FREQUENTLY ASKED QUESTIONS REGARDING THE CERTIFICATION AND AUTHORISATION PROCEDURE FOR TECHNICAL GAMBLING SYSTEMS (Version 7).

1. Document objective

After having received numerous enquiries regarding the certification and authorisation procedure, the Directorate General for the Regulation of Gambling (DGOJ) has drawn up a list of frequently asked questions. This document is subject to changes and updates.

2. Document control

Version	Date	Description of the changes
1.0	12 July 2012	Creation of document: General frequently asked questions.
1.0	30 October 2014	Creation of document: Supplementary guide to the one published in 2012.
2.0	15 June 2016	• The Basic Guide to Frequently Asked Questions published in 2012 and the one published in 2014 are consolidated in a single document. • References to the transitional period are eliminated. • The assumptions based on which it is possible to present the "provider report" are broadened. • Reference is made to the telematic management of procedures.
3.0	11 July 2017	New section: 13) Clarifications are included regarding the methods of authentication when communicating with participants.
4.0	22 August 2018	New section: 14) Clarifications are included in relation to the biennial audits.
5.0	1 April 2019	New section: 15) Clarifications are included regarding the cryptographically strong random number generators.
6.0	15 November 2019	The last paragraph of section 9.a.2, section "Final functionality certification report" has been removed in line with the changes introduced in the note on managing changes on the marketing of games and changes of CPDs

		of providers without a licence and that were previously approved by the DGOJ. Section 7) has been amended in relation to the content of the report on compliance with the regulations on personal data protection. In section 7), the regulations of the licence application terms of reference are updated, in which the content of the technical plan is developed.
7.0	13 May 2021	New sections: 16) Clarifications regarding aggregators are included. 17) Clarifications regarding the studios are included. In section 9), in the section "Certification reports and service providers / gambling software suppliers", "provider" is replaced by "supplier" to facilitate understanding.

3. Contents

4. Abbreviations used

AEPD: Spanish Data Protection Agency

CPD: Data Processing Centre

DGOJ: Directorate-General for the Regulation of Gambling

GNA: Random number generator

LG: General Licence

LS: Specific Licence

OM_AZA: Order HAP/1370/2014 of 25 July, approving the basic regulations for slot machine gambling.

RES_CERT: *Resolution of 6 October 2014, from the Directorate General for the Regulation of Gambling, approving the regulation which establishes the form and content of the final certification report on the technical systems of gambling operators and elaborates on the change management procedure.*

RES_PRE_SCI: *Resolution of 6 October 2014, from the Directorate General for the Regulation of Gambling, approving the regulation which establishes the format of preliminary reports for certification of technical plans and the format of the certification report on the internal control system, submitted by applicants for general licences.*

RES_TEC: *Resolution of 6 October 2014, from the Directorate General for the Regulation of Gambling, approving the regulation which elaborates on the technical specifications for gambling, traceability and security that must be met by the non-reserved technical gambling systems licensed under Law 13/2011 of 27 May on gambling regulation.*

SCI: Internal Control System

5. Procedure and deadline for requesting authorisation

a) Deadlines for submission of final certification reports

The deadline for the submission of the certification reports shall be four months, counted from the date on which they were notified of the resolution granting a general or provisional specific licence, a period which shall be non-extendable.

The Directorate General for the Regulation of Gambling will have a period of six months for the evaluation of the authorisation, also counted from the date on which they were notified of the resolution granting a general or provisional specific licence.

b) Consequences of failure to submit certification reports within the established period

The consequences of not submitting the certification report are as follows:

General Licences

In accordance with the Order approving the tender specifications that will govern the call for general licenses for the development and exploitation of gaming activities of Law 13/2011, the granting of the general license will be subject to the presentation, in the non-extendable term of four months from the notification to the interested party of the granting of the aforementioned license, of the report or definitive certification reports of the technical gaming systems and their subsequent approval by the Directorate General for Game Management\\.

Specific licences

In accordance with the Resolution of the Directorate General for the Regulation of Gambling, which establishes the procedure for the application and granting of Singular Licenses for the development and exploitation of the different types of gaming activities, the provisional granting of the singular license will be conditioned to obtain, within the six-month non-extendable term counted from its notification to the interested party, the final homologation referred to in the third number of article 11 of Royal Decree 1613/2011, of November 14th, by the that Law 13/2011, on gaming regulation, is developed in relation to the technical requirements of gaming activities. The provisional license will be extinguished in any case after the term referred to in the previous paragraph without the need for an express pronouncement by the Directorate General for the Regulation of Gambling

c) Deadline for submission of proof with actual data

Certain mandatory tests for certification require actual data with at least one month of data.

Should the operator not have commenced the gambling activity at the moment of submitting the final certification report, the report may be submitted without providing the results of the cited tests. However, the authorisation shall be conditional on the submission of the results of the tests.

The results of these tests must be submitted within three months from the date of the start of the corresponding gambling activity.

d) Certification reports of the operator who has not started the operation

The operator who has not started the operation of a particular licence must also submit the final certification report on the technical gambling system. The certification reports for the technical gambling system must be submitted within the established period, regardless of whether the operator has started the operation or not.

For this purpose, even if the operator has not started the operation, it must have a technical system, even if it is not being used effectively in the marketing of the gambling activity for which the certification will be performed. When the operator decides to start marketing the game, it must evaluate the need to make substantial changes to critical components and, therefore, the system must be approved before launch.

6. Scope of the certification

a) Scope of technical gambling systems

Royal Decree 1613/2011, of 14 November, elaborating on the technical requirements of gambling activities under Law 13/2011 of 27 May on gambling regulation, establishes in its article 2 the definition of the technical gambling system and its parts.

For the purposes of authorisation, the technical gambling system is "*the set of equipment, systems, terminals, means and software used by the operator for organising, operating and carrying out the gambling activity. The technical gambling system supports all necessary procedures for the organisation, operation and carrying out of the gambling activity, along with the detection and recording of the relevant transactions between the gamblers and operator".*

The organisation, operation and development of the gambling activity can broadly encompass many elements and services, such as telecommunication networks or payment methods.

With regard to the authorisation of the technical gambling systems, we must make a more restrictive interpretation taking into account the elements that can condition the development of the game, the access of the participants or the internal control system.

Examples of items to be approved (the list is not exhaustive):

- User registration and subjective exclusion checks.
- Integration with the DGOJ's identity verification services.
- The gambling account and the management of the participants' funds.
- Integration of the gambling platform with the payment gateway.
- The gambling software and random number generator.
- Back-office applications that can alter the configuration, development and outcome of games. For example, the back-office application that allows you to rectify the winner of a bet.
- Registration and traceability of data.
- With regard to the internal control system: the data capturer and the storage system.
- The user interface:
    - Webpages, scripts, flash objects, etc.
    - Downloadable applications or apps for mobile terminals.
- Physical terminals of an incidental nature.
- The physical game elements used in the game, such as roulette tables for the "live" version.
- The call centre when used to play.

Examples of items that are <u>not</u> to be approved (the list is not exhaustive):

- The participant's personal computer.
- Public telecommunications networks.
- The providers of payment methods, networks of payment methods or payment gateways.
- Identity verification service providers.
- The providers of information services on events, probabilities, risks, prices and results thereof.
- Operator information systems that cannot alter the configuration, outcome or development of games, or participate in the registration and traceability of data. For example:
    - Back-office applications that only consult data.
    - The general accounting system of the operator.
    - The datawarehouse of the operator, if not part of the registration and traceability of the game.
- The call centre when it is not used to play, but to support queries, complaints and claims.

b) Non-applicable requirements

Depending on the offer, development and marketing of an operator's game, certain requirements may not apply. In this case, the certification reports must be completed with 'N/A'.

In any case a report must be submitted with all the completed sections.

The certifying body must judge what requirements and sections of the certification report will apply in the case of each individual operator.

c) Purpose of the certification

The purpose of the certification is the technical gambling system actually used by the operator for carrying out and operating the corresponding licensed gambling.

This is true both in functionality and security certification reports.

For example, for certain security requirements it may be necessary to evaluate the existence and content of documented security procedures. Certification is not performed on the documentation, but on the actual system, so it must be certified that the procedures are operational and that the controls and measures they describe actually exist.

d) Electronic management of procedures.

Requests for authorisation and substantial change must be made through the electronic office of the DGOJ. For this purpose, a form has been made available in the section:

Electronic Procedures and Services / For the Operator / Licences

The processing of the procedures will be done entirely by electronic means and it will not be necessary to use in-person registration for any procedure. Paper executive summaries signed by the person authorised in the certifying body may be kept by the operator at the disposal of the DGOJ, which may request them if necessary.

7. Documentation to be submitted

a) Regulatory compliance with personal data protection regulations report

In the application for authorisation of the technical gambling system, together with the final certification report, the operator shall submit a detailed report on compliance with the regulations related to personal data protection pursuant to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (RGPD) and Organic Law 3/2018, of 5 December on Personal Data Protection and guarantee of digital rights (LOPDGDD).

There shall be only one such report per operator and it will apply to the all general and specific licences held by the operator.

In accordance with article 16.4 of Law 13/2011 of 27 May on gambling regulation, the Directorate General for the Regulation of Gambling shall request a report from the Spanish Data Protection Agency.

