



**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 24 Février 2026

N° 2418 /ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-CER-P-01_v5.5

PROCEDURE

CERTIFICATION DE CYBERSECURITE FONDÉ SUR LES CRITERES COMMUNS POUR LES PRODUITS ET LES PROFILS DE PROTECTION

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]



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
5.0	03/03/2022	Clarification des objectifs de la réunion de démarrage Description du processus d'obtention de la validité des certificats non publics

5.1	18/10/2024	Mise en conformité EUCC
5.2	17/12/2024	Ajout de la surveillance des marques et la surveillance des produits Précisions apportées au chapitre 9 sur les cas liés au suivi post-certification (activités de contrôle, non-conformité, réexamen, suspension et retrait) Possibilité d'archiver le certificat précédent en cas de réévaluation (§5)
5.3	13/02/2025	Précisions apportées sur les procédures post-certification notamment de continuité de l'assurance Signature électronique des certificats et rapports de certification
5.4	27/03/2025	Clarification du rôle du certificateur concernant les déplacements sur site
5.5	24/02/2026	Clarifications sur le suivi des certificats et liaison avec [VUL-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	5
2	Contexte	5
3	Demande de certification	5
3.1	La demande de certification	5
3.2	Traitement de la demande	6
4	Evaluation de la sécurité	6
4.1	Démarrage de l'évaluation	6
4.2	Livraison des fournitures	6
4.3	Réalisation des travaux d'évaluation	7
4.4	Validation du rapport d'évaluation	8
4.5	Fin de l'évaluation	8
5	Délivrance de la certification	8
6	Durée de validité	9
7	Publication du certificat	9
8	Publicité	10
8.1	Règles de communication	10
8.2	Règles d'utilisation de la marque et des logotypes	10
9	Suivi post-certification (activités de contrôle, non-conformité, réexamen, suspension et retrait)	10
9.1	Activités de contrôle	10
9.2	Constat d'une non-conformité	11
9.3	Réexamen d'un certificat	11
9.4	Suspension et retrait d'un certificat	11
10	Appel de la décision	12
ANNEXE A.	Références	13

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 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).

Ce document décrit la certification dans le cadre du schéma national et dans le cadre du schéma européen de certification de cybersécurité fondé sur les critères communs (voir [EUCC]).

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 profils de protection aux exigences de la classe APE définie dans les Critères Communs [CC]. 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'article 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 pilotage¹ 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.

¹ Son rôle est d'assurer le bon déroulé du projet d'évaluation.

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'article 2 du [DECRET]).

Si le dossier est satisfaisant, une lettre d'enregistrement est envoyée en version électronique ou en version papier 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]) et l'« *ETR for composite evaluation* » (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 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], par la documentation de référence de [EUCC] et par les notes d'interprétations 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) ;
- 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 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] en tant qu'observateur.

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.

Cas des réévaluations :

Pour une réévaluation le commanditaire doit réaliser (ou faire réaliser par le développeur du produit) une analyse de l'impact des évolutions. Les conclusions de cette analyse doivent être présentées dans un rapport, dit « rapport d'analyse d'impact » (IAR), dont le contenu est indiqué au paragraphe 5 de la procédure citée en référence [JIL-AC].

Il existe deux types de réévaluation :

- une réévaluation suite à une évolution des éléments certifiés ne pouvant être considérée comme mineure (voir [ANSSI-CC-MAI-P-01]). L'évaluation est effectuée en réutilisant tous les résultats de l'évaluation précédente qui s'appliquent encore. Un nouveau rapport technique d'évaluation est alors émis.
- une réévaluation d'un produit certifié inchangé, appelée « *re-assessment* », qui permet d'évaluer l'incidence des changements dans l'environnement des menaces. Dans ce cas, la réévaluation est effectuée par le CESTI qui a réalisé l'évaluation précédente, en réutilisant tous les résultats qui s'appliquent encore. L'évaluation se concentre sur les activités d'assurance qui sont potentiellement affectées par la modification de l'environnement de menaces lié au produit certifié, en particulier la famille AVA_VAN concernée et, en outre, la famille du cycle de vie de l'assurance (ALC). Le rapport technique d'évaluation est alors mis à jour.

Une demande de renouvellement est traitée comme un « *re-assessment* ».

