PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 26 novembre 2020

N° **2673/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-CER-P-01_v4.0**

PROCEDURE

CERTIFICATION CRITERES COMMUNS DE LA SECURITE OFFERTE PAR LES PRODUITS, LES SYSTEMES DES TECHNOLOGIES DE L'INFORMATION, LES SITES OU LES PROFILS DE PROTECTION

Application : A compter de novembre 2020.

Diffusion : Publique.

Le sous-directeur « Expertise » de l'Agence nationale de la sécurité des systèmes d'information

Renaud LABELLE
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1	27/10/2003	Création
2	08/03/2016	Refonte générale du document Prise en compte de la norme EN ISO/IEC 17065
3.0	29/06/2017	Prise en compte de la note 4 Ajout des documents de référence Suppression dans le texte (§5.4) de la référence à l'instruction interne CRY-I-01 Analyse des mécanismes cryptographiques Suppression des références des instructions « internes ANSSI » Prise en compte du formulaire de satisfaction client Fusion des documents ANSSI-CC-CPP-P-01, ANSSI-CC-SITE-P-01 et ANSSI-CC-CER-P-01 dans ANSSI-CC-CER-P-01 pour en faciliter leur mise à jour Ajout de la possibilité de faire appel d'une décision
3.1	10/01/2019	Mise en conformité avec la norme EN ISO/IEC 17065
3.2	16/9/2019	Précision sur les éventuels travaux complémentaires demandés suite aux RTE Ajout de durée de conservation Précision sur la version du formulaire de demande [CER-F-01] à utiliser obligatoirement.
3.3	13/1/2020	Mise en cohérence du §9.2.1 avec le §7.8 du MQ Reformulation du paragraphe « suspension, retrait du certificat » pour être cohérent avec la norme
4.0	26/11/2020	Prise en compte de la date de validité des certificats suite aux publications du SOG-IS Précision apportée sur les avis soumis au comité directeur de la certification Précisions apportées concernant l'enregistrement et l'archivage des documents Précisions apportées sur les règles de communication et d'usage de la marque et des logotypes Prise en compte de la nouvelle charte graphique

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

Cette procédure est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évaluations mineures ne sont pas soumises au comité directeur de la certification.

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 procédure

Ce document décrit l'ensemble du processus de certification Critères Communs (CC) depuis la demande officielle par un commanditaire jusqu'à l'attribution du certificat pour l'objet évalué. L'objet désigne un produit, un système, un site ou un profil de protection. Le processus décrit dans ce document est applicable à la fois pour une certification initiale (nouvel objet) et pour une réévaluation (nouvelle version d'un objet précédemment certifié).

2 Contexte

Le décret 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 (voir [DECRET]).

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 objet répond aux exigences de sécurité listées dans sa cible de sécurité.

Le centre de certification s'appuie sur cette même organisation pour certifier :

- la conformité des profils de protection aux exigences de la classe APE définie dans les Critères Communs [CC] ;
- la conformité des sites aux exigences des classes ASE et ALC définies dans les Critères Communs [CC] et [SITE CER].

Les certificats correspondants sont également émis au titre du décret 2002-535 modifié.

3 Demande de certification

3.1 La demande de certification

Le commanditaire de la certification transmet à l'ANSSI une demande officielle de certification par le biais du formulaire [CER-F-01]. Il transmet également des documents annexes en fonction des éléments renseignés dans le formulaire. L'ensemble des documents constitue le dossier d'évaluation. La version du formulaire à utiliser par le demandeur est obligatoirement celle publiée sur le site de l'ANSSI, faute de quoi la demande est systématiquement refusée.

Comme l'indique l'art. 2 du [DECRET], le dossier contient notamment :

- la description de l'objet à évaluer incluant la cible de sécurité ou, le cas échéant, le profil de protection ;
- 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.

Le dossier d'évaluation est signé par le commanditaire et le centre d'évaluation en charge de l'évaluation.

3.2 Traitement de la demande

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

Si le centre de certification estime au moment où commence l'évaluation que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonnes pratiques applicables ou que les travaux d'évaluation ne sont pas en adéquation avec les objectifs, il notifie au commanditaire qu'il ne pourra pas en l'état du dossier procéder à la certification envisagée (voir l'art. 2. du [DECRET]).

