Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 9 février 2004

000309/SGDN/DCSSI/SDR
Référence : CER/P/01.1

PROCEDURE

CERTIFICATION DE LA SECURITE OFFERTE PAR LES PRODUITS ET LES SYSTEMES DES TECHNOLOGIES DE L'INFORMATION

Objet : Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

Application : A compter du 1er janvier 2004

Diffusion : Publique

Vérifié par	Validé par Le sous-directeur "Régulation"	Vu l'avis du comité directeur Approuvé par Le Directeur central de la sécurité des systèmes d'information
Le responsable qualité ORIGINAL SIGNE *Le chef du centre de certification* ORIGINAL SIGNE	ORIGINAL SIGNE	ORIGINAL SIGNE

Suivi des modifications

Révision	Date	Modifications
1	27/10/2003	Création

TABLE DES MATIERES

1. Objet de la procédure

Ce document décrit l'ensemble du processus de certification depuis la demande officielle par un commanditaire jusqu'à l'attribution d'un certificat pour le produit évalué.

2. Contexte

Le décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information définit le cadre réglementaire du schéma français d'évaluation et de certification.

Ce schéma définit l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats attestant qu'un produit ou un système répond aux exigences de sécurité listées dans sa cible de sécurité.

3. Demande de certification

3.1. Références

- Norme NF EN 45011, Chapitre 8 : demande de certification
- Norme NF EN 45011, Chapitre 9 : préparation de l'évaluation

3.2. La demande de certification

Le commanditaire de la certification envoie à la DCSSI une demande officielle de certification par le biais du formulaire CER-F-01 Dossier d'évaluation qui constitue le dossier d'évaluation.

Comme l'indique l'art. 2 du décret 2002-535, le dossier contient notamment :

- la description du produit à évaluer incluant la cible de sécurité ;
- les critères d'évaluation sélectionnés ;
- le nom du centre d'évaluation sélectionné par le commanditaire pour mener les travaux d'évaluation ainsi que la liste des membres du comité de pilotage de l'évaluation ;
- le programme de travail prévisionnel pour l'évaluation.

Le dossier d'évaluation mentionne également les conditions générales de la certification que le commanditaire s'engage à respecter.

3.3. Traitement de la demande

Lorsque le dossier d'évaluation a été réceptionné par le centre de certification, ce dernier analyse son contenu en vue d'enregistrer officiellement la demande de certification.

Le détail de la procédure de traitement du dossier est décrite dans l'instruction interne CER-I-01 Traitement de la demande de certification.

Si le centre de certification estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, il notifie au commanditaire qu'il ne pourra pas en l'état du dossier procéder à la certification envisagée [art. 2. du décret 2002-535].

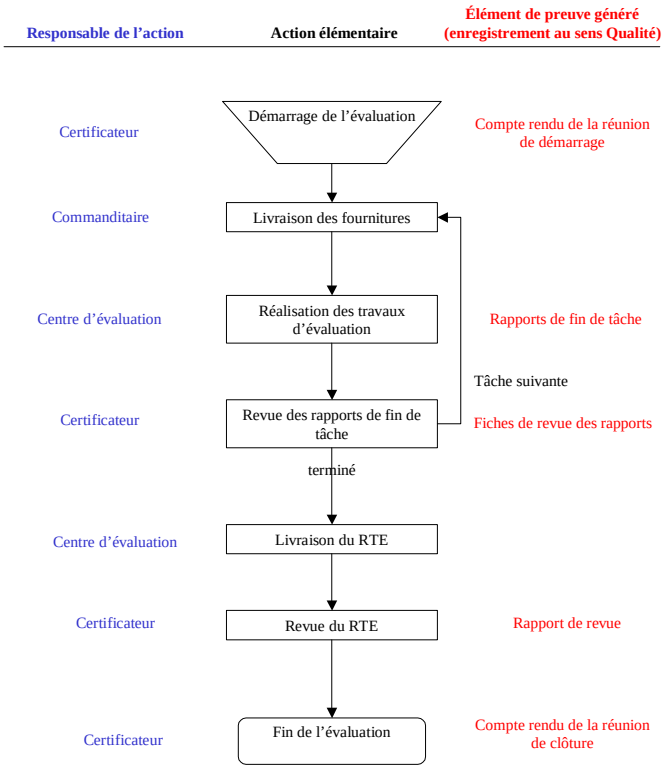
Si le dossier est satisfaisant, un certificateur est nommé pour suivre l'évaluation et une lettre d'enregistrement CER-F-03 Lettre d'enregistrement est envoyée au commanditaire.

