EUCC : le « Common Criteria » européen qui change d'échelle

Sébastien VIOU
Field Cyber-security Strategist
Fortinet

La certification cybersécurité européenne entre dans une phase opérationnelle.

Après la création du cadre européen de certification (*European Cybersecurity Certification Framework*-ECCF) par le Cybersecurity Act (2019), la proposition « Cybersecurity Act 2 » (janvier 2026) vise à accélérer et industrialiser l'adoption et la maintenance des schémas, tout en faisant de la certification un outil concret de simplification de la conformité réglementaire. (5)

Dans ce contexte, l'EUCC (EU Common Criteria) est un jalon majeur : c'est le premier schéma européen adopté par règlement d'exécution (UE) 2024/482. Basé sur une démarche volontaire, il permet de certifier des produits TIC (*Technologies de l'information et de la communication*, une terminologie que l'on retrouve aussi dans d'autres textes, comme DORA) : composants, matériels et logiciels, selon un processus d'évaluation compris et partagé à l'échelle de l'UE. (1)

Common Criteria et EUCC : continuité méthodologique, gouvernance européenne

Ne nous y trompons pas, EUCC n'abandonne pas les Common Criteria, il les européanise. Le règlement 2024/482 rappelle que la certification s'appuie sur les Common Criteria et la méthodologie d'évaluation associée, et décrit le cœur du mécanisme : le produit est évalué contre une cible de sécurité (*security target*) et, si pertinent, contre des profils de protection (*protection profiles*) qui standardisent les exigences pour une catégorie de produits. (2)

La vraie rupture est organisationnelle : un référentiel unique, une bibliothèque de documents de références (guides, état de l'art…), et une publication harmonisée et centralisée des certificats sur le portail ENISA, ce qui facilite comparaison et audit. (3)

EUCC définit deux niveaux d'assurance « substantial » et « high » et les rattache explicitement à la famille Common Criteria AVA_VAN (analyse de vulnérabilités / résistance aux attaques). Le règlement précise qu'un certificat EUCC « substantial » correspond à une évaluation couvrant AVA_VAN.1 ou AVA_VAN.2, tandis qu'un certificat "high" couvre AVA_VAN.3, AVA_VAN.4 ou AVA_VAN.5. Cette approche rend le niveau d'assurance plus lisible pour les acheteurs, en liant directement l'étiquette à la profondeur de l'analyse de vulnérabilités, tout en conservant la méthodologie Common Criteria. (1)

Ce que l'EUCC change par rapport à SOG-IS

Avant EUCC, de nombreux pays européens s'appuyaient sur l'accord de reconnaissance mutuel

SOG-IS MRA pour reconnaître les certificats CC entre états signataires. Mais la reconnaissance n'était pas uniformément « haute assurance » : elle dépendait de domaines techniques (exemples : microcontrôleurs/cartes à puce, équipements avec boîtiers sécurisés) et, hors de ces domaines, la reconnaissance se limitait typiquement à **EAL4** (et EAL2 pour la reconnaissance internationale CCRA). (4)

EUCC est explicitement conçu comme son successeur : il est construit à partir de SOG-IS (procédures et documents), afin d'assurer une transition fluide, tout en remplaçant progressivement les schémas nationaux applicables à SOG-IS.

L'ENISA indique clairement qu'« *à terme, l'EUCC remplacera les systèmes de certification nationaux qui relevaient auparavant de l'accord SOG-IS.* » (3)

En pratique, trois impacts structurants :

- **Reconnaissance à toute l'UE** : l'objectif n'est plus la reconnaissance entre pairs d'un club restreint, mais un schéma européen unique pensé pour être utilisable dans tout le marché intérieur. (1)
- **Harmonisation "haute"** : au niveau élevé, le schéma renforce l'homogénéité via des exigences additionnelles (autorisation des organismes, et mécanismes de *peer assessment*). (2)
- **Transparence** : publication des certificats et des documents de support au niveau européen, ce qui réduit les interprétations "locales" et simplifie la lecture côté clients/acheteurs. (3)

Quels Impacts pour les entreprises qui veulent certifier leurs produits

Pour un industriel, EUCC implique une grande rigueur de développement et de suivi du produit mais il offre aussi un levier de marché.

Un parcours de certification mieux standardisé

EUCC structure clairement la chaîne d'évaluation : un laboratoire (**ITSEF**) réalise les activités d'évaluation, et un organisme de certification prend la décision. Les organismes doivent être accrédités ; pour le niveau **high**, des exigences complémentaires s'appliquent (dont une autorisation par l'autorité nationale) afin de garantir la compétence de l'évaluateur et la protection des informations sensibles. (2)

Une certification vivante dans le temps

EUCC ne se limite pas à passer un audit sur une version figée. Pendant la validité du certificat, les produits sont soumis à des mécanismes de surveillance et de gestion/divulgation de vulnérabilités.
Pour les éditeurs, cela se traduit par des exigences d'industrialisation : processus de gestion des vulnérabilités, traçabilité, correctifs, et capacité à documenter l'impact sécurité dans la durée. En particulier, EUCC introduit la notion de « patch management certifié » et c'est un point qui corrige une des failles du CC qui fige la version certifiée. (1)

Transition depuis SOG-IS : migration et continuité

Le déploiement inclut une période de transition et des possibilités de conversion de certificats SOG-IS vers EUCC, sous réserve d'évaluer les exigences ajoutées ou mises à jour. Pour la France, l'ANSSI précise aussi le calendrier de bascule et le rôle renforcé de l'autorité nationale pour les certifications de niveau élevé. (3)

Conséquence sur le marché intérieur

Le bénéfice client est plus direct : moins de redondance entre pays, meilleure lisibilité pour les

appels d'offres multi-États, et un langage d'assurance commun entre acheteurs publics, grands comptes et fournisseurs. On peut ajouter à cela une ouverture du marché de la certification à l'Europe avec la mise en concurrence des organismes de certification. (1)

EUCC vs Cyber Resilience Act : redondance ou complémentarité ?

Le **Cyber Resilience Act (CRA)** pose un socle obligatoire d'exigences de cybersécurité et de gestion de vulnérabilités pour les produits avec éléments numériques. EUCC, lui, est basé sur le volontariat, il n'impose pas d'obligation en tant que telle. Il apporte ce que le CRA ne peut fournir : un **niveau d'assurance** et une **évaluation indépendante reconnue**.

Et surtout, l'articulation est désormais conçue pour éviter le double travail : la proposition «Cybersecurity Act 2 » exige que les objectifs et exigences des schémas portant sur les produits soient **cohérents avec les exigences essentielles du CRA (Annexe I)** et vise à faciliter la **présomption de conformité** lorsque la législation le prévoit. Autrement dit, un produit certifié dans un schéma européen pertinent peut, sous conditions, bénéficier d'une voie de conformité plus simple au CRA.

Conclusion

EUCC se veut la continuité des Common Criteria, mais avec une nouvelle ambition : passer d'une reconnaissance fragmentée (SOG-IS) à une certification harmonisée, gouvernée et publiée au niveau UE, et pensée pour s'emboîter dans la pile réglementaire de l'Europe (CRA, NIS2).

Pour les entreprises, le message est le suivant : investir dans l'assurance (substantial/high), la maîtrise du cycle de vie et la preuve documentaire devient une exigence de crédibilité et également un accélérateur d'accès au marché intérieur européen.

Sources :

(1) https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en
(2) https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj/eng
(3) https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme
(4) https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/comprendre-levaluation-de-securite/certification-de-produits/accords-de-reconnaissance-criteres-communs/
(5) CyberSecurity Act v2 proposal