



PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 21 octobre 2016

N° 4375/ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-NOTE-20/1.0

NOTE D'APPLICATION

REGLES RELATIVES A LA MISE EN ŒUVRE DES EVALUATIONS SECURITAIRES

Application : Dès son approbation

Diffusion : Publique

Le directeur général
de l'agence nationale de la sécurité
des systèmes d'information

P/O Vincent STRUBEL
Sous-directeur Expertise
[ORIGINAL SIGNE]



Suivi des modifications

Version	Date	Modifications
1.0	21/10/2016	Création

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

La présente note d'application est disponible sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

Table des matières

1. OBJET DE LA NOTE	4
2. REFERENCES	4
3. REGLES APPLICABLES	4
3.1. DOSSIER D'EVALUATION	4
3.2. REPRISE D'EVALUATION LORS DES EVALUATIONS CC ET ITSEC	4
3.3. DEVOIR D'INFORMATION VERS LE CENTRE DE CERTIFICATION	4
3.4. ENGAGEMENT DU CESTI	5
3.5. DEMARRAGE ET DEROULEMENT DES ACTIVITES	5
3.5.1. <i>Démarrage de l'évaluation</i>	5
3.5.2. <i>Mise à disposition des fournitures et calendrier de livraison</i>	5
3.5.3. <i>Complétude des fournitures d'évaluation en entrée d'une tâche d'évaluation</i>	5
3.5.4. <i>Refus de fournitures</i>	5
3.5.5. <i>Mise à disposition du produit à évaluer</i>	5
3.5.6. <i>Suspension de l'évaluation par le commanditaire</i>	6
3.5.7. <i>Arrêt de l'évaluation à la demande du Commanditaire</i>	6

1. Objet de la note

Les objectifs de la présente note sont de définir les règles relatives à la mise en œuvre des évaluations Critères Communs (CC) [2], Certification Sécuritaire de Premier Niveau (CSPN) [3] et ITSEC pour préserver l'indépendance, l'impartialité et l'objectivité des travaux d'évaluation des CESTI en conformité avec l'accréditation et l'agrément.

2. Références

- [1] 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 des systèmes d'information.
- [2] CER-P-01.1 – Procédure de certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- [3] ANSSI-CSPN-AGR-P-01 – Procédure d'agrément des centres d'évaluation en vue de la Certification Sécuritaire de Premier Niveau.

3. Règles applicables

3.1. Dossier d'évaluation

Le dossier d'évaluation constitue la formulation de la demande d'évaluation en vue de la certification prévue à l'article premier du décret n°2002-535 [1]. Le dossier d'évaluation comprend notamment :

- les conditions générales de la certification ;
- une description de l'objet à évaluer (incluant sa cible de sécurité), la TOE ;
- le programme de travail prévisionnel élaboré par le centre d'évaluation et le commanditaire lors de la préparation de l'évaluation de sécurité.

Comme le prévoit le formulaire CER-F-01, le dossier d'évaluation doit être contresigné par le ou les CESTI avant transmission au Centre de certification.

3.2. Reprise d'évaluation lors des évaluations CC et ITSEC

Une reprise d'évaluation consiste en la livraison par le commanditaire d'une nouvelle version d'une fourniture évaluée ou en cours d'évaluation (correction documentaire, correction de bug technique). En particulier, chaque relivraison de la TOE constitue une reprise d'évaluation si des tests ont déjà été engagés par le CESTI. Le Centre de certification en est rapidement informé par le commanditaire.

Seules deux reprises d'évaluation sont autorisées dans la demande d'évaluation soumise à l'ANSSI. Au-delà, une mise à jour du dossier d'évaluation doit être réalisée, le Centre de certification en est alors informé sans délais.

3.3. Devoir d'information vers le Centre de certification

Le CESTI informe le Centre de certification de tout retard, incident ou non-conformité avec les procédures survenant lors de l'évaluation.

Le CESTI garantit son impartialité et son indépendance lors de la conduite des travaux. Il informe sans délais le Centre de certification en cas de pression de quelque nature que ce soit pouvant porter atteinte à ses qualités.

3.4. Engagement du CESTI

L'émission du certificat et le verdict du Rapport Technique d'Evaluation (RTE) ne peuvent faire l'objet d'une quelconque contractualisation entre le CESTI et le commanditaire.

