PREMIÈRE
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 12 janvier 2023

N° **44/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CCN-MQ_v6**

MANUEL QUALITE

Application **:** Dès son approbation.

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	01/12/2003	Création
2.0	08/03/2016	Refonte du document
3.0	27/05/2019	Mise en conformité avec la norme EN ISO/IEC 17065
3.1	28/08/2019	Précisions dans l'annexe C pour faciliter la lecture Mise à jour du calcul des priorités de l'analyse de risque
3.2	29/1/2020	Suite audit interne : Le « comté des utilisateurs » devient « groupe des utilisateurs » Ajout de dispositions de préservation de l'impartialité Mise en cohérence du §7.8 avec le §9.1 de CER-P-01 Ajout de précisions dans la matrice de conformité EN ISO/IEC 17065
4.0	26/01/2021	Ajout de la publication des rapports de surveillance et gestion de la date de validité des certificats. Correction d'erreurs de typographie et ajouts de précisions Suppression du paragraphe « utilisation des certificats et usage de la marque » pour mettre son contenu dans le chapitre traitant de ce sujet Ajout d'un paragraphe traitant des mesures dérogatoires Prise en compte de la nouvelle charte graphique
5.0	23/09/2021	Précisions sur les organismes apparentés Correction pour indiquer que les CESTI sont des sous-traitants de l'ANSSI et non des organismes apparentés Précision concernant la délégation de signature du DG
6.0	12/01/2023	Ajout du dispositif de préservation de l'impartialité Refonte analyse de risques Ajout des modalités concernant les révisions et réévaluation Ajout des références Mise à jour de l'organigramme Retrait de l'annexe C

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

Ce document est également soumis pour avis lors de chaque modification majeure. Les évolutions mineures, quant à elles, ne sont pas soumises au comité directeur de la certification.

Le présent manuel est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

TABLE DES MATIERES

Chapitre 1
Le Manuel Qualité

1.1. Objet du manuel

Le manuel qualité a pour objet de présenter les méthodes et les procédures de l'organisme de certification (Centre de certification national) en vue d'assurer et de maintenir la qualité et la continuité de ses prestations en matière de certification de la sécurité des produits et des systèmes des technologies de l'information, des profils de protection et des sites indifféremment appelés « objets à certifier » ou « objets à évaluer » dans la suite de ce document.

Le manuel qualité constitue la référence pour :

- toute entité tierce faisant appel aux prestations de certification de l'ANSSI ;
- toute personne ou entité de l'Agence nationale de sécurité des systèmes d'information (ANSSI) exerçant une fonction relative à l'activité de certification, quant à son rôle et à ses responsabilités ;
- toute personne nouvellement recrutée au centre de certification pour l'informer de la politique de l'ANSSI et faciliter son intégration ;
- l'évaluation réciproque entre l'ANSSI et les autres organismes, étrangers notamment, en vue d'une reconnaissance mutuelle.

Note : pour les besoins du présent document, les termes « organisme de certification » et « centre de certification » seront indifféremment utilisés.

1.2. Élaboration, mise à jour et diffusion

Ce présent manuel est élaboré et maintenu à jour par le responsable qualité ou son suppléant, vérifié par le Chef du centre de certification puis validé et signé par l'organe de gouvernance[1]. Il est soumis à l'avis du Comité directeur de la certification.

Le responsable qualité ou son suppléant assure la diffusion du manuel qualité : les règles de diffusion du manuel sont les mêmes que celles des autres documents du système qualité.

Toutes les versions sont conservées sous forme électronique. Toutefois, seule la version française originale sous forme papier constitue la version de référence.

[1] L'organe de gouvernance est composé de tous les membres de la hiérarchie de l'ANSSI externes au centre de certification. Pour plus de détails, voir paragraphe « Interfaces de l'organisme de certification ».

Chapitre 2
Le schéma de certification

2.1. Contexte réglementaire

Le 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 précise le contexte réglementaire et l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats.

Ces règles sont mises en œuvre dans un schéma de certification tierce partie.

2.2. Le comité directeur de la certification

L'article 15 du décret 2002-535 modifié indique que le Comité directeur de la certification en sécurité des technologies de l'information a pour mission :

- de formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;
- d'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;
- d'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le décret 2002-535 modifié qui lui est soumis par les parties ;
- d'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers.

Le comité directeur se réunit au moins une fois par an. Il est présidé par le secrétaire général de la défense et de la sécurité nationale ou son représentant.

2.3. Le Groupe des utilisateurs

Le Groupe des utilisateurs du schéma français de certification est constitué de différents types d'acteurs, principalement les commanditaires des évaluations et les développeurs des produits évalués, mais aussi des donneurs d'ordre qui s'appuient sur la certification afin de spécifier les exigences de sécurité des produits qu'ils utilisent ou recommandent. Les membres de ce groupe sont invités à se réunir à l'initiative du centre de certification, leur présence reste cependant facultative. Cette rencontre est un lieu d'échange d'informations qui peuvent être partagées librement entre tous les membres compte tenu de leur caractère général.

Le Groupe des utilisateurs a pour objectifs, entre autres, de permettre à l'ANSSI :

- de présenter les évolutions des règles et normes ;
- d'identifier les besoins et attentes des utilisateurs du schéma ;
- d'échanger à propos des perspectives d'évolution.

De plus, certains membres du Groupe des utilisateurs peuvent être consultés en fonction de leurs domaines d'activité et leurs intérêts pour étayer un document en cours de finalisation. Les propositions retournées par les membres peuvent ou non être retenues, la décision finale revenant au centre de certification.

2.4. Le centre de certification

2.4.1. Statut

L'ANSSI, dont les missions sont définies par le décret n° 2009-834 du 7 juillet 2009 modifié, instruit les certifications.

L'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale, lui-même rattaché à la Première ministre. A ce titre, le centre de certification bénéficie des assurances, voire de provisions pour couvrir les responsabilités résultant de ses opérations. La stabilité financière du centre de certification est également garantie puisque ses ressources sont assurées par l'État.

Le centre de certification ne commercialise pas les résultats de ses travaux et n'effectue pas de conseil aux commanditaires ou aux développeurs.

Le centre de certification est rattaché à la division produits et services de sécurité de la sous-direction expertise de l'ANSSI.

2.4.2. Dispositions de préservation de l'impartialité

Le centre de certification de l'ANSSI doit garantir que les décisions de certification sont prises de façon objective et fiable, et qu'elles ne sont pas influencées par des considérations commerciales ou autres.

Pour ce faire, le centre de certification met en place un dispositif de préservation de l'impartialité [QUA-P-02] pour, notamment, formaliser des avis sur l'analyse de risques concernant l'impartialité de ses activités. Ce dispositif comprend un comité composé de membres ayant un intérêt significatif dans les activités de certification mises en œuvre par le centre de certification, l'analyse de risques dédiée à l'impartialité des activités du centre de certification et toutes autres pièces indispensables à la mise en œuvre de l'impartialité.

Par ailleurs le centre de certification met en œuvre les politiques et principes de certification appliqués à la fois au centre de certification, à son personnel, aux centres d'évaluation et aux personnes externes afin de garantir une totale indépendance de la décision de certification.