The report of the AEPD (Spanish Data Protection Agency) may be taken into account by the Directorate General for the Regulation of Gambling for the authorisation of the technical gambling system.

The technical note that develops the procedure for requesting substantial changes in technical gambling systems describes the change scenarios in which a new version of the report needs to be presented.

The compliance assessment report must be signed by the operator's data protection officer (DPO) and must have the following documentation:

- Record of processing activities (RAT) carried out under the responsibility of the operator as the person responsible for the processing.
- Assessment of the impact related to data protection by the data processing carried out by the operator.
- Privacy policy assessed by the DPO.

b) Description of the technical gambling system

To describe the licensed technical system, the following documentation must be provided:

1. An updated description of the technical system.
2. In the case of specific licences, the particular rules.
3. Operator's descriptive licence questionnaire.

<u>An updated description of the technical system</u>

Operators who certify a system that has undergone variations with respect to the one described in the Technical Plan must update the documentation provided to describe the system actually used that is subject to certification.

To prepare the documentation of the updated description of the technical system, the following can be taken as a reference:

- For general licences, the one required in Annex III to Order HFP/1227/2017, of 5 December, approving the terms of reference which govern the call for tenders for General Licences for the development and operation of gambling activities of Law 13/2011, of 27 May on gambling regulation.

- For singular licenses, the one required in Annex II of the Resolution of 1 December 2017, of the Directorate General for the Regulation of Gambling, whereby, in accordance with the provisions of article 17 of Royal Decree 1614/2011, of 14 November, which develops Law 13/2011, of 27 May, on the regulation of the gambling, in relation to licenses, authorizations and registrations of the gambling, establishes the procedure for the application and granting of Singular Licenses for the development and exploitation of the different types of gambling activities.

Particular rules

The particular rules of all games, forms and variants of the corresponding licence must be attached.

Operator's descriptive questionnaire

The descriptive questionnaire of the operator must be attached in electronic form.

It is essential that the "LS Other Games" tab (or, if applicable, "LS Bets" or "LS Contests") of the operator descriptive questionnaire clearly describes the offer of the B2C operator's gambling. This should include the name of the game, the name of the provider, the available access technology and the start date of the game's marketing.

c) Format for the documentation to be provided

It is advisable that the documentation provided in electronic format is organised, for which purpose we suggest a folder structure similar to the following (folders underlined):

- General/Specific Licence XXXX
  - Summary: list of certification reports provided for the licence.
  - Description of the Technical Gambling System
    - Description of the Technical System.
    - Description of the Particular Rules, in the case of specific licences.
    - Operator's descriptive questionnaire.
  - Final functionality certification report 01
  - Final functionality certification report 02
  - Final functionality certification report 03
  - Final security certification report 01
  - Final security certification report 02

Each definitive functionality certification report should have a structure similar to the following:

- Final functionality certification report 01
  - Complete final functionality certification report.
  - Technical requirements (evidence)
    - Annex RQ1…
    - Annex RQ2…
    - ...
  - Integration (evidence)
    - Annex PI1…
    - Annex PI2…

        - ...
    - Binaries (copy of technical gambling system binaries)

Each definitive functionality certification report should have a structure similar to the following:

- Final security certification report 01
    - Complete final security certification report.
    - Documentation (security documentation evaluated)
        - Security document 01
        - Security document 02
        - …
    - Technical requirements (evidence)
        - Annex RQ1…
        - Annex RQ2…
        - ...
    - ISO27001
        - ISO 27001 certification, if used.

8. Aspects to consider in certification tests

a) Testing games for testing of identity verification systems and RGIAJ

The Directorate General for the Regulation of Gambling will provide the certification bodies with a set of test kits for carrying out the tests for the integration of the checks of subjective prohibitions in the user register.

These testing games are defined for the following services provided by the Directorate General for the Regulation of Gambling:

- Enquiries from the identity verification service.
- Enquiries from the General Register of Gambling Access Bans (RGIAJ).

These test kits only cover tests of users with DNI (Spanish national identity document) or NIE (foreigner's identity number), not non-resident persons and are not useful for other verification services.

The DGOJ will send the list of test games to the representative of each of the certification bodies by e-mail. If any certifying body experiences any incidents with the receipt or use of the test games, it may contact the mailbox. dgoj.control@hacienda.gob.es

b) Details of the proof of fulfilment of technical requirements

The certification reports should contain the details that make it possible to verify that the test has been carried out and to have enough information to contrast the result. The necessary details will depend on the mechanism used for the accreditation of the requirements. In this respect, it is possible to take as a reference what is defined for the types of tests FUNCTIONAL, TRACEABILITY, ACTUAL DATA described in ANNEX VI of the Resolution of the DGOJ approving the Provision that establishes the model for and content of the certification report on the technical systems of the gambling operators and implementing the change management procedure.

In the event that other accreditation methods are used, the following observations may serve as a guide:

- DOCUMENTS: the document on which the accreditation is based must be provided as well as the reference within the document that makes it possible to accredit the requirement in question.
- CODE ANALYSIS: a brief description of the process for selecting the test cases, the coverage criteria used (rulings, decisions, structural, functional, statistical, etc.) and the results obtained must be provided.
- SIMULATION: a brief description of the simulation method used, the number of iterations performed, the analysis of the results obtained and the degree of statistical confidence of the results obtained must be provided.

c) Integration tests with actual data of the internal control system (ICS)

Certain integration tests deal with the integrity of the actual data of the internal control system. These tests are designed in a way that ensures security and prevents access to personal data to the extent that it is possible. The certification bodies will not have access to the encryption keys of the data in the warehouse:

- This requires the operator to provide certain clear ICS files to the certifying body.
- The certifying body shall include in the report certain calculations, for example, the ratio of the prize amount and the participation amount, so that the DGOJ may subsequently audit that the data

evaluated by the certifying body coincide with those that have been contributed by the operator to the ICS.
- The files to check will be RUT, CJT, OPT/ORT, JUT and JUD, which do not contain the personal data of participants.

The certifying body shall check the ICS data against lists obtained from the back office of the technical gambling system. The certifying body must be certain of the accuracy of these lists since they are the source against which the completeness of the ICS's actual data is compared.

d) Time required for integration tests with actual data

Tests with actual data in the context of the application for authorisation of the technical gambling system:

The integration tests in relation to actual data require the technical gambling system to have at least one month of data. They cannot be completed through tests or simulations.

For ICS tests with monthly files, tests A.5.1 and B.4.1, at least one monthly file should be used where the operator has marketed the game for a full month. Examples:

- For operators who started marketing on 5 June, the certification report must evaluate at least the monthly data for June and July, July being the first full month.
- For operators who started marketing on 10 July, the certification report must evaluate at least the monthly data for July and August, August being the first full month.

Tests on actual operator back office data other than those contained in the ICS, test A.3.2, will require the system to have one month of data. Example:

- For an operator who started marketing on 5 June, the first date on which this test could be performed would be 5 July.

Proof with actual data in the context of certification of a substantial change:
In certification prior to the change, it is not necessary to perform tests in the environment used effectively for marketing. When the certification is required prior to the start of production, the tests can be performed in a pre-production environment.
The certifying body must, under its own responsibility, certify that the results obtained in the test environment are comparable to the results that would have been obtained in testing the technical gambling system employed by the operator for carrying out and operating the licensed gambling. It must further certify that it has examined that any possible differences between the test environment and the actual technical gambling system do not affect the quality of the test results.
Integration tests on the internal control system, tests A.5.1 and B.4.1, shall be carried out with fictitious data as closely as possible, taking into account any considerations deemed appropriate. Testing with actual data will not be necessary.

e) Tests of all games, variants and forms

Certain tests include the following clarification or a similar comment:

NOTE: This test will be repeated for each type of application or terminal used for participation as well as for each gambling activity, version or form.

This means that all applications, terminals, games, variants or forms that may have any influence on the test must be tested. Examples:

- When testing the rules of the game of additional games it will be necessary to test each of the games, for example, *mus*, *tute* and *brisca*, as each one will have a different implementation and logic of the game.
- When testing the rules of sport betting it will not be necessary to test bets in each of the sports if the engine of the bets is common to all of them. It is possible that the engine implements a different logic for live or conventional betting so it would make sense to test each of these types.
- The operator can offer three types of Blackjack. Therefore, it will be necessary to test each one as each variant has its own logic of the game.

f) Fingerprints of critical components in certification reports

Section seven of Annex I of RES_CERT states in its last paragraph that: *"The final certification report of functionality shall include a copy of the binary files of the certified software and a digital fingerprint of the critical components."*

The final functional certification reports will include the digital fingerprints of the components qualified as critical. The digital fingerprints of these critical components will be included in the section "2. Description of the certification object" in Annex III which describes the model and content of the functional certification report.

Final security certification reports will include a specific audit analysis of the critical components, although this report does not require the inclusion of fingerprints.

9. Notes clarifying different assumptions in the submission of certification reports

When would a "provider's report" be accepted?

