Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 19 janvier 2004

000097/SGDN/DCSSI/SDR
Référence : CPP/P/01.1

PROCEDURE

CERTIFICATION DE PROFILS DE PROTECTION

Objet : Certification de profils de protection
Application : A compter du 1er février 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	08/08/2003	Création

TABLE DES MATIERES

1. Objet de la procédure

Ce document décrit l'ensemble du processus de certification de profils de protection.

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 listés dans sa cible de sécurité.

Le centre de certification s'appuie sur cette organisation pour certifier la conformité des profils de protection aux exigences de la classe APE définie dans les critères communs.

3. Références

- CC : Common Criteria for Information Technology Security Evaluation ;
- CEM : Common Methodology for Information Technology Security Evaluation ;
- Norme internationale ISO/IEC 15408 : Information technology - Security techniques - Evaluation criteria for IT security.

4. Description de la procédure

4.1. Demande de certification d'un profil de protection

Le commanditaire de la certification doit envoyer à la DCSSI une demande officielle de certification du profil de protection.

La demande doit mentionner le profil de protection à évaluer et le nom du centre d'évaluation sélectionné pour mener les travaux d'évaluation. Le profil de protection, dans sa version d'évaluation, doit être livré avec la demande.

4.2. Traitement de la demande

Lorsque la demande de certification du profil de protection et le profil de protection ont été réceptionnés par le centre de certification, ce dernier analyse leur contenu en vue d'enregistrer officiellement la demande de certification du profil de protection.

Si le contenu de la demande est satisfaisant, un chargé d'affaire est nommé pour suivre l'évaluation et une lettre d'enregistrement CER-F-03 Lettre d'enregistrement est envoyée au commanditaire.

Le chargé d'affaire en charge du projet contacte le commanditaire et le centre d'évaluation pour une réunion de démarrage de l'évaluation du profil de protection. La réunion est actée dans un compte rendu, rédigé par le chargé d'affaire, qui est envoyé au commanditaire et au centre d'évaluation.

4.3. Évaluation du profil de protection

Le centre d'évaluation mène les travaux d'évaluation conformément à la classe APE des critères communs. Ces travaux doivent également respecter les dispositions du système qualité ISO 17025 du centre d'évaluation.

Les éléments de preuve de la réalisation des travaux sont consignés dans un rapport d'évaluation du profil de protection. Ce rapport est 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.

Lorsque les travaux sont terminés ou si le commanditaire le demande, le rapport d'évaluation du profil de protection est transmis au chargé d'affaire et au commanditaire.

4.4. Validation du rapport d'évaluation

Le chargé d'affaire analyse le rapport conformément à l'instruction interne CER-I-02 Revue des rapports d'évaluation. Pour réaliser cette analyse, il peut demander au centre d'évaluation 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 chargé d'affaire.

Si les conclusions du rapport impliquent des changements dans le profil de protection, le commanditaire devra fournir une nouvelle version qui sera à nouveau évaluée.

4.5. Décision de certification

4.5.1. Préparation de la décision

Lorsque le rapport d'évaluation du profil de protection est validé par le chargé d'affaire, 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 du profil de protection ;
- le rapport d'évaluation du profil de protection ;
- 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.

4.5.2. 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 rapport de certification.

Une fois signé, un exemplaire du rapport de certification est envoyé au commanditaire par recommandé avec accusé de réception.

La liste officielle des profils de protection certifiés CER-L-05 Liste des PP certifiés est mise à jour par le responsable qualité.

4.6. Publication du rapport de certification

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

- que le profil de protection et son rapport de certification restent confidentiels ;
- que le profil de protection et son rapport de certification soit publiés sur le site internet de la DCSSI : www.ssi.gouv.fr. Dans ce cas, le responsable qualité est chargé de transmettre la demande de publication au responsable du site internet.