Politiques et principes du centre de certification :

- les travaux du centre de certification sont réalisés dans le cadre du décret 2002-535 du 18 avril 2002 modifié et non au travers de contrats commerciaux ;
- le centre de certification est une subdivision d'une administration de l'État ;
- les ressources financières sont assurées par l'État. Les services proposés par le centre de certifications sont libres du paiement de tout droit ;
- le centre de certification ainsi que l'ANSSI ne sont ni des concepteurs, ni des fabricants, ni des installateurs, ni des responsables de l'entretien de produits certifiés ;
- le centre de certification ne délivre aucune information confidentielle durant les réunions regroupant l'ensemble des membres du Groupe des utilisateurs ;
- le centre de certification ne fait pas appel à du personnel externe au centre pour assurer les activités de certification ;
- le centre de certification n'accepte pas de mettre en commun son personnel avec une entité susceptible de porter atteinte à son impartialité ;
- le centre de certification ne fournit pas de prestation de conseil ou de formation visant à l'obtention ou au maintien d'une certification ;
- le centre de certification ne fournit pas de prestation de conseil pour la conception, la fabrication, l'installation et la distribution d'un produit en cours de certification ou déjà certifié ;

- le centre de certification répond à des critères qui permettent de garantir à ses clients, une totale impartialité tant dans l'exécution des travaux que dans la décision finale de certification qu'elle soit positive ou négative.

Politiques et principes appliqués au personnel de l'ANSSI intervenant dans un projet de certification :

- chaque personne de l'ANSSI intervenant sur les projets est un agent de la fonction publique[2] habilité au minimum au niveau Secret. Il s'engage entre autres, à respecter le secret le plus absolu sur les informations sensibles qui lui sont confiées dans l'exercice de ses fonctions et à déclarer tout fait qui pourrait remettre en cause son impartialité ;
- chaque personne de l'ANSSI intervenant sur des projets de certification déclare à sa hiérarchie tout fait antérieur, présent ou à venir qui pourrait remettre en cause son indépendance lorsqu'un projet lui est proposé ;
- chaque personne du centre de certification doit refuser toute sollicitation, promesse, don, présent ou avantage quelconque, soit directement, soit par personne interposée qui pourrait nuire à son indépendance de jugement ;
- les recommandations techniques publiées par les experts techniques de l'ANSSI ne mettent pas en cause les fondements de l'impartialité puisqu'elles s'adressent à l'ensemble de la communauté et non à un développeur particulier ;
- un membre du centre de certification qui a fourni des recommandations ou qui a été employé du plaignant ne peut pas participer à la revue, ni approuver la solution apportée à la plainte et ce, durant les deux années qui suivent l'émission des recommandations ou de l'emploi chez ce plaignant ;
- la décision permettant d'apporter une solution à une plainte doit être prise, revue et approuvée par un membre du centre de certification non engagé dans les activités liées à la plainte. Par contre, un membre lié à la plainte peut intervenir dans l'élaboration de la réponse.

Politiques et principes appliqués aux centres d'évaluation :

- chaque centre d'évaluation s'engage à ne pas faire intervenir du personnel qui aurait au préalable promulgué des recommandations au développeur pour le produit évalué (rédaction de la cible de sécurité, aide à la conception ou la spécification cryptographique par exemple) ;
- chaque centre d'évaluation s'assure de l'indépendance et de l'impartialité de son personnel vis-à-vis des commanditaires ou des développeurs ;
- les centres d'évaluation peuvent être amenés à donner des recommandations à leurs clients. Toutefois, un cloisonnement est assuré entre les acteurs intervenant pour donner des recommandations et ceux réalisant les travaux d'évaluation.

Politiques et principes appliqués aux personnes externes :

- si un audit du centre de certification est réalisé par des intervenants externes (société tierce qui a contractualisé avec l'ANSSI, ou membres du COFRAC), les auditeurs accédant aux données des projets de certification sont habilités au moins au niveau Secret et signent un engagement de confidentialité lors de chaque nouvel audit ;
- les auditeurs des centres de certification étrangers n'ont accès qu'aux informations préalablement autorisées par les commanditaires des produits évalués.

Ces intervenants extérieurs ne consultent les informations qu'en présence d'une personne du centre de certification, dans les locaux du centre de certification.

Conformément à l'article 16 du décret 2002-535 modifié, la désignation des membres composant le comité directeur permet d'assurer une large représentation des parties ayant un intérêt significatif notamment lors du traitement des litiges. La politique appliquée est la suivante :

[2] Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

- les membres du comité directeur de la certification sont tenus à la confidentialité et à l'impartialité au travers du « règlement intérieur du comité directeur de la certification » signé par les parties ;
- les membres du comité directeur ont accès à toutes les informations nécessaires à l'exercice de leurs missions.

Politiques liées aux organismes apparentés :

- le *webmaster* est employé par l'ANSSI, il est donc soumis aux mêmes règles que les membres du centre de certification et est habilité au minimum au niveau Secret. Il s'engage, entre autres, à respecter le secret le plus absolu sur les informations sensibles qui lui sont confiées dans l'exercice de ses fonctions ;
- le personnel de ménage intervient dans les bureaux durant les heures ouvrées et en présence au moins d'une personne de l'ANSSI. La sélection de la société de ménage et de son personnel fait l'objet du plus grand soin par le SGDSN dans la mesure où les locaux dans lesquels ces personnes interviennent se trouvent dans une zone protégée au sens de [IGI 1300] ;
- le bailleur des locaux dans lesquels sont exercées les activités du centre de certification n'a que très rarement des relations avec les membres du centre de certification ;
- les services généraux n'ont également que très rarement des relations avec les membres du centre de certification ;
- les gendarmes qui assurent les missions d'accueil et de sécurité, de par leur statut, ne présentent que peu de risque ;
- les membres de l'Opérateur des Systèmes d'Information Interministériels Classifiés (OSIIC) sont soumis aux mêmes règles que les membres du centre de certification et sont habilités au moins au niveau Secret. A ce titre, cet opérateur est en charge d'assurer la sécurité des informations du SGDSN et donc celles liées aux travaux effectués par l'organisme de certification. Cet opérateur a également la charge d'assurer la sauvegarde, la conservation et la destruction des documents numériques produits par l'organisme de certification.

2.4.3. Missions de l'organisme de certification

L'organisme de certification a pour principales missions :

- de mettre en œuvre la stratégie de certification définie par l'ANSSI ;
- d'assurer l'instruction des dossiers d'évaluation ainsi que la mise en œuvre des processus de maintenance et de surveillance des certificats délivrés ;
- d'assurer l'instruction des demandes d'agréments des candidats comme centres d'évaluation nationaux ;
- d'effectuer des audits d'agrément des centres d'évaluation pour s'assurer de leurs niveaux de compétence pour leur domaine considéré ;
- de représenter l'ANSSI dans les instances nationales et internationales traitant des sujets de certification ;
- de définir des référentiels d'évaluation de sécurité adaptés à des catégories de produits en liaison avec les utilisateurs du schéma national ;
- d'assurer la promotion de l'utilisation du schéma national d'évaluation et de certification.