A technical gambling system is certified and authorised on the basis of the licence and operator. The operator is ultimately responsible for compliance with technical requirements, and certification reports must be prepared for the operator on their technical gambling system. However, in certain cases, it is possible to prove compliance in the authorisation procedures through provider certification reports.

a.1) Preliminary certification as part of the licence application

Sections b) and c) of the Technical plan and Preliminary reports for General Licences (GL) and Specific Licences (SL):

Sections (b) and (c) of the technical plan for GL and SL may be divided and presented, organised by providers, whereby the preliminary certification reports for GL and SL may be prepared in the name of the provider and not the final operator.

The preliminary certification report can be drawn up on the basis of the technical plan proposed by a provider and, therefore, the report can be used by several operators, provided that the operator does not modify the technical solution described in the technical plan.

In any case:

- The information contained in both the technical plan and preliminary report produced by a provider and its certifying body, and submitted by an operator in its licence application, must be fully applicable to the solution of the operator. For example, it would not be valid to submit a provider's technical plan that includes ten versions of gambling activities and two participation channels and additionally an operator's technical plan modifies the provider's information to state that only five of those gambling versions and one participation channel will be offered.
- The operator is responsible for all information contained in the documents submitted in the procedure, including the provider's technical plan; therefore, those matters that do not apply to the operator must not be included in the plan.
- Information provided must be consistent and there must not be any contradictions between the different documents of the operator and its provider.

ICS certification reports:

The final ICS certification report can be carried out as part of the licence application on the internal control system solution implemented by a provider and it can be used by different operators, provided that the implemented technical solution has not been modified.

a.2) Final certification as part of the application for initial authorisation or substantial change:

Final certification report on security:

The operator may request the certifying body to issue a single security certification report that covers its entire technical gambling system and use said report in the authorisation processes of each licence granted to the operator.

Where one or more providers of gambling services form part of the technical gambling system used by the operator for developing and operating the gambling activity to be permitted by the relevant licence, the operator applying for the licence must submit a final certification report on the security of the technical infrastructure of each one of the providers.

Some examples could be the following:

- An operator submits a security certification report on all of its technical infrastructure, and reuses the same report for all general and specific licences.
- An operator uses multiple DPCs. Some house Blackjack and others roulette. It may decide to submit a single security report covering all DPCs, or decide to submit one security report on Blackjack DPCs and another for roulette DPCs.
- An operator has its own technical infrastructure, but for of poker it relies additionally on a gambling service provider. For poker it must present:
    - The security certification report for its own infrastructure.
    - The security certification report from its poker provider.
- An operator with a warehouse provider. It must submit:
    - The security certification report for its own infrastructure.
    - The security certification report from its warehouse provider.

Final functionality certification report:

The first time an operator integrates with a software provider for the operation of a particular licence, either upon initial authorisation or through subsequent change management, it is necessary to submit a final certification report on the functionality performed to the operator, which proves the correct integration of the operator's platform[1] with the new game software provider.

In the event that there are several types of integration, the certification of all of them must be accredited. For example, if there is integration with the PC platform and integration with the mobile platform, it will be necessary to certify the correct integration of the operator with its provider in both.

Subsequently, there are substantial changes in the provider's services such as the introduction of new games, a major change in a game software version or changes that modify the generation of random numbers and the

[1] To this end, where applicable, that of its user register providers, gambling account, session software intended for the slot machines or internal control system is part of the operator's platform.

processing of this information; if the changes do not affect the integration, the operator may submit a final certification report on the provider functionality.

Certification of slot machine gambling sessions.

Depending on the business model of the operator, the software components corresponding to the gambling session for the slot machines may be implemented in the gambling software layer or in the gambling platform layer. In the latter case, the following are allowed to be submitted for certifying the technical gambling system in relation to the specific licensing of slot machines:

- A separate functionality certification report for each provider of game software, which certifies the game software.

- A functionality certification report certifying the gambling session of the slot machines and the integration of the session with each game provider and with the operator's gambling platform. The implemented solution along with the group of all providers of slot machine game software shall be described within the scope of this report. If there are several types of integration (e.g. PC, mobile, etc.), they must all be certified.

  The technical requirements that must be certified are, at a minimum, those related to the following areas:

  - ✓ Area: Configuration and carrying out of the slot machine game session.
  - ✓ Area: Duties of informing participants in relation to the gambling session intended for slot machines.

  The following must be certified in relation to integration tests: the development, due accounting and participation limits established within the framework of the slot machine gambling session, as well as the completeness of the internal control system's records. In other words, the B.1.2, B.2.1, B.4.1, and B.4.2 integration tests concerning the slot machine gambling session must be performed.

Functionality certification report on the gambling on offer

For general licences, a single report covering the entire scope shall be submitted.

For specific licences, for certifying the functionality of a set of gambling activity versions, a report for each particular version or a single report for all versions can be submitted. In the latter case, it is essential that the report's scope clearly details the set of certified versions. Furthermore, in relation to every test, analysis or technical requirement, it must be stated throughout the report whether the given assessment or any other included information refers to all versions or to particular versions.

Certification reports and service providers / gambling software suppliers

For the purposes of certification of the technical gambling system, the gambling service providers and the gambling software providers must be differentiated. Gambling service providers participate with their technical

infrastructure in the complete technical gambling system ("Software As A Service"), while gambling software suppliers provide the software but do not manage the technical infrastructure ("Software Acquisition"). The technical gambling system includes the systems of all gambling service providers participating in the complete solution and the software provided by gambling software providers.

The requesting operator must be responsible for approving the complete technical gambling system and for submitting final certification reports. This is irrespective of whether the gambling service provider or gambling software has the status of a gambling operator in Spain.

That said, a gambling service provider can certify the security of its system, and that security certification report may be submitted and reused by each of the operators it serves.

Certification reports for network co-organisers

In the procedure for the authorisation of a specific licence of an operator which is a co-organiser of a network, the co-organiser operator must submit:

- The certification report on the functionality with the following characteristics:
    - The scope of the certification must only include the elements of the technical system of the network operator dedicated to the specific licence.
    - In each specific case and depending on the technical solution adopted, certain requirements such as information obligations to participants, the promotion of games, or the publication of the rules of the game will apply.
    - The network operator must have an Internal Control System in which the ORT, BOT, JUT and JUD registers will be recorded.
- Final security certification report

Certification reports for network co-organisers that connect to a network co-operator

In the procedure for the authorisation of a specific licence of an operator whose participants access the game of a co-organising operator of a network, the operator must submit:

- The certification report on the functionality with the following characteristics:
    - The scope of certification will include both operator systems and co-organising operator systems.
    - The operator shall certify all the requirements in the system to be certified. In the integration tests, the co-organising operator's systems will also participate.
    - The operator must have an internal control system in which the OPT register will probably only be recorded.
- Final security certification report.
    - The operator can submit two reports, the security report of its own technical infrastructure and the security report of the co-organising operator.

Operator certification reports not directly related to participants

For those operators who do not have a direct relationship with the participants (user registration, gambling account, deposits, withdrawals, gambling contract), most of the requirements of a general licence are not applicable.

In the certification reports on the general licence functionality, sections 3.3.5 and 5.5 may apply if the technical system implements measures against fraud and money laundering. If measures against fraud and money laundering are not part of the technical gambling system, but are carried out through procedures or other activities, it may be considered that there is no technical gambling system associated with the general licence. In this case, it would not be necessary to present a certification report on the functionality or security, but rather a letter from the operator should be submitted to justify this circumstance.

Certification reports for operators of contests

For the certification of general licences of those operators of contests that have authorisation to participate in the game without the previous identification of the participants, the certifying body must evaluate what requirements are applicable.

Example: user registration requirements:

- Requirements for verification of pre-game identity verification are not applicable.
- The requirements of having a user register will remain applicable, only for the winners.

10. Clarifications relating to the slot machine game session

a) Definition of slot-machine game session

"A set of spins played by the participant on one or more slot machines during a period of time defined by each one of their connections to the slot machine game of the gambling operator". (Article 2.3 of the OM_AZA).

The slot machine session is a concept created within the framework of responsible gambling. The objective is to provide the player with a controlled gambling environment (monetary limits, time limits, right to information, etc.). The "Slot machine game session" concept has several technical implications, set out as follows:

b) Start and end times for the Slot machine game session

It is only possible to have one slot machine game session in progress during a user session. The slot machine game session initiated by a player must be the only such session that can be operated by the player at any one time on the operator's web page, irrespective of any other technical or commercial issues such as the number of user sessions open, the number of connections to different user terminals, or other slot machine games available on the operator's web page (by one or more providers).

The logging out of the operator's system by a player (by closing all user sessions that have been initiated) implies the conclusion of the of any initiated slot machine game session. If the player later restarts a user session on the operator's system and wishes to play on the slot machines, they must set up a new slot machine game session.

c) Simultaneous playing of slot machines and other games (roulette, blackjack, etc.)

- Can a player be involved in other games during a slot machine game session?

  Yes, but while the slot machine game session remains open, the requirements stipulated in the Ministerial Order must be respected: duty to inform in relation to time and money apportioned to the slot machines, configured limits for the slot machines, periodic warnings, etc.

- If a player wishes to play other games (roulette, blackjack, etc.) during a slot machine game session, can they interrupt the session and later resume that same session?

