Requirement matrix for the certification

(version 1.0 dated 07/10/2022)

Required for the 6 months certification?	Required for the annual certification?	Checkpoint	Label	Criticality level	Analysis elements	ANJ Comments	Relevant reports	Compliance	Certifying body comments
	YES	**PART 1 - Monitoring security audits, certifications, and approvals**							
	YES	E1	As part of the ANJ's general control mission, certifying bodies conduct security audits to verify the operators' SSI maturity level and the level of security achieved by the SMA devices and gaming platforms. Access to the site, as well as to all equipment and data of the gaming platform(s), must be granted to the ANJ or the authorized certifying bodies.	3	Documentation provided by the operator. Hosting platform configuration audit.	The operator must provide the authorized certifying body with all required access and configuration elements to allow them to perform the expected controls within the scope of their audit mission.		Compliant	
	YES	E2	The operator must address any identified minor, important, major, or critical vulnerabilities following the security audits. If no security measures directly correct them, the operator must propose temporary workaround measures to prevent the exploitation of these vulnerabilities. The associated remediation plan established by the operator must be communicated to the ANJ and the authorized certifying body.	3	Documentation provided by the operator, including: - Game software approval reports; - Configuration audit reports conducted as part of the initial certification at 6 months of the SMA device or previous annual certifications, if applicable; - Security audit reports conducted on the operator's information systems, whether performed by the ANJ or an entity authorized by the ANJ; - Remediation plans associated with the identified vulnerabilities.	It should ensure that all vulnerabilities identified during security audits are remediated and that the most relevant recommendations are implemented.		Compliant with reservations	
	YES	E3	The operator informs the ANJ of substantial changes made within its platform(s) (e.g., implementation of a new technology).	2	Documentation provided by the operator.	The operator must present to the certifier the list of changes made to its information systems (sensor + gaming platforms) at the software and infrastructure levels, including both client-side and server-side components, as well as the information communicated to the ANJ since the accreditation application submission or the last annual certification, if applicable.		Non-compliant	
	YES	E4	The operator communicates to the ANJ the results of security audits conducted on its gaming platforms by third-party organizations.	1	Documentation provided by the operator.				
	YES	E5	New game software must undergo systematic approval before being deployed.	3	Documentation provided by the operator.	The operator must list the versions of game software used (both client-side and server-side) and provide the corresponding approval reports and decisions. This requirement includes any client software deployed on smartphones or corresponding server-side interfaces. An expert opinion is expected from the certifier regarding the approvals conducted, taking into account the history of modifications made to the software on both client and server sides.			
	YES	**PART 2 - ISMS: Operator's Information Systems Security Policy and Master Plan**							
	YES	E6	The operator has an Information Systems Security Master Plan or an equivalent document. They will specify the start date of its application and the frequency of updates. They will also indicate if it is integrated into the IT Master Plan and provide the latest version and, if possible, the previous version.	1	Documentation provided by the operator + initial-level analysis.	The analysis should focus on the hosting platform of the SMA and the gaming platform(s).			
	YES	E7	The operator has an Information Systems Security Policy. If such a document does not exist, they will indicate if any document(s) fulfill a similar function. This security policy should address the following topics:	1					
	YES		- Strategic elements:						
	YES	E8	- The scope of the security policy, for example, in terms of business areas or information systems;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E9	- Strategic issues and orientations, by formulating the challenges related to the previously defined scope;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E10	- Legal and regulatory aspects related to the scope of the security policy;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E11	- A needs scale that includes weighting and reference values according to the chosen security criteria, as well as a list of impacts enriched with examples;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E12	- A description of the security needs of the operator's business areas, based on the needs scale presented in the previous section;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E13	- A selection of retained and non-retained threats for the study scope, with justifications.	1	Documentation provided by the operator + initial-level analysis.				
	YES		- Security rules, classified by theme:						
	YES	E14	- Organization: SSI organization, risk management, security and life cycle, insurance and certification, PSSI evolution;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E15	- Implementation: human aspects, contingency plan, incident management, awareness and training, operation, physical security;	1	Documentation provided by the operator + initial-level analysis.				
	YES	E16	- Technical: identification/authentication, logical access control, logging, encryption.	1	Documentation provided by the operator + initial-level analysis.				
	YES	E17	The operator implements the elements required by its security policy. This technical and detailed implementation establishes the link between the security policy and all information system-related procedures, by providing both organizational and technical means of securing the information systems and ensuring their ongoing monitoring.	2	Documentation provided by the operator + initial-level analysis.				
	YES	E18	The operator must impose security requirements on various subcontractors with whom contractual relationships are established; they will provide them if possible.	1	Documentation provided by the operator + initial-level analysis.				
YES	YES	**PART 3 - Global Architecture and Administration and Operation Procedures**							
YES	YES		The organization established to manage the operator's information system must rely on documentation and procedures to track its evolutions. The documentation includes:						
YES	YES	E19	- Procedures derived from the security policy;	1	Documentation provided by the operator + initial-level analysis.				

