Analyse des contributions reçues suite à l'appel à manifestation d'intérêt sur la certification de sécurité de niveaux substantiel et élémentaire

version 1.0, 7 octobre 2019

Préambule

Les évolutions des technologies et du marché, la maturité des acteurs dans la perception des risques et les propositions de certification de niveaux substantiel et élémentaire apparaissant dans le projet de règlement de la Commission européenne en matière de certification de sécurité soulignent la nécessité de créer de nouveaux schémas de certification de sécurité.

Ces schémas viendraient compléter les dispositifs actuellement opérés par l'ANSSI, notamment pour certifier des prestataires de service, ou des produits soumis à des exigences de sécurité plus faibles.

Plusieurs acteurs privés ou institutionnels sont susceptibles de se positionner sur ces nouveaux segments. Face à ces évolutions inévitables, il convient que l'ANSSI détermine sa posture, accompagne la mise en place cohérente et ordonnée de ces nouvelles pratiques, et fasse évoluer au besoin le cadre de son activité.

L'ANSSI a ainsi lancé mi-2018, avant même la fin des négociations sur le règlement, un appel à manifestation d'intérêt (dit « *AMI-certifUE* ») pour identifier les acteurs qui souhaiteraient se positionner sur la certification de sécurité de niveaux substantiel et élémentaire en France, et recueillir leurs recommandations.

Ouvert jusqu'au 7 septembre 2018, il a suscité l'intérêt d'une vingtaine d'entités, citées en annexe 2, dont une bonne moitié a présenté une contribution ; l'ANSSI tient tout particulièrement à remercier ces entités pour leur participation aux échanges et leurs propositions.

Un ensemble de sujets avaient été retenus par l'ANSSI au lancement d'*AMI-CertifUE* ; suite aux échanges lors d'une réunion avec une grande majorité des intéressés, cette liste a été révisée pour

définir un cadre harmonisé de réponse permettant d'aborder une douzaine de thèmes, repris dans la liste ci-après :

0. Eléments généraux
1. Présentation, sur la base de retours clients/prospects ou d'appréciation interne, d'exemples de produits, services ou processus susceptibles de répondre à un besoin de certification pour les niveaux substantiel et élémentaire, et identification d'interlocuteurs jugés pertinents pour les expressions de besoins aux niveaux visés
2. Conditions attendues de notification des acteurs (centres de certification et/ou d'évaluation) par une autorité nationale de cybersécurité, en complément de leur accréditation par le Comité français d'accréditation (COFRAC), en fonction des niveaux
3. Intérêt et conditions de rattachement d'un acteur à plusieurs autorités nationales et opportunités de développement international
4. Identification des activités d'évaluation pertinentes à mener, selon les niveaux, si possible en relation avec les autres activités d'évaluation de la conformité qui seraient déjà menées sur les mêmes gammes d'offres
5. Compétences requises estimées pour les tests d'évaluation
6. Modalités de supervision des activités permettant de s'assurer d'une homogénéité dans les travaux accomplis, et du traitement adéquat des anomalies, en lien potentiellement avec des activités de surveillance de marché
7. Durées admissibles de validité des certificats et moyens estimés viables de maintien dans la durée de ces certificats
8. Moyens envisagés d'harmonisation des méthodes et pratiques d'analyse de risques, d'évaluation et de certification
9. Besoins identifiés d'accompagnement de la montée en puissance des acteurs par l'ANSSI et l'écosystème existant (CESTI), et détermination des informations pertinentes qui pourraient être échangées (guides, vulnérabilités par exemple) avec l'ANSSI dans le fonctionnement d'un schéma
10. Outils qui permettraient d'automatiser les activités, et compétences nécessaires pour le développement et l'exploitation de ces outils
11. Identification des schémas existants et réutilisables ou à créer
12. Règles attendues de protection des activités liées à l'évaluation et à la certification de sécurité
13. Tout autre thème jugé pertinent

Pour chaque thème, des propositions d'actions résultant de l'analyse des recommandations reçues par les contributeurs sont faites ; après revue, celles qui seront confirmées deviendront des actions à engager. Les éléments ci-après repris des contributions sont cités *« en italique entre apostrophes »*.

0. Eléments généraux

La cybersécurité de produit ou de service est jugée comme un sujet très complexe, où la notion de vulnérabilité couverte par une contre-mesure est difficilement applicable selon une logique de « tout ou rien ». *« Dans la plupart des stratégies d'attaques, une première étape consiste à contourner, désactiver ou rendre inopérantes des contre-mesures, puis, ensuite, les étapes suivantes consistent à appliquer l'attaque proprement dite. »*

La résistance d'un produit est donc non seulement liée à la présence de contre-mesures, mais également à la solidité effective de ces contre-mesures, *« ce qui rend délicat la simple vérification de conformité »*.

Pour assurer la confiance des utilisateurs, qu'ils soient concepteurs, utilisateurs ou usagers, il est jugé souhaitable que *« chaque niveau d'évaluation de sécurité ait une identité propre bien définie prenant en compte le cas d'usage du produit »* et que l'on considère *« les différents niveaux d'évaluation élémentaire, substantiel, élevé comme une hiérarchie de vérification, où chaque niveau inclut automatiquement les exigences des niveaux précédents (comme le proposent par exemple les Critères Communs). »*

PROPOSITION D'ACTION : Analyser la possibilité d'une stratégie de poupées russes pour les stratégies d'évaluation selon les niveaux visés et engager un travail préparatoire de communication & marketing pour expliquer les différences des niveaux de certification.