3.5. Démarrage et déroulement des activités

3.5.1. Démarrage de l'évaluation

Le CESTI ne peut pas démarrer formellement les travaux d'évaluation avant que le dossier d'évaluation ne soit déposé par le commanditaire et accepté par le Centre de certification. Cette décision est notifiée par le Centre de certification qui adresse un courrier au commanditaire et au CESTI.

3.5.2. Mise à disposition des fournitures et calendrier de livraison

Le commanditaire doit mettre ou faire mettre à disposition du CESTI et du Centre de certification les fournitures requises pour l'évaluation, qu'il en soit propriétaire ou non.

Le commanditaire doit fournir régulièrement au CESTI et au Centre de certification le calendrier prévisionnel remis à jour de livraison des fournitures.

En cas de retard supérieur à trois mois entre la date prévue de livraison d'une fourniture dans le dossier d'évaluation et la date de livraison effective, le CESTI avertit le Centre de certification et lui présente l'impact organisationnel éventuel sur le projet d'évaluation (réaffectation des évaluateurs, augmentation de la charge de gestion de projet, etc.).

Tout arrêt de livraison de fournitures durant une durée de six mois peut conduire le Centre de certification à déclarer l'abandon de l'évaluation. Le Centre de certification avertit cependant systématiquement le commanditaire et le CESTI avant de déclarer cet abandon.

3.5.3. Complétude des fournitures d'évaluation en entrée d'une tâche d'évaluation

Chaque tâche d'évaluation ne peut démarrer avant que la totalité des fournitures requises en entrée de la tâche ne soit disponible.

Pour les évaluations CC et ITSEC, les tâches d'évaluation correspondent aux composants d'assurance des Critères Communs ou à une phase/aspect des critères ITSEC.

Pour les évaluations CSPN, une seule tâche d'évaluation est considérée ; les travaux ne peuvent débuter avant que l'ensemble des fournitures pour l'évaluation n'ait été fourni.

3.5.4. Refus de fournitures

Si le CESTI constate que les éléments de preuve (produits ou documents) fournis par le commanditaire ne permettront pas de réaliser les tâches d'évaluation dans les conditions prévues dans le dossier d'évaluation, il peut refuser formellement ces fournitures. Par exemple, le CESTI peut refuser des fournitures s'il juge que les éléments sont incomplets (documents partiels ou ne couvrant pas totalement le périmètre à évaluer) ou s'il juge que la quantité ou la qualité des éléments fournis ne permettront pas de respecter les charges d'évaluation énoncées dans le dossier d'évaluation. Le Centre de certification doit être notifié des refus de fournitures. Il pourra le cas échéant, assurer l'arbitrage entre le CESTI et le commanditaire.

3.5.5. Mise à disposition du produit à évaluer

Le produit à évaluer ainsi que les équipements nécessaires à son utilisation doivent être mis à disposition dans les locaux du CESTI. Toute dérogation à cette règle doit obtenir l'accord préalable

du Centre de certification. Pour les travaux nécessitant une analyse du code source par le CESTI, le code source doit être mise à disposition dans locaux du CESTI.

3.5.6. Suspension de l'évaluation par le commanditaire

Si le commanditaire identifie qu'il ne sera pas en mesure de livrer les fournitures dans un délai inférieur à trois mois il peut demander la suspension du projet d'évaluation. La décision de suspension d'une évaluation doit être notifiée par écrit au CESTI et au Centre de certification.

En cas de relance d'une évaluation suspendue, un préavis minimal d'un mois doit être respecté par le commanditaire entre sa décision et la date prévue de relance des travaux. Le CESTI est fondé de revoir avec le commanditaire l'impact organisationnel sur le projet d'évaluation (réaffectation des évaluateurs, réévaluation de la charge de gestion de projet, etc.). La décision de relance d'une évaluation suspendue doit être notifiée par écrit au CESTI et au Centre de certification. A cette occasion, la nouvelle organisation de projet doit être communiquée au Centre de certification.

3.5.7. Arrêt de l'évaluation à la demande du Commanditaire

Le commanditaire peut demander l'arrêt d'une évaluation et du processus de certification. Cette demande d'arrêt des travaux d'évaluation doit être notifiée par écrit au CESTI et au Centre de certification qui accuse réception de la décision.