YES	YES	E20		- A functional description of the SMA hosting infrastructure, specifying the different components, their functions, and the flows passing through them.	1	Documentation provided by the operator + expert opinion.				
YES	YES	E21	Documentation of the hosting infrastructure of the SMA and the operator's gaming platform, which includes both technical and procedural aspects, is compiled into a file called the "definition file."		1	Documentation provided by the operator + initial-level analysis.				
YES	YES	E22	Throughout the validity period of the exclusive rights accreditation or operating authorization, the operator is responsible for keeping the "definition file" up to date and consistent. Each modification to the file must be submitted as a new document to the ANJ.		1	Documentation provided by the operator + initial-level analysis.	Modifications to the "definition file" made within the year are compiled and presented to the cert ifying body. This submission during the annual certification serves as submission to the ANJ.			
YES	YES		The documentation of the hosting infrastructure of SMA and the gaming platform, which includes technical and procedural aspects, gathers the following information:							
YES	YES	E23		- a description of the architecture in terms of technical components, addressing and naming plan, flows, mentioning associated protocols, connection establishment direction, filtering rules, etc.;	2	Documentation provided by the operator (definition file) + expert opinion.				
YES	YES	E24		- the technical specifications of the information system, particularly the up-to-date configurations of its components;	2	Documentation provided by the operator (definition file) + expert opinion.				
YES	YES	E25		- a detailed descriptive list of all components, including factual elements such as software versions used, maintenance contracts, configurations, and the status of modifications made, etc.;	2	Documentation provided by the operator (definition file) + preliminary analysis.				
YES	YES	E26		- a list of operating procedures, including: - log management procedures; - alert management procedures; - regular update procedures for all components (operating systems, applications, routers, etc.); - procedures for managing frequently	1	Documentation provided by the operator (definition file) + preliminary analysis.				
	YES	**PART 4 - Network Architecture**								
	YES	E27	The operator's information systems must be subject to network segmentation and filtering in accordance with the defense-in-depth principle, especially at the level of service, administration, and platform supervision networks.		2	Documentation provided by the operator + expert opinion.	A level 3 diagram must be created by the certifier. This diagram must include the IP addresses of the most important machines.			
	YES		The operator implements network segregation using at least level 3 (OSI model) filtering mechanisms, at least between the following zones:							
	YES	E28		- zones dedicated to servers, with additional segregation based on the sensitivity level identified for each one by the security policy: - business servers (application servers, database management systems), - infrastructure servers (authenticatio	2	Documentation provided by the operator, particularly: a) configuration audit reports of hosting platforms carried out as part of the initial verification of the gaming platform; b) configuration audit reports of the 6-month certification of the SMA device; c) configuration audit reports of previous annual certifications, if applicable. Configuration audit of hosting platforms. Technical architecture audit of the gaming platform.				
	YES	E29		- the zone for equipment dedicated to administration, operation, and supervision of the information system. This zone, which notably hosts administrators' workstations and supervision servers, must receive special attention due to the privileged access th	2		Administration interface filtering must be done at level 3 (IP) and not only at level 7 (application layer).			
	YES	E30		- the dedicated areas for user workstations, if applicable, with additional segmentation that can vary in granularity depending on the missions of different business units and the criticality of the information they are responsible for.	2					
	YES	E31	The adopted network filtering policy respects the principle of least privilege: filtering rules are developed based on a whitelist principle.		2	Audit of hosting platform configurations. Technical architecture audit of the gaming platform.	The analysis should take into account inbound and outbound filtering.			
YES	YES	E32	The operator implements security mechanisms to defend against classical IP attacks and associated protocols, particularly regarding network denial of service attacks.		2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	**PART 5 - Security Maintenance**								
YES	YES	E33	As part of maintenance and security upkeep, the operator keeps up with software updates from vendors to be able to obtain security patches regularly. The operator monitors at least the advisories and alerts from a CERT, such as CERTA (https://www.certa.ssi.gouv.fr). The operator applies security patches proposed by vendors, as documented by the CERT or explicitly requested by ANJ if applicable.		2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E34	The operator must, at a minimum, prohibit the use of obsolete systems and software on its platforms, i.e., those that are no longer maintained by their vendors and no longer receive corrective support.		2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES		If no security patch is available from the vendor:							
YES	YES	E35		- the operator follows the recommendations of the vendor or a CERT for temporary workarounds;	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E36		- if the workaround requires disabling an essential system functionality, the operator commits to proposing measures to prevent the exploitation of the vulnerability.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E37	The operator maintains an up-to-date "definition file" listing the applied security patches on the servers and communicates the updated version of the document to ANJ.		1	Audit of hosting platform configurations. Documentation provided by the operator (definition file) + initial-level analysis.				