La différenciation des niveaux devrait également se refléter dans la mise en place de la certification : durée, complexité et méthodologie d'évaluation et par conséquent coût (voir détails dans le chapitre 4.). *« Les agences nationales de sécurité européennes doivent s'assurer que les méthodes et pratiques demeurent proportionnelles au risque et éviter en particulier que le niveau substantiel ne soit concurrent du niveau haut. Les deux niveaux doivent être techniquement différents afin d'éviter une course aux attaques potentielles irréalistes pour le niveau substantiel. »*

Ndr : Bien que le sujet principal de l'*AMI-certifUE* soit les niveaux substantiel et élémentaire, de nombreuses références sont faites vis-à-vis du niveau élevé, qui a l'avantage d'être connu et pratiqué depuis de nombreuses années. Notamment, en terme de niveau d'évaluation, on trouve une forme d'adhésion sur *« l'objectif de maintenir dans le niveau élevé les évaluations nécessitant un niveau d'attaque supérieur ou égal à AVA_VAN 3. Par ailleurs, tout produit ou application ayant des enjeux de sureté de fonctionnement (i.e en lien avec la sécurité des personnes) comme dans l'e-santé[1] ou la voiture autonome[2] devra relever également du niveau élevé. »*

Pour le niveau substantiel, il se dégage un consensus général sur la nécessité :

[1] Ndr : a minima les dispositifs médicaux

[2] Ndr : Considérer les fonctionnalités liées à un niveau d'autonomie supérieur à 4 (Cf. SAE J3016)

- D'une relation triangulaire entre le développeur, l'évaluateur et le certificateur, avec un intérêt pour qu'à l'image de certains schémas privés existants, une même entité puisse agir soit en tant qu'évaluateur, soit en tant que certificateur, soit les deux ;

- *« de tests dont le cas échéant des pentests ; »*

- *« de garantir une homogénéité dans les travaux et les compétences des évaluateurs et des certificateurs et donc dans la valeur des évaluations »* avec la question récurrente de l'intervention des autorités nationale ou européenne dans le processus et quelques propositions en la matière.

Aucune position tranchée ne se dégage sur la question du recours à une stratégie de certification tierce partie ou à une approche d'auto-déclaration (aussi appelée autoévaluation de la conformité) pour le niveau élémentaire (possibilité introduite par le règlement). Cependant, la cybersécurité étant un domaine en évolution continue et extrêmement rapide sous l'impulsion d'acteurs variés divulguant des vulnérabilités de produits ou de leurs composants, dans des cercles fermés ou dans la presse : hackers, chercheurs, développeurs, laboratoires d'évaluations, …, il est jugé *« naturel qu'un produit certifié, quel que soit son niveau, ne soit sensible à aucune vulnérabilité connue exploitable de manière réaliste »*, et que *« les vulnérabilités relatives à un schéma donné doivent être publiées et tous les utilisateurs du schéma informés dans le but de permettre en place les mesures adéquates. »*

PROPOSITION D'ACTION : S'assurer de la prise en compte systématique des vulnérabilités publiques (CVE) dans le cycle de vie des certifications de sécurité, pour le niveau substantiel.

PROPOSITION D'ACTION : Etudier la possibilité d'harmoniser les règles de gestion/publication des vulnérabilités pour l'information des utilisateurs, pour les différents niveaux.

PROPOSITION D'ACTION : S'assurer que l'autorité nationale de certification de cybersécurité met en œuvre une surveillance des organismes d'évaluation de la conformité et des fabricants qui procèdent à des autoévaluations.

1. Présentation, sur la base de retours clients/prospects ou d'appréciation interne, d'exemples de produits, services ou processus susceptibles de répondre à un besoin de certification pour les niveaux substantiel et élémentaire, et identification d'interlocuteurs jugés pertinents pour les expressions de besoins aux niveaux visés

a) En termes d'offres à certifier et d'offres de soutien à la certification

En lien avec les objectifs du *Cybersecurity Act* (renforcer le niveau de sécurité, développer le marché de la cybersécurité en Europe et rendre visible la sécurité des services et produits au travers de l'émission de certificats), deux approches sont ici considérées :

- *« d'une part, étendre le principe de la certification de sécurité à un ensemble important de domaines ;*

- *d'autre part, encourager le développement d'un écosystème de produits et services de sécurité et d'outils/plateformes d'aide à la construction et l'analyse de sécurité de ces produits et services. »*

Il est estimé que *« l'ensemble des produits et systèmes d'information peuvent faire l'objet d'une certification de niveau substantiel (hardware, software, couche de communications, voire même un processus de gestion - ex. : détection de fraude au paiement) dès lors qu'ils n'embarquent pas des problématiques de sûreté de fonctionnement (sécurité des personnes), avec un risque fort de transfert massif des évaluations vers le niveau substantiel. »*

La typologie des clients intéressés par le niveau substantiel est très large. *« Le domaine IoT et les solutions IT (soft, Cloud, ou hard) de taille modeste (PME < 50 personnes) semblent entre autres très demandeuses. En effet, pour les PME, une reconnaissance officielle d'un niveau sécurité ou de robustesse de leur produit est un atout commercial indéniable. Ce type de client demande par contre une période d'évaluation simple, rapide et accréditant d'un vrai niveau de sécurisation ou de robustesse. »*

Les domaines envisagés, sans être exhaustifs, pourraient ainsi couvrir :

- *« les objets connectés (utilisation dans un cadre domotique, industriel, etc.) ;*
- *les prestataires de service de confiance (PASSI, PDIS, PRIS, PAMS, PSCE, etc.) ;*
- *les produits/services spécifiques à des secteurs d'activités (dispositifs médicaux, hébergement de données de santé, etc.) ;*
- *les produits/services devant manipuler des données personnelles, bancaires, financières, liées à la propriété intellectuelles/industrielles, etc. ;*
- *les produits/services liés à des besoins étatiques (gestion/encaissement de la taxe, systèmes de vote électronique, etc.). »*

Ces domaines pourront ou non être régulés, c'est-à-dire disposer d'exigences qui rendent la certification obligatoire (alors qu'elle est définie comme volontaire dans le *Cybersecurity Act*). Pour illustrer, deux exemples sont détaillés ci-après.

Pour autant, un message fort est passé sur l'intérêt, comme c'est le cas aujourd'hui dans la certification de produits à niveau élevé, de *« schémas horizontaux appliqués aux technologies de base utilisés pour construire des objets connectés et autres produits sensibles, afin de pouvoir garantir que les produits sont construits sur une base solide. Cette idée est très similaire au modèle de composition utilisé aujourd'hui dans la certification des différentes couches d'une carte à puce (hardware, plate-forme, application). Dans le cadre de certifications aux niveaux élémentaire et même substantiel, un tel modèle est indispensable pour s'assurer que les mécanismes de sécurité sont correctement implémentés, ce qui ne peut pas être garanti par de simples checklists au niveau d'un objet complet ou d'un système complet. »*

PROPOSITION D'ACTION : Travailler sur un catalogue de technologies de base certifiées (avec un schéma générique) réutilisables pour les offres sectorielles.