Si le dossier est satisfaisant, une lettre d'enregistrement est envoyée au commanditaire et au centre d'évaluation. Cette lettre identifie notamment le nom du certificateur en charge de suivre l'évaluation. Le certificateur est déterminé en fonction de ses compétences reconnues dans le domaine concerné, de son impartialité et de sa charge de travail.

Remarque : pour de multiples raisons (départ du centre, longue maladie, gestion des ressources du centre, etc.), le certificateur nommé pourra être remplacé par un autre certificateur disposant des mêmes compétences. Dans ce cas, le commanditaire et le centre d'évaluation sont avisés de ce changement par courriel.

4 Evaluation de la sécurité

4.1 Démarrage de l'évaluation

Lorsque la demande est enregistrée, le certificateur en charge du projet convoque tous les membres du comité de pilotage de l'évaluation identifiés dans le dossier de certification pour une réunion de démarrage de l'évaluation. Le certificateur mène la réunion conformément à un ordre du jour fixé au préalable.

Cette réunion a notamment pour objectifs de :

- fixer les jalons de projet ;
- s'assurer de la disponibilité des moyens matériels et en personnel du centre d'évaluation pour respecter le planning de l'évaluation ;
- échanger avec le client et le centre d'évaluation sur le déroulé du projet afin de s'assurer que les parties en présence n'ont aucune divergence d'interprétation.

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

Remarque 1 : dans le cas d'une certification d'un profil de protection, la réunion de démarrage n'est organisée que si le centre de certification l'estime nécessaire.

Remarque 2 : exceptionnellement (par exemple, dans le cas d'une énième réévaluation d'un produit) le certificateur peut être amené à ne pas organiser de réunion de démarrage, avec l'accord de tous les membres du comité de pilotage[1]. Il appartient alors au certificateur de se faire communiquer le planning et la liste des évaluateurs.

4.2 Livraison des fournitures

Le commanditaire de l'évaluation est responsable de la livraison des fournitures nécessaires à l'évaluation, notamment le rapport de réutilisation des résultats d'une évaluation générique (voir [NOTE.17]) et l'*ETR-lite for composition* (voir [COMP]). La liste des fournitures à livrer est précisée dans le programme de travail prévisionnel du dossier d'évaluation. Le mode de livraison au certificateur doit être conforme à l'instruction [CER-I-04] et aux prescriptions de [SECU-P-01]. Toutes les fournitures sont, par défaut, envoyées au centre d'évaluation et au certificateur en charge du projet.

Si le commanditaire n'est pas le concepteur du produit ou du système, les fournitures peuvent être livrées directement par son propriétaire (par exemple un développeur ou un sous-traitant) afin de respecter la confidentialité du savoir-faire.

Les fournitures utilisées pour l'évaluation doivent être gérées par le centre d'évaluation conformément aux exigences de la norme [17025].

4.3 Réalisation des travaux d'évaluation

Le centre d'évaluation mène les travaux d'évaluation formulés par [CEM] et par les notes d'interprétations nationales ou internationales conformément aux critères d'évaluation et au niveau d'assurance sélectionnés dans la demande de certification. Ces travaux doivent également respecter les dispositions du système qualité [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, appelé également Rapport Technique Intermédiaire (RTI) ;

[1] Son rôle est d'assurer le bon déroulé des opérations en fonction des objectifs fixés en réunion de démarrage.

- ou directement dans le rapport final appelé Rapport Technique d'Evaluation (RTE).

Tous ces rapports émis par le centre d'évaluation, qu'ils soient intermédiaires ou finaux, sont envoyés simultanément au certificateur et au commanditaire. Le centre de certification en accuse réception et les intègre dans le répertoire du projet considéré.

Lorsque le verdict d'un rapport est à « FAIL », le centre de certification invite le centre d'évaluation à se rapprocher du commanditaire pour que soient corrigés les points bloquants afin que les travaux d'évaluation puissent aboutir à un verdict « PASS ». Cependant, le commanditaire conserve la possibilité à tout moment, de mettre un terme à l'évaluation en cours. Quoi qu'il en soit, le centre de certification doit être tenu informé de l'évolution du dossier.

