Exigences spécifiques pour l'accréditation des organismes procédant à la certification de cybersécurité des technologies de l'information et des communications

CERT CPS REF 48 - Révision 03

SOMMAIRE

1. OBJET

Ce document définit les exigences à satisfaire et le processus d'accréditation pour la certification de cybersécurité des technologies de l'information et des communications suivant le Règlement (UE) 2019/881 du parlement européen et du conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), dit Cyber Act.

2. REFERENCES ET DEFINITIONS

2.1. Textes de références

Ce document s'applique en complément des documents suivants :

2.1.1. Publication de l'ISO

- NF EN ISO/IEC 17065 : 2012 « Évaluation de la conformité — Exigences pour les organismes certifiant les produits, les procédés et les services »

2.1.2. Autres textes de référence

- Règlement (UE) 2019/881 du parlement européen et du conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), dit Cyber Act
- Règlement d'exécution (UE) 2024/482 de la commission du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC)
- EUCC scheme state-of-art document / Accreditation of the certification body, Version 1.6a, June 2024

  (disponible sur EUCC accreditation requirements for CB activities. (europa.eu))
- ISO/IEC 15408-1:2022, Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 1: Introduction et modèle général
- ISO/IEC 15408-2:2022, Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 2: Composants fonctionnels de sécurité
- ISO/IEC 15408-3:2022, Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 3: Composants d'assurance de sécurité
- ISO/IEC 15408-4:2022, Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes

- ISO/IEC 15408-5:2022, Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 5: Paquets prédéfinis d'exigences de sécurité
- ISO/IEC 18045:2022 - Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité
- Décret n° 2002 – 535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. Le référentiel ANSSI-PG-083 - Guides des mécanismes cryptographiques (document disponible auprès de l'ANSSI)
- Les notes spécifiques au schéma français : voir « notes d'application » : https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/procedures-et-formulaires/

2.2. Abréviations et définitions

Cofrac : Comité Français d'Accréditation
OC : organismes de certification
ANSSI : Agence National de la Sécurité des Systèmes d'Information
CSA : Cyber Act
SoA document : EUCC scheme state-of-art document / Accreditation of the certification body

3. DOMAINE D'APPLICATION

Ce document s'applique à tous les candidats à l'accréditation et aux organismes accrédités pour la certification de cybersécurité des technologies de l'information et des communications suivant le CYBER ACT pour les niveaux substantiels et élevés.

4. MODALITES D'APPLICATION

Ce document est applicable à compter du 01/11/2025.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Les modifications de fond sont marquées par un trait vertical dans la marge gauche.
Elles concernent l'adaptation du vocabulaire et des modalités d'évaluation par suite de l'évolution des règlements d'accréditation (CERT REF 05, GEN REF 06 et CERT REF 60).

6. EXIGENCES ET REGLES A SATISFAIRE PAR L'ORGANISME DE CERTIFICATION

Il appartient à tout organisme candidat ou accrédité d'appliquer les versions à jour des documents de référence cités au §2 et de prendre en compte la réglementation applicable en vigueur.

Dans la suite du document, seules les exigences spécifiques à ce domaine ont été indiquées, étant entendu que les exigences générales des référentiels d'accréditation et procédures en vigueur s'appliquent.

Ces exigences sont rapportées dans le tableau de correspondance ci-dessous au regard du paragraphe de la norme NF EN ISO/IEC 17065 qu'elles spécifient.

Objet	Norme ISO/IEC 17065 :2012	Règlement d'exécution 2024/482 de la commission du 31/01/2024	EUCC scheme state of arts documents – Accreditation of the certification body – V1.6a, June 2024
Responsabilité juridique	4.1.1		8.1 et annexe du CSA
Gestion de l'impartialité	4.2		8.1 et annexe du CSA 8.2
Responsabilités	4.3		8.1 et annexe du CSA
Non-discrimination	4.4		8.1
Confidentialité	4.5	Articles 42 et 43	8.1 et annexe du CSA
Impartialité	5.2		8.1
Compétences et ressources	6.1 et 6.2		8.1 et annexe du CSA 8.2 Annexe
Demande	7.2	Article 8	8.1 et annexe du CSA
Revue de la demande	7.3		8.1
Evaluation et certification	7.4 à 7.7	Chapitre 3	
Rapport de certification	7.4	Annexe 5	
Evaluation pour le niveau « élevé »	7.4	Article 21	
Documents de certification	7.7	Article 9 Article 10 Article 12 Annexe 7	
Surveillance	7.9	Article 13 Annexe 4 Article 26 Articles 28 et 29	
Suspension de la certification	7.11	Article 30	
Retrait de la certification	7.11	Article 14	
Maitrise des enregistrements	8.4	Article 40	

Ce tableau est une aide à la compréhension de l'interaction des différentes exigences applicables aux OC mais ne constitue pas une liste exhaustive et reste à valeur indicative.