Ndr : ces technologies de base peuvent s'entendre au sens des produits (composants, …) mais aussi au sens plus large des services et des infrastructures qui seraient mises en œuvre pour opérer les offres sectorielles, notamment – mais pas exclusivement – les offres dans le domaine du cloud.

- ***Les dispositifs médicaux et les dispositifs médicaux de diagnostic in-vitro***

Ces dispositifs présentent des enjeux évidents de santé publique. Un grand nombre d'entre eux étant désormais des objets connectés, il apparait nécessaire de garantir leur sécurité. Il est à noter que d'autres états hors de l'union européenne débattent de l'opportunité de réglementer la cybersécurité des dispositifs médicaux (https://www.congress.gov/bill/115th-congress/senate-bill/1656). La FDA (Food and Drug Administration) a par ailleurs un premier projet de bonnes pratiques sur le sujet en octobre 2018 : http://app.info.fda.gov/e/er?utm_campaign=FDA%20Releases%20Draft%20Recom%20on%20Premrkt%20Sub%20Manag%20Cybersecurity&utm_medium=email&utm_source=Eloqua&s=2027422842&lid=5192&elqTrackId=3FEAE0C7FABDF2E969EC31B9016ABE6C&elq=fc215478357440f5a7207245d7f6b588&elqaid=5530&elqat=1

Ces produits font d'ores et déjà l'objet d'une réglementation harmonisée (règlement 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux et règlement 2017/746 relatif aux dispositifs médicaux de diagnostic in-vitro). Cette réglementation existante se base sur un schéma de certification de type « nouvelle approche », assimilable à un niveau substantiel faisant intervenir des organismes notifiés pour les dispositifs présentant un risque intermédiaire et à un niveau élémentaire pour les dispositifs de faible niveau de risque (auto-déclaration).

- ***Les dispositifs de délivrance d'un temps***

De nombreux process nécessitent une synchronisation horaire exacte, traçable aux temps légal et sécurisée : dans les transports (réseaux ferrés et contrôle aérien), dans l'énergie (smart grid), dans les marchés financiers,… La sécurisation de la donnée « temps » présente dans ces process un enjeu majeur du fait de risques important d'un point de vue de la sécurité publique ou d'enjeux financier.

Ces dispositifs font parfois déjà l'objet de dispositions réglementaires, par exemple le règlement RTS 25 en application de la directive européenne 2014/65/EU (ec.europa.eu/finance/securities/.../rts/160607-rts-25-annex_en.pdf), ou de certification volontaire tel que le schéma de certification mis en place par le LNE dans le cadre du consortium SCPTime.

En complément, étant donné que de nombreux services en ligne ou produits, destinés à offrir des services de confiance, s'appuient sur des briques logicielles souvent communes, il apparait opportun *« d'encourager à la production de briques de confiance/certifiées couvrant :*

- *les framework web (Django, Symfony, Rails, Express.js, etc.) ;*
- *les produits qui ne sont pas directement des produits de sécurité, mais qui intègrent des mécanismes de sécurité (authentification, communication sécurisée, contrôle d'accès, stockage sécurisé, archivage intègre, etc.). »*

Enfin, il est également important de *« considérer les briques open source qui sont très souvent à la base d'offres de service et de produits de sécurité. Etant donné que ces briques ne sont pas toujours portées par des entreprises, l'Europe, l'ENISA et les autorités nationales devraient favoriser le financement de leur développement et la sécurisation de ces composants. En particulier, un cadre de financement de certifications de briques open source devrait idéalement être mis en place. »*

PROPOSITION D'ACTION : Favoriser via les dispositifs européens en vigueur de soutien financier et l'implication des Etats Membres la certification de briques de base sécurisées, notamment open source, et assurer la promotion de ces offres certifiées auprès des développeurs.

Par ailleurs, afin d'encourager le développement d'un écosystème de produits d'analyse pour la sécurité, *« il serait important d'encourager la réalisation de plateformes d'automatisation de tests de sécurité, qui seraient en mesure de produire automatiquement des certificats. Ces plateformes pourraient notamment couvrir les étapes d'analyse suivantes :*

- *outils d'analyse statique de code source ;*
- *scanners de vulnérabilités ;*
- *automatisation d'audit de configuration ;*
- *fuzzers de protocoles. »*

D'autre part, il serait souhaitable d'encourager au *« développement de chaines de développement logiciel certifiées, qui incluraient en particulier les étapes suivantes :*

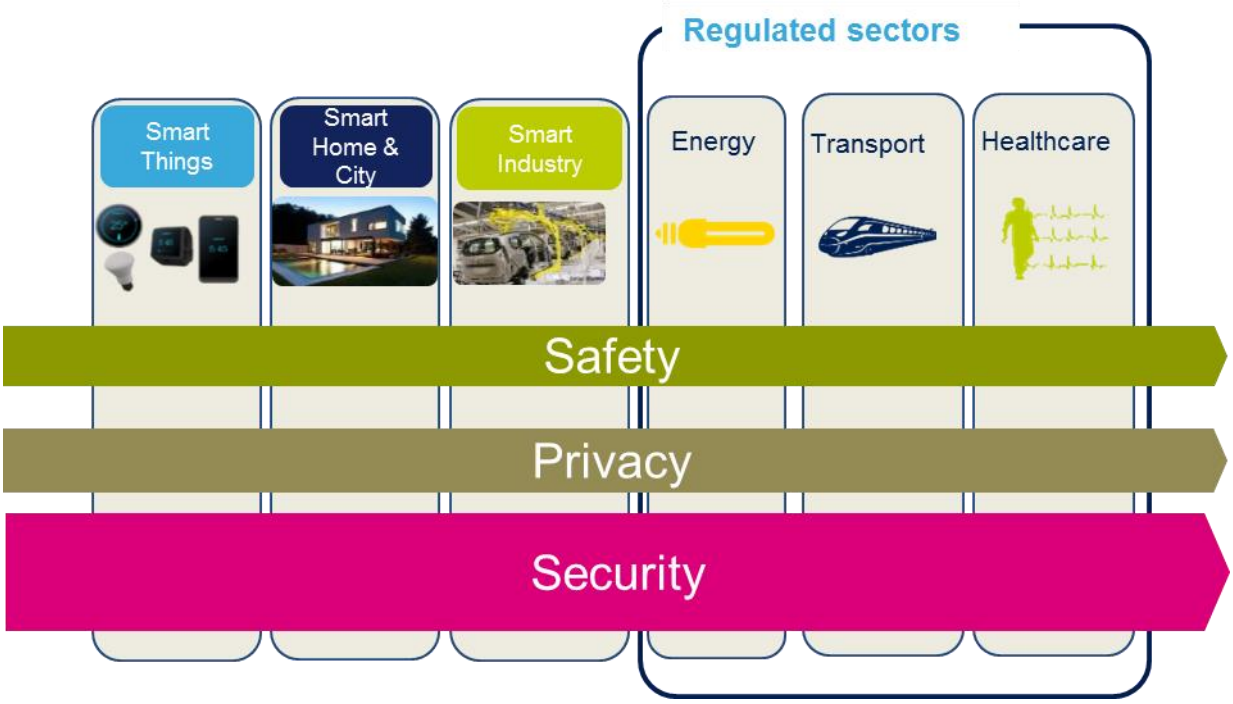
- *chaine d'intégration continue ;*
- *revue de code ;*
- *outils d'analyse statique de code ;*
- *tests unitaires, fonctionnels et d'intégration. »*

