



PREMIER MINISTRE

Secrétariat général
de la défense nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, le 25 Avril 2008

N° 915/SGDN/DCSSI/SDR

CERTIFICATION DE SECURITE DE PREMIER NIVEAU DES TECHNOLOGIES DE L'INFORMATION

Version 2.4
Phase expérimentale

Sommaire

| | | |
|-----|--|----|
| 1 | INTRODUCTION..... | 2 |
| 2 | DOCUMENTS DE REFERENCE ET DEFINITIONS | 3 |
| 2.1 | Documents de référence | 3 |
| 2.2 | Définitions | 3 |
| 3 | LES ACTEURS..... | 4 |
| 3.1 | Le commanditaire..... | 4 |
| 3.2 | Le centre d'évaluation | 4 |
| 3.3 | Le centre de certification de la DCSSI..... | 4 |
| 4 | PREALABLE A LA DEMANDE DE CERTIFICATION..... | 5 |
| 5 | CHOIX D'UN CENTRE D'EVALUATION..... | 6 |
| 6 | DEMANDE DE CERTIFICATION..... | 6 |
| 7 | ANALYSE DE LA DEMANDE..... | 6 |
| 8 | DEROULEMENT DE L'EVALUATION | 7 |
| 8.1 | Analyse de la conformité..... | 7 |
| 8.2 | Analyse de l'efficacité..... | 7 |
| 8.3 | Temps contraint..... | 8 |
| 8.4 | Rapport technique d'évaluation..... | 8 |
| 9 | CERTIFICATION | 8 |
| 10 | CONTINUTE DE L'ASSURANCE | 9 |
| 11 | SURVEILLANCE..... | 9 |
| 12 | PUBLICITE..... | 10 |

1 INTRODUCTION

En application des décisions prises lors du CISI du 11 juillet 2006, la DCSSI est chargée de proposer et d'expérimenter un processus de délivrance d'un label de premier niveau pour les produits de sécurité des systèmes d'information dans des coûts et des délais contraints permettant notamment de labelliser des logiciels libres.

Il est proposé de s'orienter, lors d'une phase expérimentale¹, vers un label reposant sur une certification de sécurité de premier niveau (CSPN) telle que présentée ci-dessous.

Il s'agit d'attester que le produit a subi avec succès une évaluation par des centres d'évaluation agréés par la DCSSI dans un temps et une charge contraints conduisant à une certification.

Les travaux d'évaluation ont pour objectifs :

- de vérifier que le produit est conforme à ses spécifications de sécurité ;
- de coter les mécanismes de façon théorique, de recenser les vulnérabilités connues de produits de sa catégorie ;
- de soumettre le produit à des tests visant à contourner ses fonctions de sécurité.

¹ Durant cette phase, il est possible que certains documents cités en référence au chapitre 2 ne soient pas disponibles sur le site www.ssi.gouv.fr. En cas de besoin, vous pouvez contacter le centre de certification de la DCSSI (certification.dcssi@sgdn.gouv.fr).

2 DOCUMENTS DE REFERENCE ET DEFINITIONS

2.1 Documents de référence

[AGREMENT] Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau, procédure CSPN-AGR/P/01 disponible sur www.ssi.gouv.fr.

[CONTINUITE] Maintien de la confiance, continuité de l'assurance, procédure CSPN-MAI/P/01 disponible sur www.ssi.gouv.fr.

[CRITERES] Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, CSPN-Critères pour l'évaluation, dernière version disponible sur www.ssi.gouv.fr.

[CRYPTO] Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, dernière version disponible sur www.ssi.gouv.fr.

[DOSSIER_EVAL] Dossier d'évaluation en vue d'une demande de certification sécurité de premier niveau, formulaire CSPN-CER/F/01 disponible sur www.ssi.gouv.fr.

[FOURNITURES_CRYPTO] Fournitures nécessaires à l'analyse de mécanismes cryptographiques, dernière version disponible sur www.ssi.gouv.fr.

[METHODE] Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, dernière version disponible sur www.ssi.gouv.fr.

[SURVEILLANCE] Surveillance des produits certifiés, CSPN-SUR/P/01 disponible sur www.ssi.gouv.fr.