2.4.4. Organisation

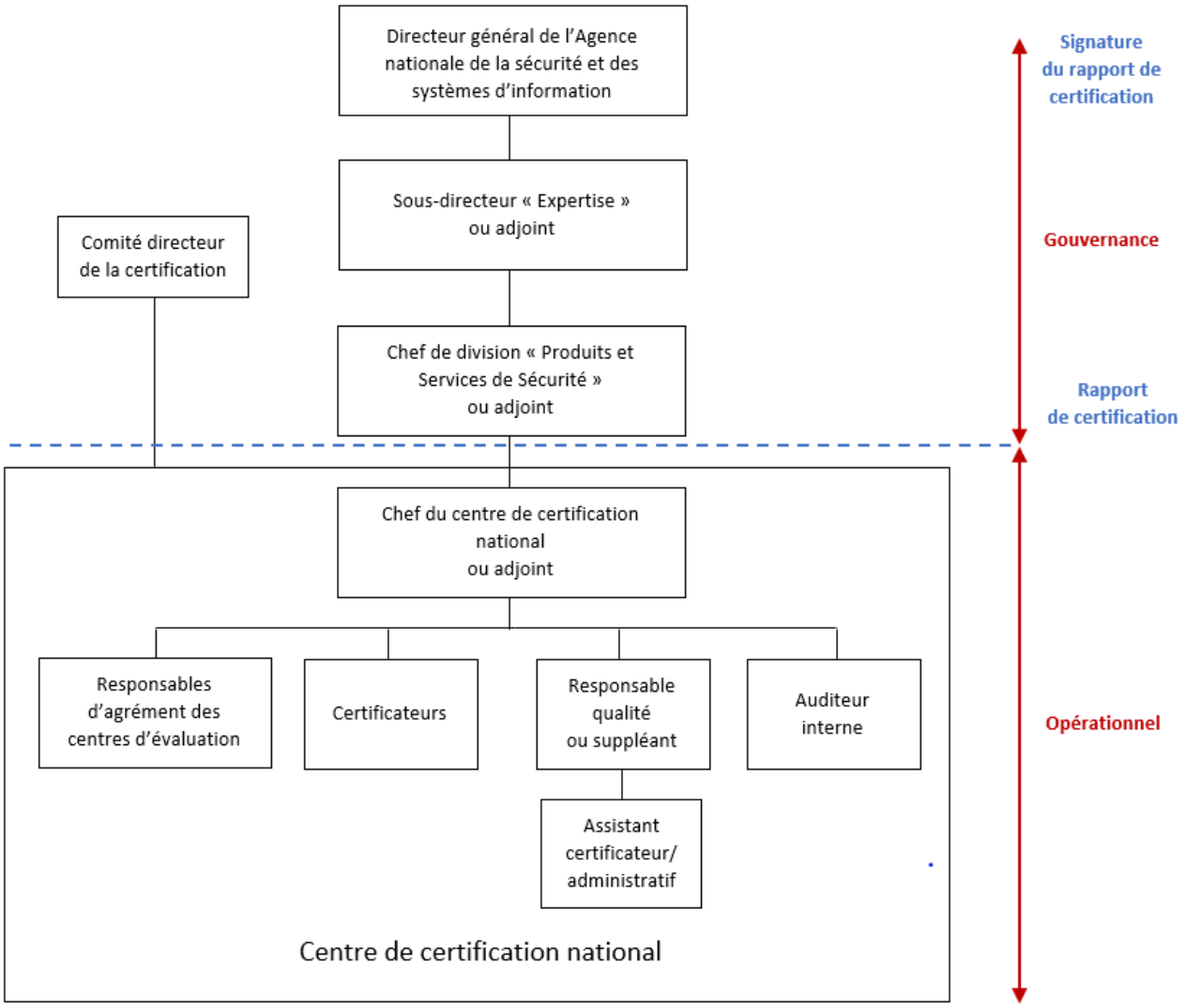


Figure 1 – Organigramme fonctionnel du centre de certification

Les responsabilités pour l'activité de certification sont réparties de la façon suivante :

- **le directeur général de l'ANSSI ou son adjoint a** pour responsabilité de délivrer les certificats et les agréments des centres d'évaluation ;
- **le sous-directeur Expertise ou son adjoint** a autorité sur le centre de certification mais n'intervient pas dans la décision de certification. Le sous-directeur ou son adjoint préside le comité directeur de la certification en tant que représentant du secrétaire général de la défense et de la sécurité nationale ;
- **le chef de division « Produits et Services de Sécurité » ou son adjoint** a autorité sur le centre de certification mais n'intervient pas dans la décision de certification. Dans le processus de certification, le chef de division assure la cohérence rédactionnelle de l'ensemble des rapports de certification, de surveillance et de maintenance ;
- **le chef du centre de certification ou son adjoint** a pour fonction la gestion et le contrôle opérationnels du centre de certification. Il définit les besoins en ressources, participe au recrutement de son personnel et s'assure de sa compétence pour les fonctions occupées en tenant à jour un dossier relatif à l'expérience et à la formation du personnel. Il s'assure de la reconnaissance des certificats à l'extérieur des frontières et entretient des relations avec ses

homologues étrangers. Il participe à la gestion des critères d'évaluation et de certification. Il est responsable de la décision de certification transmise pour signature au directeur général ;

- **les responsables d'agrément des centres d'évaluation** sont chargés de s'assurer du respect, par les centres d'évaluation, des normes et standards en vigueur ainsi que des critères d'agrément. Ils s'assurent également de la compétence des évaluateurs, du bon niveau d'équipement et du plan de développement des centres d'évaluation. Ils instruisent l'agrément des CESTI ;
- **le responsable qualité** est chargé de la mise en place, du maintien et de l'amélioration continue du système qualité. Il assure également la formation qualité du personnel du centre de certification ;
- **les certificateurs** sont chargés de suivre les évaluations afin de vérifier le respect des règles, et procédures de certification et, d'appliquer les procédures qualité en vigueur. Ils interviennent entre autres dans la revue des travaux d'évaluation ;
- Certains certificateurs, qualifiés pour cette activité, sont amenés également à réaliser des audits internes planifiés et gérés par le responsable qualité. Cependant, il convient de noter que la plupart des audits internes sont effectués par des entités extérieures à l'ANSSI ;
- **l'assistant certificateur/administratif** est chargé d'assurer le suivi administratif des documents du centre de certification et d'assister le chef de centre et les certificateurs dans leurs activités.

2.4.5. Interfaces de l'organisme de certification

L'organisme de certification ou le centre de certification national a pour interlocuteurs internes, notamment :

- l'organe de gouvernance qui est composé de tous les membres de la hiérarchie de l'ANSSI externes au centre de certification. Leurs rôles sont notamment les suivants :
    - pour le directeur général[3] :
        - signer les rapports de certification, surveillance et maintenance, tant Critères communs que Certification de sécurité de premier niveau,
        - signer les agréments aux centres d'évaluation après avoir recueilli l'avis du comité directeur de la certification,
        - signer les notes d'application utilisées pour les procédures d'évaluation et de certification après avoir recueilli l'avis du comité directeur de la certification,
        - signer les accords de reconnaissance mutuelle conclus avec les organismes étrangers après avoir recueilli l'avis du comité directeur de la certification,
        - signer une partie des documents du processus « qualité » ;
    - pour le sous-directeur « Expertise » (SDE) :
        - présider les réunions de revue de direction de la qualité,
        - signer certains documents liés au processus « qualité »,
        - représenter le secrétaire général au comité directeur de la certification.
    - pour le chef de division « Produits et Services de Sécurité » (PSS) :
        - assurer la cohérence de qualité de tous les rapports de certification,
        - valider certains documents liés au processus « qualité » ;
- les différents experts internes à l'ANSSI qui peuvent être sollicités par les certificateurs pour rendre des avis sur des sujets techniques particuliers. Dans tous les cas, les certificateurs sont totalement libres de les solliciter, d'apprécier et de tenir compte ou non des avis rendus ;

[3] Le directeur général peut être amené à déléguer sa signature, notamment au sous-directeur « Expertise » ou au chef de bureau du centre de certification.

