



dossier



Les experts de l'Anssi testent la robustesse des matériels en matière de cybersécurité en vue de leur accorder ou pas la certification Anssi.

© IFR

La certification : un vrai facteur différenciant pour les fabricants

Bien que de plus en plus de fabricants de systèmes de sécurité électronique ou autres s'engagent, volontairement, dans une démarche de certification par une tierce partie, ce n'est pas encore une généralité. Or, cette certification, imposée ou pas, constitue pour bon nombre de donneurs un facteur différenciant.

« **A** l'inverse du monde de la sécurité incendie qui jouit d'une forte culture de la certification qui est devenue un réflexe, le monde de la sécurité électronique ou physique n'a pas encore adopté le même réflexe avec les certifications existantes. Mais la cybersécurité constitue actuellement un enjeu majeur pour lequel la certification est un passeport de

confiance, souligne Amaury Lequette, directeur de CNPP Cert. Avant d'ajouter : « En effet, si pour certaines gammes de solutions, comme le contrôle d'accès

sous l'influence de l'Anssi, les choses bougent, pour le reste des solutions électroniques comme la vidéosurveillance, les fabricants commencent seulement à



« Notre démarche qualité rassure nos partenaires. »

CÉLINE STEIN, CEO PROGRAM ASSOCIATE CHEZ SIEMENS



RÉGLEMENTATIONS, NORMES, CERTIFICATIONS, QUALIFICATIONS, LABELS : QUELLE UTILITÉ ?

s'intéresser à la certification. La particularité étant, dans ce cas, le caractère volontaire de la certification. Or, dans le contexte actuel, et compte tenu des menaces que font peser sur les systèmes leur connexion aux réseaux, la certification est, non seulement, un bon moyen de rassurer les donneurs d'ordres, mais aussi de permettre aux installateurs de remplir au mieux leur devoir de conseil. »

De son côté, l'Agence nationale de la sécurité des systèmes d'information a fourni un gros travail pour inciter les fabricants à intégrer ses recommandations en matière de cybersécurité. « L'Anssi qui est rattachée au Premier ministre, via le secrétariat général de la Défense et de la Sécurité nationale (SGDSN), "chapeaute" la sécurité des administrations, des OIV ou opérateurs d'importance vitale et des OSE ou opérateurs de services essentiels, rappelle Vivien Mura, chef du bureau politique industrielle et assistance de l'Anssi. L'agence assume plusieurs missions : la défense afin de réagir en cas d'attaque informatique contre nos systèmes d'information ; la prévention en étant capable d'analyser les menaces et les risques afin de s'y préparer et élever le niveau de sécurité général ; l'information et la sensibilisation afin de partager sa doctrine cybersécurité avec le plus grand nombre d'acteurs concernés. C'est dans le cadre de ces missions que l'Anssi a défini certaines règles et exigences en matière de cybersécurité. »

DOMINIQUE AUVRAY

Directeur marketing
chez Fichet Group



© DR

« La conformité aux normes fait partie de l'ADN de Fichet et nous concevons et fabriquons nos produits dans cette logique. Mais

nous devons encore sensibiliser nos clients à l'intérêt de la certification comme gage de qualité. Il en va de même pour ce qui concerne la cybersécurité. Respecter les exigences de l'Anssi est primordial et cela nous permet d'adresser des marchés, comme celui des OIV, qui nous seraient fermés. Bénéficier de la certification et de la qualification de l'Anssi est un vrai facteur différenciant par rapport à nos concurrents. »

CÔTÉ CERTIFICATEUR

VIVIEN MURA

Chef du bureau politique industrielle et assistance de l'Anssi

« LA CYBERSÉCURITÉ EST UN ENJEU POUR TOUTES LES ENTREPRISES. »