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 ou du système en évaluation. Ils sont identifiés dans [NOTE.02].

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 sur site conformément aux prescriptions de [NOTE.02].

Cas de l'analyse des mécanismes cryptographiques :

Lorsque les fonctions de sécurité de la TOE mettent en œuvre des mécanismes cryptographiques, l'efficacité de ces mécanismes doit être analysée conformément à la procédure [CRY-P-01]. Les résultats de cette analyse sont pris en compte dans le cadre de l'analyse de vulnérabilités menée par le centre d'évaluation.

4.4 Validation du rapport d'évaluation

Dans le cas d'un rapport de certification avec un verdict « PASS », le certificateur analyse le rapport d'évaluation final et s'assure qu'il dispose bien de tous les documents référencés. Le certificateur peut être amené à demander au centre d'évaluation, au développeur ou au commanditaire, d'avoir accès à tout autre élément qu'il juge nécessaire. Le certificateur peut également demander un avis technique aux experts de l'ANSSI ; cependant, le certificateur reste maître de la décision finale.

Les conclusions de l'analyse du rapport d'évaluation sont consignées dans une fiche de revue du rapport qui est envoyée au centre d'évaluation. Ce dernier peut avoir à réémettre une nouvelle version du rapport ou à réaliser des travaux complémentaires, voire effectuer à nouveau certaines tâches si des anomalies ont été détectées par le certificateur. Les travaux complémentaires ainsi demandés doivent respecter les mêmes exigences que celles appliquées durant l'évaluation.

Il est également possible, suite à un nombre important de remarques, que le certificateur demande une réémission du rapport.

4.5 Fin de l'évaluation

Lorsqu'un RTE est reçu par le certificateur, une réunion de fin d'évaluation peut être organisée à la demande de l'un des membres du comité de pilotage.

Les modalités de la réunion ainsi que l'ordre du jour sont fixés par le comité de pilotage de l'évaluation.

5 Décision de certification initiale

A compter de la validation du RTE (verdict « PASS » uniquement) par le certificateur en charge du suivi de l'évaluation, la procédure de décision de certification est engagée. Le certificateur constitue un dossier qui comprend notamment :

- le projet de rapport de certification ;
- le projet de certificat.

Le projet de rapport de certification est adressé au commanditaire afin qu'il puisse faire ses commentaires qui peuvent être repris ou non par le certificateur.

Ce dossier est validé par le chef du centre de certification ou son adjoint avant sa transmission pour signature. Le directeur général de l'Agence nationale de la sécurité des systèmes d'information signe les deux rapports de certification et les deux certificats.

Une fois signés,

- un exemplaire du certificat et un rapport de certification sont envoyés au(x) commanditaire(s) mentionné(s) dans la demande de certification auxquels est joint un formulaire de satisfaction client [QUA-F-03] ;
- les autres exemplaires de rapport de certification et de certificat sont conservés (voir paragraphe « durée de conservation ») par le centre de certification.

La délivrance de ces documents impose au commanditaire de respecter certaines obligations notamment de signifier, sans délai à l'ANSSI (CERT-FR), copie le centre de certification, toute vulnérabilité découverte avec son analyse d'impact associée afin de permettre leur instruction.

6 Durée de validité

La certification d'un produit est délivrée pour une durée de validité de cinq ans (voir [CER_VALID]). Cette durée de validité peut être étendue si le commanditaire procède à la surveillance de son produit initialement certifié (voir [SUR-P-01]).

Pour un site, la validité des documents de certification est fixée par [NOTE.02].

Pour un profil de protection, aucune limite de validité n'est fixée.

A l'issue de la période de validité, le certificat est retiré et archivé.

7 Publication du certificat

Le commanditaire peut demander, au travers du formulaire [CER-F-01] :

- que le certificat et le rapport de certification restent confidentiels ;
- que le rapport de certification et la cible de sécurité publique soient publiés :
  - sur le site Internet de l'ANSSI : www.ssi.gouv.fr ;
  - et sur le site d'un accord de reconnaissance (par exemple, le site du CCRA[2]) si les exigences relatives à cet accord ont été satisfaites durant l'évaluation.