- les « Ressources humaines » qui interviennent sur tous les sujets qui traitent de la gestion du personnel du centre de certification (recrutement, gestion des entretiens individuels, suivi des formations, etc.) ;
- les « Affaires juridiques » qui sont sollicitées par l'organisme de certification pour tous les sujets nécessitant des avis juridiques (*Memorandum Of Understanding*, *Non Disclosure Agreement*, etc.) ;
- les donneurs d'ordre[4] internes, notamment le « Bureau Qualification et Agrément » (BQA) de l'ANSSI qui a pour missions de qualifier et agréer les produits et prestataires de service de confiance. Ces donneurs d'ordre internes n'interviennent dans le processus de certification que pour valider les problématiques de sécurité décrites dans les cibles de sécurité pour s'assurer qu'elles répondent aux besoins de l'Etat.

Les interlocuteurs externes du centre de certification sont :

- les centres d'évaluation (CESTI[5]) agréés par l'organisme de certification qui sont en charge de procéder à l'évaluation des produits conformément aux Critères communs ou à la Certification de sécurité de premier niveau. Ces centres sont en charge de remettre des rapports d'évaluation à l'organisme de certification qui se charge de les valider. Ces centres sont considérés comme des sous-traitants du centre de certification et doivent se conformer aux différents documents sur lesquels ils sont amenés à s'engager ;
- les commanditaires et/ou développeurs qui sont les demandeurs pour que leurs produits entrent dans un processus de certification ;
- les donneurs d'ordre externes qui sont en charge de valider que les cibles de sécurité soumises avec les dossiers d'évaluation répondent à leurs besoins propres ;
- les schémas homologues d'autres organisations ou d'autres pays qui participent à l'harmonisation des pratiques et référentiels internationaux et aux audits CCRA et SOG-IS (revue par les pairs) ;
- les organismes apparentés : le webmaster, le personnel de ménage, le bailleur des locaux, les services généraux du SGDSN, les gendarmes, et les membres de l'Opérateur des Systèmes d'Information Interministériels Classifiés (OSIIC).

2.4.6. Personnel du centre de certification

La direction de l'organisme de certification fixe les exigences en termes de recrutement et de suivi des compétences de son personnel.

On distingue notamment quatre niveaux de qualification :

- le niveau « théorique » : l'agent acquiert les connaissances de base soit suite à des actions de formations externes ou internes, soit dans le cadre d'auto-formations ;
- le niveau « connaissance » : l'agent est encadré par un tuteur pour chacun des projets afin de mettre en pratique ses connaissances acquises. Il réalise chacune de ces missions sous le contrôle d'un tuteur qui est chargé de statuer sur la bonne réalisation de sa mission ;
- le niveau « autonome » : concernant le certificateur, il est autorisé à suivre seul les projets d'évaluation. Concernant les postes supports, ils sont autorisés à mener seuls des actions transverses administratives liées au centre de certification national. Des formations complémentaires sont dispensées pour permettre aux agents de consolider leurs compétences ;
- le niveau « expert » : concernant le certificateur, il est autorisé à représenter seul le centre de certification dans des groupes de travail. Concernant les postes supports, ils sont autorisés à mener seuls des actions transverses administratives et d'organisation.

[4] Le terme « Donneur d'ordre » utilisé dans les bases de données des projets ne traduit en rien une quelconque relation de subordination. Cette information sert uniquement aux statistiques du centre pour identifier l'usage des produits certifiés.

[5] Centre d'Evaluation de la Sécurité des Technologies de l'Information.

Dans tous les cas, un agent ne pourra en aucun cas prendre en charge un projet pouvant remettre en cause son impartialité. Le centre de certification n'emploie pas de personnel temporaire pour les activités de certification.

Chapitre 3
Système qualité

3.1. Politique qualité

3.1.1. Objectif

Le centre de certification évolue dans un milieu où confiance, rigueur et continuité prennent tout leur sens. De par l'étendue géographique de ses activités et la dispersion culturelle de ses clients, le centre de certification doit, au travers de son système qualité, donner la plus grande confiance dans les travaux qu'il mène afin d'assurer la reconnaissance de ses certificats, notamment en raison du cadre international dans lequel il s'inscrit.

Ses objectifs sont axés sur la reconnaissance des certificats émis, à savoir :

- une reconnaissance nationale, pour établir la confiance dans les travaux de certification qu'il mène auprès de toutes les parties concernées ;
- une reconnaissance internationale, afin d'entrer dans le cadre des accords de reconnaissance mutuelle qui l'engagent.

3.1.2. Exigences

Pour obtenir et conserver durablement cette reconnaissance, le centre de certification se conforme aux exigences de la norme EN ISO/IEC 17065 et des accords CCRA et SOG-IS, notamment :

- la traçabilité : toute évaluation doit être reproductible et l'ensemble des éléments de preuves lié à la délivrance du certificat doit être identifié et conservé ;
- l'homogénéité : les certificats doivent rendre compte d'un niveau d'assurance comparable, quel que soit le personnel chargé du suivi et quel que soit le centre d'évaluation qui a mené l'évaluation ;
- la confidentialité : le centre de certification doit assurer le respect de la confidentialité des informations sensibles qui lui sont confiées ou qu'il élabore dans le cadre de la certification ;
- l'impartialité : le centre de certification doit régulièrement s'assurer que ses membres opèrent en toute impartialité.

L'organisme de certification s'engage ainsi à :

- publier et tenir à jour les règles et exigences relatives au schéma d'évaluation et de certification ;
- publier et tenir à jour la liste des certificats publics et des centres d'évaluation agréés ;
- s'assurer des compétences des centres d'évaluation qui procèdent à l'évaluation ;
- travailler avec du personnel compétent et qualifié dans son domaine.

3.2. Planification de la qualité

3.2.1. Audits internes

Des audits périodiques du système qualité sont organisés par le responsable qualité ou son suppléant et conduits par des auditeurs qualifiés et indépendants des fonctions auditées conformément au programme annuel d'audits.

Le responsable qualité ou son suppléant planifient et gèrent les audits de manière à ce que les exigences de la norme EN ISO/IEC 17065 soient auditées au moins une fois par an et veillent dans le cas où l'audit serait segmenté à ce qu'il soit achevé dans un délai de 12 mois.

3.2.2. *Analyse de risques*

Le centre de certification prend en compte, à chaque fois que nécessaire, les risques susceptibles de nuire à son impartialité.

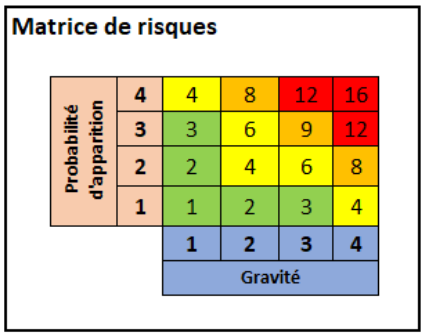
L'analyse de risques qui en découle permet d'identifier des actions pour maîtriser voire éliminer les risques identifiés. Elle est revue annuellement et approuvée dans le cadre du dispositif de préservation de l'impartialité [QUA-P-02].

La méthodologie adoptée pour effectuer l'analyse de risques concernant l'impartialité des activités du centre de certification consiste à recenser les risques bruts suivant la perception des acteurs concernés (personnel du centre de certification, l'organe de gouvernance, clients, etc.) puis à évaluer pour chacun des risques, sa gravité et sa probabilité de survenir, ceci sur une échelle de 1 à 4.

GRAVITE		
Échelle	**Caractérisation**	**Description**
1	Mineure	Evénement mineur qui ne remet pas en cause l'impartialité
2	Modérée	Evénement sans conséquences lourdes pour l'impartialité
3	Majeure	Evénement qui remet en cause l'impartialité
4	Forte	Evénement préjudiciable, nuit à l'impartialité

PROBABILITE D'APPARITION		
Échelle	**Caractérisation**	**Description**
1	Rare	Une fois par an au plus
2	Peu probable	Une fois par trimestre au plus
3	Probable	Une fois par mois au plus
4	Très probable	Plusieurs fois par mois

Le résultat de ces cotations permet d'identifier le niveau de risque brut soit G (gravité) x P (probabilité d'apparition) = risque brut.



