PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des système d'information

Paris, le 12 Août 2025

N°**1362/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-NOTE-24_1.1**

NOTE D'APPLICATION

EVALUATIONS DE GENERATEURS D'ALEA SELON AIS20/31 DANS LE SCHEMA FRANÇAIS

Application **:** Dès son approbation.

Diffusion **:** Publique.

Le sous-directeur « Expertise »
de l'Agence nationale de la sécurité
des systèmes d'information

Renaud LABELLE

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1.0	02/03/2021	Version initiale
1.1	12/08/2025	Ajout d'un niveau minimum d'assurance CC pour tout projet déposé après de la parution de la présente version. Ajout d'une réserve, relative à [ANSSI-PG-083]

En application du décret n°2002-535 du 18 avril 2002 modifié, la présente note a été soumise, lors de sa création, au comité directeur de la certification, qui a donné un avis favorable.

Cette note est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évaluations mineures ne sont pas soumises au comité directeur de la certification.

La présente note est disponible en ligne sur le site institutionnel de l'ANSSI (cyber.gouv.fr).

TABLE DES MATIERES

1 Processus

Ce document est applicable pendant les évaluations Critères Communs lorsqu'une (ou plusieurs) exigence fonctionnelle FCS_RNG de la cible de sécurité revendique la conformité du générateur d'aléa à une classe de [AIS20/AIS31].

Le niveau de l'évaluation doit être a minima EAL4. Une augmentation ATE_DPT.2 est fortement encouragée. Le développeur fournit au CESTI et à l'ANSSI les éléments de preuves (*Developer evidence*) spécifiés par [AIS20 Evid] et [AIS31 Evid], parmi toutes les fournitures requises par ailleurs pour les évaluations Critères Communs.

Le CESTI effectue les *work-units* définies dans [AIS20 ETR] et [AIS31 ETR]. Ces travaux ajoutent aux classes habituelles (ASE, ADV, ALC, ATE, AVA) une classe RNG où sont placés les argumentaires et verdicts des différentes *work-units* [AIS20 ETR] et [AIS31 ETR] applicables.

Cependant, une partie de certaines *work-units* est effectuée par l'ANSSI, c.f. section « Travaux par l'ANSSI » du présent document. En l'absence d'un rapport ANSSI sur ces travaux, le rapport technique d'évaluation[1] (RTE) conclut pour ces *work-units* « analyse restant à approfondir » et verdict « INCONCLUSIVE »[2]. Lorsque le rapport de l'ANSSI est disponible, le RTE le référence et reprend ses verdicts.

Lors d'une réévaluation, lorsqu'aucun élément de preuves (*Developer Evidence*) n'a été modifié, il est admis de réutiliser les résultats correspondants. Toute modification requiert un complément d'analyse. Par exemple, même si les modifications se limitent à des changements de valeur des paramètres (technologiques) du modèle stochastique, un complément d'analyse de P.12 est nécessaire.

2 Travaux par l'ANSSI

Pour la *work-unit* PTRNG.2-4, le CESTI effectue seulement une analyse superficielle des preuves P.12 ; l'analyse en profondeur des preuves P.12 est effectuée par l'ANSSI, qui consigne les résultats dans un rapport.

L'ANSSI doit également être sollicitée par le CESTI au cours de l'évaluation lorsque le CESTI juge nécessaire de discuter du choix de tests de panne, et en cas de comportement anormal relevé lors de l'étude statistique des sorties.

Par ailleurs, une fois le RTE disponible, le Centre de certification national (CCN) de l'ANSSI effectue une revue de toutes les tâches RNG réalisées par le CESTI (au titre général et habituel de la revue des RTE par CCN).

3 Réserve sur la méthode AIS20/31

Certaines classes de générateurs d'aléa définies par AIS20/31, dont la classe PTG.2, ne sont pas conformes à la règle RègleArchiGDA-1 du [ANSSI-PG-083].

[1] *Evaluation technical report (ETR).*

[2] Abus de langage (assumé), car « INCONCLUSIVE » veut dire que les éléments du développeur ne permettent pas de conclure, ce qui n'est a priori pas le cas ici.

ANNEXE A. Références

Référence	Document
[AIS20/AIS31]	*A proposal for functionality classes for random number generators*, v2.0, 18/09/2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[AIS31 Evid]	*Developer evidence for the evaluation of a physical true random number generator*, v0.8, 28/02/2013, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[AIS31 ETR]	*ETR-Part True Physical and Hybrid Random Number Generator*, v0.7, 28/02/2013, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[AIS20 Evid]	*Developer evidence for the evaluation of a deterministic random number generator*, v0.9, 28/02/2013, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[AIS20 ETR]	*ETR-Part Deterministic Random Number Generator*, v0.10, 28/02/2013, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[ANSSI-PG-083]	*Guide des mécanismes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, v2.04 du 1er janvier 2020, ANSSI.*

ANNEXE B. Courtesy translation

Evaluations of random number generators according to AIS20/31 in the French scheme

1. Process

This document is applicable during Common Criteria evaluations when one (or several) FCS_RNG in the security target claims conformity to a class of [AIS20/AIS31].

The evaluation assurance level must be at least EAL4 augmented with ATE_DPT.2The Developer provides ITSEF and ANSSI with the 'Developer evidence' [AIS20 Evid] and [AIS31 Evid], as part of the global developer evidence for the CC evaluation.

The ITSEF performs the work-units defined in [AIS20 ETR] and [AIS31 ETR]. The rationales and verdicts of applicable work-units are written in a « RNG » section in the ETR, next to the usual ASE, ADV, ALC, ATE, AVA sections.

However, some work-units are partly performed by ANSSI (see 'tasks by ANSSI' below). While no report by ANSSI is available, the ITSEF assigns the verdict "INCONCLUSIVE" with rationale 'analysis in progress'; when ANSSI's report is available, it is referenced in the ETR, and the verdicts are updated accordingly.

During a re-evaluation, when the Developer Evidence are unchanged, the corresponding results may be reused. Any modification requires to revisit the analysis. For instance, even if the change is limited to values of parameters in the stochastic model, the analysis must be revisited.

2. Tasks by ANSSI

For PTRNG.2-4, the ITSEF only checks with a superficial analysis the developer evidence P.12; the in-depth examination of P.12 is then performed at ANSSI and results in a report.

The ITSEF must also request support from ANSSI when in doubt about the chosen on-line tests, and when the statistical analysis of the RNG's output shows an abnormal behavior.

Furthermore, once the ETR is issued, the 'Centre de certification national (CCN)' at ANSSI reviews all the RNG work-units performed by the ITSEF (as part of the usual global review of all the work-units of the ETR).

3. Reservation on AIS20/31

Some of the functionality classes defined in AIS20/31, in particular PTG.2, are not conformant to the rule RègleArchiGDA-1 of [ANSSI-PG-083].