



PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Paris, le 27 mai 2015

N° 2095/ANSSI/SDE/PSS/CCN

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

Référence : ANSSI-CSPN-AGR-P-01/1.2

PROCEDURE

AGREMENT DES CENTRES D'EVALUATION EN VUE DE LA CERTIFICATION DE SECURITE DE PREMIER NIVEAU

Application : Dès son approbation.

Diffusion : Publique.

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

Guillaume POUPARD
[ORIGINAL SIGNE]



Suivi des modifications

Edition	Date	Modifications
Phase expérimentale	13 juin 2008	Première rédaction pour la phase expérimentale, diffusée sous le n° 1333 SGDN/DCSSI/SDR du 13 juin 2008, et abrogée par la présente procédure.
1.0	30 mai 2011	Fin de la phase expérimentale, suite à la modification apportée au décret n° 2002-535 du 18 avril 2002 par le décret n° 2010-112 du 2 février 2010. Changement de dénomination de l'organisme de certification (ANSSI) et améliorations de forme.
1.1	7 avril 2014	En annexe B, ajout des domaines d'agrément « terminal de réception numérique » et « environnement d'exécution sécurisé ». En annexe B, modification de la définition de la portée d'agrément qui ne correspond plus qu'aux domaines CSPN.
1.2	27 mai 2015	Mise à jour des portées d'agrément CSPN décrites en annexe B2 pour introduire les produits de type « automate programmable industriel » et pour préciser la portée des évaluations des produits des types « détection d'intrusions » et « anti-virus, protection contre les codes malveillants ».

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

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 PROCEDURE	4
2. REFERENCES.....	4
3. DESCRIPTION DE LA PROCEDURE	4
3.1 FORMULATION DE LA DEMANDE D'AGREMENT PAR LE CENTRE CANDIDAT	4
3.2 ENREGISTREMENT DE LA DEMANDE PAR L'ANSSI.....	5
3.3 AUDIT D'AGREMENT PRELIMINAIRE	5
3.4 ÉVALUATION PILOTE	5
3.5 AUDIT D'AGREMENT INITIAL	5
3.6 DECISION D'AGREMENT	5
3.7 SUIVI DE L'AGREMENT.....	5
3.8 MODIFICATION DE LA PORTEE D'AGREMENT	6
<i>a</i> Modification de la portée d'agrément à la demande du centre d'évaluation	6
<i>b</i> Modification de la portée d'agrément à l'initiative du centre de certification	6
3.9 RENOUELEMENT DE L'AGREMENT	6
3.10 SUSPENSION DE L'AGREMENT	7
3.11 RETRAIT DE L'AGREMENT.....	7
3.12 CONSEQUENCES DE LA PERTE DE L'AGREMENT.....	7
4. CAS DES CESTI AGREES POUR LES EVALUATIONS « CRITERES COMMUNS » OU « ITSEC ».....	8
Annexe A : Critères d'agrément	9
Annexe B : Portée d'agrément	11
Annexe C : Obligations résultant de l'agrément	12

1. Objet de la procédure

La présente procédure décrit le processus d'agrément des centres qui réalisent des évaluations de produits en vue de leur certification de sécurité de premier niveau (CSPN).

La procédure d'agrément d'un centre d'évaluation permet de s'assurer :

- de son aptitude à appliquer les critères d'évaluation en vigueur et la méthodologie correspondante ;
- de sa compétence technique sur les types de produits qui font partie de sa portée d'agrément ;
- de son indépendance vis-à-vis des développeurs pour son activité d'évaluation ;
- de la compatibilité de sa structure juridique et de son organisation avec cette activité.

2. Références

- 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.
- ANSSI-CSPN-CER-P-01 – Certification de sécurité de premier niveau des produits des technologies de l'information.

3. Description de la procédure

3.1 Formulation de la demande d'agrément par le centre candidat

Un centre d'évaluation candidat à l'agrément doit adresser sa demande au centre de certification de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à l'aide du formulaire [ANSSI-CSPN-AGR-F-01 Demande d'agrément](#). Il s'engage alors notamment à respecter les obligations précisées en annexe C.