2.2 Définitions

| | |
|---------------------------------------|--|
| Cible de sécurité ou CdS | Cible de Sécurité, document décrivant en particulier les fonctionnalités de sécurité du produit qui font l'objet de l'évaluation et de la certification. |
| Cible d'évaluation | Produit réel soumis à l'évaluation. |
| Centre d'évaluation | Organisme agréé par la DCSSI qui réalise l'évaluation de la sécurité du produit en vue de la CSPN. |
| CSPN | Certificat de sécurité de premier niveau (ou certification de sécurité de premier niveau selon le contexte). |
| Commanditaire | Le commanditaire est celui qui paye l'évaluation et qui réalise la demande de certification auprès de la DCSSI. |
| Rapport technique d'évaluation ou RTE | Rapport consignait les résultats de l'évaluation menée par le centre d'évaluation sur la cible d'évaluation. |

3 LES ACTEURS

Les acteurs du processus de certification sont :

- les commanditaires ;
- les centres d'évaluation ;
- le centre de certification de la DCSSI ;
- éventuellement, les développeurs des produits soumis à l'évaluation.

3.1 Le commanditaire

Il est responsable de la fourniture de la cible de sécurité du produit, du produit lui-même et de son éventuelle documentation. Si des fonctions de sécurité essentielles du produit sont implémentées par des mécanismes cryptographiques, le commanditaire doit s'assurer de la disponibilité de la documentation de ces mécanismes (voir [FOURNITURES_CRYPTO]).

Il établit un contrat avec un centre d'évaluation agréé par la DCSSI pour réaliser l'évaluation de la sécurité.

Il fournit le dossier de demande de certification à la DCSSI.

Il est destinataire du Rapport Technique d'Evaluation (RTE) dans sa version finalisée et validée par la DCSSI.

Il décide de la publication ou non du rapport de certification élaboré par la DCSSI.

3.2 Le centre d'évaluation

Il est agréé par la DCSSI dans un ou plusieurs domaines techniques pour réaliser des évaluations en vue de la CSPN.

Il établit un contrat avec les commanditaires en vue de réaliser des évaluations de produits dans le domaine technique pour lequel il est agréé.

Il réalise l'évaluation du produit en suivant les critères et la méthodologie élaborés par la DCSSI en vue de la CSPN.

Il rédige le RTE qu'il envoie à la DCSSI pour validation.

Le centre d'évaluation a une obligation de secret professionnel concernant les produits qu'il évalue et les résultats qu'il obtient durant l'évaluation.

La liste des centres d'évaluation agréés pour la CSPN est tenue à jour sur le site www.ssi.gouv.fr.

3.3 Le centre de certification de la DCSSI

Il élabore les critères et la méthode générique d'évaluation pour la CSPN.

Il rédige les procédures, formulaires, guides, etc. permettant de mettre en œuvre la CSPN. On peut citer notamment :

- la procédure d'agrément des centres d'évaluation ;
- la procédure de demande de CSPN ;
- les modèles pour la rédaction des cibles de sécurité, RTE, rapport de certification ;
- les formulaires pour les demandes de CSPN.

Il agréé les centres d'évaluation qui vérifient les critères énumérés dans la procédure d'agrément des centres de certification (voir [AGREMENT]). On peut citer notamment les points suivants :

- les centres d'évaluation ne doivent pas se mettre en position de conflit d'intérêt lors d'une évaluation ;
- les centres d'évaluation sont agréés dans les domaines techniques pour lesquels la compétence a été estimée suffisante par la DCSSI. Ces compétences pouvant dépendre de personnels particuliers, la DCSSI est informée de tout mouvement de personnel dans le

centre d'évaluation. Le départ d'un personnel clé pour une compétence particulière peut entraîner la suspension ou la suppression de l'agrément pour ce domaine ;

- les centres d'évaluation ne peuvent évaluer des produits en vue d'une CSPN que dans les domaines techniques pour lesquels ils ont été agréés. Toutefois, plusieurs centres d'évaluation peuvent associer leurs compétences afin de couvrir l'intégralité des compétences nécessaires pour évaluer un produit ;
- les personnels du centre d'évaluation sont soumis au secret professionnel.

Il analyse la demande de certification (cible de sécurité, durée des tests ...) et autorise ou non le lancement de l'évaluation.

Il valide les RTE élaborés par les centres d'évaluation.

Il décide de la suite à donner à chaque évaluation (certification ou pas).

