PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 26 janvier 2021

N° **172/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-CRY-P01_v4.1**

PROCEDURE

MODALITES POUR LA REALISATION DES ANALYSES CRYPTOGRAPHIQUES ET DES EVALUATIONS DES GENERATEURS DE NOMBRES ALEATOIRES

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	15/07/2010	Première édition officielle.
2.0	20/12/2011	Clarification des travaux attendus pour l'analyse des générateurs de nombres aléatoires (chapitre 5.2). Intégration de l'instruction CRY/I/01.1 (réf. 423/SGDN/DCSSI/SDR).
3.0	05/05/2015	Clarification des fournitures attendues dans les cas d'évaluation d'un produit utilisant un coprocesseur cryptographique (annexe A).
4.0	10/02/2020	Clarification des travaux attendus pour l'analyse cryptographique.
4.1	26/01/2021	Clarification des fournitures attendues. Mise à jour du référentiel applicable.

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

Cette procédure 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 procédure est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

TABLE DES MATIERES

1 Objet de la procédure

La présente procédure fixe les modalités de réalisation des analyses cryptographiques dans le cadre du schéma français d'évaluation et de certification [DECRET].

2 Contexte et définitions

2.1 Justification de la procédure

L'évaluation de la résistance des mécanismes de nature cryptographique fait l'objet d'un traitement particulier dans les évaluations de la sécurité des technologies de l'information. Pour les critères ITSEC, cette analyse prend la forme « d'une déclaration de confirmation par l'organisme national approprié » de « l'adéquation des mécanismes cryptographiques au niveau de résistance visé ». Pour les Critères Communs, l'analyse de « la qualité inhérente des algorithmes cryptographiques » est exclue ; les modalités pour la réalisation des analyses cryptographiques restent à l'appréciation du schéma de certification dans lequel l'évaluation est réalisée. Quoi qu'il en soit une analyse cryptographique est toujours requise dans le cadre des évaluations du schéma français tant pour les Critères communs (CC) que pour la Certification de sécurité de premier niveau (CSPN).

Par ailleurs, l'ANSSI recommande que les mécanismes cryptographiques mis en œuvre dans les produits évalués répondent aux préconisations de son référentiel sur la cryptographie (voir [ANSSI-PG-083] sur www.ssi.gouv.fr). La mise en œuvre de ces préconisations devient obligatoire lorsque les produits sont destinés à être « qualifiés » par l'ANSSI. Un mécanisme cryptographique qui ne répondrait pas à ces préconisations pourrait néanmoins éventuellement répondre aux exigences des CC ou CSPN concernant l'analyse de vulnérabilité. Plus précisément, un produit utilisant un mécanisme cryptographique non conforme au [ANSSI-PG-083] peut être certifié si cette non-conformité d'induit pas une vulnérabilité exploitable pour le niveau d'attaquant visé par l'évaluation.

Historiquement l'ANSSI réalisait elle-même une partie des travaux associés à l'analyse cryptographique. Au vu de l'augmentation du nombre d'évaluations traitées par le schéma français, les travaux d'analyse sont désormais confiés aux CESTI. Cependant, dans quelques cas particuliers identifiés au paragraphe suivant, l'ANSSI interviendra également dans ces travaux.

Cette note présente les travaux attendus au titre de l'analyse cryptographique et de l'évaluation des générateurs de nombres aléatoires, ainsi que la démarche d'agrément des CESTI pour déterminer leur capacité à réaliser ces travaux.

2.2 Contenu de l'analyse cryptographique et de l'analyse de nombres aléatoires

Le tableau ci-après décrit les travaux qui sont à réaliser au titre de l'analyse de la cryptographie, et précise qui en est responsable par défaut.

