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 12 Juillet 2024

N° 1239 /**ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-NOTE-29_v1.1**

NOTE D'APPLICATION

TRANSPOSITION DES NORMES CC:2022 ET CEM:2022 DANS LE SCHEMA FRANÇAIS DE CERTIFICATION DE LA SECURITE

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	12 Mars 2024	Création du document
1.1	12 Juillet 2024	Ajout et correction de certaines typos

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

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

La présente note est disponible en ligne sur le site institutionnel de l'ANSSI (www.cyber.gouv.fr).

TABLE DES MATIERES

1 Objet de la note

La présente note d'application rappelle et complète les règles pour la transition des CC v3.1 [CC v3.1] et CEM V3.1 [CEM v3.1] vers les CC :2022 [CC:2022] et CEM:2022 [CEM:2022] qui ont été publiés par le *Common Criteria Recognition Arrangement* (CCRA) en novembre 2022. Cela comprend les règles établies par le *CC Management Committee* (CCMC) et les règles spécifiques au schéma français, présentées dans les sections 2 et 3 respectivement.

2 Règles CCRA

Les règles de certification de produits et de profils de protection (PP) éditées par le CCMC dans le cadre du CCRA pour la transition des CC v3.1 et CEM V3.1 vers les CC:2022 et CEM:2022, s'appliquent dans le schéma français (voir [CCMC Transition policy]). Ces règles sont applicables aux accords de reconnaissance [CCRA] et [SOG-IS].

Pour la certification de produits le tableau de compatibilité des versions et les conditions d'applicabilité sont les suivants dans le schéma français :

Produit à certifier (date de fin ou de démarrage de la période d'applicabilité)	**Conforme à un PP/PP-Configuration**		**Réutilisation des résultats d'une évaluation ALC**		**Certificat de plateforme/composant de base** (pour une évaluation composite)	
	CC v3.1	**CC:2022**	**CC v3.1**	**CC:2022**	**CC v3.1**	**CC:2022**
En CC v3.1 (demande de certification initiale reçue au plus tard le 30 juin 2024 ou demande de ré-évaluation /maintenance reçue après le 30 juin 2024 et au plus tard 2 ans après la date d'émission du certificat initial)	**Oui**	**Non**	**Oui**	**Oui** (mais uniquement pour une re-évaluation /maintenance du même produit)	**Oui**	**Oui** (mais uniquement si la certification de la plateforme ne repose pas sur des concepts hors CC v3.1, e.g. multi-assurance, qui n'ont pas été déjà établis dans des *Supporting Documents*)
En CC:2022 (dès publication de la présente note)	**Oui** (demande reçue au plus tard le 31 décembre 2027)	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**

Concernant les PP conformes aux CC v3.1, la recommandation consiste à les actualiser dès que possible pour les rendre conformes aux CC:2022, ainsi que les PP-Modules et PP-Configurations associés.

3 Règles spécifiques au schéma français

3.1 Utilisation de méthodes d'évaluation *ad-hoc*

Le projet d'utilisation de méthodes d'évaluation non approuvées par les accords de reconnaissance du CCRA ou du SOG-IS ou non approuvées par le schéma français dans le cadre d'une certification de produit, ou d'une certification de profil de protection (PP), doit faire l'objet d'une déclaration dans le formulaire de demande d'enregistrement de l'évaluation[1].

L'utilisation de méthodes d'évaluation non approuvées par les accords de reconnaissance CCRA ou SOG-IS[2] ou par le schéma français, proposées par le commanditaire, est strictement encadrée et décidée au cas par cas. L'utilisation de ces méthodes n'est autorisée que dans le cas où le schéma a accès à l'ensemble des éléments de définition. Elles ne pourront être utilisées que dans le cadre d'évaluations pilote, qui pourraient imposer des évolutions de ces méthodes. Si le centre de certification ne se satisfait pas des méthodes produites, le projet d'évaluation pourrait être déclaré « abandonné » par le centre de certification et ne pas donner lieu à l'édition d'un certificat.

Si le centre de certification valide la méthode d'évaluation proposée, une publication sera réalisée sur le site web de l'ANSSI. Cela s'applique par exemple aux méthodes d'évaluation définies ou référencées dans des profils de protection et dans des cibles de sécurité. A noter que cela concerne tout type de méthode y compris les méthodes conformes aux règles définies dans [CC:2022] *Part 4*, mais sans limitation.

De plus, la certification d'un PP dans le schéma français, si elle a lieu, entrainerait *de facto* la validation de la méthode. L'ANSSI se réserve le droit de ne prononcer la certification d'un tel PP qu'à la suite d'une évaluation de produit pilote en utilisant la méthode d'évaluation *ad-hoc*.

3.2 Usage de PP rédigé en CC v3.1 en évaluation de produit CC:2022

Dans le cadre d'une évaluation de produit conforme aux CC:2022 s'appuyant sur un PP conforme aux CC v3.1, le centre de certification attend du CESTI qu'il traite dans son rapport d'évaluation la pertinence de la transposition du contenu du PP en CC v3.1 dans la cible de sécurité CC:2022 proposée par le commanditaire.