Les documents suivants doivent être fournis avec la demande d'agrément :

- une photocopie d'un extrait Kbis de la société ;
- un dossier technique permettant d'apprécier les capacités professionnelles du candidat, comprenant :
 - une présentation générale de l'entreprise, précisant notamment les différentes responsabilités. Si le centre d'évaluation fait partie d'une organisation plus large, un ou plusieurs organigrammes doivent présenter sa place dans l'entreprise mère ;
 - les expériences et références nationales et internationales récentes de prestations similaires et les périodes de réalisation des prestations. Le candidat devra justifier notamment de ses compétences pour les activités d'évaluation de la sécurité des technologies de l'information ;
 - la liste et les curriculum vitae des experts techniques identifiés pour réaliser les prestations d'expertise ;
- les éventuelles habilitations de la société à traiter des informations classifiées de défense ;
- une proposition d'évaluation pilote ;
- les types de produits pour lesquels l'agrément est demandé (voir annexe B sur la portée d'agrément), et les experts techniques qu'il est prévu de faire intervenir en expertise pour chaque type de produit ;
- tout autre élément pouvant apporter des informations utiles sur le candidat.

3.2 Enregistrement de la demande par l'ANSSI

L'ANSSI confirme l'enregistrement de la demande. Le membre du centre de certification responsable de l'agrément des centres d'évaluation pour le domaine considéré prend en charge le suivi du candidat tout au long de la procédure d'agrément. Il organise notamment l'audit préliminaire du candidat.

3.3 Audit d'agrément préliminaire

Un audit préliminaire est effectué dans les locaux du candidat pour évaluer sa capacité à répondre aux critères d'agrément cités en annexe A. Un rapport d'audit est rédigé à l'issue de l'audit par le responsable d'agrément.

Si les conclusions sont satisfaisantes, le candidat obtient l'autorisation d'effectuer une évaluation pilote.

3.4 Évaluation pilote

Le candidat doit mener une évaluation pilote pour permettre à l'ANSSI d'apprécier sa capacité à mener à bien une évaluation.

Il est de la responsabilité du candidat de négocier et d'obtenir un projet d'évaluation pilote auprès d'un commanditaire. Ce dernier devra être informé de la situation du candidat et des risques encourus quant au résultat de l'évaluation. Aucun certificat ne pourra être délivré tant que le centre d'évaluation n'est pas agréé.

L'évaluation pilote doit être menée conformément aux procédures en vigueur. Elle fait l'objet d'un suivi renforcé par l'ANSSI.

Le candidat dispose d'un an à compter de la demande d'agrément pour réaliser l'évaluation pilote. Au-delà, il doit refaire acte de candidature.

3.5 Audit d'agrément initial

Au terme de l'évaluation pilote, l'ANSSI effectue si nécessaire un nouvel audit. Il est notamment vérifié que les non-conformités identifiées lors de l'audit préliminaire ont été corrigées.

Le responsable d'agrément rédige le rapport final de l'audit d'agrément, qui indique si le candidat satisfait tous les critères d'agrément listés en annexe A.

3.6 Décision d'agrément

La décision d'agrément est prononcée par le Premier ministre, après avis du comité directeur de la certification. Cette décision peut énoncer les obligations particulières auxquelles est soumis le centre d'évaluation. La décision d'agrément indique notamment la portée de l'agrément pour laquelle le centre d'évaluation peut réaliser des évaluations en vue d'une certification. Les différentes portées d'agrément sont décrites en annexe B.

L'agrément est valable deux ans.

La décision est notifiée au centre d'évaluation par courrier.

3.7 Suivi de l'agrément

L'ANSSI suit de façon continue les activités du centre d'évaluation et s'assure que les obligations liées à l'agrément précisées en annexe C sont respectées. Elle peut s'assurer à tout moment par un audit que le centre d'évaluation continue à satisfaire aux critères d'agrément et à ses engagements.

3.8 Modification de la portée d'agrément

Cette procédure peut être initialisée :

- à la demande d'un centre d'évaluation qui désire modifier sa portée d'agrément ;
- à la demande du centre de certification, s'il estime que la situation du centre d'évaluation a changé (compétences, statut, etc.). Par exemple, en cas de départ de membres du centre d'évaluation qui disposent de compétences clés, le centre de certification peut restreindre la portée de l'agrément pour tenir compte de cette perte de compétence.

a Modification de la portée d'agrément à la demande du centre d'évaluation

Le centre d'évaluation transmet au centre de certification, par courrier libre, l'ensemble des éléments qui justifient sa demande. Cette demande peut entraîner la reprise d'une partie de la procédure d'agrément (a priori, à partir des § 3.3 ou 3.4). En particulier, la vérification des éléments justifiant la demande peut se faire sous la forme d'un audit complémentaire du centre d'évaluation.