Sur ce sujet, il existe déjà plusieurs cadres de processus de développement sécurisé sur lesquels il serait jugé pertinent de s'appuyer (par exemple, S-SDLC, ASVS, ou encore ISA Secure SDLA), on trouvera quelques illustration en chapitre 11.

b) <u>En termes de positionnement entre certification de sécurité et certification sectorielle</u>

Pour les produits relevant déjà de normes, standards ou règlements, il semble essentiel que *« les aspects cybersécurité viennent s'ajouter aux caractéristiques soit performance soit sécurité*[3] *de ces produits »*. C'est ainsi que de multiples acteurs industriels, *pure players* de la SSI, abordent le marché de la certification de sécurité sectorielle, en offrant leurs services aux organismes et laboratoires n'ayant pas cette compétence actuellement (mais qui maîtrisent le volet métier et notamment *safety*), pour offrir une offre complète aux développeurs, d'un point de vue européen.

[3] au sens *safety*. Le volet *privacy* est également évoqué.



Pour certains systèmes ou services, *« la cybersécurité sera aussi une composant de la sécurité (une attaque cyber pouvant conduire à une défaillance de performance ou de sécurité par exemple en automobile, un système de contrôle commande dans une raffinerie, un système de sécurité incendie) ».* Le risque cyber deviendrait ainsi un élément d'entrée de l'analyse de risque et il semblerait opportun que *« pour les produits déjà couverts par une directive ou un règlement européen ou une norme nationale ou internationale ou un référentiel de certification volontaire, de compléter ces documents sur l'aspect cyber sécurité ».*

PROPOSITION D'ACTION : S'assurer de l'intégration de la certification de sécurité (et du processus associé) dans les exigences sectorielles (énergie, sécurité machine, …).

Ndr : A titre d'illustration, on peut citer la démarche engagée par CNPP qui a intégré le volet cyber sécurité aux certifications et référentiels métier déjà existants pour les secteurs de la sûreté et de la sécurité incendie[4], cette approche garantissant la pleine prise en compte des exigences règlementaires, des exigences fonctionnelles « métier » spécifiques et de cyber sécurité pour des niveaux de risque s'inscrivant en amont du niveau CSPN, et donc pour des niveaux jugés Substantiels, tout en pointant vers la CSPN pour les enjeux de sécurité dépassant le cadre générique prévu pour ce type d'équipements. Cette approche a fait l'objet d'échanges et de coordination avec les différentes parties prenantes du secteur (assureurs, professionnels de la sécurité, exploitants de systèmes de sécurité) et avec l'ANSSI. Elle répond selon l'ANSSI aux exigences typiquement requises pour le développement d'un schéma de certification tel que préconisé dans le *Cybersecurity Act*.

[4]A ce stade, cela recouvre les produits de sécurité électronique (détection intrusion vol, caméras de vidéosurveillance, enregistreurs vidéonumériques, serrures électroniques de coffres forts), les serrures de bâtiment connectées, et les services d'installation et de maintenance de produits de sécurité électronique (détection intrusion, vidéosurveillance et contrôle d'accès).

En complément de cette approche sectorielle, on peut également citer les offres « *d'appréciation de la sécurité d'applications mobiles qui prennent en charge des vérifications de sécurité de façon systématique et automatiques avec des logiciels spécialisés, sous la dénomination de demonstration of compliance ».*

c) <u>En termes de portabilité des certifications existantes</u>

En matière de services, il est mis en avant la nécessité de *« portabilité des qualifications actuelles des prestataires (PASSI, PRIS, PDIS, SecNumCloud…) »*, et la nécessité de convergence *« dans des standards internationaux. »*

Ndr : Concernant ce dernier point, on peut d'ores et déjà noter le travail engagé par l'ANSSI de portage de ses référentiels dans les travaux UE, que ce soit dans la norme (déclinaison du référentiel PDIS dans la norme ETSI/ISI/007) ou dans les travaux préliminaires à un schéma de certification européen par la promotion de SecNumCloud.

PROPOSITION D'ACTION : Définir et partager la stratégie de portabilité et de promotion des qualifications existantes de prestataires ANSSI dans un schéma européen de certification.

2. <u>Conditions attendues de notification des acteurs (centres de certification et/ou d'évaluation) par une autorité nationale de cybersécurité, en complément de leur accréditation par le Comité français d'accréditation (COFRAC), en fonction des niveaux</u>

Dans le cadre de la mise en œuvre du *Cybersecurity Act* (Art. 61 & Art. 58), l'autorité nationale de certification doit notifier à la Commission le nom des organismes d'évaluation de la conformité (avec les niveaux d'assurance appropriés).

