



STORMSHIELD

SOLUTIONS DE SÉCURITÉ QUALIFIÉES

LE CHOIX D'UNE SOLUTION DE CONFIANCE

Julien Paffumi

Product Marketing
Manager - Stormshield

Quelle confiance avez-vous dans la solution de sécurité qui protège votre système d'information ? Une question centrale, mais trop peu souvent posée. Que vous soyez une entreprise ou une administration, vous devez avoir pleine confiance dans la solution chargée de vous protéger. À quoi bon mettre en place un produit de sécurité s'il est peu efficace... ou pire, s'il comporte des portes dérobées mettant vos informations à la portée de personnes externes.

Pour vous accompagner dans votre choix, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) met à disposition un catalogue de solutions porteuses du label « Visa de Sécurité ». Ces solutions sont reconnues par l'État comme fiables et de confiance, après des tests rigoureux et une analyse approfondie sous le contrôle de l'ANSSI.

Ce visa peut se matérialiser, selon le contexte et le besoin, par une certification ou une qualification délivrée par l'ANSSI.

Certification ou qualification, quelle différence ?

On distingue plusieurs types de labellisations : Certification Critères Communs, Certification de Sécurité de Premier Niveau (CSPN), et Qualification, elle-même pouvant être Élémentaire, Standard, ou Renforcée. Dès lors, comment s'y retrouver ?

LA CERTIFICATION

La certification constitue une attestation de **robustesse** du produit de sécurité. L'éditeur définit une « cible de sécurité », décrivant les fonctions de sécurité qui sont évaluées et dans quel contexte d'utilisation. Un laboratoire indépendant accrédité « Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) » réalise l'évaluation des processus de développement du produit et sa résistance face à un niveau d'attaque donné.

La **Certification Critères Communs (CC)** est reconnue et délivrée dans de nombreux pays.

Elle indique jusqu'à quel niveau d'attaque la résistance du produit a été évaluée. Un pare-feu peut par exemple être certifié au niveau EAL3+, EAL4+...



COMMON
CRITERIA



COMMON
CRITERIA

La **Certification de Sécurité de Premier Niveau (CSPN)** a été mise en place par l'ANSSI pour proposer une alternative aux évaluations de Certifications CC, dont le coût et la durée peuvent être un obstacle. Les tests sont effectués en temps et charge contraints (typiquement 2 mois, 25 à 35 jours/homme). Contrairement à la Certification CC qui a une reconnaissance internationale, la CSPN est actuellement une labellisation purement française. L'objectif est cependant qu'elle obtienne une reconnaissance au niveau européen dans le futur.



Attention - Ce que vous ne savez peut-être pas à propos de la certification

- À moins que la Certification ne mène par la suite à une Qualification, l'ANSSI n'intervient pas dans la définition de la cible de sécurité, et ce, même pour les certifications délivrées en France. L'éditeur peut donc dans une certaine mesure adapter la cible à sa convenance et potentiellement exclure de l'évaluation certaines fonctions de sécurité présentes sur le produit.
- Il est donc capital de bien étudier la cible de sécurité choisie par l'éditeur, par rapport à votre besoin de sécurisation : ceci relève de votre responsabilité lorsque vous choisissez la solution de sécurité en question.
- Le rapport de certification peut soulever des réserves ou des recommandations d'usage, à bien étudier par rapport à votre contexte
- Enfin, une certification s'applique à des versions logicielles ou matérielles spécifiques, assurez-vous donc que la certification obtenue ne concerne pas un produit ou une version datant de plusieurs années, qui pourrait ne plus être vendu ou supporté.

LA QUALIFICATION

Au-delà de la simple certification, la qualification constitue une **recommandation** par l'ANSSI et atteste de la **confiance** accordée par l'État français au produit de sécurité et à son éditeur.

Le premier prérequis est d'obtenir une certification de niveau suffisant*, mais avec une **cible de sécurité validée par l'ANSSI**. De plus, au-delà du processus de certification, l'ANSSI réalise des analyses supplémentaires, dont un **audit du code source du produit évalué**.

