Device Commissioning procedure

This procedure is performed once per RAM clear of the Device or whenever sealed cabinet access detection erases private key.

Device commissioning must be undertaken by a trusted third party, preferably a QOGR inspector at the operator's expense. The trusted third party follows a detailed checklist to perform this procedure.

If not already cleared, the Device is RAM cleared according to procedure.

The Device's processor p.c.b. is inspected as follows. The Program Storage Devices (PSDs) are confirmed to be of the right number, the correct type/size (PSD labels must not cover PSD type information) and have the correct digital signature (or preferably a bit per bit comparison). All PSDs must be easily removable for isolated verification.

The Device's securable processor cabinet is inspected for integrity.

The Device must allow its processor cabinet access/tamper detection circuitry to be tested at commissioning to be in working order before finally closing & sealing.

If everything is acceptable, the Device is sealed and the seal number/ID noted and signed off by the inspector. (Note, physical seals and seal registries are not critical to the Electronic Seal, a simple lockable cabinet is also acceptable, so long as there is some physical deterrent to opening the secured cabinet of the Device)

Once sealing is complete the inspector will enter/transmit the following information:-

- A serial number for identification purposes. Once entered, the serial number cannot be changed without re-commissioning the Device.
- Various public keys. Ie. For the QOGR and Device manufacturer. They are subsequently used for applications such as remote software upgrades of the Device. It should be possible to change a public key in the device once set by using two public keys for each party. One for general use and one reserved solely to change keys.

The Device will then seed its RNG using an approved method and then randomly select a public/private key pair for itself. The seeding methodology must use at least three reasonable random sources XOR'ed together. For example; the current time, the time between activation of an input (eg. keyboard), the time since last power down, a randomly entered/received number, and so on.

The Device's public keys may be retrieved upon request at any time and are recorded. Note keys should never be transferred by hand at any time to avoid errors.

The Device is now ready for operation and will use its private key to authenticate itself to the system and send authenticated messages as necessary. This would be required at least whenever the Device connects to the host system each session, or to digitally sign large win jackpot events and meters as required.

Any subsequent access to the Device's sealed cabinet would require the Device to be re-commissioned due to the corresponding erasure of the private key.

7 Risks and Threats

- Defeat the physical security of the Device. Highest risk, a cost benefit analysis would determine if the physical security is adequate.

  Assuming full knowledge, the cost of defeating the Electronic Seal, comes down to the cost of defeating the physical access detection switch on the secured cabinet. However, a little effort in protecting the switch and cable from being hot-wired can make this type of attack extremely difficult and costly

- It is possible the private key could be defeated using a cryptographic attack, but if a well proven algorithm and key length is used then this remains too costly to consider defeating the system in this way.
- Weak key seeding method is used. Low risk.
- Trojan horse in placed in software. Medium risk, reduced by the fact that source code is also monitored by the QOGR well as the JS developers
- Assumption. Commissioning personnel are trusted.

8 Revision History

Version	Changes	QIR	Who	Release Date	Incept Date
1.0	Appendix A from the 'Jackpot System Minimum Requirements' was extracted and became this document.		RLL	11/9/2001	NA
1.1	Updated to DEEDI report template		RLL	20/8/2010	