Il élabore le rapport de certification qu'il propose au commanditaire pour accord sur la publication.

Il publie les cibles de sécurité et les rapports de certification des produits ayant obtenus un CSPN sur le site www.ssi.gouv.fr.

4 PREALABLE A LA DEMANDE DE CERTIFICATION

En préalable à la demande de CSPN, pour un produit donné, le commanditaire doit s'assurer :

- qu'il dispose d'une cible de sécurité rédigée en français pour le produit, contenant au minimum :
 - o le nom commercial du produit et une référence permettant d'identifier sans ambiguïté le produit et la version soumise à l'évaluation ;
 - o un argumentaire du produit décrivant en langage naturel :
 - l'usage pour lequel le produit a été conçu et décrivant par qui et dans quel contexte d'emploi il est censé être utilisé ;
 - l'environnement technique dans lequel le produit fonctionne (modèle d'ordinateur, système d'exploitation...) ;
 - les biens sensibles que le produit doit protéger ;
 - les menaces contre lesquelles le produit offre une protection ;
 - les fonctionnalités de sécurité implémentées par le produit pour parer les menaces identifiées. Ce sont ces fonctionnalités qui feront l'objet de l'évaluation.

Le plan de la cible de sécurité est imposé et disponible sur le site de la DCSSI (www.ssi.gouv.fr).

- qu'il dispose d'une documentation en français permettant à un utilisateur final d'utiliser le produit de façon sûre (documentation utilisateur, éventuellement d'administration et d'installation) ;
- si des fonctions de sécurités essentielles du produit sont implémentées par des mécanismes cryptographiques, qu'il dispose d'informations complémentaires sur ces mécanismes ainsi que de jeux de tests permettant à l'évaluateur de vérifier la conformité de la mise en œuvre des mécanismes par le produit par rapport à leur description ;

- que le produit peut-être associé à un ou plusieurs des domaines techniques suivants :
 - 1 - détection d'intrusions ;
 - 2 - anti-virus, protection contre les codes malveillants ;
 - 3 - firewall ;
 - 4 - effacement de données ;
 - 5 - administration et supervision de la sécurité ;
 - 6 - identification, authentification et contrôle d'accès ;
 - 7 - communication sécurisée ;
 - 8 - messagerie sécurisée ;
 - 9 - stockage sécurisé ;
 - 10 - matériel et logiciel embarqué.

Si le produit ne rentre dans aucune des catégories citées ou en cas de doute, le commanditaire peut contacter le centre de certification afin de déterminer si le produit est évaluable au sens de la CSPN et si c'est le cas, quels sont le ou les centres d'évaluation qui pourraient réaliser l'évaluation.

- que le centre d'évaluation pourra disposer d'un accès au produit ;
- que le centre d'évaluation pourra disposer d'un accès à des équipements de test si ceux-ci sont spécifiques ou dédiés.

5 CHOIX D'UN CENTRE D'EVALUATION

Le commanditaire établit un contrat avec un centre d'évaluation agréé (ou une association de centres d'évaluation) pour le ou les domaines techniques dans lesquels est classé le produit à faire évaluer.

6 DEMANDE DE CERTIFICATION

Le commanditaire complète et envoie la demande de certification (voir [DOSSIER_EVAL]) et la cible de sécurité du produit au centre de certification.

7 ANALYSE DE LA DEMANDE

Le centre de certification analyse la demande et la cible de sécurité du produit. Après acceptation de ces éléments par le centre de certification, le projet de certification est enregistré et les acteurs (commanditaire, centre d'évaluation) sont avertis du démarrage du projet.

Plusieurs raisons peuvent justifier un refus du dossier :

- demande incomplète ;
- cible de sécurité non conforme aux canevas ;
- cible de sécurité manifestement trompeuse (par exemple, le produit est un pare-feu et la seule fonction de sécurité décrite comme devant être évaluée est l'authentification de l'utilisateur pour modifier la configuration de son produit) ;
- centre d'évaluation non agréé pour le domaine technique du produit ;
- produit dont la complexité est telle qu'il n'est pas envisageable de réaliser une évaluation dans le cadre de la CSPN ;
- utilisation d'algorithmes cryptographiques n'ayant pas fait l'objet d'un standard ou d'une norme ;
- refus du commanditaire de divulguer les vulnérabilités connues du produit, corrigées ou non ;

- absence d'engagement du commanditaire qu'il n'en connaît pas d'autres ;
- ...