De manière générale, l'accréditation préalable à une reconnaissance par l'Autorité Nationale pour délivrer des services d'inspection, de tests et mesures ou de certification de produits, systèmes ou personnel est requise dans la très grande majorité des directives et règlements européens[5] (équipement sous pression, machines, dispositifs médicaux, produits de la construction, homologation des véhicules …) où une accréditation suivant les standards ISO/IEC 17020, 17025 ou 17065 dans le domaine concerné est un des éléments du dossier de notification par l'autorité nationale en charge. Les exigences complémentaires de l'autorité concernent principalement :

- le statut juridique de l'organisme et de son groupe d'appartenance et notamment le devoir d'informer en cas de modification significative (statuts, actionnaires, dirigeants …) ;
- l'assurabilité ;

[5] Il est à noter que cette approche n'est pas restreinte aux cas des directives européennes ; en France certaines lois (qualité de l'air intérieur dans les établissements recevant du public ou en qualité de l'air dans les locaux de travail, émissions ou rejets atmosphériques d'installations classées …) requièrent une accréditation NF EN ISO 17025 dans le domaine concerné préalablement à l'agrément de l'organisme.

- l'engagement d'un membre de la direction de l'organisme à appliquer les lois, directives et instructions afférentes à cette activité et à avertir l'Autorité en cas de manquements ou de produits défectueux (devoir de vigilance et d'information, participation à la surveillance du marché) ;

- la communication de résultats ou d'information soit sous la forme d'un rapport annuel soit sur un site internet ;

- la participation à des instances de coordination mixtes (organismes agréés, autorités, organismes de normalisation …) au niveau français ou européen (Participation au retour d'expérience, à sa capitalisation, à l'évolution des pratiques et à l'interprétation des règlements) ;

- le maintien de dossiers justificatifs de la décision de certification et sa mise à disposition éventuelle à l'Autorité.

Dans la mesure où certains organismes déjà notifiés, agréés ou accrédités sur d'autres règlements souhaitent délivrer des services de certification de produits, systèmes et processus en matière de cyber sécurité, il est proposé *« de reprendre le contexte existant de notification ou d'agrément, qui a fait ses preuves et a une portée est non seulement française mais européenne via la décision n° 768/2008/CE*[6] *sur les produits et le Guide bleu*[7] *»*.

Dans ce cas de figure, il est estimé que :

- *« la notification doit rester sectorielle auprès des autorités notifiantes nationales déjà en place (DHUP pour le RPC, ministère de la santé pour les dispositifs médicaux, BSERR pour les appareils à pression …)* ;

- *l'accréditation doit être évaluée et délivrée par le COFRAC avec la participation d'experts cyber (extérieurs) pour les aspects techniques tels que : Sécurité physique / Logique (CID) des installations et des entités évaluatrices ;*

- *les entités évaluatrices doivent participer à des groupes techniques d'experts autour d'un réseau d'information essentiellement technique permettant l'harmonisation des bonnes pratiques d'évaluation. Nous recommandons que le pilotage de ce groupe soit assuré par l'ANSSI (à l'identique de ce qu'il se fait dans d'autres domaines tels que la réglementation sur les Equipements Sous Pression Nucléaires, les produits de construction avec le GT10 animé par le Direction de l'Habitat de l'Urbanisme et des Paysages, etc.). Ces groupes de travail pourraient être répliqués à l'échelon européen pour un plus large partage d'informations (tel que les Sector Groups pour la coordination des organismes notifiés dans le cadre du règlement européen des produits de construction) ».*

[6] Notamment les exigences de son chapitre R4 (notification des organismes d'évaluation de la conformité).

[7] Guide bleu relatif à la mise en œuvre de la règlementation de l'Union européenne sur les produits 2016 (2016/C 272/01).

Si les secondes et troisièmes appréciations ne soulèvent pas forcément de débat, l'ANSSI souhaite souligner que la première entre nettement en contradiction, pour ce qui relève du champ cybersécurité, avec le règlement et appelle à une action de concertation entre autorités de notification.

PROPOSITION D'ACTION : S'assurer de la cohérence entre les décisions de notifications des CAB par les autorités sectorielles compétentes et par l'autorité nationale de cybersécurité.

Concernant le volet de l'expertise en sécurité des CAB, une exigence supplémentaire est évoquée à plusieurs reprises, celle qu' *« au-delà de l'accréditation par un organisme national d'accréditation de type COFRAC, un groupe d'experts en sécurité audite les CAB sur des critères techniques, et valide leur conformité aux exigences définies par les schémas de certifications concernés. Ce groupe doit s'assurer que les produits et les services sont bien évalués selon les méthodes définies par les schémas de certification, et en particulier que les efforts et l'expertise technique engagés sont en ligne avec les attentes des schémas. Ces audits techniques doivent aussi s'assurer que les méthodes, les efforts, et l'expertise engagés sont homogènes dans l'ensemble des CAB opérant dans les Etats membres de l'Union Européenne. Les experts de ce groupe doivent être indépendants des entités commerciales impliquées dans les schémas de certification. »* La possibilité que les experts en question proviennent des agences nationales de sécurité et en particulier de l'ANSSI, de ses agences homologues et de l'ENISA, est évoquée.

Ndr : L'ANSSI voit dans le texte du règlement approuvé en trilogue une double possibilité de satisfaire cet objectif : notification des CAB par l'autorité nationale, d'une part, revue par les pairs d'autre part.

En complément des éléments évalués par le COFRAC au titre de l'accréditation et de ce sujet expertise de sécurité, il est jugé *« approprié de maintenir à minima les éléments suivants :*

- *Le statut juridique de l'organisme et de son groupe d'appartenance et notamment le devoir d'informer en cas de modification significative (statuts, actionnaires, dirigeants …) ;*
- *L'engagement d'un membre de la direction de l'organisme à appliquer les lois, directives et instructions afférentes à cette activité et à avertir l'Autorité en cas de manquements ou de produits défectueux (devoir de vigilance et d'information, participation à la surveillance du marché) ;*
- *La participation à des instances de coordination mixtes (organismes agréés, autorités, organismes de normalisation …) au niveau français ou européen (Participation au retour d'expérience, à sa capitalisation, à l'évolution des pratiques et à l'interprétation des règlements). »*

PROPOSITION D'ACTION : Prendre en compte ces éléments complémentaires à l'accréditation (en part. sur la revue par les pairs) dans le suivi de notification opérée par l'autorité nationale cyber.

Pour les CAB qui délivrent la certification[8], la norme d'accréditation jugée la plus pertinente est l'ISO/IEC 17065 même si dans le cadre d'une certification sur la base de tests, la norme ISO/IEC 17025 pourra être acceptée. Par contre, étant donné la nature des tests à réaliser dépendant du niveau de confiance du produit, de son environnement, de son usage et des menaces, il est mentionné que *« le recours à une portée flexible[9] s'impose de fait »*.