7. PROCESSUS D'ACCREDITATION

Le processus d'accréditation décrit dans les règlements d'accréditation CERT REF 05, GEN REF 06 et CERT REF 60 s'applique, avec les précisions et spécificités décrites dans les paragraphes suivants.

7.1. Généralités

Les activités de certification objet du présent document constituent un domaine d'accréditation.

7.2. Portée d'accréditation demandée

La portée de demande d'accréditation est établie selon les documents de nomenclature CERT CPS INF 02.

La portée d'accréditation doit correspondre :

- Pour les catégories de produits 'Logiciels et équipements réseau', 'Cartes à puce et dispositifs similaires' et 'Equipements matériels avec boîtiers sécurisés' :
    - Au minimum au niveau EAL 3 tel que défini dans la norme ISO/IEC 15408-5, pour un organisme visant une accréditation pour le niveau d'assurance Substantiel ;
    - Au minimum au niveau EAL 3 augmenté du composant AVA_VAN.3 tels que définis dans les normes ISO/IEC 15408-3 et ISO/IEC 15408-5, pour un organisme visant une accréditation pour le niveau d'assurance Elevé ;

  Les composants d'assurance de sécurité doivent être détaillés par l'organisme conformément aux normes ISO/IEC 15408 applicables.
- Pour les Profils de protection : selon l'ensemble des composants d'assurance de sécurité des classes APE et ACE tels que définis dans la norme ISO/IEC 15408-3.

La portée d'accréditation délivrée par le Cofrac est considérée comme étant en portée flexible de type FLEX 2 et doit être gérée par l'OC conformément au document CERT REF 08, et n'est donc pas détaillée.

Il revient donc à l'OC de tenir à jour sa portée détaillée, en cohérence avec les libellés des certificats émis et la portée minimale associée au niveau d'assurance revendiqué, et qui doit comprendre, pour chaque catégorie de produits concernée, les composants d'assurance de sécurité revendiqués (soit sous la forme d'une liste exhaustive, soit sous la forme d'un niveau EAL et ses éventuelles augmentations tel que prévu par la norme ISO/IEC 15408-5).

7.3. Modalités d'évaluation

7.3.1 Modalités de démarrage

En accord avec le §8.3 du *SoA document*, les organismes de certification ayant obtenu la recevabilité opérationnelle de leur demande d'accréditation pour la certification selon le Cyber Act sont autorisés à démarrer le processus de certification et prendre des décisions de certification mais ne pourront en revanche émettre de certificats qu'une fois l'accréditation obtenue.

7.3.2 Modalités de candidature et évaluation initiale

Toute demande d'accréditation pour la délivrance de la certification de la sécurité offerte par les produits, les systèmes ou les profils de protection (dans le domaine des technologies de l'information) est traitée comme une demande d'accréditation initiale (si l'organisme n'est pas accrédité selon l'ISO/IEC 17065) ou d'extension de la portée d'accréditation à un nouveau domaine technique (si l'organisme est accrédité selon l'ISO.IEC 17065 pour des activités autres que celles objets du présent document). L'évaluation inclut des examens de traçabilité dossiers et d'une observation d'activité.

Lorsqu'un organisme demande une accréditation pour le niveau « Elevé », il doit avoir au préalable déposé une demande d'autorisation auprès de l'ANSSI.

Toute demande d'un organisme déjà accrédité pour la certification de profils de protection et souhaitant étendre sa portée à une ou plusieurs catégories de produit est considérée comme une extension à un nouveau domaine technique, dont l'évaluation inclut à minima des examens de traçabilité dossiers et une observation d'activité.

Toute demande d'un organisme déjà accrédité pour la certification d'une catégorie produit selon le présent document et souhaitant étendre sa portée à une autre catégorie de produit ou aux profils de protection est considérée comme une extension au sein d'un domaine technique déjà accrédité, dont l'évaluation inclut à minima une évaluation documentaire.