Les risques sont ensuite catégorisés de la façon suivante :

Grille d'identification du risque	
Niveau du risque	**Description**
Faible 1-3	Risques résiduels connus ne nécessitant pas d'actions particulières
Moyen 4-6	Risques connus et maitrisés ne nécessitant pas d'actions particulières
Fort 8-9	Risques qui doivent faire l'objet d'actions préventives
Très fort 12-16	Risques qui doivent impérativement et obligatoirement faire l'objet d'actions correctives

Le niveau de risque brut (élément d'entrée) associé aux moyens et actions de maîtrise permettent de déterminer le risque net (élément de sortie). Certains risques sont considérés comme faibles, ils ne nécessitent alors pas d'action de réduction du risque.

La classification des actions mises en place pour détecter les risques bruts en fonction de leur efficacité permet d'établir une grille de cotation de la détectabilité.

Grille de cotation de la détectabilité		
Échelle	**Détectabilité**	**Description**
1	Se détecte facilement	Les mesures mise en place permettent de détecter facilement le risque
2	Détectable	Les mesures en place permettent de détecter le risque
3	Moyennement détectable	Les mesures en place permettent une détection partielle du risque
4	Impossible à détecter	Les mesures en place ne permettent pas de détecter le risque

Ainsi une nouvelle cotation est émise et permet de classifier le risque net (le risque net est évalué comme le produit de la gravité (G), de la probabilité d'apparition (P) et de la détectabilité (D)). Cette classification permet d'identifier les risques qui nécessitent des actions à mettre en place afin de les corriger pour les réduire ou les éliminer en traitant en priorité les risques de niveau « Très fort ».

Grille d'identification du risque net	
Niveau du risque	**Description**
Faible 1-3	Risques ne nécessitant pas d'actions particulières
Moyen 8-12	Risques ne nécessitant pas d'actions particulières
Fort 24-27	Risques qui doivent faire l'objet d'actions préventives
Très fort 48-64	Risques qui doivent faire l'objet d'actions correctives

Le centre de certification réalise une revue interne une fois par an afin d'identifier le ou les nouveaux risques et les mesures qui sont ou peuvent être mises en place pour y remédier.

Les actions à mettre en place sont suivies et traitées dans le cadre du dispositif de préservation de l'impartialité.

3.2.3. Revue de direction

Lors de la réunion annuelle de revue de direction de la qualité, organisée par le responsable qualité ou son suppléant, la gouvernance du centre de certification s'assure que le système de management de la qualité demeure pertinent, adéquat et efficace, qu'il est maintenu à jour et disponible à l'ensemble des parties intéressées. À cette occasion, il est notamment fait part à l'organe de gouvernance des résultats des audits internes et externes, des nouveaux points de l'analyse de risques, des appels et plaintes des clients.

Durant l'année, d'autres revues peuvent être organisées à la demande de la direction ou du centre de certification.

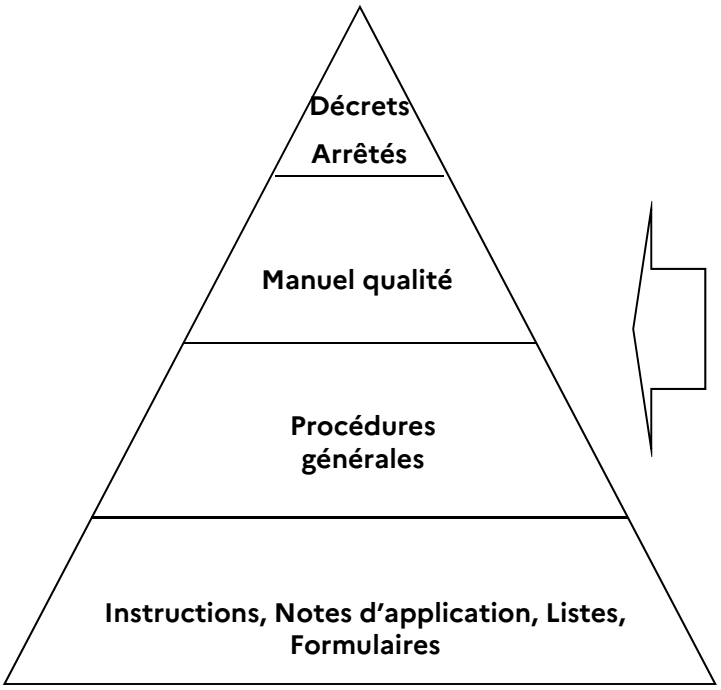
3.3. Architecture documentaire

Le centre de certification dispose d'une collection documentaire couvrant l'ensemble de l'activité de certification et répondant aux exigences de la norme EN ISO/IEC 17065.

Au moins une fois par an, une revue documentaire du système de management de la qualité est effectuée afin de s'assurer notamment pour les documents externes mis à disposition des membres du centre de certification et des autres utilisateurs du schéma correspondent bien à leurs dernières versions.

3.3.1. Structure documentaire

La structure de cette collection documentaire est la suivante :



	Entrées	Sorties	
Application	Demandes d'évaluation en vue d'une certification Rapports d'évaluation Enquêtes de satisfaction à remplir	Lettres d'enregistrement Revues des rapports d'évaluation Rapports de certification et certificats Lettres de clôture Rapports d'audits d'agrément Décisions d'agrément Enquêtes de satisfaction renseignées par le commanditaire / développeur	Enregistrements relatifs à la certification et à l'agrément Enquête de satisfaction
	Présentations pour « revue de direction de la qualité » Programmes d'audits internes et externes	Comptes rendus de la revue de direction de la qualité Rapports d'audits internes et externes	Enregistrements relatifs au système qualité

3.3.2. Maîtrise de la documentation

Le centre de certification possède des règles d'élaboration et de maîtrise de la documentation liées à son activité de certification conformément à la procédure [DOC-P-01].

Le responsable qualité ou son suppléant tiennent à jour la liste de tous les documents qualité utilisés par le centre de certification.

3.3.3. Enregistrements liés à la certification

Il existe trois types d'enregistrements démontrant que toutes les procédures et instructions relatives à l'activité de certification ont bien été appliquées :

- les enregistrements sur support papier conservés au centre de certification ou dans un local d'archives ;
- les enregistrements numériques ;
- les échantillons remis par les commanditaires, conservés au centre de certification.

La durée de conservation des enregistrements est de dix ans au minimum.

Chapitre 4
Modalités de la certification

4.1. Accès et traitement non discriminatoires

Tous les développeurs et commanditaires d'objets à évaluer ont accès aux services du centre de certification de l'ANSSI et ce, sans aucun caractère discriminant de quelque nature qu'il soit.

Le centre de certification de l'ANSSI veille à l'égalité de traitement entre les différents objets à certifier et limite ses exigences aux éléments spécifiquement en rapport avec la portée de la certification « Critères communs » ou celle de la « Certification de sécurité de premier niveau ».

L'attribution de la certification n'est subordonnée qu'au respect des règles de fonctionnement du schéma et à la satisfaction des critères d'évaluation.

4.2. Documents de référence

L'ensemble des documents publics relatifs à la certification est disponible ou référencé sur le site Internet de l'ANSSI.