« La cybersécurité est l'affaire de tous. Et non du seul ressort des concepteurs de produits de sécurité informatique comme les fabricants de pare-feu. C'est pourquoi l'Anssi a élaboré des exigences précises en matière de cybersécurité et dont la prise en compte permet d'obtenir soit la certification Anssi au sens de "certification délivrée par l'Anssi", soit la qualification Anssi. Elles ont toutes les deux, pour point commun, de permettre d'évaluer la résistance, la robustesse d'un produit, d'un service à la menace cyber. La différence majeure réside dans le fait que la qualification Anssi répond à un besoin étatique de disposer de solutions de confiance sur le long terme. On s'inscrit dans une notion de durée, de confiance et de pérennité. Dans le cadre de la qualification, l'Anssi demande au fabricant, au prestataire, plus de choses que pour la certification mais cela ne veut pas nécessairement dire que le niveau de robustesse des fonctions évaluées du produit, du service est plus grand. Tout dépend du périmètre évalué et du niveau d'assurance visé. Cette qualification peut être retirée – elle est attribuée pour trois ans – si nous constatons un changement dans le produit, dans la stratégie de l'entreprise, ou un changement d'actionnaire qui peut avoir des conséquences en matière de confiance, car on n'attend pas nécessairement un actionnariat français. La certification est plus "à la main" de l'entreprise demandeuse qui choisit le périmètre de l'évaluation. À charge pour l'Anssi de vérifier que le produit testé répond à la menace définie par le demandeur. »

→ En savoir plus : www.ssi.gouv.fr

■ Des utilisateurs de plus en plus sensibles

Si pour certains, la certification n'est pas encore un critère de choix, pour un nombre croissant d'utilisateurs finaux, donneurs d'ordres, la certification fait partie de leurs exigences. « D'une manière générale, tous les acteurs concernés prennent conscience de l'intérêt de la certification, poursuit Vivien Mura. Par ailleurs, il faut comprendre que la qualification Anssi est aujourd'hui associée à des obligations légales d'approvisionnement pour les OIV (pour leurs systèmes d'importance vitale). On peut en revanche imaginer que les OSE devront un jour recourir à des produits certifiés (au sens de la certification européenne). Pour les autres secteurs d'activités, la certification est un vrai facteur différenciant par rapport à la concurrence. Les utilisateurs y sont de plus sensibles car ils ont compris, qu'en matière de menaces cyber, personne n'est à l'abri. »



© DR

« Dans les marchés publics, la certification devrait être un minimum requis. »

STÉPHANE MATHIEU, RESPONSABLE QUALITÉ DU PÔLE EXPERT CHEZ PRYNTEC

RÉGIS COUSIN

Président de la FFMI



© DR

« Le secteur de l'incendie est soumis à une certification réglementaire qui permet aux produits d'être mis sur le marché : le marquage

CE qui confirme que le produit en question est conforme aux textes européens le concernant. S'y ajoute une marque volontaire : la marque NF. Son but, dans le cadre d'une collaboration avec les pouvoirs publics, est de garantir la qualité et la performance des systèmes et des produits. Le monde de l'incendie a ainsi mis en place un système vertueux, certes exigeant, mais qui permet de rassurer les utilisateurs finaux. C'est un modèle vertueux qui pourrait inspirer d'autres domaines de la sécurité. D'ailleurs, la démarche de l'Anssi en matière de sécurité cyber est assez proche de ce que nous faisons dans l'incendie. »



De plus en plus de fabricants font l'effort de se lancer dans la certification. Un gage de qualité du service pour leurs clients, qu'ils soient professionnels ou particuliers.

Si l'on s'en tient au sujet de la cybersécurité, la certification, incontournable pour certains marchés, au sens non réglementaire, en conséquence d'exigences de la part des utilisateurs/clients, devrait s'imposer. Rappelons que l'Europe travaille actuellement à l'élaboration d'un Cyber Act qui devrait consacrer des schémas de certification volontaire pour la robustesse des systèmes aux attaques numériques. «Le niveau "high" de ce Cyber Act devrait être assez proche des exigences de l'Anssi, estime Amaury Lequette. De notre côté, au CNPP, nous avons fait en sorte que nos certifications soient compatibles avec le texte européen.»