Code couleur :

	OUI par défaut
	OUI sauf exception
	NON sauf exception
	NON sans exception

Type d'analyse	ANSSI	CESTI non agréé pour la cryptographie	CESTI agréé pour la cryptographie
A. Analyse théorique. Cette analyse vise notamment à assurer que les mécanismes cryptographiques mis en œuvre sont conformes aux prescriptions des référentiels de l'ANSSI.	(1)	(2)	
A1. Algorithmes cryptographiques, modes opératoires et adéquation aux objectifs recherchés (confidentialité, intégrité, disponibilité, authenticité, performances, etc.).	(1)	(2)	
A1bis. Cas particulier : Résistance intrinsèque des algorithmes cryptographiques et modes opératoires non reconnus utilisés : ce cas devrait être rare dans le domaine civil et n'est pas encouragé par l'ANSSI. S'il se présente, l'ANSSI effectuera l'analyse du mécanisme proposé et fournira une cotation au CESTI. À noter que lorsque l'implémentation d'un algorithme reconnu introduit une différence par rapport à ses spécifications celui-ci n'est plus considéré comme reconnu.			
A2. Protocoles cryptographiques mis en œuvre pour réaliser la fonctionnalité visée.	(1)	(2)	
A3. Procédures de génération et de gestion des clés	(1)	(2)	
A4. Générateur de nombres aléatoires : **Caractéristiques des sources d'aléas (physique ou non) ;** **Analyse du retraitement cryptographique.**	(1)	(2)	
A4bis. Cas particulier : Retraitement cryptographique non reconnu utilisé : ce cas devrait être rare dans le domaine civil et n'est pas encouragé par l'ANSSI. S'il se présente, l'ANSSI effectuera l'analyse du mécanisme proposé et fournira une cotation au CESTI.			
B. Analyse de la conformité de l'implémentation de la cryptographie (y compris du générateur de nombres aléatoires). La forme de cette analyse peut dépendre des éléments disponibles (disponibilité du code source, interface de test, etc.).		(2)	
C. Analyse des vulnérabilités de l'implémentation de la cryptographie (indépendamment de la résistance intrinsèque des algorithmes, leur implémentation permet-elle d'envisager des attaques pouvant porter atteinte aux objectifs de sécurité de la TOE ?).		(2)	

(1) selon la nature du projet, l'ANSSI peut imposer que ces analyses soient réalisées par ses soins. Ce cas est précisé, au plus tard, lors de l'acceptation du dossier de demande de certification. Il appartient au CESTI de renégocier ou non le contrat qui le lie au commanditaire.

De plus, l'ANSSI continue d'être en mesure de réaliser ces analyses cryptographiques à la place des CESTI dans des situations où des CESTI français seraient susceptibles de se trouver en concurrence avec des CESTI étrangers qui n'auraient pas à supporter la charge d'analyse de la cryptographie, réalisée par leur agence nationale de sécurité, et ce afin de ne pas créer de distorsion de concurrence.

(2) l'ANSSI peut autoriser un CESTI non agréé pour la cryptographie à sous-traiter cette tâche à un CESTI agréé pour la cryptographie.

3 Agrément des CESTI dans le domaine de la cryptographie

Conformément à la procédure [AGR-P-01], les CESTI peuvent demander une extension de leur portée d'agrément au domaine de la cryptographie afin de pouvoir réaliser des évaluations cryptographiques.

3.1 Appréciation de la compétence des CESTI dans le domaine de la cryptographie

La compétence des laboratoires pour réaliser ces analyses est appréciée par l'ANSSI sur la base :

- d'entretien avec les personnes du CESTI en charge des analyses cryptographiques ;
- d'examen des éventuelles références du CESTI dans le domaine de la cryptographie ;
- de la disponibilité d'outils d'analyse, en particulier, dans le domaine de l'analyse des générateurs de nombres aléatoires ;
- de leur capacité à connaître et comprendre les référentiels de l'ANSSI dans ce domaine ;
- des analyses déjà effectuées par le personnel du CESTI en charge des analyses cryptographiques ;
- d'autres éléments pouvant conforter l'appréciation de l'ANSSI sur la compétence des CESTI dans ce domaine.

3.2 Agrément provisoire dans le domaine de la cryptographie

Si les informations recueillies sont jugées satisfaisantes, le CESTI reçoit l'autorisation provisoire de réaliser l'analyse cryptographique sur un ou plusieurs projets d'évaluation pilote.

3.3 Agrément dans le domaine de la cryptographie

A l'issue d'un premier ensemble de résultats (provenant d'une ou plusieurs évaluations pilotes ou éventuellement, de travaux d'expertise hors évaluation) jugés significatifs et satisfaisants par l'ANSSI, le CESTI est agrée pour le domaine de la cryptographie (voir [AGR-P-01]).

