Office of Liquor and Gaming Regulation

Hashing Algorithms

Version 1.7

Queensland Government

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

Contents

1 Introduction

Policy

The Office of Liquor Gaming and Regulation (OLGR) has a policy for a wide range of regulated gaming equipment in Queensland, such as gaming machines, jackpot systems and other regulated gaming systems in general that they be able to produce a hash, or fingerprint of their software or firmware for verification and auditing purposes using an acceptable hashing algorithm.

Hashing algorithms are also used extensively by OLGR throughout the submission and approval process and for auditing purposes.

Purpose

The purpose of this document is to list the acceptable hashing algorithms for use with OLGR technical requirements documents. For example:

- OLGR EGM Communications Protocol (QCOM v1.x)
- Program Storage Device Verification minimum requirements.
- Jackpot System Minimum Requirements.
- Submission Requirements.
- System Auditing.

Scope

This document is applicable to all organisations designing regulated gaming equipment, systems, or software to any of OLGR's technical requirements documents, or submitting software to OLGR.

Please refer to the revision history for incept dates of each release of this document.

2 General

2.1 List of acceptable hash algorithms for new gaming equipment and systems:

1. SHA-256

This algorithm is the current algorithm for all digital verification, auditing, submission and approvals to OLGR where HMAC-SHA (see below) is not being used.

2. HMAC-SHA-256

HMAC-SHA is the seeded version of the used SHA-256 algorithm.

Notes:

- Industry recognised and endorsed algorithms considered better than those listed above may be used provided OLGR raises no objections. (OLGR typically just needs to be certain it can support the intended algorithm in the context in which it is used, if applicable.)
- Algorithms like 16 & 32 bit CRCs and weak hashing algorithms such as MD5 and SHA-1, may still be utilised for purely error checking applications, for example CRCs in communications protocols and data integrity checks. If a particular application of a hashing algorithm has any aspect relating to security, then SHA-256 or better algorithm must be used.
- QCOM protocol v1.x gaming machines must continue to use the SHA-1 algorithm.

3 Regulated Gaming Equipment

This section applies to regulated gaming equipment, such as Gaming Machines and Jackpot Triggering Devices etc. that are required to produce a 'program hash'. The remainder of the document will refer to them simply as a '**Device'**. However where required, particular reference is made to Gaming Machines and the QCOM v1.x Protocol.

3.1 Data that must be included in an overall Device program hash.

The program hash calculation must encompass all data stored within the Device for which it is physically possible to be executed by the Device's CPU/s (regardless of whether or not this is normally done by the device during operation). "CPU" refers to the CPU(s) & micro-controllers (including FPGAs & CPLDs) which may control, or could potentially affect play/gamble outcomes and critical meters or areas, or data which is considered a significant integrity or security risk by the regulator. This also includes data which can be loaded and executed from Device RAM.

At this time this does not include peripheral device programs such as banknote or coin acceptor program data, or configuration data which may change on a day to day basis.

If unsure of whether to include a Program Storage Device into the hash calculation, then either include it by default, or check with OLGR.

Acceptance of the data and device set to be included in the hash calculation is at the discretion of the Executive Director of OLGR.

With the increased use of new devices containing file systems, such as flash chips, the above requirement may not be suitable in all cases. If a storage device has a file system then it is acceptable for the hash calculation to encompass only the file data on the device.

Also, to expedite hash calculations with regards to QCOM v1.x Gaming Machines, sound and graphics data may be exempted from direct inclusion in the hash calculation. This exemption may be granted provided the following conditions are met:

1. A non-seeded hash result of the excluded sound and graphics data must be hard coded in the data region that is contained in the hash calculation.

2. The sound and graphics data must be verified against this hard coded hash result at least every time the CPU is reset.

3. OLGR is provided with a method of verifying that the hash of the sound and graphics in source code is identical to the hard coded value.

3.2 Unused space on storage devices.

Unused space does not need to be included in the program hash calculation.