Pour aller plus dans le détail, il est de plus fait référence aux *« documents d'exigences spécifiques qui sont de nature à servir d'exemples pour la création de nouveaux schémas dans le cadre du Cybersecurity Act, à savoir :*

- *le document d'exigences spécifiques CERT CPS REF 33 – utilisé pour la certification des Prestataires d'Audit de la Sécurité des SI (PASSI) selon le référentiel PASSI – en complément de la norme d'accréditation ISO/IEC 17065 ; ceci pourrait correspondre au niveau substantiel et niveau élémentaire ;*
- *le document d'exigences spécifiques LAB REF 14 dans le cadre de l'accréditation selon la norme d'accréditation ISO/IEC 17025 des CESTI ; ceci est estimé correspondre au niveau élevé. »*

PROPOSITION D'ACTION : Dans le cadre de l'accréditation, s'assurer que l'ISO/IEC 17065 est la norme d'évaluation privilégiée des CAB qui délivrent des certificats (organisme de certification), et que pour les laboratoires de tests (organisme d'évaluation), c'est l'ISO/IEC 17025 avec portée flexible qui est retenue.

PROPOSITION D'ACTION : Veiller à s'assurer avec le soutien du COFRAC à ce que les exigences spécifiques associées aux normes ISO/IEC 17065 et ISO/IEC 17025 (par exemple CERT CPS REF 33 du Cofrac sur les PASSI), éventuellement déclinées par niveau du *Cybersecurity Act*, soient harmonisées au niveau européen (European Accreditation) (éventuellement au niveau de la définition du schéma de certification via l'EA 1/22[10]).

3. Intérêt et conditions de rattachement d'un acteur à plusieurs autorités nationales et opportunités de développement international

Dans le cadre de la mise en œuvre du *Cybersecurity Act* en France, il est jugé *« essentiel pour répondre aux attentes du marché de voir la pleine application du Règlement européen (CE) n° 765/2008 et de la*

[8] Contrairement aux CESTI qui eux ne délivrent pas la certification.

[9] Le concept d'accréditation en portées flexibles, autorise l'organisme évaluateur à étendre la portée d'accréditation dans un champ préalablement défini. Cette extension n'est pas soumise à une nouvelle évaluation intermédiaire entre deux évaluations du cycle d'accréditation.

[10] Document « EA Procedure and Criteria For the Evaluation of Conformity Assessment Schemes by EA Accreditation Body Members » de l'European Accreditation

décision n° 768/2008/CE[11] à savoir la reconnaissance systématique d'un organisme reconnu par une autorité d'un des états membres sur une norme harmonisée ou un schéma de certification approuvé par les autres états membres sans demande supplémentaire. Cette demande du marché semble naturelle dès lors que l'on parle de produit car l'aspect cybersécurité sera un complément par rapport à d'autres directives et règlements (basse tension, CEM, RPC …) pour lesquels ce principe s'applique déjà par une reconnaissance mutuelle des organismes notifiés par les états membres de l'EU. Le caractère « hors frontière » d'un service ou système entraîne aussi de facto l'application de ce principe. »

Ce principe est jugé unanimement de nature à *« renforcer la concertation, la cohérence et la collaboration sur les schémas de certification au travers de groupes professionnels sectoriels et des échanges entre organismes de certification et autorités nationales à l'échelon national et européen ».* Un point d'attention est cependant évoqué sur le besoin impérieux *« de s'assurer de l'application uniforme de règles de confidentialité par les autorités nationales concernées. ».* Un second point d'attention est que *« le rattachement à plusieurs autorités doit être possible à condition unique d'avoir exactement le même niveau. »*

En matière de services (car il est pressenti que les acteurs PASSI, PDIS, PRIS… joueront un rôle dans les schémas de certification, comme on le verra au chapitre 4), une reconnaissance supranationale est vue comme *« un changement d'échelle important permettant une réelle plus-value dans la mutualisation des pratiques entre les parties, un accroissement des échanges, du marché et du niveau de sécurité profitable l'ensemble de l'écosystème dédié à la cybersécurité. »*

PROPOSITION D'ACTION : Prévoir un système de notification croisée - *cross-notification* - des CAB et des centres et prestataires d'évaluation agissant à leur profit vis-à-vis de plusieurs autorités nationales de certification (dans différents pays européens).

4. Identification des activités d'évaluation pertinentes à mener, selon les niveaux, si possible en relation avec les autres activités d'évaluation de la conformité qui seraient déjà en vigueur sur les mêmes gammes d'offres

Comme évoqué précédemment, il semble nécessaire que *« les activités d'évaluation et de certification (tests en laboratoire, audits et revues) soient menées par les CAB en cohérence avec les schémas de certification déjà existants pour caractériser la performance des produits. »*

Les certifications de sécurité informatiques des produits réalisés par les CAB pour le niveau substantiel doivent se caractériser par le fait que *« les essais réalisés sont prédéterminés et répondent à un schéma de certification décrivant les méthodes d'essai et exigences applicables aux produits pour obtenir leur certification. »*

[11] Sachant dans le cadre de notification basé sur la décision 768/2008, *« un organisme ne peut être notifié que par l'autorité notifiante de son pays d'appartenance. »*

Les procédures d'évaluation de la conformité pertinente de l'annexe II de la décision 768/2008 précitée et notamment la procédure d'examen de type (module B) associé à la procédure conformité au type sur la base de l'assurance de la qualité du procédé de fabrication (module D) sont citées *« comme ayant le mérite de sa baser sur un cadre juridique européen existant et éprouvé. »*

« Il faut rendre les choses accessibles, et considérer de pouvoir mettre en place un système qui prend en charge des vérifications de sécurité de façon systématique et automatiques avec des logiciels spécialisés. » C'est notamment ce que l'on peut retrouver dans diverses offres d'appréciation de la sécurité d'applications mobiles mentionnées en chapitre 1.

Il est mentionné, pour le niveau substantiel, la possibilité de définition de *« plusieurs niveaux de classification correspondant aux analyses de risques spécifiques définies pour les catégories de produits couvertes par les CAB. Cette analyse de risque prend en compte l'impact global (financier et humain) d'une attaque et aide à déterminer la criticité potentielle des vulnérabilités découvertes sur les produits »*.

