Witness Build Guidelines

Version 1.3 (draft)

Contents

Introduction

Policy

For evaluations of equipment where source code is required, it is standard practice to confirm that the source code reconciles with the submitted object code via the building/compilation of the source code. Preferably the process of building a submission from source is performed at the premises of the tester using a trusted hardware and software environment, but under some circumstances this is not practical for the applicant, e.g. licensing costs.

In these cases, the tester and applicant will collaborate to perform a onetime build of the source code. The output of this build, along with the source code will form part of the submission. Alternatively, a tester monitors and verifies the build process conducted from a different location, only if approved by the regulator.

This has generally become known as a 'Witness Build' and this term will be used throughout the document.

Witness builds are charged at the relevant evaluation fee of the tester. Travel/accommodation costs will also be charged where applicable.

Applicants should take into account the frequency multiplied by the cost of witness builds in comparison to the cost of providing another development environment before deciding to propose a witness build.

For high-risk products or environments, witness builds may not be an option. This is at the discretion of the regulator.

Purpose

The purpose of this document is to:

- Advise the industry of the Office of Liquor and Gaming Regulation (OLGR) position on witness builds.
- Ensure approaches to witness builds are consistently applied.
- Achieve an equitable standard of integrity for equipment being witness built with respect to risk.

Scope

This document is of most interest to testing facilities and applicants who submit equipment to OLGR for evaluation and approval under the following legislation:

- Casino Control Act
- Charitable and Non-Profit Gaming Act
- Gaming Machine Act (excluding electronic gaming machines. Refer to ANZ GMNS Rev11 or later)
- Keno Act
- Liquor Act
- Lotteries Act
- Wagering Act

Prerequisites

This document assumes the reader has an IT background with previous experience in building software.

Glossary

Term	Definition
Development Environment	Refers to the necessary compiler software and tools needed in order to build/compile the source code and verify it with the submitted object code.
OS	Operating System
Reproducible builds	Also known as deterministic compilation, is a process of compiling software which ensures the resulting binary code can be reproduced. Source code compiled using deterministic compilation will always output the same binary.
ANZ GMNS	Australian/New Zealand Gaming Machine National Standard
Remote Witness Build	A process in which the compilation of software is witnessed by the tester from a different location rather than being physically present at the build site. This approach allows for real-time oversight and validation of the build process through the use of video conferencing, screen sharing or other remote communication tools, ensuring that agreed procedures are adhered.
Compile	Also referred to as building, is a process of translating source code written in a high-level programming language into a low-level language e.g. assembly language, object code, or machine code to create an executable program.

Witness build guidelines

Pre-build preparation

Applicants seeking equipment approval under the Acts mentioned above should be mindful of the requirement pertaining to the verification of source code with object code and therefore at the very early product stages, utilise a development environment that facilitates:

1. Reproducible and verifiable builds
2. The ability for the development environment to be authenticated and trusted with respect to associated risk of the target gaming equipment in operation.

The procedure for the witness build must be agreed upon by the regulator (or other delegated authority) to ensure that it contains enough security/integrity to offset risk, including whether a build can be witnessed remotely. Remote witness builds will be considered only on a case-by-case basis and will require additional controls as determined by the regulator.

Initially, the storage media on the computer used for the witness build at the applicant's premises should be erased (no OS installed) and the computer should not be on a network.

Build procedure guidelines

The OS and development environment should be installed from media for which its authenticity has been verified (e.g., publicly available disk images). In other cases (such as the development environment) the installation media can be hashed and verified from the website of the product provider. The same applies to the necessary patches needed of the OS and development environment. To save time, all necessary software and patches should be downloaded and submitted in advance, as much as possible, before the scheduled build day. In high-risk environments, a demonstration of the build process must first occur prior to the scheduled build day. This rehearsal must result in no issues related to building and verification of the software.

The source code, build scripts, etc. should be loaded onto the development environment for building/compilation from the source media that was submitted to the tester or utilise a strict version control practice that ensures the exact source code used in the build is preserved and unaltered.