Les différentes possibilités offertes en matière de publication sont listées dans la note [NOTE-04].

A noter que la décision initiale de publication, prise lors du dépôt de la demande d'évaluation, peut être modifiée sur demande par courriel du commanditaire (certification@ssi.gouv.fr).

Passée la période de validité (voir chapitre 0), les documents publiés seront alors déplacés dans la liste de certificats archivés.

[2] Common Criteria Recognition Arrangement, www.commoncriteriaportal.org

8 Publicité

Le commanditaire peut faire état de la certification au travers de documents, brochures ou publicité, sauf dispositions spécifiques précisées par l'ANSSI lors de l'enregistrement de la demande d'évaluation.

8.1 Règles de communication

Les commanditaires ont le devoir d'informer dans des termes honnêtes et compréhensibles les utilisateurs de produits, sites ou profils de protection certifiés. Ils doivent impérativement indiquer :

- la référence du certificat ;
- la date de certification de l'objet ;
- les références et la version de l'objet certifié ;
- si l'objet entre dans le champ d'une procédure de surveillance ;
- la date de fin de validité le cas échéant.

Ils doivent également :

- délivrer des copies conformes aux originaux des rapports de certification et des cibles de sécurité si un donneur d'ordre en fait la demande ;
- ne pas faire d'annonce trompeuse sur le produit.

8.2 Règles d'utilisation de la marque et des logotypes

La marque « TI SECURITE CERTIFICATION » ainsi que les logotypes des accords CCRA et SOG-IS peuvent être utilisés pour faire valoir l'obtention d'un certificat, leurs descriptions et leurs modalités d'usage sont décrites par les procédures [MAR-P-01] et [MAR-P-02].

9 Suspension et retrait

9.1 Suspension de la certification

Le centre de certification de l'ANSSI peut être amené à suspendre la certification d'un produit ou d'un site si, par exemple :

- un fait nouveau lui permet de démontrer que des informations transmises par le commanditaire ou le développeur au cours de l'évaluation n'étaient pas exactes et qu'elles ont pu fausser le jugement des évaluateurs et donc le résultat final ;
- une vulnérabilité est découverte sur un produit certifié.

Le centre de certification informe sans délai le commanditaire et éventuellement communique les actions possibles qui permettraient de rétablir la certification.

Le commanditaire dispose alors d'un mois au maximum pour identifier les actions qu'il compte prendre pour rétablir la situation.

A l'issue de ce mois, plusieurs cas sont à envisager :

- si le centre de certification considère que les actions proposées ne répondent pas à la problématique ou si le commanditaire prend la décision de ne pas rétablir la situation, les documents publiés sont alors archivés ;
- si le centre de certification estime que le plan d'actions fourni par le commanditaire est adapté, le commanditaire dispose alors de trois mois au maximum pour mettre en œuvre son plan d'actions et fournir la preuve (par exemple en fournissant les résultats d'une surveillance ou d'une réévaluation) au centre de certification que les actions entreprises, conformément au programme de certification, ont bien permis de résoudre définitivement la situation.

Deux cas sont alors possibles :

- soit après examen des preuves, le centre de certification estime les résultats adaptés, la suspension est levée ;
- soit les preuves ne répondent pas à la problématique, le certificat est alors retiré.

Le centre de certification dispose d'un mois pour statuer sur ces deux cas possibles.

9.2 Retrait de la certification

Le centre de certification est amené à retirer une certification si, par exemple :

- un produit n'est pas surveillé dans la période de cinq ans qui suit la certification initiale ou qui suit la dernière surveillance (voir les conditions dans [SUR-P-01]) ;
- la période d'un mois, pour permettre au commanditaire de présenter les actions qu'il compte prendre suite à une suspension, est dépassée ;
- le plan d'actions, proposé par le commanditaire pour remédier à la suspension, est inadapté ;
- la période de trois mois pour la mise en œuvre du plan d'actions est dépassée.