Clarifications:

- Empty tables such as unused jump table entries or similar, must not be considered as unused space.

3.3 Devices / applications where an overall single hash result is required.

For example, the QCOM v1.x protocol requires gaming machines to produce a single overall hash result.

For devices where multiple hash results are inherent and where an overall single hash result is also required, permissible options to give a single hash result are:

- Perform the hashing sequentially in a deterministic order as if it were a single combined block of data.
- XOR combination of hash results. (This option is permissible only for QCOM v1.x gaming machines)

Except for QCOM v1.x gaming machines, a device must never combine multiple hash results via modulo 2 addition (XOR).

4 Submission requirements regarding program hashes

4.1 OLGR must be supplied with exact details of how the Device performs the hash over its software/firmware.

4.2 For QCOM v1.x gaming machines, a utility program and/or procedure must also be provided where required, that converts the Device's object code into one or more files, in such a way so that if a byte order hash over those files is performed, then the combined result (via XOR if necessary) would yield the same result as the Device's program hash calculation. (These files are required for upload onto the OLGR program hash server which generates hashes for use with QCOM and system audits.)

5 Revision History

Version	Changes	QIR	Who	Release Date	Incept Date
1.0	Initial Release		RL	30/05/1997	
1.1	• Fixed up copyright notice as per policy • Added additional PSA examples • Minor clarifications elsewhere, refer redline etc		RL	29/01/1998	
1.2	• Converted to Word • Document is to be generally released • Made general clarifications prior public release of this document		RL	12/02/2001	
1.3	• General review • Added option on request to remove direct inclusion of sound and graphic data from the overall signature result		RL	28/06/2004	
1.4	• Deleted all references to PSA16 (never utilised) • Added new Program Signature Algorithm for use with QCOM version 1.6.x. Namely HMAC-SHA		RL	19/10/2004	
1.5	• Draft release 11 April 2008 • Yearly review (QIR 626) removed references to EGMs, made more generic, removed references to 'signatures', implemented standard Min.Req template, clarified section on 'What data must be included in the overall Device program hash?'	626	RL	01/05/2008	
1.6	• Updated to new DEEDI report document template • QOGR->OLGR		RL	20/8/2010	
1.6.1	• Updated to new DJAG report document template		JG	12/4/16	
1.7 draft	• Updated to docx format. • Updated copyright notice to 2019 and scope. • Updated re SHA-256. • Made all QCOM references specific to QCOM v1.x. • Removed section on examples – no longer needed.		RL	8-Apr-19	
1.7	• QCOM v1 machines must still use sha-1		RL	17-Jun-19	See below
Incept notes:					

All new products submitted for approval to OLGR must use SHA-1 in security related operations within **1 year** from the above date.

The SHA-1 QCOM protocol program hash will unlikely never be updated to mandate SHA-256 as the specification is close to retirement. FYI; QCOM 3 already mandates SHA-256.

As for all other existing uses of SHA-1 by approved gaming equipment (including EGMs), developers should start using SHA-256 in all security related roles in all newly developed code asap.

As for existing / ongoing uses SHA-1 in approved gaming equipment: developers should start updating *long-term-supported* code to SHA-256 as convenient with an aim to finish this process within **2 years**. However if a product is due to be retired before or shortly after this period, then check with OLGR for a possible dispensation.

In systems where there are many discrete physical devices to update. If a system wide update is not possible without having to physically visit or manually update every single discrete physical device, then unless the level of operating risk is high, it may be acceptable to take an attrition based approach to upgrading. Contact the OLGR in this case to discuss.

In all cases, each licensee of approved gaming products in QLD must contact the OLGR for confirmation and agreement in relation to the ongoing use of SHA-1 in approved gaming equipment.

Incept date: Where not stated otherwise the incept date for new or changed minimum requirements in this version of the document is 6 months from the release date of the document in all new submissions to OLGR.