YES	YES	**PART 6 - Communications Security and Administrative Access Control**								
	YES	E38	All data exchanges must be secured using cryptographic methods to ensure component authentication, confidentiality, and authenticity of communications. All file exchanges (administration data, content updates, etc.) must use mechanisms based on recognized encryption algorithms and protocols standardized by the IETF (IPsec, TLS, SSH, etc.). These exchanges primarily include the following communications: - Communications between the operator and ANJ; - Network communications between players and the operator; - Network communications between modules within the SMA.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES		Administrative access to equipment, including SMA equipment, must be protected using the following mechanisms:							
YES	YES	E39	- primarily, authentication using X.509v3 certificates, RSA public key, or two-factor systems (including one-time password), if supported by applications and systems;	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E40	- alternatively, password-based authentication with composition and renewal rules that comply with the best practices recommended by CERTA, as detailed by the operator. These passwords should be used in the case of challenge/response authentication protoc	2	Audit of hosting platform configurations. Documentation provided by the operator.	Clear-text authentications are prohibited; encryption of communications is mandatory. The measure must demonstrate password robustness.			
YES	YES	E41	- access control based on IP adresses is operational	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	**PART 7 - Configuration Management**								
YES	YES	E42	After implementing a new equipment or installing a new application, the operator provides ANJ with an updated version of the "definition file" containing all the information related to the configuration of that new element.	1	Audit of hosting platform configurations. Documentation provided by the operator (definition file) + initial-level analysis.				
YES	YES	E43	The system, network, and application components implemented by the operator must undergo security hardening, including restricting applications executed at startup, limiting the number of applications listening on the network, disabling unnecessary or dangerous features (application server administration interface), removing manufacturer accounts and passwords, etc.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E44	To detect potential manipulation errors and the results of attacks, the integrity of equipment configuration files must be regularly verified. This verification must be performed upon ANJ's request, and a diagnostic report must be provided to ANJ.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	**PART 8 - Security Management in Development Lifecycles**								
YES	YES	E45	The operator manages security at each stage of the development lifecycle of its systems, including definition, development, operation, use, maintenance, and evolution.	2	Documentation provided by the operator.	This requirement includes verifying the technical procedure related to this transmission and the operator's duty to perform it.			
YES	YES	E46	The operator contracts with its service providers to adhere to a secure development framework for projects that are outsourced.	1	Intrusive application audit. Documentation provided by the operator.				
YES	YES		The secure development framework should specifically address parameter validation, including:						
YES	YES	E47	- verifying all user-transmitted data based on criteria such as size, type, and allowed characters, using a whitelist mechanism;	2	Intrusive application audit. Documentation provided by the operator.				
YES	YES	E48	- validating input and output data;	2	Intrusive application audit. Documentation provided by the operator.				
YES	YES	E49	- use a unique and centralized data verification function	2	Intrusive application audit. Documentation provided by the operator.				
YES	YES	E50	The operator must be able to provide ANJ with the complete source code of game software components, as defined by the Technical Requirements (ET2) volume, used on its platforms, if requested by ANJ.	3	Documentation provided by the operator.				
YES	YES	**PART 9 - Data Backup Management**								
YES	YES	E51	The operator provides the means to implement an archiving service to ensure the preservation of all its processing data, particularly those stored in the SMA's vault component.	3	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E52	These backups are made available to ANJ by the operator for consultation and archiving.	2	Documentation provided by the operator.				
YES	YES	E53	The type of media and the format of the backup are indicated by the operator to allow ANJ to verify the usability of these backups and their contents.	3	Documentation provided by the operator.				
YES	YES	E54	The data that the operator is required to make available to ANJ (cf. articles 30 and 31 of decree n 2010-518) must be retained for a period of 6 years. For personal data concerning each player, this 6-year period starts from the closure of the corresponding player account.	3	Documentation provided by the operator.				
YES	YES		Throughout the entire retention period, the archives and their backups must:						
YES	YES	E55	- be protected for integrity;	3	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E56	- be accessible only to authorized personnel;	3	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E57	- be readable and exploitable.E93- maintain	3	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E58	The level of protection for backup archives must be at least equivalent to the level of protection for the archives: the operator will present in its response the archiving mechanisms as well as the means of protecting the archives that it is capable of implementing.	2	Audit of hosting platform configurations. Documentation provided by the operator.				

YES	YES	E59	The accuracy of the clock against which information systems synchronize to date logged or archived events must be within one second of UTC time. The time source must be reliable.	2	Audit of hosting platform configurations. Documentation provided by the operator.	The auditor must demonstrate compliance with the requirement.			
YES	YES	**PART 10 - Technical and Functional Logging Management**							
YES	YES	E60	The operator must maintain and be able to provide ANJ with logs of technical traces for key events. An initial list of the events concerned - access to SMA modules; - maintenance operations performed; - opening and closing of betting, poker bets, etc.	2	Documentation provided by the operator.				