Le centre de certification de l'ANSSI peut également retirer une certification si, par exemple :

- l'utilisation ou l'affichage du rapport de certification ou du certificat est effectuée de manière frauduleuse, erronée ou abusive ;
- l'utilisation ou l'affichage de la marque « Ti SECURITE CERTIFICATION » et des logos CCRA et SOGIS est frauduleuse, erronée ou abusive ;
- les engagements de certification ne sont pas respectés scrupuleusement.

Dès que le centre de certification a connaissance de l'un de ces motifs, il en informe par courrier électronique et sans délai le commanditaire et, éventuellement, communique les actions possibles qui permettraient de maintenir la certification. Le commanditaire dispose alors de quatre semaines au maximum pour rétablir la situation, sinon la certification est retirée.

L'ANSSI communique sur le retrait par tout moyen qu'elle juge approprié afin que les utilisateurs du produit certifié soient informés, notamment au travers :

- de l'archivage des documents publiés sur le site de l'ANSSI ;
- du retrait des documents de certification publiés sur le site du CCRA, le cas échéant.

9.3 Information du commanditaire

Une fois validée par le chef de centre ou son adjoint, la décision de suspension ou de retrait est adressée au commanditaire par courrier du directeur général de l'ANSSI dès lors que le motif de retrait n'est pas lié à la fin de période de validité du certificat ou à une décision du commanditaire (voir [SUR-P-01]). Dans ces deux derniers cas, les conditions de retrait étant décrites dans la présente procédure de certification et la procédure de surveillance [SUR-P-01], elles ne sont donc pas rappelées au commanditaire avant exécution du retrait.

Quel qu'en soit le motif, le commanditaire doit impérativement et immédiatement cesser d'utiliser l'ensemble des moyens de communication qui fait référence au certificat dès lors que celui-ci est suspendu ou retiré.

10 Appel de la décision

Le commanditaire peut faire appel de toute décision du centre de certification afin que la décision soit reconsidérée (voir [ANO-P-01]).

ANNEXE A. Références

Référence	Document
[DECRET]	Décret 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.
[CC]	*Common Criteria for Information Technology Security Evaluation.*
[CEM]	*Common Methodology for Information Technology Security Evaluation.*
[17065]	Norme EN ISO/IEC 17065 : Exigences pour les organismes certifiant les produits, les procédés et les services, version en vigueur.
[17025]	Norme EN ISO/IEC 17025 : Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais, version en vigueur.
[SITE CER]	*Site Certification, Supporting Document*, référence CCDB-2007-11-001.
[NOTE.02]	Visite de l'environnement de développement, référence ANSSI-CC- NOTE/02, version en vigueur.
[NOTE.17]	Réutilisation des composants d'assurance ALC_v1.0, référence ANSSI-CC-NOTE-17, version en vigueur.
[NOTE.20]	Règles relatives à la mise en œuvre des évaluations sécuritaires, référence ANSSI-CC-NOTE/20, version en vigueur.
[COMP]	Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices.
[CER_VALID]	SOG-IS Recognition Agreement Management Committee - Certificate validity, version 1.0.
[CER-F-01]	Dossier d'évaluation, référence ANSSI-CC-CER-F-01, version en vigueur.
[CER-I-04]	Livraison des fournitures à l'ANSSI, référence ANSSI-CC-CER-I-04, version en vigueur.
[SECU-P-01]	Gestion de la confidentialité au centre de certification, référence ANSSI-CC-SECU-P-01, version en vigueur.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques, référence ANSSI-CC-CRY-P-01, version en vigueur.
[QUA-F-03]	Formulaire Satisfaction Client, référence ANSSI-CC-QUA-F-03, version en vigueur.
[NOTE-04]	Publication et reconnaissance internationale des certificats, référence ANSSI-CC-NOTE-04, version en vigueur.
[ANO-P-01]	Traitement des anomalies, référence ANSSI-CC-ANO-P-01, version en vigueur.
[MAR-P-01]	Utilisation de la marque « TI Securite Certification », référence ANSSI-CC-MAR-P-01, version en vigueur.
[MAR-P-02]	Utilisation des logotypes du CCRA et SOGIS, référence ANSSI-CC-MAR-P-02, version en vigueur.

[SUR-P-01]	Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01, version ne vigueur.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.ssi.gouv.fr).