Ces documents sont :

- les textes réglementaires relatifs à la certification de la sécurité des produits et des systèmes des technologies de l'information ;
- les documents publics de fonctionnement (procédures, instructions, formulaires et notes d'application) du centre de certification ;
- les formulaires dont la « Demande d'évaluation » tant pour les Critères communs que pour la Certification de sécurité de premier niveau ;
- les critères d'évaluation libres de droits.

4.3. Critères d'évaluation

Les critères et méthodologies d'évaluation utilisés sont approuvés par le Comité directeur de la certification.

Ces critères d'évaluation sont susceptibles d'évoluer ou d'être complétés par des guides techniques en fonction de la technologie considérée ou de contextes particuliers.

4.4. Modification des exigences de certification

Les exigences relatives à la certification peuvent être amenées à évoluer dans le temps conformément à la procédure [MOD-P-01], elles sont communiquées aux intéressés.

Ces évolutions peuvent être :

- des évolutions des critères d'évaluation provenant des instances normatives internationales ou nationales : elles sont directement disponibles auprès de ces instances de normalisation ;
- des adaptations d'exigences pour un domaine particulier : si elles sont obligatoires ou dépendantes du schéma national, elles sont notifiées par une note d'application du schéma qui précise son délai d'application ;
- des évolutions de pratiques du schéma de certification : en cas d'évolutions majeures, elles nécessitent l'avis du Comité directeur de la certification.

Chapitre 5
Demande de certification

5.1. Contenu du dossier d'évaluation

Le commanditaire, après avoir sélectionné un centre d'évaluation agréé par l'organisme de certification, demande l'ouverture d'un dossier de certification « Critères communs » ou de « Certification de sécurité de premier niveau » au centre de certification par le biais d'un dossier d'évaluation disponible sur le site de l'ANSSI.

Le dossier d'évaluation comprend notamment :

- les conditions générales de la certification ;
- l'engagement du commanditaire et du centre d'évaluation à respecter les règles de certification ;
- une description de l'objet à évaluer (incluant sa cible de sécurité) ;
- le planning prévisionnel de livraison des fournitures délivrées par le commanditaire ou développeur au centre d'évaluation et à l'ANSSI ;
- le programme de travail prévisionnel élaboré par le centre d'évaluation lors de la préparation de l'évaluation « Critères communs » ou le délai estimé de livraison des résultats pour les évaluations « Certification de sécurité de premier niveau ».

5.2. Enregistrement de la demande

Sur la base du dossier d'évaluation, le centre de certification :

- vérifie que la signature de la demande vaut engagement de la société ;
- procède à une revue documentaire approfondie, notamment de la cible de sécurité et du programme de travail prévisionnel. Si le centre de certification estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, il notifie au commanditaire qu'il ne pourra pas en l'état du dossier procéder à la certification envisagée ;
- vérifie la pertinence des charges prévues pour l'évaluation ;
- vérifie que la portée d'agrément du centre d'évaluation lui permet d'évaluer le produit considéré ;
- indique le nom du certificateur désigné pour assurer le suivi de l'évaluation.

Par défaut, l'existence même de l'évaluation est considérée comme confidentielle, elle ne fait donc l'objet d'aucune publicité par le centre de certification, sauf demande du commanditaire, approuvée par l'organisme de certification.

Chapitre 6
Évaluation

6.1. Les centres d'évaluation

6.1.1. Rôles et responsabilités

Les centres d'évaluation réalisent les évaluations : ils constituent une tierce partie indépendante des développeurs de produits et des commanditaires et sont considérés comme des sous-traitants du centre de certification.

Les centres d'évaluation sont agréés par l'ANSSI après avis du comité directeur de la certification et, à ce titre, sont tenus de respecter toutes les règles du schéma. Le centre de certification intervient dans cette démarche d'agrément notamment au travers d'audits techniques pour s'assurer de la capacité du centre d'évaluation à mener à bien ses missions dans son ou ses domaine(s) de compétence revendiquée conformément aux procédures [CC-AGR-P-01] et [CSPN-AGR-P-01].

Les centres d'évaluation sont constitués d'équipes d'experts et de responsables, intégrés le plus souvent dans un organisme à vocation plus large. Toutefois, les critères d'agrément imposent un cloisonnement vis-à-vis des autres activités de l'organisme auquel le centre d'évaluation est rattaché.

6.1.2. Procédure d'agrément

Les critères d'agrément Critères communs comprennent, entre autres, l'accréditation des centres d'évaluation par le COFRAC (COmité FRançais d'ACcréditation) selon la norme EN ISO/IEC 17025. Des guides techniques d'accréditation, élaborés par le COFRAC, précisent le domaine particulier de l'évaluation de la sécurité des technologies de l'information.

L'agrément impose des exigences qui permettent de s'assurer de la maîtrise par le centre d'évaluation de certaines techniques particulières ainsi que de sa capacité à traiter des informations sensibles.

L'agrément d'un centre d'évaluation est ensuite accompagné d'une procédure de suivi qui permet de s'assurer de la pérennité du respect des exigences d'agrément.

6.1.3. Réalisation des travaux d'évaluation par le centre d'évaluation

Le centre d'évaluation mène les travaux d'évaluation conformément aux critères d'évaluation choisis. Ces travaux sont suivis par le certificateur désigné.

Le commanditaire de l'évaluation est responsable de la livraison des fournitures nécessaires à l'évaluation. La liste exacte des fournitures à livrer au centre d'évaluation et au centre de certification dépend des critères d'évaluation choisis.

Le centre d'évaluation analyse l'objet à évaluer et sa documentation afin de vérifier que les exigences spécifiées dans les critères d'évaluation sont satisfaites. Certains critères d'évaluation peuvent exiger une visite des sites de développement ou de production de l'objet à évaluer.

6.1.4. Le Rapport Technique d'Évaluation

Le centre d'évaluation rédige un rapport technique d'évaluation (RTE) qui décrit les travaux effectués lors de l'évaluation et expose les résultats obtenus. Ce RTE est transmis :

- au centre de certification et au commanditaire dans le cadre des évaluations CC ;
- uniquement au centre de certification qui donne son accord avant transmission au commanditaire dans le cadre des évaluations CSPN.

Le RTE est soumis pour validation au certificateur en charge du projet.

Lorsque toutes les tâches d'évaluation ont été menées par le centre d'évaluation et que l'ensemble des travaux a été validé par le centre de certification, l'évaluation est considérée comme terminée.

Le RTE contient une conclusion statuant sur la Réussite ou l'Echec de l'évaluation.

Le RTE contient des données sensibles couvertes par le secret industriel et commercial. Sa diffusion est contrôlée : les clauses de confidentialité imposées par l'ANSSI peuvent être précisées contractuellement entre le centre d'évaluation et le commanditaire lors de la phase de préparation de l'évaluation. Toute diffusion en dehors de ces parties est soumise à l'approbation du centre de certification.

Chapitre 7
Certification

7.1. Préambule

La certification est un processus global qui permet, par un ensemble d'actions, de s'assurer que l'évaluation s'est déroulée avec la compétence et l'impartialité requises conformément aux procédures [CC-CER-P-01] et [CSPN-CER-P-01].

7.2. Rapport de certification

Après validation d'un RTE positionné à « Réussite », le certificateur rédige un rapport de certification qui propose la certification. Le rapport de certification est, avec la cible de sécurité, le seul document produit dans le cadre de l'évaluation qu'un acheteur potentiel est amené à consulter.

Le rapport de certification décrit fidèlement l'objet évalué, l'environnement d'évaluation considéré et recommande éventuellement la mise en œuvre de mesures nécessaires à une utilisation sécurisée de l'objet certifié.