Cas de l'évaluation des correctifs :

Dans l'attente de la mise en œuvre de l'annexe IV.4 de [EUCC], l'évaluation des correctifs est effectuée dans le cadre d'une réévaluation telle que décrite précédemment.

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

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.

Suite à la décision de certification sur la base de ce projet, ce dossier est transmis pour signature. Le directeur général de l'Agence nationale de la sécurité des systèmes d'information signe alors électroniquement² le rapport de certification et le certificat :

- le certificat et le rapport de certification signés sont envoyés au(x) commanditaire(s) mentionné(s) dans la demande de certification auxquels est joint un formulaire de satisfaction client [QUA-F-03] ;
- dans le cadre [EUCC], le certificat et le rapport de certification signés sont envoyés à MCS (Mission contrôles et supervision). MCS envoie à l'ENISA (Agence de l'Union européenne pour la cybersécurité) un exemplaire du certificat et du rapport de certification ;

Le certificat et son rapport de certification signés 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.

Dans le cadre d'une réévaluation (non certification initiale), le précédent certificat peut être archivé.

6 Durée de validité

La certification d'un produit est délivrée pour une durée de validité de cinq ans (voir [CER_VALID] pour SOG-IS et, sauf exceptions validées par MCS, pour [EUCC]).

Pour un profil de protection, la durée de validité est de vingt ans.

A l'issue de la période de validité, le certificat est 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, sous certaines conditions, demander au travers du formulaire [CER-F-01] que le certificat et le rapport de certification restent confidentiels. Par défaut, le certificat, le rapport de certification et la cible de sécurité publique seront publiés :

- sur le site Internet de l'ANSSI : www.cyber.gouv.fr et le cas échéant, sur le site www.ncca.cyber.gouv.fr et le site de l'ENISA ;
- le cas échéant, sur le site d'un accord de reconnaissance (par exemple, le site du CCRA³) 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).

² Sauf si les documents sont classifiés ou marqués Diffusion Restreinte

³ Common Criteria Recognition Arrangement, www.commoncriteriaportal.org.

Passé 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 directement sur le produit ou 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 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 ;
- 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

Les marques « TI SECURITE CERTIFICATION » et « EUCC » 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 (activités de contrôle, non-conformité, réexamen, suspension et retrait)

9.1 Activités de contrôle

Pour [EUCC], le centre de certification contrôle :

- le respect, par les titulaires d'un certificat, de leurs obligations au titre de [EUCC] et du [CSA] à l'égard du certificat EUCC qui a été délivré par l'organisme de certification ;
- la conformité des produits TIC qu'il a certifiés avec les exigences de sécurité correspondantes ;
- l'assurance indiquée dans les profils de protection certifiés.

L'organisme de certification fonde ses activités de contrôle sur :

- les informations fournies sur la base des engagements du candidat à la certification ;
- les informations provenant des activités des autorités compétentes de surveillance du marché ;
- les plaintes reçues ;
- les informations relatives aux vulnérabilités transmises par le CERT-FR susceptibles d'avoir une incidence sur les produits certifiés.

Les opérations de contrôle sont effectuées :

- de manière périodique pour la surveillance des produits marqués et des marques conformément à la procédure [MAR-P-03];

- de manière ponctuelle suite à la réception d'une information particulière ou d'une plainte conformément à la procédure [ANO-P-01] ;
- ou sur demande de MCS.

9.2 Constat d'une non-conformité

Suite au constat d'une non-conformité d'un produit, d'un profil de protection ou du non-respect par le titulaire d'un certificat de ses obligations, le centre de certification informe le titulaire du certificat EUCC 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.

9.3 Réexamen d'un certificat

Le centre de certification de l'ANSSI peut décider de réexaminer la certification d'un produit ou d'un profil de protection :

- à la demande du titulaire du certificat afin de permettre la continuité de l'assurance dans les cas suivants :
 - o le certificat expire dans les neuf mois ;
 - o un changement apporté au produit certifié ou à un autre facteur pourrait avoir une incidence sur la fonctionnalité de sécurité du produit ;
 - o le titulaire du certificat exige que l'évaluation de la vulnérabilité soit effectuée à nouveau afin de reconfirmer l'assurance du certificat associée à la résistance du produit contre les cyberattaques actuelles,
- afin d'examiner la pertinence de mesures correctives suite au constat d'une non-conformité ;
- suite à la découverte d'une vulnérabilité conformément au chapitre VI d'[EUCC]. Dans ce cas, la procédure [VUL-P-01] s'applique ;
- ou pour d'autres raisons justifiées découvertes notamment lors de ses activités de contrôle, 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 (voir paragraphe 4.3). C'est notamment le cas en matière de continuité de l'assurance dans les cas non couverts par la procédure de maintenance ([MAI-P-01]).