YES	YES	E61	If natural persons are the originators of the traced events: - logging must allow establishing a link between the technical identifier used in the trace and the natural person responsible for the actions; - events are logged based on a reliable time source.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E62	Regarding administration (creation of a Linux user account, modification of permissions on a Windows directory, addition of a Linux package, etc.), all available traces at the equipment level are enabled to identify the administrator who performed the action in case of detected issues.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E63	The operator consolidates all traces from the technical logging of different equipment (network, system, applications, and security), for example, via the syslog application and protocol.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E64	Security traces from the technical logging of the platforms are periodically analyzed by the operator to identify any anomalies.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E65	Technical logs produced by the different equipment must be retained for a minimum of three months as archives.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E66	The operator may provide ANJ with the raw logs produced by the different equipment or software.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	E67	Incidents or abnormal behaviors that may impact the service's security must be addressed and systematically reported in written form, which can be communicated to ANJ.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
YES	YES	**PART 11 - Physical Access Management**							
YES	YES	E68	Technical premises must only be accessible to authorized personnel designated by the operator.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES		The operator must:						
	YES	E69	- be able to clearly identify individuals who need to intervene in its premises and on its equipment;	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	E70	- keep up to date the access grants of this staff	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	E71	Persons who need to work on the gaming platforms' equipment must be aware of information system security (e.g., confidentiality of passwords and hosted data, etc.).	1	Documentation provided by the operator.				
	YES	E72	The operator must formalize and implement necessary organizational procedures regarding the stakeholders, including verifying the absence of conflicts of interest, candidates applying for sensitive positions, as well as procedures for securing information when they leave the company (retrieving badges, password management, etc.).	1	Documentation provided by the operator.				
	YES	E73	The premises housing the equipment must be secured with high-security locks, opening alarms, access records, video surveillance, etc.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	E74	Physical access to the premises housing the equipment must be restricted, including personnel filtering and physical access control.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	**PART 12 - Physical Environment Management**							
	YES	E75	IT equipment and media (backup media, etc.) must be placed in physically secure areas designed to prevent intrusion attempts and protect against environmental disasters and accidents.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	E76	The hosting facility has fire protection measures in place.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	E77	The hosting facility has dual power supply, uninterruptible power supplies, and a primary and secondary generator system for electronic security.	2	Audit of hosting platform configurations. Documentation provided by the operator.				
	YES	E78	A redundant and independent air conditioning system per room ensures temperature and humidity stability.	2	Hosting platforms configuration audit. Documentation provided by the operator.				
	YES	E79	All equipment (air conditioners, electrical panels, etc.) used by the operator are covered by a maintenance contract.	1	Hosting platforms configuration audit. Documentation provided by the operator.				
	YES	E80	Operating sites must be monitored 24/7.	2	Hosting platforms configuration audit. Documentation provided by the operator.				
	YES	**PART 13 - Security Team**							
	YES	E81	The operator must have a security team responsible for monitoring all network equipment, systems, and applications. The logical security of the equipment will be carried out under the control of this team.	1	Documentation provided by the operator.				
	YES	**PART 14 - Prohibited Activities**							

	YES	E82	The DNS server must be secured according to the state of the art, particularly in terms of: - updating, - hardening of the underlying operating system, - hardening of the configuration (especially with limiting recursion to only authorized hosts of the gaming platform, through an access control list). The IP addresses of the operator's DNS servers are communicated to the ANJ to implement network filtering rules and application-level access control lists.	3	Hosting platforms configuration audit. Documentation provided by the operator.	The requirement regarding time synchronization applies in particular to DNS servers performing queries to ensure the proper functioning of the TSIG security extension.			
	YES	**PART 15 - Data on Demand**								
	YES	E83	In addition to the data tracked in the SMA or systematically made available, the ANJ may occasionally require more detailed reports or data established with specific search criteria, which may include personal information. Thus, the operator must be able to execute queries on its business systems to extract data within reasonable timeframes. These reports will complement the information that can be obtained through the SMA and the information automatically sent to the ANJ's information system. These include: - providing the ANJ with all technical and non-technical data related to a specific event; - requests for investigation by the ANJ regarding detected and considered abnormal events; - detailed player identity; - detailed payment account details of a player; - details of a poker game, including full visibility of all participating players (all cards, regardless of the operator to which the players are affiliated in the case of player pooling networks); - certain statistics not provided in the supervision data; - details of a specific bet; - providing technical data (logs) concerning certain elements of the gaming architecture (SMA, platform, etc.).	3	Documentation provided by the operator.	For each of the elements mentioned as an example, the operator must specify the nature of the retained data, the corresponding retention period, and the procedures implemented to make this information available to the ANJ.			
YES	YES	**PART 16 - SMA: General**								
YES	YES	E84	The operator must set up a dedicated website, exclusively accessible through a top-level domain name ending in .fr.	3	Documentation provided by the operator (technical information about the fully qualified domain name: Whois, DNS resolutions, etc., and about all domain names declared with the ANJ)				
YES	YES	E85	All connections to the operator's website or one of its subsidiaries' websites originating from a French IP address or from a player's account with a registered address in France must be redirected to this website.	3	Hosting platforms configuration audit. Documentation provided by the operator.				
YES	YES	E86	As part of its gaming activities, the operator implements a technical device called "SMA" for control purposes. The SMA is a data collection and archiving device related to a gaming event or a player account. This device is:	3	Audit of hosting platforms configuration. Documentation provided by the operator.				
YES	YES	E87	- developed and operated under the responsibility of the operator;	2	Documentation provided by the operator (identification of providers: developers, operators, etc.).				
YES	YES	E88	- installed on A support located in metropolitan France.	3	Audit of hosting platforms configuration. Documentation provided by the operator.				