■ Des certifications méconnues

Force est de constater que malgré leur existence, les certifications sont assez mal connues. «Des certifications existent dans nos métiers, tient à rappeler Luc Jouve, président de GPMSE Installation et président du comité de certification NF service Apsad intrusion et vidéosurveillance. Citons, par exemple, la NF Services Apsad qui permet aux utilisateurs d'avoir la certitude qu'ils font appel à un installateur contrôlé par un organisme tierce partie. Or, si cette certification est demandée dans la télésurveillance, elle est méconnue pour la partie installation et maintenance.»

On peut jeter la pierre aux professionnels qui ne s'engagent pas dans une démarche

certifiante mais il faut aussi admettre que pour qu'ils le fassent, encore faudrait-il que les certifications soient poussées par certains. Or, dans le cas de la NF Services Apsad par exemple, les assureurs ne font plus ce travail. Pourquoi? Parce qu'ils disposent tous aujourd'hui de filiales vendant des offres de télésurveillance locatives, pour lesquelles elles utilisent des installateurs non-certifiés...

Comment faire si certains ne font pas leur part du travail? «Lors des comités de certification, mes confrères du collège



LES VISAS DE SÉCURITÉ DE L'ANSSI

Les visas de sécurité que délivre l'Anssi permettent d'identifier facilement les solutions les plus fiables et reconnues comme telles à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.

→ www.ssi.gouv.fr/administration/visa-de-securite/

LE POINT DE VUE DE L'ANITEC

STÉPHANIE TUCOULET
Secrétaire générale de l'Anitec



« BIENTÔT UN NOUVEAU LABEL CONFORMITÉ RGPD. »

«À l'Anitec, ce qu'on regroupe parfois abusivement sous le terme de certification, recouvre trois niveaux : label, qualification et certification. Cette dernière (notamment celle délivrée par le CNPP dans nos métiers), le plus haut niveau, valorise les professionnels qui en bénéficient, et les installateurs et

intégrateurs ont grand intérêt à se faire certifier. La qualification mise en avant est délivrée par Qualifelec, une organisation certifiée par le Cofrac. Avec l'entrée en vigueur du RGPD, on se rend compte que les donneurs d'ordres commencent à demander des preuves quant à la bonne application des exigences. C'est pour cette raison que l'Anitec, en partenariat avec le CNPP, va publier *Le Livre blanc : bonnes pratiques RGPD à l'attention des secteurs des intégrateurs, installateurs, mainteneurs de technologies connectées, sécurisées et pilotées*. Ce livre blanc sera la base d'un label du CNPP sur la conformité RGPD, prévu pour début avril.»



LE POINT DE VUE DU CNPP

AMAURY LEQUETTE

Directeur de CNPP Cert.



« LA CERTIFICATION VÉHICULE DE LA CONFIANCE. »

« Pour appuyer et renforcer la confiance véhiculée par les certifications volontaires A2P et APSAD, nous avons complété les caractéristiques fonctionnelles sécurité/sûreté déjà certifiées, avec la robustesse aux attaques numériques. Les travaux cyber menés par CNPP ont été réalisés en liaison avec l'Anssi afin de constituer une réponse adaptée aux produits de sécurité/sûreté, pleinement compatible et complémentaire des reconnaissances spécifiques Anssi (CSPN*, critères communs, etc.). Le but de la certification est de véhiculer de la confiance sur toute la chaîne de la sécurité, des produits aux services. »

* À noter que la CSPN est une certification de premier niveau et non une qualification.

installateur se joignent à moi très régulièrement pour demander aux certificateurs que sont l'Afnor et le CNPP de communiquer sur cette certification NF Services Apsad. Afin de la faire connaître et qu'elle soit demandée par nos clients», recommande Luc Jouve.