8 DEROULEMENT DE L'EVALUATION

Les évaluations se déroulent dans un cadre méthodologique formalisé (voir [CRITERES] et [METHODES]) afin de garantir l'objectivité des évaluations et l'homogénéité des résultats entre les différents centres d'évaluation. Ce cadre méthodologique permet également de faciliter la comparaison des résultats d'évaluations de produits similaires lorsqu'elles sont réalisées par des centres d'évaluation différents.

La DCSSI peut demander à participer à tout ou partie des tâches d'évaluation réalisées par le centre d'évaluation.

En cas de dépassement du délai prévu pour l'évaluation, la DCSSI peut décider de clore le projet de certification. Pour autant, le commanditaire n'est pas libéré de ses éventuelles obligations vis à vis du centre d'évaluation.

Le but de l'évaluation est d'apprécier en temps contraint :

- la conformité du produit à sa cible de sécurité (§8.1) ;
- l'efficacité des fonctionnalités (§8.2).

Le déroulement de l'évaluation repose sur :

- la documentation existante ;
- au minimum, les bases publiques de vulnérabilités pour le test des vulnérabilités connues ;
- le produit lui-même, installé sur une plate forme de test aussi représentative que possible de l'environnement prévu d'utilisation.

Les résultats sont consignés dans un RTE qui est transmis au centre de certification.

8.1 Analyse de la conformité

L'analyse de la conformité se fait sur une plate-forme de test qui doit être décrite dans le RTE.

L'objectif de cette phase est double. Il s'agit :

- d'une part de vérifier si le produit est conforme à ses spécifications de sécurité, toutes les non conformités découvertes devant être tracées et rappelées dans le RTE ;
- d'autre part de permettre à l'évaluateur chargé de l'évaluation de bien comprendre le produit dans sa globalité pour être pertinent dans les analyses d'efficacité.

L'analyse de la conformité peut également comporter, lorsque cela est possible et lorsque cela à un sens :

- une analyse des performances ;
- une description éventuelle de l'interopérabilité du produit avec d'autres produits.

8.2 Analyse de l'efficacité

Les principaux objectifs sont :

- de coter la résistance théorique des fonctions et mécanismes de sécurité ;
- d'identifier les vulnérabilités de construction ou en exploitation ;
- de donner un avis sur les risques de mauvaise utilisation ;
- de donner un avis d'expert sur l'efficacité du produit ;

- éventuellement, de proposer un paramétrage et un environnement d'utilisation qui permettent de limiter l'exploitabilité des vulnérabilités et, dans ce cas, de donner un second avis d'expert sur l'efficacité du produit dans son nouvel environnement d'utilisation.

8.3 Temps contraint

L'évaluation est réalisée en temps et charges contraints afin de répondre à des exigences de maîtrise des coûts et délais.

La DCSSI propose une charge nominale de 20 homme.jour et un délai calendaire de 8 semaines. Le commanditaire et le centre d'évaluation peuvent renégocier à la hausse (cela peut-être le cas lorsque l'évaluation nécessite la participation de plusieurs centres d'évaluation par exemple) ou à la baisse la charge et le délai. La DCSSI se réserve la possibilité de refuser une évaluation pour laquelle elle considérerait la charge insuffisante ou le délai comme excessif.

Si des fonctions de sécurité essentielles du produit sont implémentées par des algorithmes cryptographiques, la charge pourra être augmentée, de l'ordre de 10 homme.jour supplémentaires, afin d'en permettre l'analyse.

8.4 Rapport technique d'évaluation

Le RTE comporte au minimum les informations suivantes :

- le rappel du contexte de l'analyse (contexte d'emploi, durée de l'analyse, fonctions de sécurité...);
- une synthèse de la documentation donnant une description des fonctions de sécurité ou liées à la sécurité ;
- ce qui est attendu fonctionnellement du produit (résumé de ses caractéristiques de sécurité notamment) ;
- l'inventaire des vulnérabilités du produit (CERTA, bases publiques, informations du développeur) et des correctifs disponibles applicables ;
- la liste des principaux outils d'analyse utilisés ;
- une synthèse des résultats des tests effectués sur le produit ;
- une estimation de la cotation de la résistance des mécanismes de sécurité ;
- un bilan et une cotation des éventuelles vulnérabilités exploitables identifiées ;
- un bilan du produit et des préconisations d'utilisation ou de paramétrage dans le contexte d'emploi prévu.