Le responsable d'agrément suit l'ensemble de ces étapes. Il consigne les résultats et éléments de preuve de chaque étape dans le dossier de suivi du centre d'évaluation. A l'issue de l'analyse de l'ensemble des résultats, il rédige une note à l'attention du directeur général de l'ANSSI, qui décide, par délégation du Premier ministre et après avis du comité directeur de la certification, du maintien ou de la modification de la portée d'agrément.

La décision est prise par le Premier ministre et notifiée par courrier au centre d'évaluation.

b Modification de la portée d'agrément à l'initiative du centre de certification

Lorsque l'ANSSI considère que des conditions de l'agrément ne sont plus satisfaites et doivent conduire à modifier la portée d'agrément du centre d'évaluation, elle en prévient par courrier le centre d'évaluation, en indiquant la période allouée pour la mise en place des mesures correctives nécessaires. Le centre d'évaluation dispose de quinze jours calendaires, à compter de la réception du courrier de l'ANSSI, pour faire valoir ses observations.

Le responsable d'agrément suit l'ensemble de ces étapes. Il consigne les résultats et éléments de preuve de chaque étape dans le dossier de suivi du centre d'évaluation.

A l'issue de la période allouée, il rédige une note comprenant l'ensemble des éléments de preuve à l'attention du directeur général de l'ANSSI, qui décide, par délégation du Premier ministre et après avis du comité directeur de la certification, du maintien ou de la modification de la portée d'agrément.

La décision est prise par le Premier ministre et notifiée par courrier au centre d'évaluation.

3.9 Renouvellement de l'agrément

Il appartient au centre d'évaluation de faire, s'il le souhaite, une demande de renouvellement de son agrément. Il adresse sa demande au centre de certification de l'ANSSI au plus tard quatre mois avant l'échéance de la validité de son agrément en cours.

Un nouvel audit d'agrément est alors mené. Il permet de vérifier que les critères et obligations de l'agrément sont toujours respectés. Il permet également de faire le point sur les écarts constatés et formalisés pendant la période d'agrément, ainsi que sur les actions mises en œuvre pour les corriger.

Si les conditions sont satisfaites, une nouvelle décision d'agrément est prononcée par le Premier ministre, après avis du comité directeur de la certification, et notifiée par courrier au centre d'évaluation.

Si le centre d'évaluation ne souhaite pas renouveler son agrément, il en informe si possible l'ANSSI. Il peut aussi ne pas envoyer de demande de renouvellement. A l'échéance de l'agrément, l'ANSSI adresse au centre d'évaluation une lettre notifiant la perte d'agrément. Le paragraphe 3.11 ci-après s'applique alors.

3.10 Suspension de l'agrément

L'agrément peut être suspendu par le Premier ministre lorsque le centre d'évaluation ne répond plus aux obligations liées à son agrément (voir annexe C) ou à une activité insuffisante dans les domaines de sa portée d'agrément.

L'ANSSI adresse au centre d'évaluation une lettre lui notifiant son intention de suspendre son agrément et le mettant en demeure de mettre en place les mesures correctives nécessaires avant un délai qui lui est fixé. Le centre d'évaluation dispose de quinze jours calendaires, à compter de la réception du courrier de l'ANSSI, pour faire valoir ses observations. Le cas échéant, la suspension de l'agrément est alors confirmée et notifiée par courrier au centre d'évaluation.

Au terme du délai fixé, si le centre de certification estime que les causes ayant entraîné la suspension ne sont pas corrigées ou en voie de l'être, une procédure de retrait de l'agrément est engagée. Dans le cas contraire, la suspension est maintenue jusqu'à la correction de l'ensemble des causes l'ayant entraîné.

Durant la période de suspension, le centre de certification décide au cas par cas :

- de l'acceptation de nouveaux dossiers de certification soumis par le centre d'évaluation ;
- de la prise en compte des résultats des évaluations effectuées par le centre d'évaluation.