Au-delà de cette criticité en termes de sécurité du service ou du produit Il est également important de *« rapprocher le coût de l'évaluation au regard du prix de vente du service ou du produit évalué ».*

*E*n terme de méthodes, il est préconisé que *« Les méthodes utilisées par les CAB se basent sur des outils du marché adaptés à la composition des produits (y compris aux communications et aux logiciels de gestion associés aux produits), pertinents pour l'état de l'art et mis à jour. L'évaluation se base sur l'exploitation de vulnérabilités propres aux produits, aux protocoles de communication utilisés ainsi qu'aux applications logicielles associées. Ces vulnérabilités sont connues (sur les bases de données publiques) à l'instant t. »*

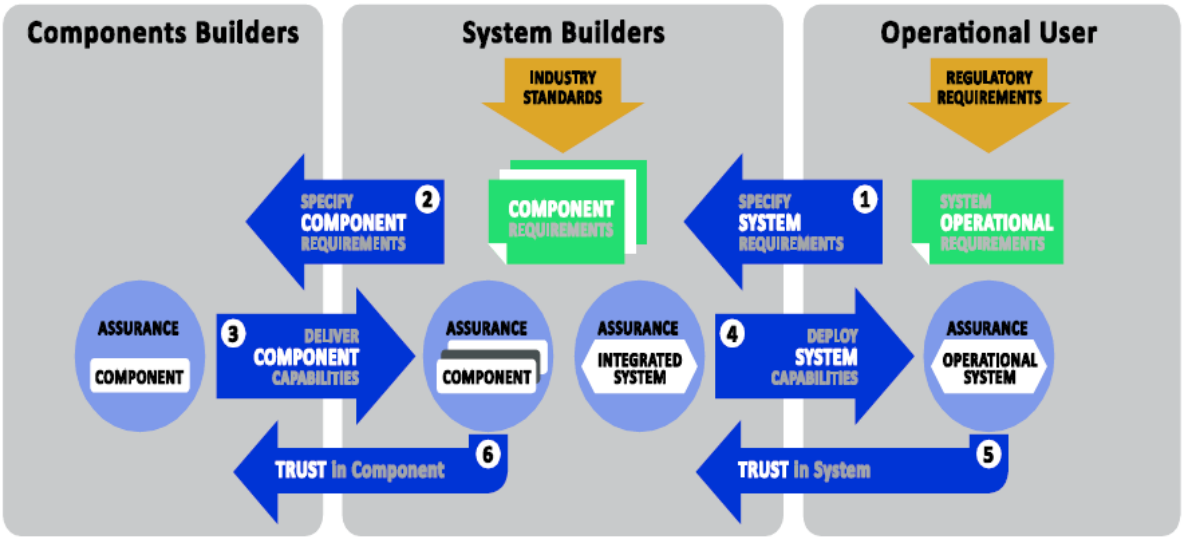
En termes de travaux, sont mentionnées la nécessité de combiner *:*

- *une analyse de sécurité des architectures du produit avec des tests de sécurité concrets ;*
- *de réaliser une étude non seulement sur le produit lui-même (pour les sociétés de développement) mais aussi sur le système complet où est utilisé le produit (Produit + Couche de communication + éléments centralisés dans le cloud par exemple). Rentre donc en cause l'évaluation de l'écosystème ; »*

et celle de *« conduire des évaluations dans le temps (maintien en condition opérationnelle de la certification de niveau substantiel). »*

Ndr : des discussions récentes avec des acteurs sectoriels engageant avec l'ANSSI des travaux de définition de stratégies de certification normalisée pour des objets complexes (comme une automobile) tendent à confirmer ce point de vue, et à mettre en avant l'apport de certains prestataires existants (PASSI, notamment) pour certaines tâches (revue d'architecture, par exemple). Une illustration de la complexité de la portée de l'assurance et donc de la certification est donnée ci-dessous ; elle ne remet pas en question l'approche SSI classique, mais met en avant que le champ de la certification est de nature à évoluer significativement, tout en continuant à militer pour la certification de briques élémentaires : *« Components are the foundations of all devices. Security*

evaluation and certification of components helps OEM & integrators to select the optimal fit-for-purpose chip, at the best cost/benefit ratio. »



Sujet très important mais controversé dans les débats du fait de la difficulté de reproductibilité des tests, de multiples contributeurs évoquent la nécessité que les tests prévoient des activités de *pentesting* (ou *ethical hacking*) *: « le « Ethical Hacking » mis en œuvre par des experts techniques doit être l'élément central de l'évaluation des produits et services. Les CAB doivent en effet être en mesure d'identifier les chemins d'attaque les plus prometteurs (c'est-à-dire les chemins offrant le meilleur ratio gain/coût), et d'estimer leur coût et leur durée de mise en œuvre, et les compétences requises. Une certification de niveau substantiel doit pouvoir fournir avec un bon degré de fiabilité un niveau d'assurance sur la résistance d'un produit. »*

Il est évoqué que ces activités puissent prendre des formes variées, allant même jusqu'à évoquer la possibilité de *« programmes de bug bounty et d'audits ou tests d'intrusions externes. »*

Ndr : comme évoqué publiquement à de multiples reprises, l'ANSSI a œuvré pour que le niveau élevé prenne en compte la nécessité de *pentesting*, mais n'a pas exclu la possibilité que les niveaux inférieurs y fassent appel.

PROPOSITION D'ACTION : Définir la stratégie de tests (tests des fonctionnalités de sécurité, tests d'intrusion, bug bounty, …) dans le schéma de certification du niveau substantiel.

