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 09 Janvier 2025

N° **2164 /ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-SITE-P-01_v1.0**

PROCEDURE

CERTIFICATION CRITERES COMMUNS DE LA SECURITE OFFERTE PAR LES SITES

Application : A compter de sa publication.

Diffusion : Publique.

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

Renaud LABELLE

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1.0	09 Janvier 2025	Création de la procédure dédiée à la certification de sites (issue de ANSSI-CC-CER-P-01)

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.cyber.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 site.

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 applicable à ce processus de certification (voir [DECRET]) qui régit à la fois le schéma national et la mise en œuvre au niveau national du schéma européen de certification de cybersécurité fondé sur les critères communs (voir [EUCC]).

Ce décret 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 sites aux exigences des classes AST 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;
- 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[1] 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.

[1] Son rôle est d'assurer le bon déroulé du projet d'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 en format dématérialisé 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 demande au comité de pilotage identifié dans le dossier d'évaluation si une réunion de démarrage est nécessaire.

Le cas échéant, le certificateur mène la réunion conformément à un ordre du jour fixé au préalable. La réunion est actée dans un compte rendu rédigé par le certificateur, qui est envoyé au comité de pilotage.

Qu'il y ait une réunion de démarrage ou non, le certificateur doit acter les points ci-après :

- les éventuelles évolutions du projet depuis le dépôt de la demande ;
- la disponibilité des moyens matériel et personnel du centre d'évaluation.

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]). 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 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 propriétaire du site, les fournitures peuvent être livrées directement par son propriétaire 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 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 peuvent être initiées par chacune des parties du comité de pilotage.

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].

4.4 Validation du rapport d'évaluation

Dans le cas d'un rapport d'évaluation final avec un verdict « *PASS* », le certificateur l'analyse et s'assure qu'il dispose bien de tous les documents référencés. Le certificateur peut 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 de validation finale.

Les conclusions de l'analyse du rapport d'évaluation sont consignées dans une fiche de revue de 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 sont notifiées. 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 de l'évaluation.

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

5 Délivrance de la 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 délivrance 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 peut être 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 par le chef de pôle certification avant sa transmission pour signature. Le directeur général de l'Agence nationale de la sécurité des systèmes d'information signe le rapport de certification et le certificat, chacun en double exemplaire.

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 (rapport de certification et certificat) sont conservés 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), et au 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 site est délivrée pour une durée de validité fixée par [NOTE.02].

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

Si le certificat n'est pas public, sa validité peut être demandée par messagerie électronique au commanditaire de l'évaluation en mettant en copie le centre de certification. Ce dernier pourra alors confirmer ou infirmer la réponse qui sera fournie.

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 certificat, le rapport de certification et la cible de sécurité publique soient publiés :
    - sur le site Internet de l'ANSSI : www.cyber.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 6), les documents publiés seront alors déplacés dans la liste de certificats archivés.

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 sites. Ils doivent impérativement indiquer :

- la référence du certificat ;
- la date de certification de l'objet ;
- les références du site certifié ;
- 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 en lien avec le site certifié.

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 Suivi post-certification (non-conformité, réexamen, suspension et retrait)

9.1 Constat d'une non-conformité

Suite au non-respect par le titulaire d'un certificat de ses obligations, le centre de certification informe le titulaire du certificat de la non-conformité constatée et lui demande de prendre des mesures correctives dans un délai de trente jours calendaires. Si les mesures correctives ne sont pas prises dans le délai imparti, le certificat correspondant peut être suspendu ou retiré.

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

9.2 Réexamen d'un certificat

Le centre de certification de l'ANSSI peut décider de réexaminer la certification d'un site :

- à la demande du titulaire du certificat ;
- afin d'examiner la pertinence de mesures correctives suite au constat d'une non-conformité ;
- ou pour d'autres raisons justifiées, par exemple : un fait nouveau lui permet de suspecter 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.

Le réexamen peut nécessiter la réévaluation par un CESTI.

Suite à ce réexamen, il peut être procédé, le cas échéant :

- à la suspension du certificat ;
- à son retrait et, le cas échéant, à l'émission d'un nouveau certificat ;
- à la modification du certificat.

9.3 Suspension et retrait de la certification

Suspension : Suite au constat d'une non-conformité, le centre de certification peut suspendre un certificat pendant une période qui ne dépasse pas quarante-deux jours calendaires. Le centre de certification indique au titulaire du certificat la raison de la suspension, les mesures demandées et la durée de la suspension, la suspension n'affecte pas la validité du certificat.

Retrait : Suite au constat d'une non-conformité, au réexamen d'un site ou à l'issue d'une suspension, le centre de certification peut retirer un certificat. Il en notifie le titulaire avec les raisons invoquées. Le centre de certification communique sur le retrait, notamment au travers de l'archivage des documents publiés sur le site de l'ANSSI.

Dans les cas de suspension ou de retrait, les clients sont notifiés par le commanditaire et MCS est notifié par le centre de certification. L'ENISA est notifiée par MCS.

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.*
[ISO] <Vérifier la révision utilisée>	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003. Ou - *Part 1 : Introduction and general model*, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ; - *Part 2 : Security functional components*, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ; - *Part 3 : Security assurance components*, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003. Ou - *Part 1 : Introduction and general model*, novembre 2022, version CC:2022, révision 1, référence CCMB-2022-11-001 ; - *Part 2 : Security functional components*, novembre 2022, version CC:2022, révision 1, référence CCMB-2022-11-002; - *Part 3 : Security assurance components*, novembre 2022, version CC:2022, révision 1, référence CCMB-2022-11-003 ; - *Part 4 : Framework for the specification of evaluation methods and activities*, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-004; *Part 5 : Pre-defined packages of security requirements*, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-005.
[CEM]	- *Part 1 : Introduction and general model*, août 2022, référence ISO/IEC 15408-1; - *Part 2 : Security functional components*, août 2022, référence ISO/IEC 15408-2 ; - *Part 3 : Security assurance components*, août 2022, référence ISO/IEC 15408-3; - Part 4 : Framework for the specification of evaluation methods and activities, août 2022, référence ISO/IEC 15408-4; *Part 5 : Pre-defined packages of security requirements*, août 2022, référence ISO/IEC 15408-5.
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482)

[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.
[COMP]	*Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices*, version en vigueur.
[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.
[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.

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