  No. A slot machine game session can never be interrupted and later resumed on account of the fact that the player stopped interacting with the slot machines and played other games. A slot machine game session concludes in the following circumstances:

  - ✓ The limits fixed by the user in setting up the session are reached.
  - ✓ Voluntary closure of the session by the user, whether expressly (termination of the particular slot machine session), or by closure of the user session or browser, where appropriate.

- ✓ Involuntary closure or interruption of the session occurring due to circumstances outside the control of the user or operator, e.g., as a consequence of an unexpected interruption in connection between customer and server.

If, on the basis of technical criteria, the operator decides to interrupt the slot machine game session when a player wishes to play other games, the operator must force the closure of the slot machine game session (and comply with the relevant stipulated duties) and later require the player to set up a new slot machine game session (different from the previous one) for the purpose of playing the slot machines again.

d) Existence of slot machine game software providers on the web page of a single operator

The slot machine game session initiated by a player must be the only such session that can be operated by the player at any one time on the operator's web page, irrespective of any other slot machine games available on the operator's web page, by one or more providers.

We can find multiple technical implementations of the slot machines session:

- ✓ The session can be implemented on the general platform, controlling from the general platform the time and money spent on all the slot machine games integrated with the general platform.

- ✓ The session can be implemented at the level of the game software provider, and, therefore, obliging the player to close a slot machine game session and starting a new session in order to change provider, in addition to incorporating the mechanisms necessary for preventing the player from simultaneously opening more than one slot machine game session.

In summary, any technical solution may be valid as long as the slot machine game session, between its commencement and conclusion, remains the only such session operational between the player and operator, regardless of the number of providers.

e) Configuration of the slot machine session and obligations regarding information

Some of the aspects related to the configuration of slot machine sessions and duties to inform the participant will now be described and clarified.

- "*Article 14.1. Prior to commencing an slot machine game session, the participant must stipulate the maximum amount of playing time and the maximum amount of money that they are willing to wager from their gambling account during the session. These amounts must be expressly stipulated every time upon accessing an slot machine game session. They may not be set as default amounts nor be saved from previous sessions.*"

With the aim that the player can stipulate the maximum amount of playing time and the maximum amount of money that they are willing to wager from their gambling account, one possible technical solution is to offer a set of predetermined values with the following qualifications:

- ✓ The range of values must be sufficiently wide.
- ✓ The maximum time values must be specific numbers.

- ✓ A maximum value with reference to the player's balance could be included among the values for setting the maximum amount of money that the player is willing to wager from their gambling account. There is no need to explicitly include the player's balance since the gambling account balance must always appear on the user's interface (Art. 3.9.2 of the RES_TEC).
- ✓ Neither the offered minimum values nor the distribution of ranges must pervert the purpose of the self-limitation measures, especially, by encouraging the player to select high values.
- ✓ It is not permissible to include a specific button for expanding the menu of values with the maximum balance/time option already highlighted.

➢ *Article 14.1): "In any case, the gambling operator must notify the participant of approaching the limits configured prior to the session, for the purpose of allowing the participant to close the session in an orderly manner if so chosen."*

Essentially, this rule states that a warning must appear whenever the player approaches the end of the session due to having almost reached the limit allocated to time or amount available to wager. In the case of approaching the time limit, the warning will only occur once. Conversely, with the warning on approaching the monetary limit, the application of such warnings may occur more often; the warning threshold may be approached or exceeded several times within a short, or longer, period of time. In this regard, the initial warning does not need to be shown again until 15 minutes after its first appearance (15 minutes coincides with the maximum interval between recurrent warnings on gambling that must be shown in parallel during the entire gambling session). Once the warning for approaching a limit occurs for the first time, it will not be necessary to show it again for approaching that particular limit over the course of the next 15 minutes.

➢ *“Article 14.2. In configuring the slot machine game session, the participant may temporarily restrict their access to any future session, provided that the session to be played concludes automatically as a consequence of expending the entire amount of one of the limits stipulated in section 1 of this article.*

One possible technical solution so that a player can establish a period of self-restriction is to offer a set of predetermined values, with the following provisos:

- ✓ The range of values must be sufficiently wide, and provide at least the values of "1 day", "1 week" and "1 month".
- ✓ A minimum value of "1 hour" is permissible within the range of values.
- ✓ Once the player has configured and confirmed a period of self-restriction under the terms of article 14.2, any revisions or changes to that configuration will not be possible.

➢ *Article 14.3. "Prior to commencing the session, the participant shall decide on the frequency of the warning referred to in section 2 of article 8 of this ministerial order; the minimum frequency shall be fifteen minutes counting from the commencement of the slot machine game session or from the last warning."*

The longest possible time interval between appearances of the warnings is 15 minutes. In other words, the player can set up the session so that the warning may appear every 5, 10, or any other value equal or less than 15 minutes.

➢ *Article 8.1.2.i) "During the course of each session, the balance of the slot machine game session with a breakdown of the wagered amounts and, where appropriate, obtained winnings. This information will be visible on the game interface from the moment the slot machine game session commences."*

At all times, during the slot machine game session, the user's interface (including mobile terminal interfaces) must show the following figures:

- ✓ The balance of the session (the sum of all winnings minus the sum of wagered amounts).
- ✓ The sum of wagered amounts.
- ✓ The sum of winnings.

This requirement applies to all user interfaces, including those of mobile devices. This requirement may not be implemented by providing a link that will redirect the player to another section.

A history including information on each spin, round, balances during the session, etc. is not required to be made available to the player.

➢ *Article 8.1.2.j): "A list of the previous amounts gambled and winnings obtained in each slot machine game session, as well as the final balance of previous sessions."*

A player must have access to a record including information on each and every one of the concluded slot machine game sessions, and in particular, with regard to each one:

- ✓ The final balance of the session (the sum of all winnings minus the sum of wagered amounts).
- ✓ The sum of wagered amounts.
- ✓ The sum of winnings.

➢ *Art. 13.2 "At the conclusion of each slot machine game session, operators shall provide the participant with an accrediting document summarising the amounts wagered and results obtained through the same means by which the latter participated in the session.*

The accrediting document referred to in article 13.2 must include at least the following:

- ✓ The sum of wagered amounts.
- ✓ The sum of winnings.

Where the slot machine game session is not closed in an orderly manner, such as, the player closes the browser directly or the connection between customer and server is unexpectedly interrupted, the operator will not need to comply with the duties to inform under the terms of art. 13.2 because of its technical impossibility. Nevertheless, data from a session closed involuntarily will be included in the history of the slot machine game session.

➢ *Article 8.1.2.e): "Mathematical expectations regarding gambling returns, calculated over a year, as well as the actual percentage of paid winnings over amounts gambled for every game in each of the six preceding months. The calculation of said percentage shall not include winnings from jackpots, without prejudice to any additional information the operator chooses to provide in relation to jackpots.*

For slot machines, there is a duty to publish the theoretical RTP and the monthly actual RTP of the last six months (excluding amounts intended for jackpots and paid-out jackpots). The operator can include other additional values, which may cover the RTP including information related to the jackpots.

f) Application of specific elements for slot machine sessions to other games

Operators can choose to apply the configuration of the participant's time and monetary limits, as well as the other elements involved in the commencement of the specific session for slot machines (warnings on approaching limits and recurrent gambling), to the commencement of the user session, thereby extending the application of the aforementioned elements to all games on offer.

This is an acceptable and viable option with the placement of the following safeguards regarding elements applicable only to the slot machines:

- ✓ The information during the course of each session (article 8.1.2 of the OM_AZA) must be related to the particular slot machine session. Especially the sections on:
  - The balance of the slot machine game session with a breakdown of the wagered amounts and, where appropriate, obtained winnings. This information will be visible on the game interface from the moment the slot machine game session commences.
  - A list of past amounts gambled and winnings in each slot machine game session, as well as the final balance of previous sessions.
- ✓ The possibility to play with the winnings once the particular session of the slot machines has commenced. This possibility refers only to the winnings gained from the slot machines and not any other games (Article 12.2 OM_AZA).

g) Other meanings of session

The term "session" is used in different contexts in gambling regulations: in technical contexts such as "*user session*", in the context of responsible gambling for slot machine games such as "*slot machine game session*" and lastly, in the context of monitoring for the data model of the internal control system. The different contexts are explained below:

➢ Slot machine game sessions

The term slot machine game sessions is a concept created in the framework of responsible gambling under which it has been previously highlighted.

➢ User session

Definition: *A user session is the period of time during which a user remains connected to the operator's website, counting from the moment of authentication of the user on the system until disconnection of said user* (3.8 of the RES_TEC).

Clarification: This technical concept is usually marked off by an exchange of passwords and a closure of the session, which can be caused by, among other reasons, the player's request, loss of connection between the customer and server or player inactivity.

Obligations regarding information:

In the context of a user session, there are a set of obligations, among which the following are highlighted:

- *The interface shall show a clock with the current time visible or the duration of the session. When the user commences a session, the user shall be shown the time at which they last connected.* (Order inviting applications for General Licences, Appendix II: Content of the operational plan, 3.1.c).
  This requirement applies to all user interfaces, including those of mobile devices. This requirement may not be implemented by providing a link that will redirect the player to another section.

- Game number and participant's balance (3.9.1 and 3.9.2 of the RES_TEC):
  The name of the game being played by the participant must be clearly visible on all related screens.
  The screen must show both the current balance of the participant at least in euros and the bets wagered in unit and total amounts.