3.4 Non décision d'agrément dans le domaine de la cryptographie

Si les résultats des analyses effectuées par le CESTI ne sont pas satisfaisants, l'ANSSI peut prononcer le retrait du caractère provisoire de l'extension d'agrément. Le CESTI est alors dans l'obligation de sous-traiter les analyses cryptographiques qu'il aurait en cours à un autre CESTI agréé pour ce domaine.

3.5 Suivi de l'agrément dans le domaine de la cryptographie

Comme pour ses autres personnels, le CESTI doit indiquer tout changement de personnels identifiés comme étant en mesure de réaliser les analyses cryptographiques.

3.6 Retrait de l'agrément dans le domaine de la cryptographie

L'ANSSI se réserve la possibilité de prononcer le retrait de l'extension. Ce retrait est notamment prononcé dans les cas suivants :

- perte de compétences dans le domaine ;
- absence de suivi de l'état de l'art dans le domaine ;
- résultats des analyses non satisfaisants.

4 Réalisation des analyses

4.1 Fournitures nécessaires pour la réalisation des analyses cryptographiques

Pour réaliser efficacement une évaluation cryptographique complète, l'évaluateur a besoin de deux éléments :

- un document relatif aux aspects cryptographiques du produit évalué ;
- la totalité du code source cryptographique du produit évalué.

4.1.1 *Fourniture d'un document relatif aux aspects cryptographiques du produit évalué*

Cette fourniture des spécifications cryptographiques est systématique, car elle est nécessaire pour l'analyse théorique et l'analyse de la conformité et des vulnérabilités de l'implémentation.

Le commanditaire de l'évaluation est responsable de la fourniture à l'ANSSI et au CESTI d'un document relatif aux aspects cryptographiques du produit évalué. Ce document doit décrire précisément et complètement les algorithmes, modes opératoires et protocoles cryptographiques présents dans le produit évalué, ainsi que l'architecture de gestion de clés utilisées. Il doit contenir en outre, une spécification des générateurs de nombres aléatoires (description de l'éventuelle source physique, principe du retraitement, etc.).

Le document [FOURNITURES] « Fournitures nécessaires à l'analyse de mécanismes cryptographiques » (disponible sur www.ssi.gouv.fr) précise le contenu attendu par l'ANSSI. Pour compléter leur analyse, l'ANSSI et le centre d'évaluation peuvent demander des informations supplémentaires après la livraison de la fourniture.

4.1.2 *Fourniture du code source cryptographique du produit évalué*

Cette fourniture n'est pas systématique pour toute évaluation cryptographique, elle dépend du niveau d'évaluation visé.

Le code source cryptographique est un élément essentiel pour mener efficacement une évaluation cryptographique. Sa fourniture est requise pour les évaluations CSPN et pour les évaluations CC à partir du niveau AVA_VAN.3.

Le commanditaire de l'évaluation est responsable de la fourniture du code source cryptographique au CESTI, et ce avant le début de l'analyse cryptographique. En plus de l'implémentation des fonctions cryptographiques, le commanditaire doit fournir au CESTI les appels à ces fonctions afin d'avoir accès à leur paramètres. Le CESTI est en droit de demander des informations complémentaires sur ces paramètres afin de mener correctement l'analyse cryptographique.

Pour les évaluations CC de niveau inférieur à AVA_VAN.3, si le commanditaire de l'évaluation ne souhaite pas fournir volontairement le code source cryptographique, d'autres moyens (interfaces de tests, etc.) doivent être mis à disposition de l'évaluateur pour effectuer certaines tâches de l'analyse (voir 4.2.2).

4.2 Analyse de la cryptographie

L'analyse de la cryptographie s'applique à tout mécanisme cryptographique participant aux objectifs de sécurité de la TOE.

Elle est constituée de deux parties : d'une part l'analyse théorique des mécanismes cryptographiques - autrement appelée cotation cryptographique - réalisant les fonctions de sécurité du produit et d'autre part l'analyse de la conformité et des vulnérabilités de l'implémentation. Les deux parties sont nécessaires afin d'obtenir une analyse cohérente et complète de la robustesse des mécanismes cryptographiques.