4. Evaluation de la sécurité

4.1. Références

- Norme NF EN 45011, Chapitre 10 : évaluation
- Norme ISO/CEI 17025 : prescriptions générales concernant la compétence des laboratoires d'étalonnages et d'essais

4.2. Déroulement de l'évaluation



4.3. Démarrage de l'évaluation

Lorsque la demande est enregistrée, le certificateur en charge du projet contacte tous les membres du comité de pilotage de l'évaluation identifiés dans le dossier pour une réunion de démarrage de l'évaluation. Le certificateur mène la réunion conformément au modèle d'ordre du jour CER-F-05 Réunion de démarrage.

La réunion est actée dans un compte rendu, rédigé par le certificateur, qui est envoyé à tous les membres du comité de pilotage.

4.4. Livraison des fournitures

Le commanditaire de l'évaluation est responsable de la livraison des fournitures nécessaires à l'évaluation. La liste des fournitures à livrer est précisée dans le programme de travail prévisionnel du dossier d'évaluation.

Toutes les fournitures sont, par défaut, envoyées au centre d'évaluation et au certificateur en charge du projet.

Si le commanditaire a demandé la réalisation d'une analyse des mécanismes cryptographiques, un document de synthèse relatif aux aspects cryptographiques du produit visant une certification, doit être fourni à la

DCSSI et au centre d'évaluation. Le contenu attendu est précisé dans le document « fournitures nécessaires à l'analyse de mécanismes cryptographiques ».

Si le commanditaire n'est pas le concepteur du produit et pour des raisons de confidentialité, ces fournitures peuvent être livrées directement par le propriétaire du document (par exemple un développeur ou un sous-traitant).

La liste des fournitures utilisées pour l'évaluation doit être gérée par le centre d'évaluation conformément aux exigences du chapitre 5.8 de la norme ISO/CEI 17025.

4.5. Réalisation des travaux d'évaluation

Le centre d'évaluation mène les travaux d'évaluation conformément aux critères d'évaluation sélectionnés et au niveau d'assurance visé pour la certification. Ces travaux doivent également respecter les dispositions du système qualité IS 17025 du centre d'évaluation.

Les éléments de preuve de la réalisation des travaux sont consignés dans le rapport de fin de tâche associé à chaque tâche de l'évaluation. Ce rapport de fin de tâche doit être intégré au système qualité du centre d'évaluation.

Au cours de l'évaluation, des réunions techniques ou particulières peuvent être initiées par chacune des parties.

Cas des travaux sur site :

Certains travaux doivent être effectués par le centre d'évaluation sur le site de développement, de production ou d'exploitation du produit en évaluation.
Des accords doivent être établis entre le commanditaire, le développeur et le centre d'évaluation pour la réalisation de ces travaux. Ceux-ci doivent être identifiés dans le dossier d'évaluation afin que l'accès aux sites par les évaluateurs soit autorisé au moment opportun.
Le certificateur, s'il en fait la demande, doit pouvoir également assister à ces travaux.

Cas de l'analyse des mécanismes cryptographiques :
Si le commanditaire en a fait la demande, une analyse des mécanismes cryptographiques est réalisée conformément à l'instruction interne CRY-I-01 Analyse des mécanismes cryptographiques. Les résultats de cette analyse sont pris en compte dans le cadre de l'analyse de vulnérabilités menée par le centre d'évaluation.

4.6. Les rapports de fin de tâche

Lorsque la tâche est terminée ou si le commanditaire le demande, le rapport de fin de tâche est transmis au certificateur et au commanditaire.

Le certificateur analyse le rapport conformément à l'instruction interne CER-I-02 Revue des rapports d'évaluation. Pour réaliser cette analyse, le certificateur peut demander au centre d'évaluation, au développeur ou au commanditaire, à avoir accès à tout élément qu'il juge nécessaire.