➢ Session in the context of monitoring

Within the framework of the data model for the internal control system, a series of guidelines has been published on how to record information related to session games, in particular, roulette, blackjack, additional games and slot machines.

The reader is recommended to view the specific guide on the data model for more details. The most relevant issues are below:

Roulette, blackjack and additional games:

The operator can choose how to record data related to games of roulette, blackjack and additional games by one of the following three options:

- Recording by gambling session: Recording according to gambling session groups together all turns occurring during the session of one particular game.

- Recording by user session: Recording according to the user session groups together all turns played during the one user session, i.e., from the moment the user confirms entry onto the platform until disconnection.

- Recording by hand or turn: Each turn or hand is recorded separately.

Slot machines

Slot machine data will always refer to the session on the slot machines. The recording of slot machine sessions must specify the times and dates of when the slot machine game sessions commenced and ended, as well as the duration and maximum amount that the participant configured beforehand.

11. Clarifications relating to redirection to the ".es" domain name.

Art. 3.2 of the RES_TEC Appendix.

This requirement is mainly aimed at those operators with a dot-com website in order to prevent, among other things, fraudulent behaviour by players who, under the scope of Law 13/2011 of 27 May on Gambling Regulation, attempt to access and gamble on web pages outside the remit of the Act through the use of techniques that conceal the IP address.

The purpose of this is not to prohibit the use of VPNs within controlled environments (certification work, remote access of system administrators, etc.).

However, from a purely technical point of view, technological developments make it impossible to have 100% effective mechanisms for preventing a player from hiding their IP address in order to gamble on a dot-com website from within Spain. In any case, mechanisms to mitigate this risk are called upon to be implemented insofar as possible. The technical controls must be supplemented with organisational measures that allow the checking of the players' place of residence.

12. Clarifications relating to penetration testing and vulnerability analysis.

Art. 4.17 of the RES_TEC Appendix.

The new wording responds to criteria on flexibility, however, it does not entail, under any circumstances, a decrease in the effectiveness of the tests. An operator with sufficient technical and human resources may conduct their own penetration testing and vulnerability analysis.

In any case, a DGOJ-appointed certification entity must assess these tests. Where the entity deems them compliant, this will be understood to be a guarantee that they were properly conducted. In other words, the certification entity is responsible for issuing a compliance certificate for the test and analysis. A test laboratory must not certify test compliance where there are any doubts on its effectiveness. In the event of a serious failure, the system cannot be certified as compliant. Where minor or moderate security failures are detected, the system can be deemed compliant as long as there exists a plan of action with corrective measures.

13. Clarifications are included regarding the methods of authentication when communicating with participants.

Section D) of Annex VII of *the Resolution of 6 October 2014 of the Directorate General for the Regulation of Gambling, approving the provision which establishes the form and content of the final certification report on the technical systems of gambling operators and elaborates on the change management procedure* (RES_CERT) establishes the authentication requirements when communicating with participants.

The DGOJ has analysed the best practices of the market in the field of authentication and the current state of technology in order to adapt the authentication requirements to the evolution of technology. The standards analysed were as follows:

1. ICT security standard (CCN - National Security Scheme), which defines three levels of security (low, medium and high).

2. PCI DSS Version 3, which establishes authentication by means of two factors (hereinafter, 2FA) or multi-factor (hereinafter, MFA).
3. NIST 800-63-2, which provides guidelines for the choice of authentication factors.
4. OWASP Mobile Top 10 2016, specifically in its category M4-Insecure Authentication, where notions on how to avoid insecure user authentication are provided.

The PCI standard defines the following authentication factors:

1. Something that the user knows (password, PIN, etc.).
2. Something that the user has (smart card, physical device, etc.).
3. Something that the user is (biometric feature, such as their fingerprint).

Taking into account these technical directives and the requirements established in the regulations, the following scheme for authentication of technical gambling systems has been defined:

1. Low-level authentication: It is not considered to be in compliance with the regulations.
2. Medium-level authentication. It is considered to be in compliance with the requirements established in the regulations under one or other of the following criteria:
   a. A password of at least 8 characters in length and three types of characters with associated blocking policies (hereinafter, 8C-BP); or
   b. Low-level means associated in two-factor authentication schemes (2FA) with associated blocking policies (hereinafter, BP).
3. High-level authentication. It is considered to be in compliance with the requirements established in the regulations under one or other of the following criteria:
   a. Biometric patterns with a second authentication factor such as a physical device; or
   b. Low-level means associated in multi-factor (MFA) authentication schemes with BP.

Examples are set out below according to the following scheme:

Case	Compliant	Security	Observations
Mobile application	NO	Low	A multi-factor authentication scheme must be associated.
Linear pattern	NO	Low	A multi-factor authentication scheme must be associated.
PIN	NO	Low	A multi-factor authentication scheme must be associated.
NFC Proximity Card	NO	Low	A multi-factor authentication scheme must be associated.
Mobile application with a PIN	NO	Low	A physical device application with a single associated low-level factor is considered a low level of security, due to the risk of terminal theft.
Mobile application with a pattern	NO	Low	A physical device application with a single associated low-level factor is considered a low level of security, due to the risk of terminal theft.
Mobile application with an SMS	NO	Low	A physical device application with a single associated low-level factor based on sending an SMS is considered a low level of security due to the vulnerability associated with SMS protocols.
NFC proximity card with SMS	NO	Low	A low level of security is considered due to the vulnerability associated with SMS protocols.

Password (8C-BP)	YES	Medium	Included in Annex VII. D of the RES_CERT.
Mobile application with PIN (BP)	YES	Medium	It is considered a medium level of security, because the risk of theft of the terminal is mitigated by a blocking policy with a limited number of attempts so that the terminal cannot be hacked by brute force (2FA).
Mobile application with a pattern (BP)	YES	Medium	It is considered a medium level of security, because the risk of theft of the terminal is mitigated by a blocking policy with a limited number of attempts so that the terminal cannot be hacked by brute force (2FA).
Mobile application with an e-mail	YES	Medium	It is considered a medium level of security because the risk of theft of the terminal is mitigated by a policy of sending an e-mail with each authentication in the system (2FA).
NFC proximity card with PIN (BP)	YES	Medium	It is considered a medium level of security because the risk of theft of the card is mitigated by a blocking policy with a limited number of attempts so that the card cannot be hacked by brute force (2FA).
NFC proximity card with an e-mail	YES	Medium	It is considered a medium level of security because the risk of theft of the terminal is mitigated by a policy of sending an e-mail with each authentication in the system (2FA).
Mobile application with a password (8C-BP)	YES	High	A high level of security is considered because a two-factor scheme is used in which one of the factors has a medium security level (2FA).
Mobile application with a fingerprint	YES	High	A high level of security is considered because a two-factor scheme is used in which one of the factors has a medium security level (2FA).
Mobile application with a pattern (BP) and e-mail	YES	High	A high level of security is considered because a multi-factor scheme (MFA) is used.
Mobile application with a pattern (BP) and e-mail	YES	High	A high level of security is considered because a multi-factor scheme (MFA) is used.

Factors applied to "mobile applications" could be applied as native functionality in the device as long as the operating system allows it securely.

Furthermore, the operators must consider the possible loss of the token and/or the player forgetting the password, for which reason there must exist a "password recovery" process that involves a level of security similar to the methods of authentication used. For example, an authentication method based on answering several secret questions is considered a medium security level analogous to the “Password (8C-BP)” case.

The introduction of new authentication methods when communicating with the participants has a substantial change in the technical gambling system and is therefore subject to certification and authorisation prior to being introduced. With the request for a substantial change authorisation, the following documentation must be attached:

- Technical and regulatory analysis with the impact study and risk analysis of the implemented solution.
- Updated security certification report. The following areas must be certified:

  - Security of communications with participants
  - Vulnerability analysis and penetration testing.
- Updated technical plan. Section c) 7 must be updated for the technical plan corresponding to the General Licence: “Description of measures to ensure the security, confidentiality and integrity of communications with the participant.”

As an example in relation to the technical and regulatory analysis, the following are the main considerations to take into account when implementing a method of authentication based on a mobile application with fingerprint recognition:

1. Technical analysis: Standard hardware for fingerprint recognition, TouchID for iOS and hardware with encryption similar to that stipulated in Google standards in the case of Android must be used. The following implementation of this type of solution could therefore be considered to be erroneous at the technical level: obtaining the fingerprint using recognition software that is not approved or which is different from that stipulated by the main mobile operating systems.

2. Regulatory analysis: With the entry into force of the General Regulation on Data Protection[2], to those already considered as specially protected data (ideology, religion, trade union affiliation, beliefs, health, racial origin and sex life) are added biometric data aimed at unequivocally identifying a person. If it were considered to store this data in the technical game system of the operator, it would imply the realization of a “Prior Impact Assessment” (EIP) according to said regulation.

3. Conclusions and recommendations on implementation:
    a. Obtaining the fingerprint using a hardware device approved by OS or meeting its specifications.
    b. Save a mathematical association of the fingerprint with a username/password in a safe place in the device itself and in an encrypted form, resulting in the connection to the technical gambling system with the double username/password associated with the application.