YES	YES	E89	All data exchanges related to a gaming event or a player account, between a player considered French and the gaming platform, must pass through the SMA.	3	Audit of hosting platforms configuration. Documentation provided by the operator.				
YES	YES		In particular, connections from players considered French must be redirected to the SMA. The gaming platform must redirect the following requests to the SMA:						
YES	YES	E90	- prior to player authentication, if the connection originates from a French IP address (country of IP address assignment for the Internet terminal from which they connect is France in the RIPE NCC database);	3	Audit of hosting platforms configuration, particularly the description of technical devices implemented by the operator on the SMA/gaming platform side (e.g., description of the geolocation module implemented at the HTTP or DNS level), supported by configuration excerpts (e.g., Apache geolocation module) and code snippets (post-authentication redirection).				
YES	YES	E91	- or, after player authentication, if the player has indicated a domicile in France when opening their game account.	3					
YES	YES	E92	The operator must allow the ANJ to access the SMA hosting site at any time to retrieve all or part of the stored data. For this purpose, the ANJ must inform the operator's representative of its intention to access the site at least two hours in advance and provide the time at which access should be granted to them.	3	Procedures implemented by the operator and the SMA host, if applicable, to authorize such access.	This notably concerns access to the hosting site of the SMA's vault component.			
YES	YES		The following data exchanges must be secured to ensure authenticity, integrity, and confidentiality:						
YES	YES	E93	- exchanges between the player and the SMA;	3	Audit of hosting platforms configuration, particularly the technical description of the security protocols implemented (e.g., algorithms, X.509 certificates, if applicable, etc.).	Expert opinion on HTTP/HTTPS interactions for web applications, especially for access to the authentication form and session ID management, etc.			
YES	YES	E94	- exchanges between different modules of the SMA; - exchanges between the SMA and the operator's gaming platform; - exchanges between the SMA and the ANJ platform.	2	Audit of hosting platforms configuration, including the architectural diagram.	Technical description of the flows and protocols involved, specifying the means of encryption/authenticity of the flows (IPsec transport, SSL/TLS, or equipment co-location, for example), and authentication mechanisms implemented by the parties.			
YES	YES		The SMA must have security features to protect it from saturation attacks, acting as follows:						
YES	YES	E95	- at the transport level, if this component terminates TCP connections initiated by clients: protection against network denial-of-service attacks that aim to exhaust TCP resources through SYN Flood attacks or attacks that rely on completing a TCP connecti	2	Audit of hosting platform configuration, including the description of technical devices implemented by the operator, supported by configuration elements, or incident management procedures implemented with the upstream service provider, if applicable, for example.				
YES	YES	E96	- at the application level, with the sending of multiple HTTP requests that would aim to saturate the SMA, which potentially represents a single point of failure in the architecture, in order to protect it from (i) resource exhaustion (saturation of tempo	2	Audit of hosting platform configuration, intrusive application audit of the sensor application, including the description of technical devices implemented by the operator supported by configuration elements.				

YES	YES	**PART 17 - SMA: "Coffre-fort" module**								
YES	YES	E97	The "Coffre-fort" must hold a level one security certification (CSPN) issued by ANSSI (https://www.ssi.gouv.fr).		3	The absence of CSPN certification is a major obstacle to obtaining the SMA certification.				
YES	YES		The level one security certification must, at a minimum, take into account the following elements in terms of threats:							
YES	YES	E98		- unauthorized deposit or injection of records;	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E99		- alteration of records;	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E100		- data theft;	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E101		- denial of service.	3	Report and target of the ANSSI/CSPN certification.				
YES	YES		The level one security certification must, at a minimum, take into account the following elements in terms of security functions:							
YES	YES	E102		- strong authentication of users and administrators;	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E103		- encryption, signature, and timestamping of events;	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E104		- chaining of events.	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E105	Any deletion or alteration of archived data, whether malicious or not, must be identifiable by the ANJ.		3	Audit of hosting platform configuration. Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES		Four authorization profiles must be definable:							
YES	YES	E106		- "depositor" profile: profile assigned to the "sensor" module of the SMA. It only allows writing traces in the log. The SMA sensor module authenticates itself to the "Coffre-fort" part using an X.509v3 certificate associated with this profile;	1	Audit of hosting platform configuration. Documentation provided by the operator.				
YES	YES	E107		- "reader" profile: profile assigned to ANJ agents with control and auditing powers, which allows extraction of recorded data either on removable media or through a file deposit accessible via a web service;	1	Audit of hosting platform configuration . Documentation provided by the operator.				
YES	YES	E108		- "technical and operational administrator" profile: profile assigned to the technical personnel of the operator responsible for the administration and technical supervision of the "Coffre-fort";	1	Audit of hosting platform configuration. Documentation provided by the operator.				
YES	YES	E109		- "functional administrator" profile: profile assigned to individuals from ANJ or designated by ANJ, who can define roles and associate them with an authentication certificate. This operation is necessary for initializing vaults, as well as for certificat	1	Audit of hosting platform configuration. Documentation provided by the operator.				