Le plan du RTE est imposé (voir [METHODE]).

9 CERTIFICATION

A l'issue de l'évaluation, le RTE est transmis au centre de certification de la DCSSI. Le processus de certification comporte nominalelement les étapes suivantes :

1. Analyse du RTE. La DCSSI peut être amenée à demander des précisions, voire des travaux supplémentaires au centre d'évaluation si ceux-ci ne sont pas estimés suffisants.
2. Présentation des travaux et des résultats de l'évaluation par le centre d'évaluation. A cet effet, la DCSSI peut demander que lui soit faite une démonstration du produit. Le commanditaire de l'évaluation est invité à cette présentation.
3. Rédaction du rapport de certification. Celui-ci comporte en particulier une cotation de la résistance des fonctions et mécanismes de sécurité du produit aux attaques, d'éventuelles

recommandations d'usage et signale tous problèmes potentiels relevés lors de l'évaluation et qui sont susceptibles d'intéresser un utilisateur. Il est rédigé en français.

4. Proposition du rapport de certification au commanditaire pour décision de publication.
5. Si le commanditaire donne son accord, le rapport de certification est proposé à la signature du directeur central de la DCSSI pour certification et publication. Si le directeur central donne son accord, la cible de sécurité et le rapport de certification sont publiés sur le site de la DCSSI. La marque TI est apposée sur le rapport de certification et atteste que le produit a reçu une certification de sécurité de premier niveau.



Si le RTE fait apparaître que le produit ne répond pas ou ne répond que partiellement à sa cible de sécurité et qu'il n'est pas possible d'identifier des contre-mesures environnementales réalistes pour améliorer cette situation, le processus de certification est arrêté à l'issue de l'étape 1. ou 2. Le commanditaire est averti de cette situation. Parmi les raisons pour lesquelles la DCSSI pourrait estimer que le produit répond imparfaitement à sa cible de sécurité, on peut citer :

- résistance trop faible des fonctions et mécanismes de sécurité ;
- dysfonctionnement de certaines fonctions de sécurité ;
- dysfonctionnement de certaines fonctionnalités du produit n'en permettant pas un usage normal ;
- certaines informations nécessaires à la compréhension des fonctionnalités de sécurité du produit n'ont pu être obtenues et cet état de fait ne permet pas d'estimer correctement la résistance des fonctions et mécanismes de sécurité ;
- etc.

De même, le fait que le produit utilise des mécanismes cryptographiques n'atteignant pas le niveau standard du référentiel cryptographique de la DCSSI [CRYPTO] peut entraîner un refus de la certification.

10 CONTINUITÉ DE L'ASSURANCE

Un certificat n'est associé qu'à une version donnée d'un produit. En cas d'évolution de ce produit, les nouvelles versions ne sont pas certifiées par défaut. Le processus de continuité de l'assurance (voir [CONTINUITÉ]) permet de déterminer à moindre coût si une nouvelle version d'un produit peut bénéficier du certificat d'une version précédemment certifiée. Ce processus est applicable à la CSPN.

11 SURVEILLANCE

L'état de l'art dans le domaine de la sécurité évolue constamment. Un produit certifié peut devenir vulnérable à de nouvelles attaques. Un commanditaire peut s'en assurer en demandant périodiquement que soient réalisées de nouvelles analyses de vulnérabilités. La procédure [SURVEILLANCE] décrit le processus proposé par la DCSSI pour surveiller dans le temps la résistance d'un produit aux nouvelles attaques. Ce processus est applicable à la CSPN.

12 PUBLICITE

Le développeur peut faire état du fait que son produit a reçu une CSPN. Il doit le faire dans des termes honnêtes et compréhensibles pour l'utilisateur final. Il doit impérativement indiquer :

- la référence du certificat ;
- la date de certification initiale du produit ;
- les références du produit certifié (version ...) ;
- l'adresse du site de la DCSSI où l'utilisateur peut consulter la cible de sécurité du produit et le rapport de certification.

La DCSSI se réserve la possibilité de faire connaître, par tout moyen qu'elle considère comme efficace, tout usage abusif de la CSPN.