Les technologies et les types d'évaluation listés dans l'annexe au *SoA document* dans lesquels l'OC a prouvé sa compétence technique sont détaillés dans le rapport d'évaluation.

7.3.3 Evaluations périodiques

Le domaine technique est évalué à chaque évaluation périodique.

Lors de chaque évaluation, il est réalisé une observation d'une activité de certification, dont la nature est fonction du processus de certification (un audit, l'activité d'un sous-traitant entrant dans de la portée d'accréditation, l'audit d'un CESTI, une instance de décision), sauf si les procédures d'évaluation de la conformité sont basées sur un examen de dossiers. Dans ce dernier cas, l'observation n'est pas réalisée et est remplacée par un entretien avec les personnes en charge de l'examen de dossiers, qui est intégré dans l'évaluation du siège de l'OC.
Dans la mesure du possible et si applicable, chaque observation concerne une catégorie de produit différente de manière à couvrir sur un cycle d'accréditation les différentes catégories entrant dans la portée accréditée.

7.4. Attestation d'accréditation

L'attestation d'accréditation délivrée est établie selon le document de nomenclature CERT CPS INF 02.

7.5. Confidentialité – Echange d'informations

Le Cofrac informe l'ANSSI, dans les plus brefs délais, de la mesure d'octroi, d'extension, de suspension, de résiliation ou de retrait (total ou partiel) d'accréditation et de son motif.

Au titre du §1.1 du *SoA document*, le Cofrac peut transmettre les rapports d'évaluation à l'ANSSI si celle-ci en fait la demande.

L'OC doit informer sans délai le Cofrac si son autorisation délivrée par l'autorité nationale relative aux certifications de la sécurité offerte par les produits, les systèmes ou les profils de protection est suspendue, retirée, résiliée ou non renouvelée (partiellement ou totalement). Le Cofrac analysera ensuite si l'accréditation correspondante est remise en cause.
De même, si le Cofrac reçoit des informations de la part de l'ANSSI concernant les OC accrédités pour ce domaine, les mêmes interlocuteurs seront informés de leur traitement. Toute information transmise par ces autorités sera considérée comme une donnée d'entrée du suivi de l'accréditation.

7.6. Dispositions à prendre en cas de suspension, de retrait d'accréditation ou de cessation d'activité de l'organisme certificateur

Les dispositions suivantes s'appliquent en complément de la procédure GEN PROC 03.

Le Cofrac informe sans délai l'ANSSI de toute mesure de suspension, de résiliation ou de retrait d'accréditation d'un organisme certificateur.

7.6.1 Dispositions à prendre en cas de suspension d'accréditation

Les actions à mettre en œuvre par l'organisme concernant les certificats en vigueur émis sous accréditation sont établies au cas par cas en fonction de la raison de la suspension et sont indiquées dans le courrier de notification de suspension.

7.6.2 Dispositions à prendre en cas de retrait de l'accréditation ou de cessation d'activité d'un organisme certificateur.

7.6.2.1 Retrait d'accréditation d'un organisme certificateur

L'organisme n'est plus autorisé à délivrer de certificats ni à maintenir les certificats existants. Il doit informer les clients concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue.

Ce dernier doit alors demander à l'organisme de certification ayant délivré le certificat en cours de validité de lui adresser le dossier du client (suivi de projet et documents émis ou rédigés par l'OC, non conformités en suspens, plaintes reçues et suites données). Il peut également demander au client tous compléments d'informations nécessaires conformément au processus de certification sollicité.

Au cas où l'OC « repreneur » serait dans l'impossibilité de se procurer le dossier du client auprès de l'organisme précédent, la demande de l'entreprise serait traitée comme une certification initiale en appliquant les procédures correspondantes.
Dans tous les cas, il revient à l'organisme certificateur « repreneur » d'évaluer les éléments fournis et d'établir si le cycle de certification peut être repris à l'identique.

7.6.2.2 Cessation d'activité d'un organisme certificateur

L'organisme certificateur doit informer les clients concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue, dans les conditions énoncées au § 7.6.2.1.

8. MODALITES FINANCIERES

Les modalités énoncées dans les documents CERT REF 06 et CERT REF 07 s'appliquent, en considérant les activités de certification objet du présent document comme un domaine technique d'accréditation.