YES	YES		Certificates associated with the "reader" profile are used as follows:							
YES	YES	E110		- either by individuals for on-site controls, using RSA smart cards and an X.509v3 authentication certificate, for example, stored on hardware provided by the operator;	1	Audit of hosting platform configuration. Documentation provided by the operator.				
YES	YES	E111		- or by collection agents for remote consultations, with authentication based on an X.509v3 client SSL/TLS certificate, as part of a mutually authenticated SSL/TLS tunnel negotiation.	1	Audit of hosting platform configuration. Documentation provided by the operator.				
YES	YES		Regarding encryption, signing, and timestamping key management:							
YES	YES	E112		- key sizes must comply with the rules set forth in the general security repository of ANSSI (https://www.ssi.gouv.fr/);	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E113		- the cryptography used for pseudo-random number generators, hash functions, symmetric, and asymmetric algorithms must comply with the best practice rules specified in the general security repository of ANSSI (https://www.ssi.gouv.fr/);	3	Report and target of the ANSSI/CSPN certification.				
YES	YES	E114		- an HSM is used for signature operations; the signing key pair can either be generated within the HSM or injected into it;	3	Report and target of the ANSSI/CSPN certification.	If the signing key is injected, an expert opinion on the security of the key generation method outside the HSM is required.			
YES	YES	E115		- The encrypted data is encrypted using The public key of The certificate transmitted by ANJ: only ANJ can decrypt The content of The archived data. Note: data encryption operations can be performed using either hardware or software means.	3	Audit of hosting platform configuration. Documentation provided by the operator.				
YES	YES	E116	In terms of vault trace storage, the "Coffre-fort" implements segregation between the storage space intended for administrative data and the one(s) intended for traced game data. In the case of a shared vault among multiple approvals, each approval must have a specific storage space. Segregation of storage spaces must be implemented, a fortiori, in the context of interoperator mutualization, if applicable.		3	Report and target of the ANSSI/CSPN certification.				
YES	YES		Physical access security to the "Coffre-fort" is ensured by:							
YES	YES	E117		- hosting in a secure location;	2	Audit of hosting platform configuration: a preliminary analysis of the physical security of the hosting infrastructure is expected.				
YES	YES	E118		- implementation of access control;	2	Audit of hosting platform configuration: a preliminary analysis of the physical security of the hosting infrastructure is expected.				
YES	YES	E119		- Implementation of intervention monitoring procedures (all safe configuration operations must be tracked);	2	Audit of hosting platform configuration: a preliminary analysis of the physical security of the hosting infrastructure is expected.				

YES	YES	E120		- Implementation of physical protections.	2	The sealing method of the safe must be subject to a procedure which, regardless of the method used, must be probative and ensure the safety of any intervention that would result in breaking said device.				
YES	YES	**PART 18 - SMA: "sensor" module**								
YES	YES	E121	The sensor must implement defense mechanisms to protect its buffer memory and prevent any saturation of the memory or the safe itself.		2	Intrusive application audit of the sensor application. Documentation provided by the operator.				
YES	YES		The "sensor" module must:							
YES	YES	E122		- be authenticated by certificate to the safe, with a session opened with the 'depositor' profile;	2	Documentation provided by the operator, supported by elements from the intrusive application audit of the sensor application.	The analysis must be supported by source code excerpts from the sensor.			
YES	YES	E123		- await an acknowledgement from The safe in The form of proof of deposit.	2	Documentation provided by the operator, supported by elements from the analysis of the intrusive application audit of the sensor application. See the requirements dedicated to trace creation and storage functions.				
YES	YES	E124	All SMA components must be time-synchronized with a reliable time source.		3	Audit of hosting platform configuration.				
YES	YES	**PART 19 - SMA: trace creation and storage functions**								
YES	YES		The trace creation function of the sensor must adhere to the following principles:							
YES	YES	E125		- The trace creation function corresponds to writing data related to a gaming event or player account in the SMA safe module. This function must be called systematically for each event or data exchange that requires tracing;	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E126		- The trace creation function is implemented upstream of the game logic. It intercepts or relays the application flow between the player and the operator (e.g., proxy-type operation);	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements from the analysis of the intrusive application audit of the sensor application.	Implementing the trace creation function upstream of the game logic specifically concerns events to be traced to the safe where player acknowledgment is expected or is a direct consequence of a player action. In contrast, when the event originates from the operator and does not require player acknowledgment, the trace creation function is directly called by the game platform.			
YES	YES	E127		- The SMA must provide an architecture with very high availability and redundancy mechanisms to strictly limit potential storage incidents;	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E128		- The principle of canceling A game affected by A storage incident must be adopted.	2	Description of the technical devices implemented by the operator, supported by configuration elements and elements from the analysis of the intrusive application audit of the sensor application.				