3.11 Retrait de l'agrément

L'agrément peut être retiré par le Premier ministre, soit parce que le centre d'évaluation demande à cesser son activité, soit à l'initiative de l'ANSSI. Dans ce dernier cas, la décision est prise après avis du comité directeur de la certification.

Une liste non limitative des causes de retrait à l'initiative de l'ANSSI est donnée ci-dessous à titre d'exemple :

- le centre d'évaluation ne répond plus aux obligations fixées par la décision d'agrément (voir annexe C) ;
- les causes ayant entraîné une suspension d'agrément n'ont pas été corrigées ;
- un motif lié aux intérêts de la défense et de la sécurité nationale.

L'ANSSI adresse une lettre au centre d'évaluation lui notifiant son intention d'engager une procédure de retrait de son agrément. Le centre d'évaluation dispose de quinze jours calendaires, à compter de la réception du courrier de l'ANSSI, pour faire valoir ses observations devant le comité directeur de la certification. Le cas échéant, la décision de retrait est notifiée au centre d'évaluation par courrier.

3.12 Conséquences de la perte de l'agrément

En cas de perte de l'agrément (retrait ou non renouvellement), le nom du centre d'évaluation concerné est supprimé de la liste des centres d'évaluation agréés.

Aucune nouvelle évaluation ne peut être engagée.

Les évaluations en cours peuvent être soit menées à leur terme par le centre d'évaluation, en accord avec le centre de certification, soit arrêtées.

Le centre d'évaluation doit remettre à l'ANSSI l'ensemble des dossiers relatifs aux évaluations menées.

L'ANSSI peut prévenir les commanditaires, développeurs et autres acteurs concernés par les évaluations en cours.

4. Cas des CESTI agréés pour les évaluations « Critères Communs » ou « ITSEC »

Un Centre d'évaluation de la sécurité des technologies de l'information (CESTI) agréé pour les évaluations « Critères Communs » ou « ITSEC » au titre du décret 2002-535 peut prétendre être reconnu apte à réaliser des évaluations en vue d'une certification de sécurité de premier niveau.

Cette aptitude ne vaut que pour les types de produits pour lesquels il est déjà agréé, ainsi que pour les éventuelles compétences cryptographiques pour lesquelles il est reconnu. Dans ce cas, le CESTI envoie un courrier à l'ANSSI demandant son agrément au titre de cette procédure en indiquant les types de produits pour lesquels l'agrément est demandé. Il est alors dispensé d'audit préliminaire, d'évaluation pilote et d'audit d'agrément. L'audit de renouvellement d'agrément est réalisé conjointement avec l'audit pour les évaluations « Critères Communs » ou « ITSEC ».

Pour les types de produits hors de son domaine d'agrément « Critères Communs » ou « ITSEC », la procédure d'agrément est celle décrite au § 3.

Annexe A : Critères d'agrément

Indépendance et impartialité des évaluations

- C1 Le centre d'évaluation doit apporter les éléments de preuve et les engagements permettant de garantir que les évaluations qu'il réalise ou réalisera sont ou seront faites :
- de façon impartiale : le centre d'évaluation ne peut subir de pressions visant à modifier les résultats des travaux d'évaluation ;
 - de façon indépendante : le centre d'évaluation n'accepte pas d'évaluation qui le mettrait en conflit d'intérêt avec le développeur, le distributeur ou l'importateur du produit.

Confidentialité des évaluations

- C2 Le centre d'évaluation doit avoir mis en place des dispositions permettant d'assurer la confidentialité des évaluations et de leurs résultats. En particulier, il ne doit pas faire état des développeurs et commanditaires avec lesquels il est ou a été en lien (avant-projet, projet, ...) dans le cadre de cette activité d'évaluation, ni des produits dont il a connaissance et qui ont pu faire l'objet d'une demande d'évaluation ou d'une évaluation. Cette exigence ne porte que sur les informations qui ne sont pas du domaine public.