If an operator intends to implement another equivalent solution not included in the previous list of practical cases, it may submit an enquiry to the mailbox dgoj.control@minhafp.es, including the analysis and control of risks, and also incorporating the “compensation controls” implemented, understanding that these types of

2 Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

controls must comply with the same rigour as the previously defined scheme, providing a similar level of defence.

14. Clarifications regarding the biennial audit of the technical systems games.

The following section aims to clarify the doubts raised by the operators in relation to the deadline for submission and the scope of the technical audit that operators must perform on their technical gaming system.

a) Scope of the audit when the technical gaming system consists of different gaming software providers.

From the administrative point of view, the period of completion and presentation of the audit of the technical gaming system is determined by the date of approval of each license available to each operator. However, the reality of the market is that the technical gaming systems are systems in constant evolution and one of the most evident indicators in this sense is the continuous incorporation of new suppliers of machines of chance in the systems of the operators.

The purpose of this section is to clarify the deadline for presentation and the scope of the audit in these cases. For this, it will be necessary to distinguish fundamentally between the technical level and the administrative level.

From the administrative point of view, analogous to the certification and approval process, the auditing of the technical gaming system is done by License and Operator. The operator is ultimately responsible for the presentation of audit reports that include its complete technical game system.

However, as has happened with the certification process, the industry has been organized itself in such a way that each supplier works with a single certification entity for each of the required jobs. In this sense, the operator can certify compliance with the audit of its technical gaming system, through the audit report of its supplier (s).

From a technical point of view, gaming software providers must submit to the audit of their operators, since they are part of their technical gaming system. However, suppliers may choose to conduct their own audit with their own certification body, at least with respect to those requirements that cannot or will be met through the audit carried out by each of the operators with whom is integrated. In these cases, the first audit must be carried out within six months after two years from the date of the first Resolution approving its integration with an operator licensed under Law 13/2011. That is, a provider can be integrated with several operators. However, the first operator with whom it is integrated, and in particular, the date on which this operator obtains the resolution by which the integration is approved, is the one that marks the calendar of performance of supplier audits. Note that the first type approval can take place through an approval resolution or a substantial change resolution. The successive audits must be carried out in the six months following four, six and eight years from the date indicated.

The operators, at the time of presenting the audit report, must include under the scope of this the gaming providers that have been commercializing for at least two years.

As a practical example, let's analyze the following scenario:

Stage:

1. An operator obtains the approval of its technical game system, which includes providers A and B.

2. One year later, the operator incorporates a third C game provider through a change management procedure.

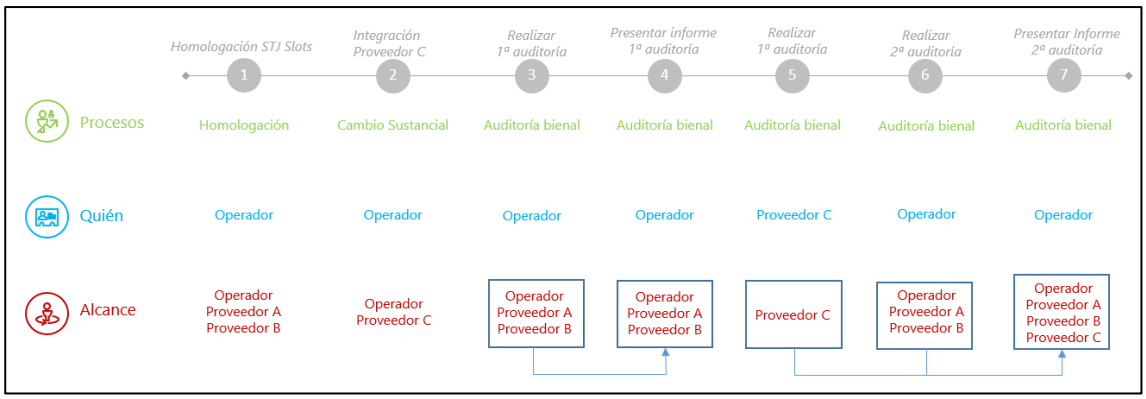
3. Two years after the approval, the operator carries out the first audit of his system, which includes suppliers A and B.

4. Two years and 6 months after the approval, the operator presents an audit report that includes suppliers A and B.

5. Two years after the substantial change resolution approving the integration of supplier C with the operator, supplier C (which has decided to carry out its own audit with its own certification body) carries out its first audit.

6. Four years after the approval, the operator carries out the second audit of its system, which includes suppliers A, B and C. In relation to supplier C, the aspects that only depend on the supplier have already been audited and should not be of being audited again

7. Four years and 6 months after the approval, the operator presents the audit reports that certify the complete audit of the operator and suppliers A, B and C (that is, it presents its operator's report and the supplier's report C).



b) Is a supplier audit report strictly necessary?

No. As indicated above, the industry itself has been organized in such a way that each gaming entity (operator or supplier) works with a single certification entity for each of the required jobs. In this sense, the operator could accredit compliance with the audit of its technical gaming system, through the audit report of its supplier (s). However, it would be equally acceptable for the operator to present a single audit report carried out by a single certification body and to include within its scope the set of technical requirements applicable to both the technical system of the operator and that of its suppliers.

c) What is the scope of a supplier audit report?

The supplier audit report must include all aspects that have not been audited in the audit conducted directly by the operator.

From the security point of view, analogous to the initial certification to which the supplier was submitted, the scope of the audit must cover the total of defined security areas.

d) Should a system that is not in production be audited?

No. A platform that is not in production at the date of compliance with the deadline for submission of the audit report is exempt from submitting to the audit. This circumstance must be formally communicated to the DGOJ. However, the reactivation of said platform will require the prior presentation of the audit report.

e) Audit and platform changes.

The first audit will be carried out in the six months following the expiration of the two-year term from the initial initial approval of a single license or from the date of resolution of change management approval whose scope includes the operator's complete technical game system . From there, the successive audits will be carried out every two years, always within a maximum period of six months.

In other words, when an operator undergoes a full platform change, the dates are restarted and a "first" audit of the new platform will be resubmitted, once it has been in operation for two years.

f) Incompatibility of the certification body for certification and auditing.

The certification body conducting the audits may not have participated in the initial certification or certification processes of substantial changes to the audited system.

A single certification entity can perform all audits, as long as it has not participated in the certification processes of the audited system.

For example, in a scenario in which an operator makes a complete change of platform, the certification entities that participated in the certifications and audits of the previous platform are irrelevant, in that they are two different platforms.

15. Clarifications regarding the cryptographically strong random number generators.

The Resolution of October 6th, 2014, of the Directorate General for the Regulation of Gambling, which approves the provision by which the technical specifications of game, traceability and security that must be met by technical gaming systems of a non-competitive nature are developed. reserved object of licenses granted under the Law 13/2011, of May 27, regulation of the game establishes in its section "3.5 Generator of random numbers (GNA). 3.5.1 Operation of the GNA. "Of Annex I:

"The random number generator will be cryptographically strong."

This regulatory modification comes to respond to the need to update the technical requirements of the random number generator from the point of view of its design and its security against new threats that could put at risk the proper functioning of chance in the game and, consequently, fair play. With this modification it is achieved, on the one hand, to establish a requirement that de facto already includes most generators, by the state of the art of the industry in this matter and, on the other hand, to match the requirements of the generators to the most of the jurisdictions of our environment.

A random number generator is cryptographically strong when its results are unpredictable even when the attacker has information about the algorithm, seed or previously generated results. That is, for a random number generator to be considered cryptographically strong, not only must it successfully pass statistical tests of randomness, but it must also overcome severe attacks, even if part of its state is available to an attacker.

In the previous version of the Resolution it was stated that "The generated random data must be unpredictable (its prediction must be unrealizable by computation without knowing the algorithm and the seed)." A cryptographically strong random number generator increases its entropy in its own design , avoiding the prediction of its results before a possible attacker. For example, in a random number generator software, it is necessary that the source that generates the seed is cryptographically unpredictable to be able to affirm that the generator is cryptographically strong.

The changes that must be made in the systems of generation of random numbers of the game operators (in their own and those of their suppliers) to make them cryptographically strong have consideration of substantial change in the technical system of game so that their put into production needs the prior authorization of the General Directorate for the Regulation of Gambling after the presentation of the corresponding certification report. Gaming operators have until January 1, 2020 to adapt their systems.