Les conclusions de cette analyse sont consignées dans une fiche de revue du rapport CER-F-06 Fiche de revue de rapport qui est envoyée au centre d'évaluation. Ce dernier peut avoir à ré-émettre une nouvelle version du rapport ou à réaliser des travaux complémentaires si des anomalies ont été détectées par le certificateur.

4.7. Le Rapport Technique d'Evaluation (RTE)

Lorsque toutes les tâches d'évaluation ont été menées par le centre d'évaluation, ce dernier rédige le rapport final appelé Rapport Technique d'Evaluation ou RTE.

Le RTE est envoyé au certificateur et au commanditaire.

Comme pour les autres rapports issus de l'évaluation, le certificateur analyse le rapport conformément à l'instruction interne CER-I-02 Revue des rapports d'évaluation.

Les conclusions de cette analyse sont consignées dans une fiche de revue du rapport CER-F-06 Fiche de revue de rapport qui est envoyée au centre d'évaluation. Ce dernier peut avoir à ré-émettre une nouvelle version du rapport ou à réaliser des travaux complémentaires si des anomalies ont été détectées par le certificateur.

4.8. Fin de l'évaluation

Lorsque le RTE est validé par le certificateur, ce dernier contacte tous les membres du comité de pilotage pour la réunion de clôture de l'évaluation.

Le certificateur mène la réunion au cours de laquelle le centre d'évaluation doit résumer les travaux réalisés et les problèmes rencontrés lors du projet.

La réunion fait l'objet d'un compte rendu rédigé par le certificateur en charge du projet et transmis à tous les membres du comité de pilotage de l'évaluation.

5. Décision de certification

5.1. Références

- Norme NF EN 45011, Chapitre 12 : décision de certification

5.2. Préparation de la décision

A compter de la validation du RTE par le certificateur en charge du suivi de l'évaluation, la procédure de décision de certification est amorcée. La préparation de la décision de certification est détaillée dans l'instruction interne CER-I-03 Préparation de la décision de certification.

Le certificateur constitue un dossier qui comprend notamment :

- la demande de certification ;
- la version finale de la cible de sécurité ;
- le rapport de l'analyse des mécanismes cryptographiques (si elle a été réalisée) ;
- le RTE ;
- une proposition de rapport de certification. Ce rapport, qui précise les caractéristiques des objectifs de sécurité proposés, conclut soit à la délivrance d'un certificat, soit au refus de la certification. Il peut comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité [art. 7 du décret 2002-535].

Ce dossier est revu par le responsable technique puis validé par le chef du centre de certification avant sa transmission pour la décision de certification.

5.3. Décision de certification

Le Directeur central de la sécurité des systèmes d'information, par délégation du Premier ministre, décide d'accorder ou de refuser la certification. Il signe alors le certificat et son rapport de certification.

Une fois signés, des exemplaires du certificat et du rapport de certification sont envoyés au(x) commanditaire(s) mentionné(s) dans la demande de certification par recommandé avec accusé de réception.

La liste officielle des certificats CER-L-02 Liste des produits certifiés est mise à jour par le responsable qualité.

5.4. Publication du certificat

Le commanditaire peut demander, par le formulaire CER-F-13 Demande de publication du rapport de certification :

- que le certificat et son rapport de certification soient confidentiels ;
- que le rapport de certification soit publié sur le site internet de la DCSSI : www.ssi.gouv.fr. Dans ce cas, le commanditaire doit impérativement fournir la cible de sécurité.

Le responsable technique du centre de certification est chargé de transmettre la demande de publication au responsable du site internet.

Reconnaissance mutuelle :

Si un certificat entre dans le cadre des accords de reconnaissance mutuelle signés par la DCSSI, le responsable qualité informe les autres organismes de certification signataires de ces accords de la publication du certificat.

6. Retrait du certificat

6.1. Références

- Norme NF EN 45011, Chapitre 4.6 : conditions et procédures pour l'octroi, le maintien, l'extension, la suspension et le retrait de la certification

6.2. Conditions de retrait

Si le centre de certification obtient les éléments de preuve permettant de démontrer qu'un produit certifié ne répond plus aux exigences de sécurité listées dans sa cible de sécurité, le certificat peut être retiré.

Ces éléments de preuve peuvent provenir de travaux réalisés dans le cadre d'un programme de maintenance, d'un programme de surveillance ou de tout autre travaux d'évaluation impactant le produit concerné.