Prescriptions relatives au personnel

- C3 Les personnes autorisées à signer les rapports d'évaluation doivent avoir été nommément indiquées au centre de certification. L'ANSSI se réserve le droit de refuser qu'un membre indiqué par le centre d'évaluation soit signataire des rapports d'évaluation.
- C4 Le personnel du centre d'évaluation doit être compétent en technologies de l'information, ainsi que qualifié et expérimenté en évaluation de la sécurité. Notamment, la compétence du personnel du centre d'évaluation doit être en adéquation avec la portée de son agrément (connaissances techniques et expérience nécessaires pour exercer les activités correspondantes). Le jugement relatif à ces conditions est du ressort du centre de certification.
- C5 Le personnel qui réalise les évaluations doit être indiqué au centre de certification. Ses compétences doivent être suivies (au minimum, projets d'évaluations auxquelles les personnes ont participé, tâches réalisées, dates). L'ANSSI se réserve le droit de refuser qu'un membre indiqué par le centre d'évaluation participe aux évaluations réalisées dans le cadre de cet agrément.

Prescriptions relatives aux contrats

- C6 Les aspects commerciaux doivent être réglés par contrat entre le centre d'évaluation, le commanditaire et, dans certains cas, le ou les développeurs.
- C7 Tout contrat d'évaluation doit préciser que le centre de certification est destinataire de l'ensemble des informations du processus d'évaluation.

Compétences techniques

- C8 A la demande du centre de certification, le centre d'évaluation doit être en mesure de démontrer les compétences qui correspondent à sa portée d'agrément. Cette démonstration se fait dans un délai fixé par le centre de certification.

Méthodes et procédures de travail

- C9 Les rapports d'évaluation doivent faire l'objet d'un processus de validation interne avant leur envoi, afin de limiter les biais et les conséquences d'erreurs.
- C10 Les rapports transmis aux commanditaires et au centre de certification doivent être signés par l'autorité identifiée auprès du centre de certification pour l'agrément (voir critère C3).

Annexe B : Portée d'agrément

B.1 Définition de la portée d'agrément

La portée d'agrément est définie en termes de type de produits.

L'ANSSI peut accorder des dérogations pour des tâches exceptionnelles non couvertes par la portée d'agrément.

B.2 Types de produits

Les types de produits retenus pour la certification de sécurité de premier niveau sont les suivants :

- 1 - détection d'intrusions¹ ;
- 2 - anti-virus, protection contre les codes malveillants² ;
- 3 - pare-feu ;
- 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 - environnement d'exécution sécurisé ;
- 11 - terminal de réception numérique (*Set top box*, STB) ;
- 12 - matériel et logiciel embarqué ;
- 13 - automate programmable industriel.

Au sein de chacune de ces catégories, des restrictions peuvent être émises par l'ANSSI sur les types de produits que le centre d'évaluation peut évaluer.

B.3 Affichage de la portée

Le site internet de l'ANSSI mentionne, pour chaque centre d'évaluation agréé, les types de produits sur lesquels porte l'agrément.

¹ À ce stade, l'objectif principal de l'évaluation de ces produits est d'analyser leur innocuité sur le réseau ou le système hôte.

² Idem.

Annexe C : Obligations résultant de l'agrément

Le centre d'évaluation s'engage à respecter les procédures définies par le centre de certification de l'ANSSI et qui lui sont transmises pour application. Il s'engage à respecter les critères d'agrément, et en particulier :

- O1 à refuser toute évaluation qui le mettrait dans une situation de conflit d'intérêt avec un fournisseur au regard de son activité d'évaluation ou à en avertir au plus tôt le centre de certification dans le cas où cette situation se produirait au cours d'une évaluation ;
- O2 à n'accepter la sous-traitance de tout ou partie d'une évaluation qu'après accord formel de l'ANSSI ;
- O3 à ne pas faire participer à une évaluation toute personne ayant participé à la réalisation du produit évalué (conseil, conception, réalisation...) ;
- O4 à rendre compte immédiatement au centre de certification de tout changement de la structure de sa société, de son organisation ou de son personnel, et à fournir les pièces justificatives de ces modifications ;
- O5 à autoriser l'accès du centre de certification à ses locaux et à l'ensemble des documents, matériels ou outils utilisés dans le cadre des évaluations couvertes par la portée d'agrément ;
- O6 à autoriser les membres de l'ANSSI désignés par le centre de certification à contrôler à tout moment le déroulement d'une évaluation, à assister à des travaux d'évaluation et à contrôler que les critères d'agrément sont respectés ;
- O7 à se conformer aux obligations de protection de l'information qui lui seraient imposées de manière permanente ou temporaire par l'ANSSI ;
- O8 à participer aux réunions organisées par le centre de certification de l'ANSSI.