YES	YES		The trace creation function of an event must:							
YES	YES	E129		- to be invoked following a request issued by the player (if it requires registration). This request may result from: (i) an action by the player, initiated by them, such as placing a bet, (ii) an acknowledgement by the player, following a message transmi	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E130		- to be invoked following an action initiated by the operator, without acknowledgement by the player, whose trace is required (e.g., correction of player account information).	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E131		- based on a state-based application module: the generated event traces must be temporarily stored at the sensor level in a buffer or equivalent temporary storage device (e.g., a database), pending acknowledgement from the gaming platform validating the c	3	Compliance with the state-based operating mode ensures that events transmitted to and generated by the player's initiative (action or acknowledgement) are validated by the platform before being stored in the safe.	Any deviation from this operating mode must be technically justified (e.g., POPARTIE events generated by the gaming platform and transmitted to the player for acknowledgement before storage). A technical analysis of the security of the event validation process by the sensor is expected, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application. An operating mode in which data transmitted by the player would be directly logged by the safe is prohibitive for SMA certification.			
YES	YES	E132		- managing acknowledgement from The gaming platform in order to limit The risks of attacks aiming to saturate The safe with random events or to record falsified events generated by A malicious player.	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E133		- in case of a negative acknowledgement from the gaming platform, the pre-recorded event at the sensor level must be destroyed. An error must be generated and recorded in the sensor's technical log.	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E134		- in case of a positive acknowledgement from the gaming platform, the event present in the buffer at the sensor level can be transformed into the format required by ANJ for storage in the safe.	3	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.				
YES	YES	E135		- managing cases of negative acknowledgements from The safe in case of recording failure.	2	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.	Error recovery mechanisms can be implemented at the sensor level, for example, by attempting to retransmit the event to the safe.			

YES	YES	E136		- Ensure the recording of a game event at the safe, under penalty of canceling the game operation.	2	Description of the technical devices implemented by the operator, supported by configuration elements and elements resulting from the analysis of the intrusive application audit of the sensor application.	This requirement is based on a synchronous operating mode between sensors and safes. In this model, the sensor must wait for a positive acknowledgment from the safe before continuing the transaction. In practice: - The introduction of batch processing, if applicable, prohibits strict synchronous operation, - The approval of using queue-based mechanisms between sensors and safes also prohibits this mode of operation. Therefore, a technical expert opinion is expected on: - The synchronization between the sensor and the deposit mechanism at the safe, describing the queues, detection mechanisms, and error recovery (e.g., retransmission by the sensor); - The redundancy and reliability of the device ensuring the processing of events between their emission by the sensor and their storage in the safe (e.g., analysis of the message broker-type queue mechanism).			
YES	YES		The storage function corresponds to archiving traced data in a digital safe to ensure their integrity and completeness over time. The data storage consists of the following steps:							
YES	YES	E137		- Establishing a secure channel, following mutual authentication between the depositor (i.e., the sensor) and the safe, via a mutually authenticated TLS session with X.509v3 certificate.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E138		- verifying The authorization of The profile to deposit traces.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.	The approval of using queue-based mechanisms between sensors and safes also prohibits this mode of operation.			
YES	YES	E139		- Chaining with the previous trace, linking the data fingerprint to the fingerprint of the previous trace, and including the unique event identifier for the operator.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E140		- Calculating The fingerprint using A hash function. The fingerprint should not be calculated at The time of addition but should be stored in memory since The previous operation.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E141		- Sealing The data with A timestamped signature including The chaining element to Ensure integrity and link them to A specific time.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E142		- Timestamping, which should be performed on the event (or batch of events) in clear.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES		Regarding the operations of signing and encryption:							
YES	YES	E143		- The signature format is XADES-T with a timestamp token compliant with RFC 3161.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.	Another signature format may be implemented, provided that it is justified.			
YES	YES	E144		- Data encryption is performed using the ANJ's public key to ensure confidentiality.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.	The encryption method may involve a symmetric encryption algorithm, following precisely described operations.			
YES	YES		Regarding batch processing:							
YES	YES	E145		-Batch processing should be configurable for A maximum duration or number of events.	1	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E146		- The granularity of Batch processing should be The event.	1	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	**PART 20 - SMA: Traces Access Function**								
YES	YES		The authorized operator or holder of exclusive rights must provide the following elements for each accreditation or scope of activity under exclusive rights:							
YES	YES	E147		- A data access mechanism allowing data entry on-site (copy of all or part of the safe).	3	Documentation provided by the operator.				
YES	YES	E148		- A data access mechanism allowing remote data querying through A collection tool.	3	Documentation provided by the operator.				
YES	YES	E149		- A tool for validating SMA data and extracting game operation traces usable on the SMA site and in ANJ laboratories (offline mode).	3	Documentation provided by the operator.				
YES	YES		The architecture of the SMA's safe part must distinguish:							
YES	YES	E150		- A data storage space located in A secure network zone.	3	Configuration audit of the hosting platform. Documentation provided by the operator. Report and target of the ANSSI/CSPN certification.				
YES	YES	E151		- an access layer to The storage space.	3	Configuration audit of the hosting platform. Documentation provided by the operator. Report and target of the ANSSI/CSPN certification.				
YES	YES	E152	The data stored in the safe must be permanently accessible remotely from ANJ premises (i.e., from one or more identified IP addresses).		3	Configuration audit of the hosting platform. Documentation provided by the operator.	This ensures that measures are implemented to guarantee high availability of the data stored in the safe.			