This ensures that:

1. The submission is complete and able to be completely built from the submission material and,
2. It saves having to do hashing or comparisons of the source code.

Additional Considerations for the Build Procedure

1. Any additional source code or software required during the build procedure must be installed and authenticated against a trusted source before use. All dependencies must be locked to a specific version to ensure consistency and security.

2. In general, the build environment must be isolated to minimise external factors that could cause variability. The use of containers, virtual machines or dedicated build systems is highly recommended.

3. The build PC should be locked/secured by the tester if it is to be left unattended by the tester/s at any time during the witness build e.g., removing the hard drive, sealing the build PC and locking the screen within the booted OS (provided the tester is the only user with admin rights).

4. For reproducible builds, the object code should be securely reconciled against the object code on the previously submitted submission material. E.g., direct comparison or via the use of a secure hashing algorithm. Otherwise, for a non-reproducible build: a secure hash of the object code is to be generated and a copy of the object code is to be made immediately and stored securely along with all logging information generated by the build system.

5. Once a build is completed, the tester digitally signs the build artifacts to certify that they were created by an authorised entity and have not been tampered with since their creation.

6. The software that is compiled during the witness build is the version that will be evaluated by the tester and must be the software deployed to production following necessary approvals by the regulator.

Remote Witness builds

A request for a remote witness build must be first made to the regulator.

A proposal for a remote witness builds must demonstrate that the process is secure, reliable, and auditable. It must be achieved through:

1. End to end encryption for data transmission between the observer and the remote build environment.

2. Implement strict access controls to the build environment, such as multi-factor authentication and/or secure (SSH) keys.

3. Video streams that are being monitored by an observer must be demonstrated to be real-time and not previously recorded.

4. Sufficient evidence must be recorded to reconcile all actions undertaken during the build.

5. Any additional measures deemed appropriate by the regulator.

Witness Build Checklist v1.1

(This checklist template must be completed in full and submitted for each witness build)

Product Name		Remote Witness Build	☐ YES ☐ NO
Product Version		Date	
Location			
Build Environment and Version			
Development Environment and Version			

Check	Pass	Not Done / Not Applicable	Reasons for Not Done / Not Applicable
OS installation media authenticated	☐	☐	
Install OS	☐	☐	
OS patches authenticated	☐	☐	
Patch OS as required	☐	☐	
Development environment installation media authenticated	☐	☐	
Install development environment	☐	☐	
Development environment patches authenticated	☐	☐	
Patch development environment	☐	☐	
Other tools installation media authenticated (state versions below)	☐	☐	
Install other tools	☐	☐	
Initial State of the Build Environment	☐	☐	
Build source code	☐	☐	
Hash build output	☐	☐	
Attach the approved witness build procedure that was followed and build logs	☐	☐	
If the build was witnessed remotely, ensure all relevant evidence (e.g., video recordings, screenshots, logs etc) has been submitted	☐	☐	

(changes shown and initialed if there where deviations from expected procedure)

Any additional steps undertaken not mentioned in the witness build procedure should be summarised here:	
Representative/s for Applicant (please print name, sign and date):	
	___/___/_____
Representative/s for Testers/Witnesses (please sign and date):	
	___/___/_____

Revision history

Release date	Summary of Amendments	Version	Inception Date
9/9/2009	Initial release	1.0	Immediate
20/8/2010	Updated to DEEDI template	1.1	Immediate
31/5/2016	Updated to JAG template	1.1.1	Immediate
14/12/2021	• Updated to latest JAG template • Changed repeatable for reproducible • Updated example for OS • Updated glossary • Updated scope • Updated policy • Removed references to gaming	1.2	Immediate
TBA (draft)	• Updated to latest JAG template • Updated policy • Updated glossary • Refined phrasing of various sections • Updated build procedure guideline • Updated to include remote witness builds • Updated checklist (version 1.1) and required to be completed in full and submitted for each witness build	1.3	Immediate