La qualification d'un produit est reconnue en France, et en Europe dans certains contextes.



Attention - Ce que vous ne savez peut-être pas à propos de la qualification

- L'éditeur n'a pas le droit de communiquer sur sa démarche de qualification tant que son dossier de candidature n'a pas été validé par l'ANSSI, sous peine de briser un accord de non-divulgence.
- L'éditeur reçoit un courrier officiel de l'ANSSI lorsque sa demande est acceptée et que le processus de qualification commence. C'est seulement à partir de ce moment qu'il a l'autorisation de faire la promotion de sa démarche de qualification.
- La prudence est donc de mise si un éditeur affirme être bientôt qualifié, mais n'est pas en mesure de prouver que le processus a débuté en présentant le courrier délivré par l'ANSSI.
- De plus, le processus de qualification prend du temps : au moins un an à partir de l'acceptation par l'ANSSI du dossier de candidature de l'éditeur.



Le label « NATO restricted » / « restreint OTAN »

Sont classifiées « NATO restricted » les informations dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'OTAN ou de certains de ses états membres.

Pour figurer dans le catalogue de solutions habilitées à sécuriser de telles informations, la certification ne suffit pas : le produit doit avoir obtenu la Qualification Standard de la part de l'ANSSI.



Le label « EU restricted » / « restreint UE »

Sont classifiées « EU restricted » les informations dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union Européenne ou de certains de ses états membres.

Pour figurer dans le catalogue de solutions approuvées par l'UE pour sécuriser de telles informations, un produit doit avoir obtenu la qualification de la part de deux agences d'états membres de l'Union Européenne (en France, la Qualification Standard). Ici aussi, la certification seule ne suffit pas.

* La certification requise dépend du niveau de qualification visé :

- Qualification Élémentaire = CSPN requise
- Qualification Standard = Certification CC EAL3+ requise
- Qualification Renforcée = Certification CC EAL4+ requise

Pour aller plus loin, sur le site de l'ANSSI :

Les [visas de sécurité ANSSI](#) et le [catalogue des solutions qualifiées](#)

Plus de détails sur la [qualification](#) et la [certification](#)

Les [recommandations pour choisir des pare-feux maîtrisés](#) dans les zones exposées à Internet

Pourquoi choisir un produit qualifié et pas seulement certifié ?

Si vous êtes une administration ou un Organisme d'Importance Vitale (OIV) relevant de la Loi de Programmation Militaire (LPM), du règlement européen iDAS, ou du Référentiel Général de Sécurité (RGS), vous devez utiliser une solution recommandée par l'État français, et donc une solution qualifiée par l'ANSSI. En effet, dans ce contexte l'ANSSI indique qu'il faut utiliser une solution à double barrière technologique, et que l'une d'entre elles au moins soit qualifiée au niveau Standard.

Stormshield propose actuellement le seul pare-feu qualifié Standard par l'ANSSI

En choisissant un produit de sécurité **Stormshield, actuellement le seul pare-feu qualifié Standard par l'ANSSI**, vous avez donc l'assurance de respecter cette directive et vous vous dégagez de toute responsabilité.

Mais les solutions qualifiées ne sont certainement pas réservées aux organisations soumises à de telles législations !

Comme l'indiquent les différents guides de l'ANSSI, et plus particulièrement le schéma « **Quel visa de sécurité choisir** », il est recommandé de choisir une solution **qualifiée** même si vous ne relevez pas d'un cadre législatif particulier :

- Vous bénéficierez alors d'un **produit dont la robustesse a été éprouvée** lors du processus de certification,
- Sur **une cible d'évaluation et d'utilisation validée** par l'ANSSI,
- Dont **le code source a été audité**,
- Et produit par **une société dont les processus** de développement, livraison, support **sont reconnus comme étant de confiance** par l'État français

Aujourd'hui, disposez-vous d'éléments concrets vous permettant d'avoir confiance en votre solution de sécurité actuelle et la société qui l'édite ?



STORMSHIELD



Stormshield, filiale à 100% d'Airbus CyberSecurity, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

www.stormshield.com