4.2.1 *Analyse théorique de la cryptographie (cotation cryptographique)*

Cette analyse correspond à une analyse théorique des mécanismes cryptographiques s'appuyant sur le document relatif aux aspects cryptographiques du produit (4.1.1) et établissant la conformité au [ANSSI-PG-083] (ou [SOGIS_ACM] sur demande du commanditaire).

Cette analyse s'applique à tous les mécanismes cryptographiques (algorithmes, protocoles, modes opératoires) et aux procédures de gestion des clés, mais également aux mécanismes de génération de nombres aléatoires ainsi qu'à leur éventuelle utilisation par les autres mécanismes cryptographiques (par exemple génération de la clef utilisée par un algorithme de chiffrement). Elle porte également sur l'adéquation entre les mécanismes cryptographiques et de gestions des clés mis en œuvre et les objectifs de sécurité recherchés.

Le tableau ci-dessous récapitule les points concernés :

A1. Algorithmes cryptographiques, modes opératoires et adéquations aux objectifs recherchés (confidentialité, intégrité, disponibilité, authenticité, performances, etc.).
A2. Protocoles cryptographiques mis en œuvre pour réaliser la fonctionnalité visée.
A3. Procédures de génération et de gestion des clés.
A4. Générateur de nombres aléatoires : **i. Caractéristiques des sources d'aléas (physique ou non) ;** **ii. Analyse du retraitement cryptographique.**

L'analyse théorique s'appuie essentiellement sur le document fourni. Elle a pour objectif de détecter des éventuelles vulnérabilités dans les mécanismes cryptographiques utilisés pour atteindre les objectifs de sécurité du produit dans son environnement d'exploitation. Dans le cas des services cryptographiques, la résistance de ces mécanismes doit être analysée dans leur contexte d'emploi. Il est néanmoins possible d'émettre des recommandations pour leur utilisation.

La première tâche de l'évaluateur est de vérifier que le document qui a été livré pour réaliser l'analyse est complet et cohérent avec les autres documents fournis pour l'évaluation du produit.

L'évaluateur doit analyser les spécifications de tous les mécanismes cryptographiques décrits ci-dessus (A1, A2, A3, A4) afin de déterminer s'ils sont conformes aux exigences du ou des référentiel(s) utilisé(s) ([ANSSI-PG-083], [SOGIS_ACM]). En outre, l'évaluateur effectue les analyses proposées par le ou les référentiel(s) utilisé(s).

4.2.2 *Analyse de la conformité et des vulnérabilités de l'implémentation*

Cette analyse correspond à une analyse de la conformité et des vulnérabilités de la mise en œuvre des mécanismes cryptographiques s'appuyant sur les résultats de l'analyse théorique (4.2.1). La forme de cette analyse dépend des éléments disponibles (4.1.2).

Cette analyse concerne les points suivants :

B. Analyse de la conformité de l'implémentation de la cryptographie (y compris du générateur de nombres aléatoires).

L'évaluateur doit vérifier que l'implémentation des mécanismes cryptographiques fournie est conforme aux spécifications fournies par le commanditaire.

L'évaluateur prend en compte les résultats de la précédente analyse (4.2.1) pour vérifier la conformité entre les spécifications du produit et son implémentation et chercher les éventuelles vulnérabilités.

C. Analyse des vulnérabilités de la mise en œuvre de la cryptographie (indépendamment de la résistance intrinsèque des algorithmes, leur implémentation permet-elle d'envisager des attaques pouvant porter atteinte aux objectifs de sécurité de la TOE ?).

Dans le cadre de l'analyse de vulnérabilités, l'évaluateur devra déterminer si ces vulnérabilités sont réellement exploitables dans l'environnement d'utilisation du produit.

Si le code source cryptographique est disponible, cette analyse concerne également l'analyse des vulnérabilités de l'implémentation de la cryptographie.

Si des recommandations sur l'utilisation d'un service cryptographique ont été émises lors de la phase d'analyse théorique, l'évaluateur doit vérifier que ces recommandations sont clairement indiquées dans au moins l'un des guides (utilisation, administration) du produit.