Operators that already have a cryptographically strong random number generator must submit a document issued by their functional certification entity in which this circumstance is accredited. The presentation of said writing must be done electronically, through the procedure called "Generic Communications to the DGOJ" available in the section of the electronic headquarters of the DGOJ "Procedures and Services / General utility", with the following information:

Unit: S.G. of Game Inspection

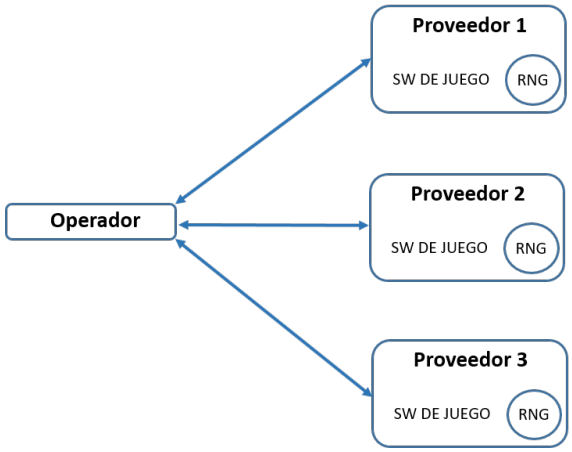
Subject: Random number generator

16. Clarifications regarding aggregators

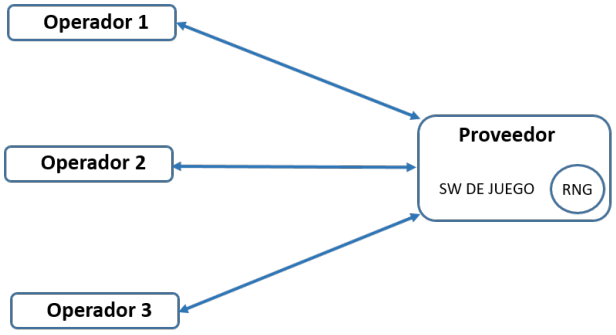
Introduction

In recent years, the use of aggregators in technical gambling systems has been snowballing. The advantage of this type of service is obvious: the integration between an operator and a gambling software provider is a costly and technically complex process. Using an aggregator allows an operator to connect with multiple providers through a single interface and a provider to connect with multiple operators through a single interface.

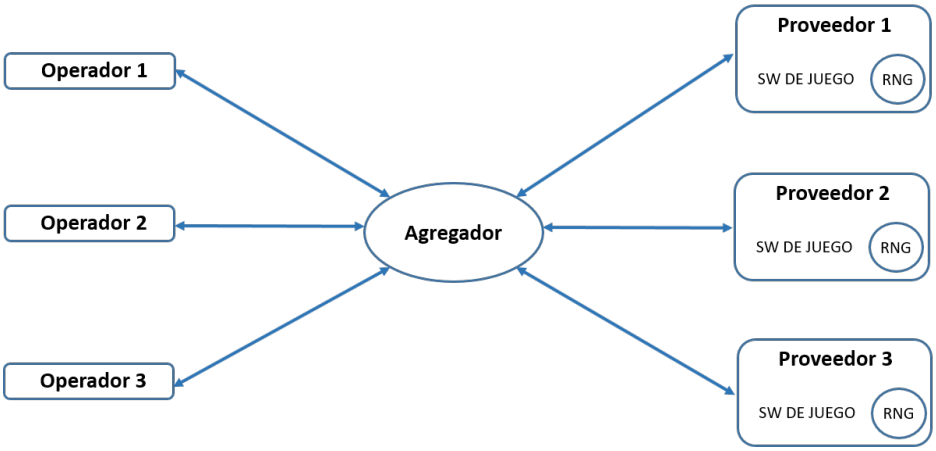
Direct integration between an operator and several providers implies a different connection between the operator and each provider, as represented below:



Similarly, direct integration between a provider and several operators implies a different connection between the provider and each operator, as represented below:



However, if we introduce an aggregator into this diagram, the structure is simplified, as there is a single connection between each operator and the aggregator; and a single connection between the aggregator and each provider:



Gambling regulations do not establish restrictions with regard to the architectures that make up the technical gambling system, and specifically, in the use of aggregators. However, it is necessary for this business model to be accompanied by an effort to clarify and structure the documentation presented, which allows a clear and complete identification of the technical structure of the operator's technical gambling system.

Definitions

In accordance with that stated in the previous section, three types of entities are identified that make up the technical gambling system:

- Operator: The entity that holds the licence, and as far as the technical architecture is concerned, it represent the game's platform.
- Gambling software provider: the entity that provides games.
- Aggregator: the entity in charge of interconnecting the gambling platforms with the gambling software providers. Aggregators process information, such as a player identifier or a wallet. Aggregators are part of the operator's technical gambling system and, as a consequence, are subject to certification and authorisation.

Note: The same entity can act as a gambling software provider and an aggregator at the same time.

Notable issues regarding authorisation

1. Each provider that is part of the technical gambling system must certify their security (gambling platform, gambling software provider and aggregator).

2. Gambling software needs to be certified by each gambling software provider.

3. Each integration that is part of the technical gambling system must be certified. This therefore includes the operation of aggregators, whose function is, ultimately, to integrate gambling platforms and gambling software providers.

4. For each specific licence, the integration with each provider that is part of the technical gambling system must be certified. In other words, the integration with the same provider for different specific licences must be independently certified and authorised within the framework of each specific licence.

5. Introducing a new gambling software provider into an operator's technical gambling system for a specific licence is always considered a substantial change and is therefore subject to prior authorisation. In other words, although it is technically a transparent process for the operator because the interface with the aggregator is unique, including games from a new gambling software provider, it is considered a substantial change for a specific licence.

6. Introducing a new aggregator into an operator's technical gambling system is always considered a substantial change and is therefore subject to prior authorisation.

7. A change in the integration model is considered a substantial change. For example, if the integration between the gambling platform and the gambling software provider changes from being direct to being through an aggregator, this is considered a substantial change.

Documentation to be provided

The documentation that must be attached to the request for a substantial change must include the following elements as a minimum:

- Updated technical plan. The following must be clearly identified:
    - List of gambling software providers.
    - List of aggregators.
    - Integration model between the gambling platform and each gambling software provider and aggregator that makes up the technical gambling system.
    - CPDs where the software of each gambling software provider and each aggregator is hosted.
    - Description of the aggregators:
        - roles they perform
        - description of the information processing and/or retention
        - description of the information received and sent from/to the gambling platform and the gambling software providers
        - integration model with the gambling platform and the gambling software providers
        - description of the security measures adopted by the aggregator
        - list of data centres that host the aggregator's software
- Contract (or service order or whatever corresponds) between the operator and each gambling software provider and aggregator that makes up the technical gambling system.
- Security certification report for each gambling software provider and aggregator that make up the technical gambling system.
- Functionality certification report for each of the existing integrations. In their scope, the reports must clearly and explicitly indicate the integration purpose of the certification, with exact references to the parts that are integrated and the way in which they are integrated, whether directly or through an aggregator.

Importance of clarity

The considerable number of gambling software providers in each operator, as well as the introduction of aggregators, introduces greater complexity when it comes to understanding the entire technical gambling system. For this reason, the Directorate wants to emphasise the importance of presenting the documentation with a clear and concise structure. The introduction of tables, descriptive texts or graphics can help the technical architecture be understood.

As an example, the following scenario is offered:

We analysed an operator offering four gambling software providers. One of these software providers also acts as an aggregator. There is additionally a second aggregator.

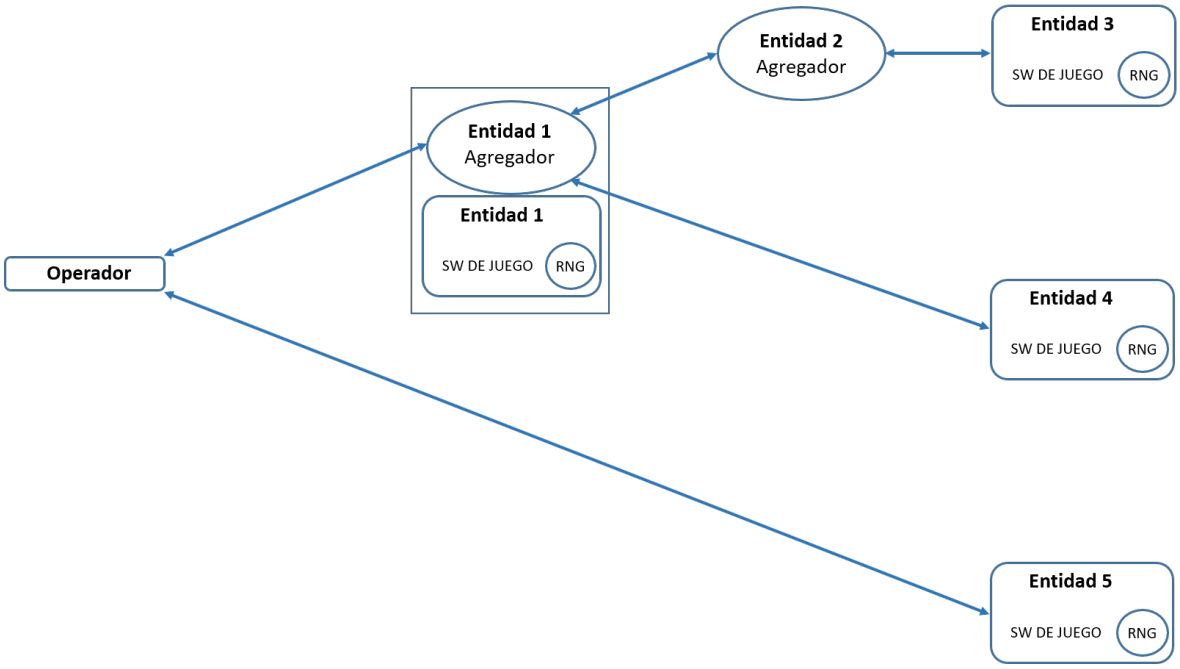
The integration models are described below:

- E1 is a gambling software provider and aggregator and is directly integrated into the platform.
- E2 is an aggregator and is integrated into the platform through the aggregator E1.
- E3 is a gambling software provider and is integrated into the platform through the aggregator E2.
- E4 is a gambling software provider and is integrated into the platform through the aggregator E1.
- E5 is a gambling software provider and is directly integrated into the platform.