■ Sortir du moins-disant

« Si certains de nos clients sont sensibles à la certification, la plupart sont assez peu éduqués sur le sujet. Or, la certification est une démarche vertueuse, qui prouve la qualité d'un produit, insiste Stéphane Mathieu, formateur et responsable qualité du pôle Expert chez Pryntec dont la solution Digipryn a obtenu pour ses enregistreurs vidéo numériques la certification CNPP en 2019. Soit nos clients ne la

demandent pas car ils ne la connaissent pas, soit ils craignent que l'exiger réduise le nombre de répondants, éliminant, ainsi, les produits les moins chers. Alors que ces produits faussent le débat! Ils poussent, en effet, à comparer le prix de solutions non certifiées, et à la qualité incertaine, à des solutions qualitatives intégrant le coût de la certification. »

Méconnaissance sans doute... Mais aussi logique du moins-disant aux effets pervers. Les professionnels qui s'engagent dans la certification ne sont pas récompensés à la hauteur de leurs investissements. Trop d'appels d'offres, et les marchés publics ne sont pas les moins fautifs, ne tiennent aucun compte des certifications produits.

« Cela est dommageable car si les entreprises publiques et les pouvoirs publics exigeaient certaines certifications, ils permettraient d'enclencher un cercle vertueux qui inciterait les fournisseurs à améliorer leurs pratiques industrielles et commerciales... », ajoute Stéphane Mathieu.

L'État ne joue donc pas assez son rôle en matière de certification. On peut regretter qu'on puisse encore passer des appels d'offres sans mention d'une quelconque certification, a fortiori quand il s'agit de sécurité.

■ Un facteur différenciant

Tous les fabricants le disent : la certification est véritable atout.

De même, engager une démarche de labellisation est aussi vertueux. « Le fait d'avoir obtenu le label Comité stratégique de filière (CSF) "Industries de sécurité", nous permet d'expérimenter nos solutions dans une démarche de cocréation avec nos clients afin de vérifier

ANNE PEREZ

Directrice sécurité et relation client chez Verisure Securitas Direct



« Dans la télé-surveillance, la certification APSAD R3I est essentielle et obligatoire pour une entreprise

qui veut protéger les biens et les personnes. Notre certification APSAD R3I P3 assure à nos clients que nos trois stations de télésurveillance sont sécurisées, que les données sont protégées et confidentielles mais également que l'ensemble de nos chargés d'assistance jouissent du certificat "Agent de télésurveillance" et d'un agrément professionnel, renouvelé régulièrement. La certification est nécessaire mais pas suffisante. Il faut y associer des technologies innovantes, des systèmes fiables et des services efficaces. »

qu'elles répondent bien aux besoins de sécurité des infrastructures de grands événements, sportifs par exemple, explique Céline Stein, directrice sûreté France chez Siemens. Car nous ne devons pas nous reposer sur la notoriété de Siemens. Afin de répondre aux enjeux de l'avenir, il faut continuellement prouver que nos solutions sont innovantes et sécurisées et éventuellement se faire certifier, être labellisé. Cela rassure nos partenaires, leur prouve que nous sommes engagés dans une vraie démarche continue de qualité et de cybersécurité. » ■

VINCENT DUPART

PDG de STid



« Lorsque nous avons obtenu, dès 2013, la Certification de sécurité de premier niveau (CSPN) de l'Anssi, cela constituait un vrai

facteur différenciant. Depuis, nos partenaires ont des solutions certifiées comme Til Technologies, Alcea, Synchronic... – et ont été certifiés Anssi en intégrant nos lecteurs. L'intérêt de la qualification Anssi est d'instaurer sur des marchés comme celui des OIV une barrière à l'entrée à des acteurs peu soucieux du niveau de sécurité. Mais nous devons aller au-delà des certifications françaises. C'est pour cela que vient d'être créé SPAC (Smart Physical Access Control) pour positionner les savoir-faire français au niveau européen, dans le cadre du Cyber Act. »

VOIR LES PRINCIPALES NORMES PAGE 39