Dans le cadre de la réévaluation d'un PP où la modification traite uniquement de la transposition en CC:2022, à titre exceptionnel, celle-ci pourra être menée par un CESTI n'étant pas intervenu dans l'évaluation initiale effectuée par un centre de certification (France ou homologue). Les exigences non impactées par la transposition pourront alors être considérées positionnées à « Réussite », même si le CESTI réalisant les travaux n'a pas accès aux résultats précédents.

3.3 Usage de SD rédigé en CC v3.1 en évaluation de produit CC:2022

Tant que l'ensemble des documents supports (SD) des accords de reconnaissance [CCRA] et [SOG-IS] et les notes du schéma français n'ont pas tous été transposés en CC:2022, les CESTI sont autorisés à utiliser les versions CC v3.1 de ces documents. Si une clarification s'avère nécessaire, la demande devra être soumise au centre de certification.

3.4 Évaluation formelle (ADV_SPM.1)

Les règles du schéma français pour ce type d'évaluation en CC v3.1 sont définies dans la [NOTE12].

[1] A préciser dans la partie « Méthodes spécifiques à l'évaluation de l'objet / *Evaluation specific methods of the target* » du formulaire de demande d'évaluation [CER-F-01].

[2] La certification d'un PP comportant des méthodes d'évaluation spécifiques par un centre de certification homologué n'est pas équivalente à l'approbation de la méthode d'évaluation par un accord de reconnaissance.

Pour les évaluations de ce type en CC:2022, le schéma français s'appuie sur la note d'interprétation [JIL Note SPM].

3.5 Évaluation de « *random bit generation* »

Les [CC:2022] *Part 2* introduisent un nouveau composant fonctionnel FCS_RBG qui sert à spécifier les caractéristiques de la génération de bits aléatoires. Dans le schéma français, l'évaluation de tels mécanismes ne se limite pas aux travaux décrits dans la norme mais est assujettie aux modalités d'évaluation définies dans la procédure [CRY-P-01].

3.6 Agrément des CESTI

Dans le schéma français, l'extension de l'accréditation des CESTI aux CC:2022 et CEM:2022 est gérée au moyen de la portée flexible COFRAC FLEX3. Les CESTI ayant officialisé leur extension d'accréditation aux CC:2022 et CEM:2022 devront en informer le centre de certification pour que soit prononcée une extension d'agrément.

4 Retours

Les CESTI et les utilisateurs du schéma français peuvent contacter l'ANSSI pour toute question relative à l'application des CC:2022 et CEM:2022, ils sont encouragés à fournir des retours du terrain et à communiquer toute ambiguïté ou difficulté dans l'application des nouvelles normes.

Ces communications doivent être transmises à certification[at]ssi.gouv.fr.

ANNEXE A. Références

Référence	Document
[Décret 2022-535]	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.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security*, mai 2002.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, janvier 2010, *Management Committee of Agreement Group*.
[CCMC Transition policy]	*Transition policy to CC:2022 and CEM:2022*, référence CCMC-2023-04-001, 20 avril 2023. https://www.commoncriteriaportal.org/files/ccfiles/CC2022CEM2022TransitionPolicy.pdf
[CC v3.1]	*Common Criteria for Information Technology Security Evaluation*, version 3.1, révision 5, avril 2017 : - *Part 1: Introduction and general model*, référence CCMB-2017-04-001 ; - *Part 2: Security functional components*, référence CCMB -2017-04-002 ; - *Part 3: Security assurance components*, référence CCMB-2017-04-003.
[CEM v3.1]	*Common Methodology for Information Technology Security Evaluation* : *Evaluation methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CC:2022]	*Common Criteria for Information Technology Security Evaluation*, CC:2022, révision 1, novembre 2022 : - *Part 1: Introduction and general model*, référence CCMB-2022-11-001 ; - *Part 2: Security functional components*, référence CCMB-2022-11-002 ; - *Part 3: Security assurance components*, référence CCMB-2022-11-003 ; - *Part 4: Framework for the specification of evaluation methods and activities*, référence CCMB-2022-11-004 ; - *Part 5: Pre-defined packages of security requirements*, référence CCMB-2022-11-005. **Documents respectivement équivalents aux normes ISO/IEC 15408-1:2022, 15408-2:2022, 15408-3:2022, 15408-4:2022 et 15408-5:2022.**
[CEM:2022]	*Common Methodology for Information Technology Security Evaluation - Evaluation methodology*, CEM:2022, Revision 1, novembre 2022, référence CCMB-2022-11-006. **Document équivalent à la norme ISO/IEC 18045:2022.**
[NOTE12]	Note d'application, *Modélisation formelle des politiques de sécurité d'une cible d'évaluation*, version en vigueur.
[JIL Note SPM]	*Joint Interpretation Library*, *ADV_SPM.1 interpretation for [CC:2022] transition*, version en vigueur.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version en vigueur.

[CER-F-01]	Dossier d'évaluation, référence ANSSI-CC-CER-F-01, version en vigueur.

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