YES	YES	E153	The remotely accessible data must cover at least the last 12 months of the operator's activity (rolling period).		3	Documentation provided by the operator.	This means being able to access real-time data over a period of 12 rolling months. Access to older data may require specific requests.			
YES	YES	E154	The data must remain accessible on the SMA hosting site for the entire duration required by law (Article 31 of Decree No. 2010-518 of May 19, 2010).		3	Documentation provided by the operator.				
YES	YES	E155	The extraction of the safe must be possible for a data slice, corresponding to an activity period or a range of event identifiers, using the remote collection tool provided by the operator.		3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E156	The access layer to the storage space must itself be secured, at the application and network levels, against external threats, including denial-of-service attacks, and unauthorized access other than those initiated by ANJ.		2	Configuration audit of the hosting platform. Documentation provided by the operator. Report and target of the ANSSI/CSPN certification.				

YES	YES		The access layer exposes a web service with the following two main interfaces:							
YES	YES	E157		- A query interface: it allows the extraction of a single trace or a set of traces based on a specific date or a date range. Several events may correspond to the same date;	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES	E158		- A synchronization interface: it allows The extraction of A single trace or A set of traces based on an event identifier or A range of event identifiers.	3	Report and target of the ANSSI/CSPN certification. Documentation provided by the operator.				
YES	YES		The tool developed by the operator must enable:							
YES	YES	E159		- Remote querying of the operator's safe to download the requested traces (collection tool);	3	Documentation provided by the operator.				
YES	YES	E160		- Extraction of the downloaded traces, followed by decryption and verification of data integrity (extraction and validation tool). This extraction must be possible offline.	3	Documentation provided by the operator.				
YES	YES		The tool must implement:							
YES	YES	E161		- The WSDL interface defined by ANJ, or propose an equivalent query interface based in particular on the operator's identifier, safe identifier, accreditation or scope of activity under exclusive rights, and a range of events or dates down to the hour;	1	Documentation provided by the operator.				
YES	YES	E162		- The following command-line options: - Configuration of a URL, including a fully qualified domain name identifying the Web service; - Configuration of a safe identifier, in case the architecture implemented by the operator includes multiple safes	1	Documentation provided by the operator.				
YES	YES	E163		- The TLS 1.3 transport protocol. Prefer the use of cryptographic suites that comply with the recommendations stated by ANSSI.	2	Configuration audit of the hosting platform. Documentation provided by the operator + expert opinion.	The TLS v1.2 version is tolerated. Outdated versions SSLv2, SSLv3, TLS 1.0, and TLS 1.1 should be avoided.			
YES	YES	E164		- Cryptographic algorithms handling keys must have sizes that comply with The rules stated in The general security repository available on The ANSSI website.	3	Documentation provided by the operator.				
YES	YES		The network access for remote access must:							
YES	YES	E165		- Be subject to filtering implemented as a whitelist at the level of a perimeter security device such as a firewall;	2	Configuration audit of the hosting platform. Documentation provided by the operator + expert opinion.				
YES	YES	E166		- Be subject to logging and incident processing procedures, if applicable.	2	Configuration audit of the hosting platform. Documentation provided by the operator + expert opinion.				
YES	YES	E167	The extraction and validation tool for traces must implement the following options: - Configuration of a decryption X509v3 certificate, in PEM format, and the associated RSA key pair in PEM PKCS#8 format, to be used for decrypting traces (encrypted using the ANJ's public key transmitted to the operator); - Configuration of a passphrase, which can be provided via command line, in a file, through standard input, or via the environment, and allows the potential decryption of the RSA key pair in PEM PKCS#8 format; - Configuration of a signing X509v3 certificate, in PEM format, for validating timestamped signatures; - Configuration of a certification authority, in the form of a certificate in PEM format, to validate the signing X.509v3 certificate; - Configuration of file system paths pointing to the respective source files of the encrypted data and the destination files for the decrypted data; - Configuration of a file system path pointing to the tool's configuration file; - Configuration of a verbosity cursor, allowing adjustment of the level of debug information displayed.		1	Documentation provided by the operator.				
YES	YES	**PART 21 - SMA: XML events: generalities**								
YES	YES		The XML records are:							
YES	YES	E168		- Encoded in UTF-8 format. Particular attention shall be paid to the handling of accented characters (Ú, Þ, Ó);	3	Code audit				
YES	YES	E169		- Compliant with the XML standard (especially in terms of XML entity encoding);	3	Code audit				
YES	YES	E170		- Compliant with the XSD schema published by ANJ;	3	Code audit				
YES	YES	E171		- Filtered in terms of content, following the regular expressions (pattern facet) described in the XSD schema;	3	Code audit	The analysis should demonstrate the use of filters in the source code.			

YES	**YES**	**E172**		- Filtered in terms of content, to prevent classical web attacks such as injection attacks (SQL injections, XPath injections, and possibly XSS, in addition to output encoding using HTML entities, for example, etc.).	3	Code audit	The analysis should demonstrate the use of filters in the source code.			