The following table shows the above in a structured manner:

	Gambling software provider	**Aggregator**	**Integration into the platform**	**List of CPD's**
Entity 1 (E1)	Yes	Yes	Direct	(…)
Entity 2 (E2)	No	Yes	Through the aggregator E1	(…)
Entity 3 (E3)	Yes	No	Through the aggregator E2	(…)
Entity 4 (E4)	Yes	No	Through the aggregator E1	(…)
Entity 5 (E5)	Yes	No	Direct	(…)

The following diagram shows the above in a structured manner:



Approaches to certifying the integration

As stated above, each and every integration in the technical gambling system, both direct integrations and integrations through aggregators, need to be authorised. The DGOJ regulations and – in particular – the functionality certification report model does not establish a specific model integration through aggregators. In this sense, it is understood that the approach must respond to a technical criterion of good practices by the certification body. To date, different approaches have been identified when looking into certifying an integration when it is through an aggregator.

The first classification varies depending on the scope of the certification; two types are distinguished:

- First, we can speak of an "end-to-end" integration. In an integration between a gambling platform and a gambling software provider through an aggregator, the certification body certifies the correct execution of the gambling software provider's games on the operator's gambling platform.

  This is an ad-hoc certification report for the specific operator and provider, and is not able to be used by other operators.

  In these cases, it is essential that the certification body verifies, certifies and states in the report that the integration between the gambling platform and the gambling software provider is done through an aggregator.

- Second, we can speak of an ad-hoc integration between the aggregator and the operator or between the aggregator and the gambling software provider.
  This is not an "end-to-end" integration.
  In addition, in the case of an ad-hoc integration between the aggregator and the gambling software provider, the report can be used by other operators who share the same aggregator and want to use the same gambling software provider through the same aggregator. In this case, the report can be reused if the integration is identical, even if the operator isn't.

The second classification varies depending on the means of addressing the certification; two types are distinguished:

- Performing the integration tests defined in the Resolution that establishes the functionality certification report model (RES_CERT).

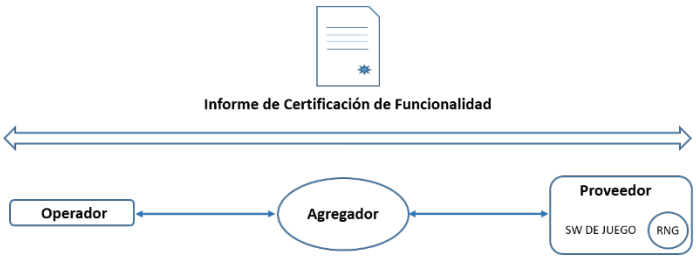
- Analysis of APIs, code and complementary tests that the certification body deems appropriate.

For the DGOJ, any approach is valid as long as the certification body can offer guarantees as to the correct integration between the parties that are subject to the work. Again, the importance of the certification body describing, explaining and providing sufficient detail on the purpose and scope of the certification, the tests carried out and the parties involved must be emphasised.

Example:

The operator requests integration with a gambling software provider through an aggregator.

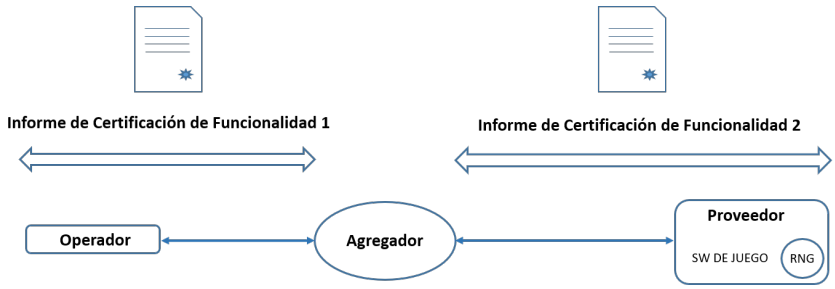
- Scenario 1:
  The operator contracts the certification body to certify the "end-to-end" integration. The certification body certifies the correct execution of the provider's games on the operator's gambling platform.



- Scenario 2:

The operator contracts the certification body to certify the integration of the gambling platform with the aggregator. From this work, a certification report is produced (1).

On the other hand, the aggregator (or whomever) contracts the certification body to certify the integration between the aggregator and the gambling software provider. From this work, a second certification report is produced (2). This certification report can be used by other operators, as long as the integration is identical, irrespective of the operator.



17. Clarifications regarding the studios

Introduction:

In reviewing the operators' technical documentation, this Directorate has identified an additional type of entity that makes up the operators' technical gambling systems; this Directorate calls them "studios". The purpose of this section is to publish what the Directorate understands by studio, so as to establish a common nomenclature and avoid confusion when describing the technical gambling systems.

Definition and concept

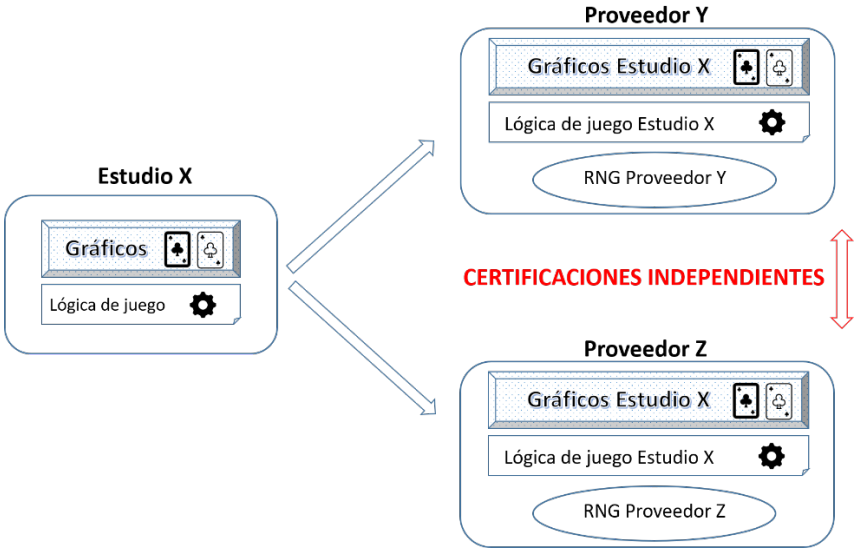
A studio is a manufacturer or developer of games for a certain provider. Unlike a gambling software provider, a studio does not manage the software in production, nor the security of the software. For this reason, a studio

is not considered a gambling software provider. Therefore, for regulatory and certification purposes, the studio is irrelevant.

Although it has been stated that the studio is irrelevant for regulatory and certification purposes, the truth is that operators and certification bodies often refer to software by the name of the studio instead of the name of the gambling software provider, which creates confusion and makes it difficult to understand the technical gambling system.

Sometimes studios only develop the graphics of the game and/or the logic of the game, but they do not have a random number generator, and it is up to the gambling software provider to bring randomness into the game.

Studios can work for a single or multiple gambling software providers. Where they work for multiple gambling software providers, we can find games developed by a studio for two gambling software providers, which gives rise to an identical game in appearance and rules, but with different software management, security management, data centre and random number generation for each gambling software provider. For certification and authorisation purposes, these are two different games from two independent gambling software providers.



Studios and certification framework:

As has been stated, for regulatory and certification purposes, the studio is irrelevant. Certification is the responsibility of the gambling software provider; the entity that manages the software in production, manages the security of the software and has CPDs that hosts the gambling software in production runs.

Importance of clarity with the documentation:

It is therefore essential that operators, gambling software providers and certification bodies are clear and concise when referring to and issuing documentation related to gambling software providers and studios.

In the event that the documentation presented refers to studios, it is essential that the gambling software provider that manages the games of said studio be explicitly stated.

As an example, the following scenario is offered:

We analyse an operator that shows two gambling software providers, E1 and E4 and three studios, E2, E3 and E5.

Gambling software provider E1 manages their own games and games from two studios, Studios E2 and E3. All games share a single GNA and all games are hosted in the same data centres.

Gambling software provider E4 manages their own games and games from one studio, Studios E5. All games share a single GNA and all games are hosted in the same data centres.

The following table shows the above in a structured manner:

	Gambling software provider	**Studio**	**For the studios, gambling software provider that manages the studio's software**	**GNA**	**List of CPDs**
Entity 1 (E1)	Yes	No	Not applicable	GNA E1	CPD's E1
Entity 2 (E2)	No	Yes	E1	GNA E1	CPD's E1
Entity 3 (E3)	No	Yes	E1	GNA E1	CPD's E1
Entity 4 (E4)	Yes	No	Not applicable	GNA E4	CPD's E4
Entity 5 (E5)	No	Yes	E4	GNA E4	CPD's E4

The documentation to provide in this scenario is:

- Security certification report on the two gambling software providers
- Functionality certification report that certifies the integration with the two gambling software providers
- Functionality certification report on all gambling software, both from gambling software providers and studios.