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

- à la suspension du certificat à la modification du certificat notamment une réduction de portée conformément aux dispositions de [NOTE-25] ;
- à l'émission d'un rapport de maintenance [MAI-P-01] ;
- à son retrait et le cas échéant, à l'émission d'un nouveau certificat.

9.4 Suspension et retrait d'un certificat

Suspension : Suite au constat d'une non-conformité ou au réexamen d'un certificat, le centre de certification peut suspendre un certificat pendant une période qui ne dépasse pas quarante-deux jours calendaires excepté dans le cas de la mise en œuvre d'un plan de remédiation conformément à [VUL-P-01] ou si MCS a autorisé une extension d'un maximum d'une année. En conséquence, les sites suivants internet de publication sont mis à jour en indiquant l'état suspendu du certificat :

- le site Internet de l'ANSSI ;
- le site de l'ENISA (cas EUCC).

Retrait : Suite au constat d'une non-conformité, au réexamen d'un produit ou à l'issue d'une suspension, le centre de certification peut retirer un certificat. En conséquence, les sites suivants internet de publication sont mis à jour :

- le site Internet de l'ANSSI : le certificat est mis dans la liste des produits archivés ;
- le site de l'ENISA (cas EUCC) : retrait de la liste ;
- le site du CCRA (Common Criteria Recognition Arrangement), lorsque le certificat est reconnu dans le cadre international des Critères Communs : retrait de la liste.

Dans les cas d'une suspension ou d'un retrait, le centre de certification notifiera les commanditaires via un courrier [CER-F-22].

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]	<p><i>Common Criteria for Information Technology Security Evaluation:</i></p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003. <p>Ou</p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ; - <i>Part 2: Security functional components</i>, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ; - <i>Part 3: Security assurance components</i>, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003. <p>Ou</p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-001 ; - <i>Part 2: Security functional components</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-002 ; - <i>Part 3: Security assurance components</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-003 ; - <i>Part 4: Framework for the specification of evaluation methods and activities</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-004 ; - <i>Part 5: Pre-defined packages of security requirements</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-005.
[ISO]	<ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, août 2022, référence ISO/IEC 15408-1; - <i>Part 2: Security functional components</i>, août 2022, référence ISO/IEC 15408-2 ; - <i>Part 3: Security assurance components</i>, août 2022, référence ISO/IEC 15408-3; - <i>Part 4: Framework for the specification of evaluation methods and activities</i>, août 2022, référence ISO/IEC 15408-4; - <i>Part 5: Pre-defined packages of security requirements</i>, août 2022, référence ISO/IEC 15408-5.
[CEM]	<p><i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology</i>, version 3.1, révision 5 ou version CC:2022</p> <p>Ou</p> <p><i>Information technology — Security techniques — Methodology for IT security evaluation</i>, ISO/IEC 18045:2008 ou ISO/IEC 18045:2022</p>

[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482).
[CSA]	Règlement (UE) 2019/881 (règlement sur la cybersécurité), 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]	<i>Site Certification, Supporting Document</i> , référence CCDB-2007-11-001, version en vigueur.
[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]	<i>Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices</i> , version en vigueur.
[CER_VALID]	<i>SOG-IS Recognition Agreement Management Committee - Certificate validity</i> , version 1.0.
[CER-F-01]	Dossier d'évaluation en vue d'une certification de Critères communs, référence ANSSI-CC-CER-F-01, version en vigueur.
[CER-F-22]	Lettre de suspension, surveillance ou retrait, référence ANSSI-CC-CER-F-22, 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 des marques à CCN, 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.
[MAR-P-03]	Surveillance des marques de certification, ANSSI-CC-MAR-P-03, version en vigueur.
[NOTE-25]	Réduction de portée d'un certificat CC, référence ANSSI-CC-NOTE-25, version en vigueur.

[JIL-AC]	Joint Interpretation Library - Assurance Continuity, version en vigueur.
[VUL-P-01]	Procédure de gestion des vulnérabilités des produits certifiés, référence ANSSI-CC-VUL-P-01, version en vigueur.

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