Le rapport de certification constitue, avec la cible de sécurité éventuellement expurgée de certaines informations propriété du commanditaire/développeur, la documentation minimale à fournir pour la reconnaissance internationale du certificat.

7.3. Délivrance du certificat

Dans le cas où le centre de certification décide de certifier l'objet évalué, il transmet les projets de rapport de certification et de certificat au directeur général de l'ANSSI ou son adjoint. Le directeur général de l'ANSSI ou son adjoint qui en a reçu délégation par la Première ministre signe le certificat et le rapport de certification.

7.4. Maîtrise des enregistrements

Toutes les fournitures et documents électroniques délivrés par les commanditaires et les centres d'évaluation, ainsi que ceux produits par l'organisme de certification, sont systématiquement enregistrés, stockés et conservés sur les réseaux homologués du Secrétariat général de la défense et de la sécurité nationale.

Les originaux signés des documents papier spécifiques aux procédures de certification sont conservés par l'organisme de certification dans un lieu sécurisé au minimum durant dix ans.

7.5. Publication du certificat

Si le commanditaire en fait la demande, le rapport de certification et la cible de sécurité correspondante sont publiés sur le site Internet de l'ANSSI.

Passée leur date de validité, les documents publiés sur le site de l'ANSSI sont déplacés dans une liste de produits certifiés archivés si le commanditaire n'a pas, entre temps, obtenu une extension de sa durée via le processus de surveillance de produit (valable uniquement pour une évaluation CC).

7.6. Indice de satisfaction

Aux termes de la certification, le commanditaire et/ou le développeur a la possibilité de remplir un questionnaire de satisfaction, qui lui est soumis par le centre de certification, et qui vise à l'amélioration des services rendus.

7.7. Suspension, retrait du certificat

Le centre de certification de l'ANSSI peut être amené à suspendre, voire retirer un certificat pour diverses raisons techniques (découverte d'une vulnérabilité, fin de période de validité du certificat, etc.) ou de communication incomplète, voire frauduleuse.

Chapitre 8
Utilisation du certificat et de la marque

Le centre de certification engage contractuellement les parties impliquées à respecter scrupuleusement l'usage des certificats et de la marque.

8.1. Règles de communication

Le commanditaire et, le cas échéant, les développeurs, ont le devoir d'informer fidèlement et honnêtement les utilisateurs de produits certifiés et l'ANSSI. En particulier, le commanditaire a le devoir de :

- fournir le rapport de certification et la cible de sécurité chaque fois qu'un donneur d'ordre en fait la demande. Les copies de documents de certification à autrui doivent être conformes en tout point aux originaux délivrés. Les destinataires des copies peuvent vérifier leur exactitude auprès de l'organisme de certification de l'ANSSI ;
- ne pas faire d'annonce trompeuse sur le produit en laissant entendre par exemple que le produit est certifié alors qu'il n'est qu'en cours d'évaluation ou qu'un produit est certifié alors qu'il ne s'agit pas de la version exacte certifiée ;
- informer ses utilisateurs si une vulnérabilité susceptible d'impacter une ou des versions déjà déployées est découverte au cours de l'évaluation ;
- signifier systématiquement et sans délais à l'ANSSI (CERT-FR[6]) toute vulnérabilité avec son analyse d'impact associée afin de permettre son instruction pour qu'elle soit corrigée ou contournée et permettre l'établissement d'un message vers les utilisateurs des produits certifiés.

8.2. Règles d'utilisation de la marque

La marque « certification sécurité TI » reproduite ci-dessous est la marque de certification française de la sécurité offerte par les technologies de l'information accordée par l'ANSSI. Cette marque est déposée à l'Institut national de la propriété industrielle sous le numéro 023 175 658.

Elle identifie les produits et systèmes certifiés dans le cadre du décret 2002-535 modifié. Son usage est défini dans une procédure spécifique [MAR-P-01].

L'usage des logotypes des accords CCRA et SOG-IS pour la reconnaissance internationale des certificats est également décrit dans une procédure spécifique [MAR-P-02].

[6] *Computer Emergency Response Team* ; Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatique.

Chapitre 9
Surveillance et continuité de l'assurance

Le certificat atteste, au moment de sa signature, de la conformité d'un produit ou d'un système aux exigences listées dans sa cible de sécurité. Pour prolonger la confiance dans cette conformité ou faciliter la prise en compte des évolutions d'un produit précédemment certifié, le centre de certification propose des programmes de surveillance et de continuité de l'assurance.

9.1. Surveillance

Le centre de certification propose un programme de surveillance des certificats qui consiste à effectuer un suivi du produit pour maintenir la confiance dans le certificat émis conformément à la procédure [CC-SUR-P-01].

Ce suivi, laissé à l'initiative du commanditaire, consiste à réaliser régulièrement (la période est définie par le commanditaire) des travaux de mise à jour de l'analyse de vulnérabilité du produit certifié et à effectuer d'éventuels tests de pénétration. Le centre de certification peut publier les résultats de la surveillance des produits sur le site de l'ANSSI à la demande des commanditaires. Ces publications conditionnent les dates de validité des certificats des produits et l'archivage des certificats.

9.2. Continuité de l'assurance

Un certificat s'applique uniquement à la version et à la configuration évaluée du produit. Or, il est probable que le produit, son environnement de développement ou de production soient amenés à évoluer.

Le commanditaire peut alors demander un avis sur les nouvelles versions du produit dans le cadre de la « continuité de l'assurance » conformément aux procédures [CC-MAI-P-01] et [CSPN-MAI-P-01]. Le rapport produit par l'organisme de certification dans le cadre de cette procédure ne se substitue pas à une réévaluation ou à une surveillance de la nouvelle version du produit qui seule permet de maintenir le niveau de confiance dans le temps.

9.3. Réduction de portée d'un certificat CC

Au cours de la vie d'un produit certifié de nouvelles attaques qui impactent la sécurité d'une partie des fonctions du produit sans en affecter d'autres peuvent apparaître.

Pour faire face à ce genre de situation, l'approche classique, recommandée par l'ANSSI, consiste à corriger le produit afin de parer aux vulnérabilités exploitées par ces nouvelles attaques. Une réévaluation du produit est alors nécessaire afin de vérifier que les modifications apportées sont efficaces et qu'elles n'impactent pas les autres fonctions de sécurité du produit voir [CC-MAI-P-01].

Cependant une telle approche n'est pas toujours compatible avec les contraintes de coût et de délai des commanditaires des évaluations CC. Ainsi le centre de certification propose une démarche de réduction de portée d'un certificat CC permettant, à faible coût et dans un délai réduit, l'édition d'une mise jour d'un certificat [CC-NOTE-25].

Chapitre 10
Confidentialité des informations traitées

10.1. Accès aux locaux

Le centre de certification dispose du même niveau de sécurité que celui appliqué au Secrétariat général de la défense et de la sécurité nationale ; il bénéficie donc des mesures de protection et de sécurité élevées de ce dernier.

10.2. Confidentialité de l'information

L'ensemble des personnes impliqué dans les dossiers de certification est habilité ou en cours d'habilitation. Il s'engage également par écrit à respecter la confidentialité des informations échangées dans le cadre du schéma d'évaluation et de certification de la sécurité des technologies de l'information.

Le personnel de l'organisme de certification traite également avec le même soin de confidentialité toute information relative à un client obtenue par d'autres sources.

Toutefois, en cas de procédure de justice, l'organisme de certification peut être amené à fournir des informations confidentielles sans que l'aval du client ait été demandé. Dans la mesure du possible, le client sera informé de cette mise à disposition.

