Nº	Description	Details
3.	Source code review	The source code review verified that the implementation of the RNG is in accordance with the technical requirements. This includes, but is not limited to: a) Identification of algorithm; b) Security of internal state, seeding and re-seeding, thread safety; c) Shuffling for card games.
4.	Statistical tests	The statistical tests undertaken by iTech Labs are: a) Diehard tests b) Chi-square tests
5.	Theoretical basis of algorithm and supporting crypto-analysis evidence	Literature is readily available, describing the theoretical basis of the algorithm (refer to Section 2.2) https://www.schneier.com/cryptography/paperfiles/fortuna.pdf https://en.wikipedia.org/wiki/Fortuna_%28PRNG%29 Fortuna is an algorithm devised by Bruce Schneier and Niels Ferguson and published in the book Practical Cryptography in 2003. It is classified as a Cryptographically Secure Pseudo Random Number Generator (CSPRNG), and is considered to possess adequate security to be used in Cryptographic applications. The Fortuna algorithm consists of a DRBG (Deterministic Random Bit Generator) which uses a 128 bit state vector (typically a counter) that is encrypted using a block cipher (Typically AES) using a 256 bit key. This results in a DRBG with a cycle period of 2^128, but the Fortuna algorithm also reseeds the PRNG periodically by changing the value of the encryption key using data accumulated from various entropy sources, and this reseeding breaks the output cycle and results in a random output stream with a cycle period which is indeterminate.

2.5 Limitation of use of RNG

Nº	Description	Details
1.	Acceptable degrees of freedom (DOF) permitted	Acceptable DOF's are listed in Section 3.1 Item 5 (below).
2.	Dependency on operating system functionality	None
3.	Library-based implementation	The RNG uses the library "javascript-fortuna" from the nodejs npm repository "https://www.npmjs.com/package/javascript-fortuna". Hence this RNG certification is restricted to nodejs npm repository version 1.0.10.
4.	Other	None

3 Detailed test results

3.1 Tests methodology

The testing methodologies listed below were used to ensure the RNG complies with the relevant jurisdictional technical requirements and the scope of work.

Nº	Test Performed	Test Methodology	Result
1.	Review of RNG documentation	Review of RNG documentation was conducted to understand the implementation of RNG in the gaming system.	Comply
2.	Research conducted about RNG algorithm/ hardware	Research conducted about the RNG algorithm to ensure there is no publicly known weakness or vulnerabilities associated with the RNG under evaluation.	Comply