4.2.3 *Rapport technique d'évaluation de la cryptographie*

Un rapport d'analyse est réalisé par le CESTI incluant tous les résultats de 4.2.1 et de 4.2.2. Il indique les éventuelles vulnérabilités détectées (potentielles et avérées). En conclusion de ce rapport, un chapitre récapitulant les recommandations devant être mises en œuvre pour la mise en conformité au référentiel sélectionné doit impérativement être disponible.

Lorsque l'analyse théorique est réalisée par l'ANSSI, le rapport de cette partie est fourni au CESTI et au commanditaire de l'évaluation.

Le rapport d'analyse complet est fourni au centre de certification pour validation. L'ANSSI peut faire éventuellement des retours, voire demander au CESTI des tests et des vérifications complémentaires.

Après validation du rapport par l'ANSSI, le CESTI doit également le fournir au commanditaire de l'évaluation.

4.3 Certification

Le rapport de certification comporte toutes les mentions utiles permettant d'indiquer les éventuelles limites de l'analyse et de l'utilisation de la cryptographie. Il doit mentionner si la cryptographie est conforme au référentiel de l'ANSSI ainsi que les conditions de conformité établies lors de l'analyse. Le rapport indique également les résultats de l'analyse du ou des générateur(s) de nombres aléatoires (ou indique qu'il n'y a pas de fonction de génération de nombres aléatoires utilisée par le produit le cas échéant).

ANNEXE A. Guide pour l'utilisation d'un coprocesseur cryptographique

Un produit peut utiliser un élément matériel, pour tout ou partie des traitements cryptographiques nécessaires à la protection d'un bien de la TOE[1] ou à la réalisation d'une fonction de sécurité de la TOE. Si cet élément ne peut pas être inclus dans le périmètre de l'évaluation ni certifié à un niveau d'assurance permettant une composition, un justificatif doit être fourni et les contraintes définies ci-dessous doivent être prises en compte en complément des éléments présentés dans le corps du document.

A.1 Restriction d'usage pour l'utilisation d'un coprocesseur cryptographique non maitrisé dans le cadre d'une certification

Un coprocesseur cryptographique non maitrisé ne doit être employé que pour le calcul de fonction de primitive cryptographique symétrique et de hachage ne manipulant aucune clé racine ou de longue durée. Un tel coprocesseur ne peut être utilisé pour des calculs non déterministes comme la génération d'aléa ou la préparation d'IV[2].

La conformité des résultats du coprocesseur sera vérifiée au travers d'un certain nombre de vérifications cryptographiques mises en œuvre dans le produit (au minimum autotest et comparaison avec une implémentation logicielle de référence disponible dans le produit évalué). Celles-ci devront être effectuées au démarrage et de manière dynamique (non bloquante) tous les x appels au coprocesseur (1<x<1000, un *jitter* aléatoire devant être introduit).

A.2 Fournitures attendues

Une description théorique de l'ensemble de la cryptographie au niveau système d'exploitation devra être fournie ainsi que le code source des fonctions cryptographiques dont y compris celui de l'implémentation logicielle de référence. Une plateforme permettant de tester le coprocesseur directement aux interfaces devra également être mise à disposition.

A.3 Tâches d'évaluation spécifiques

Les précédentes restrictions d'usage devront être vérifiées par le CESTI. La pertinence de l'implémentation logicielle de référence devra également être évaluée par le CESTI.

[1] *Target Of Evaluation* : cible d'évaluation.

[2] *Initialization Vector* : vecteur d'initialisation.

ANNEXE B. Références

Référence	Document
[DECRET]	Décret n° 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
[AGR-P-01]	Procédure ANSSI-CC-AGR-P-01 : Agrément des centres d'évaluation.
[FOURNITURES]	Fournitures nécessaires à l'analyse de mécanismes cryptographiques disponible sur le site institutionnel de l'ANSSI.
[ANSSI-PG-083]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.
[SOGIS_ACM]	SOG-IS Agreed Cryptographic Mechanisms (ACM) - version 1.1, juin 2018. Disponible en ligne : https://www.sogis.org/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.ssi.gouv.fr).