10.3. Accès aux informations

Les informations échangées pendant l'évaluation présentent le plus souvent un caractère sensible. Le centre de certification traite ces informations selon des règles de protection adéquates.

Dans le cadre de l'agrément, le centre de certification s'assure que les centres d'évaluation appliquent des règles similaires pour la gestion des informations sensibles qu'ils traitent.

Le personnel de l'organisme de certification a accès à l'ensemble des documents clients. D'autres intervenants peuvent également avoir accès à certains documents « client » concernant le produit en cours d'évaluation ou certifié. Il s'agit notamment :

- des experts techniques de l'ANSSI ayant signé les engagements de confidentialité de la certification ;
- du personnel du « Bureau Qualification et Agrément » de l'ANSSI si une demande de qualification du produit a été demandée par le commanditaire ou le développeur ;
- des membres de la hiérarchie impliqués dans la revue des rapports techniques et certificats ;
- du directeur général de l'ANSSI ou son adjoint;
- de l'Opérateur des Systèmes d'Information Interministériels Classifiés (OSIIC) pour assurer les enregistrements et sauvegardes des dossiers.

10.4. Enregistrement et durée de conservation

Tous les documents et fournitures utilisés durant l'évaluation sont enregistrés et conservés avec des exigences fortes de confidentialité [SECU-P-01].

Chapitre 11
Anomalies : plaintes, appels et écarts

11.1. Auprès du centre de certification

11.1.1. Enregistrement et traitement

Le centre de certification conserve un enregistrement des anomalies en matière de certification afin de prendre les mesures qui s'imposent et agir sur la cause et les facteurs précurseurs ou prédisposant conformément à la procédure [ANO-P-01].

11.1.2. Litiges

Le Comité directeur de la certification examine, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le décret 2002-535 modifié qui lui est soumis par les parties.

11.2. Auprès des commanditaires

Le centre de certification exige pour les objets certifiés que le commanditaire l'avise de toute plainte portée à sa connaissance à propos de la conformité de l'objet aux exigences listées dans la cible de sécurité correspondante.

Chapitre 12
Mesures dérogatoires

Dans le cas où le centre de certification serait amené, dans des circonstances exceptionnelles, à déroger aux règles préconisées dans son processus qualité, le centre de certification ne pourra prendre aucune mesure dérogatoire sans avoir évalué au préalable les risques encourus par une telle décision, notamment ceux ayant attrait à l'impartialité. Dans ce dernier cas, les risques éventuels seront tracés dans l'analyse de risques (voir §3.3.2).

Annexe A
Documents de référence

Textes réglementaires

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, version consolidée au 9 novembre 2019.
Arrêté du 1er avril 2014 portant délégation de signature (secrétariat général de la défense et de la sécurité nationale).

Décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », version consolidée au 1er juillet 2020	
IGI 1300	Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 13 novembre 2020 sur la protection du secret de la défense nationale

Textes relatifs à l'accréditation

EN ISO/IEC 17065	Exigences pour les organismes certifiant les produits, les procédés et les services.
CPS-Ref-02	Critères d'accréditation concernant les organismes de certification procédant à la certification de produits et de services, révision 01, novembre 2002.
EN ISO/IEC 17025	Exigences générales concernant la compétence des laboratoires d'étalonnage et d'essais.
CERT-REF-04	Recueil des notes de doctrines

Accords de reconnaissance

CCRA	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, CCRA Management Committee.*
SOG-IS	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOG-IS Management Committee.*
BSZ_CSPN	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed-time certification process, BSI/ANSSI.*

Critères d'évaluation

ITSEC	Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC).
ITSEM	Manuel d'évaluation de la sécurité des technologies de l'information (ITSEM).
CC	*Common Criteria for Information Technology Security Evaluation.*
CEM	*Common Methodology for Information Technology Security Evaluation*.
CSPN	Certification de Sécurité de Premier Niveau

Références

[SECU-P-01]	Gestion de la confidentialité au centre de certification CCN, ANSSI-CC-SECU-P-01, version en vigueur.
[QUA-P-02]	Dispositif de préservation de l'impartialité, ANSSI-CCN- QUA-P-02, version en vigueur.
[CC-CER-P-01]	Certification Critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI-CC-CER-P-01, version en vigueur.
[CSPN-CER-P-01]	Certification de sécurité de premier niveau des produits des technologies de l'information, ANSSI-CCN-MQ, version en vigueur.
[CC-AGR-P-01]	Agrément des centres d'évaluation, ANSSI-CC-AGR-P-01, version en vigueur.
[CSPN-AGR-P-01]	Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau, ANSSI-CCN-MQ, version en vigueur.
[DOC-P-01]	Elaboration et mise à jour de la documentation du système qualité du centre de certification, ANSSI-CSPN-AGR-P-01, version en vigueur.
[MOD-P-01]	Modification des exigences de certification, ANSSI-CC-MOD-P-01, version en vigueur.
[QUA-P-01]	Revues de direction, ANSSI-CC-QUA-P-01, version en vigueur.
[QUA-P-03]	Audits Internes, ANSSI-CC-QUA-P-031, version en vigueur.
[ANO-P-01]	Traitement des anomalies, ANSSI-CC-ANO-P-01, version en vigueur.
[MAR-P-01]	Utilisation de la marque « TI Sécurité Certification », ANSSI-CC-MAR-P-01, version en vigueur.
[MAR-P-02]	Utilisation des logotypes du CCRA et du SOGIS, ANSSI- MAR-P-02, version en vigueur.
[PER]	Recrutement et qualification du personnel, ANSSI-CC-PER-P-01, version en vigueur.
[CC-SUR-P-01]	Surveillance des produits certifies, ANSSI-CC-SUR-P-01, version en vigueur.
[CC-MAI-P-01]	Continuité de l'assurance, ANSSI-CC-MAI-P-01, version en vigueur.
[CSPN-MAI-P-01]	Maintien de la confiance, continuité de l'assurance, ANSSI-CSPN-MAI-P-01, version en vigueur.
[CC-NOTE-25]	Réduction de portée d'un certificat CC, ANSSI-CCN-NOTE-25, version en vigueur.

Annexe B
Définitions et acronymes

Définitions

Centre de certification national	Bureau de l'ANSSI dont les membres instruisent les dossiers de certification.
Centre d'évaluation	Organisme accrédité selon le référentiel EN ISO/IEC 17025 et agréé par le centre de certification pour conduire des évaluations de la sécurité en vue d'une certification dans le cadre du décret 2002-535 modifié.
Certificateur	Personnel du centre de certification chargé de l'instruction des dossiers de certification.
Certificat	Il atteste que l'exemplaire d'un produit ou d'un système répond aux exigences de sécurité spécifiées dans sa cible de sécurité. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8 du décret 2002-535 modifié).
Certification	Action de fournir l'assurance de conformité à des normes et autres documents normatifs.
Commanditaire	Personne ou organisme qui demande l'évaluation en vue de la certification.
Comité directeur de la certification	Comité directeur de la certification en sécurité des technologies de l'information défini par le Chapitre III du décret 2002-535 modifié.
Cible de sécurité	Ensemble d'exigences de sécurité constituant le référentiel de certification pour les évaluations ITSEC, Critères communs, Certification de sécurité de premier niveau.
Organisme de certification	Autre dénomination du centre de certification national.

Acronymes et abréviations

SGDSN	Secrétariat général de la défense et de la sureté nationale
ANSSI	Agence nationale de la sécurité des systèmes d'information
SOG-IS	Senior Officer Group Information Security
RTE	Rapport technique d'évaluation
CC	Critères communs
CSPN	Certification de sécurité de premier niveau