Matrix of Certification Requirements

version 1.0 dated 07/10/2022

Notice	
Checkpoint	Checkpoint marked as "En". Note: The numbering of the checkpoint is specific to this document.
Reference	Reference to the document (Technical Requirements and its annexes, including Law and Decree) and the section providing information on the checkpoint.
Label	Description of the checkpoint.
Criticality Level	Criticality level of the checkpoint: - Level 1 criticality mainly corresponds to requirements related to the existence of documentation or procedures (e.g., security policy, update procedure, system hardening, etc.) ; - Level 2 criticality mainly corresponds to requirements where non-compliance has operational impact: failure to implement a procedure, failure to comply with operational compliance and security requirements defined by the ANJ, or failure to follow good practices in information system security ; - Level 3 criticality corresponds to requirements whose non-compliance is considered highly critical, often in terms of regulatory compliance or security (on an exposed component and/or handling critical data).
Certification Analysis Element at 6 Months	Elements on which the analysis is based: 1) Documents provided by the operator, for example: - The definition file of the PSM hosting platform; - The functional and technical documentation of the sensor software; - The CSPN certification report conducted for the certification of the safe and the security target of this certification; - The security audit reports already performed by the operator – especially if the sensor is integrated into the gaming platform – or the operator's SSI maturity analysis report; 2) Audits conducted by the certifying body, aiming to understand and technically validate the checkpoints and assess the declarative elements described by the operator in its documentation, particularly: - Functional, technical, and security audit of the sensor software component; - First-level configuration audit of the PSM hosting infrastructure. The associated report is referred to as 'hosting platform configuration audit' in the rest of the document. The requested level of analysis can be specified: 'first-level analysis' means a pragmatic and common-sense analysis is expected. Conversely, an 'expert opinion' will be more in-depth, technical, and substantiated (configuration element, code excerpt, etc.).
Certification Analysis Element for Annual Certification	Elements on which the analysis is based: 1) Documents provided by the operator, for example: - Updated definition file of the PSM and gaming platform hosting platform; - Updated functional and technical documentation of the sensor software and gaming platform; - Initial 6-month certification report of the PSM component; - Homologation reports conducted on the gaming software; - Security audit reports conducted by the operator independently of the certifications required by regulations; - Statements of no modification for a component (e.g., sensor); - Remediation plans for non-compliance and vulnerabilities identified during previous certifications. 2) Audits conducted by the certifying body, aiming to understand and technically validate the checkpoints, and appreciate the declarative elements described by the operator in its documentation, particularly: - Technical architecture audits of the gaming platform; - First-level configuration audits of the PSM and gaming platform hosting infrastructure. These reports are labeled as 'hosting platform configuration audits' in the rest of the document; - Intrusive application audits that focus on the software components of the gaming platform not subject to homologation. The requested level of analysis can be specified: 'first-level analysis' means a pragmatic and common-sense analysis is expected. Conversely, an 'expert opinion' will be more thorough, technical, and substantiated (configuration element, code excerpt, etc.). The annual certification is based on a set of mandatory analyses that can be updated. ET5 indicates the analyses for which this update can be performed.
ANJ Comments	Clarifications provided by the ANJ to aid in understanding the checkpoint.
Relevant Reports	References to the document(s) and chapters on which the analysis was conducted, if applicable, by the certifying body.
Compliance	Observation resulting from the analysis conducted by the certifying body.
Certifier Comments	Clarifications provided by the certifying body to aid in understanding the analysis results of the checkpoint.