En termes d'outils, l'exploitation par l'utilisation d'outils spécifiques permet la confirmation de la présence de ces vulnérabilités et permet au CAB de déduire le niveau de performance en sécurité informatique du produit. Il est à noter le souhait général *« de mettre en place une procédure de qualification/validation des outils utilisés pour l'évaluation*[12] *» ; « l'ANSSI pourrait jouer un rôle "d'expertise" pour confirmer (ou non) que les solutions de tests ont des conclusions pertinentes. Cela impliquerait peut être d'envisager un tampon dessus. »*

[12] *« A l'image du PCI COUNCIL qui valide les outils de sécurité dans le cadre de PCI DSS. »*

Il est d'ailleurs évoqué dans une contribution un lien de dépendance potentiel entre la décision de mise en œuvre de *pentests*, pour le niveau substantiel, et la disponibilité d'outils de tests : *« Sur les plates-formes matérielles et logicielles destinées aux objets connectés, nous avons identifié un besoin de test de pénétration physique limités correspondant à des schémas d'attaques bien connus. Par exemple, on pourrait considérer l'usage de glitchs pour perturber un secure boot, ou pour contourner des vérifications d'authentification ou de contrôle d'accès. De telles attaques sont bien connues et relativement accessibles, bien que leur mise en œuvre ne puisse pas être totalement automatisée. Les attaques en canaux cachés les plus simples présentent des propriétés similaires. Une possibilité pourrait être de n'autoriser de tels tests de pénétration que quand il existe sur le marché des outils de référence. »*

PROPOSITION D'ACTION : Identifier les conditions de référencement et qualification/validation des outils utilisés pour l'évaluation de niveau substantiel dans le schéma de certification.

En complément, on peut noter plusieurs commentaires sur le besoin de considérer, dans le périmètre des outils de la certification (et donc sur lesquels des critères de choix doivent être établis), les méthodes utilisées pour exprimer les exigences de sécurité qui seront ensuite à évaluer. Sont cités notamment :

- les méthodologies d'analyse de risque - telles qu'EBIOS RM – dont on note d'une part le besoin *« qu'elles définissent des critères et métriques établis et reconnus pour unifier les objectifs de sécurité »* et d'autre part le potentiel besoin d'évoluer *pour « permettre de créer des besoins génériques couvrant des systèmes d'architecture de type IoT »* ;
- les formats des Profils de Protection ou de sécurité, qui devraient évoluer pour permettre *« d'échelonner les contrôles de sécurité et les activités de processus liées à la sécurité en fonction des risques identifiés, c'est-à-dire de concentrer les efforts là où les risques sont les plus élevés ».*

PROPOSITION D'ACTION : Elargir la thématique du choix des méthodes/outils d'évaluation aux méthodes d'expression des besoins de sécurité, en prenant en compte les facteurs processus et multiniveaux (choix des étapes et des composants particulièrement critiques à valider), et identifier les acteurs d'évaluation pertinents. Compléter également l'approche de labellisation des outils en s'intéressant aux chaines de développement logiciel (cf. liste du chapitre 1).

En termes d'efforts à consacrer aux évaluations, sachant que l'ANSSI propose que la CSPN soit une des références du niveau élevé, le niveau substantiel est jugé, sur la base des éléments de réflexion généraux du chapitre 0, comme devant *« être significativement plus simple, plus rapide et moins couteux que cette CSPN tout en assurant un niveau de confiance des produits/services adaptés aux risques. La CSPN étant définie par un temps d'évaluation de 20 hommes*jours (30 avec de la cryptographie), on devrait donc cibler le niveau substantiel avec un effort moindre ».*

Les estimations pour cette charge d'évaluation varient entre 5 à 15 jours d'intervention d'un laboratoire, cette variabilité du nombre de jours d'intervention d'un laboratoire tenant compte d'une remarque précédente sur la possibilité de niveaux multiples dans le niveau substantiel, et également du nombre de mécanismes de sécurité à évaluer ainsi que la complexité du produit/système.

Une estimation de quelques jours (moins de 5) est donnée pour la charge d'évaluation du niveau élémentaire, avec une proposition de tâches suivantes : *« Approche auto-déclarative de prise en compte des exigences de sécurité par les fournisseurs de solutions, avec contrôle de preuves, par échantillonnage, par une autorité nationale, qui pourrait mandater un organisme d'évaluation. En particulier, il pourrait être vérifié que les exigences de sécurité sont bien prises en compte au niveau du cycle de développement :*

- *prouver avoir formé ses équipes à la conception et au développement sécurisés (ce qui aurait pour effet d'augmenter le marché de la formation continue) ;*
- *prouver l'existence de document détaillant le cycle de développement et les points de contrôle de sécurité mis en place ;*
- *prouver l'utilisation d'outils d'analyse de sécurité dans la chaine de développement et d'intégration logicielle (analyse statique, tests unitaire, fuzzing, etc.). »*

On notera cependant le message de précaution suivant : *« il convient de faire attention à certains produits complexes dont le temps de prise en main fonctionnel peut être important, et pourrait risquer de laisser moins de place au temps réel d'évaluation, notamment du fait des charges réduites des niveaux élémentaire et substantiel. Pour ces situations, il serait souhaitable d'introduire dans les prérequis aux travaux d'évaluation, la notion de support éditeur et/ou la fourniture d'un environnement d'exécution complet de la part de l'éditeur. »*

5. Compétences requises estimées pour les tests d'évaluation

Plusieurs éléments de réponses sont déjà donnés au chapitre 2.

Parmi les compétences requises des évaluateurs, on va retrouver *« les fondamentaux : sécurité hardware, sécurité software (firmware + programmation de plus haut niveau), sécurité des couches de communications (sans fil et filaire : IP / GSM, BT etc), sécurité des applications et architecture dans le cloud, cryptographie embarquée & classique IT, compétence en fuzzing. »*

Pour les niveaux substantiel et élémentaire, l'aptitude à recourir à un outillage et des méthodologies formalisées voire certifiées (voir chapitre précédent) semble un complément indispensable.

Les compétences seront donc liées à l'analyse, à la mise en place et l'exécution des méthodologies et protocole d'évaluation, et à la maitrise des outils d'évaluation (mise en œuvre et interprétation des résultats).

En particulier, les éléments qui semblent pertinents à fournir lors du processus d'accréditation sont :

- *« l'identification des personnes clés et compétences associées (analyse/revue préalable, sélection des méthodes et outils d'essais, analyse/revue des résultats) ;*
- *la démonstration des équipements (outils prédéfinis) ;*
- *la capacité à démontrer la méthode d'évaluation ;*

- *le maintien de compétences en veille pour assurer la mise à jour de l'outil au regard de l'état de l'art qui ne cesse d'évoluer. »*

Dès le niveau élémentaire, *« la certification CEH (Certified Ethical Hacker Certification) des testeurs »* est évoquée *« comme un niveau d'exigence minimal, avec possibilité de laisser ces tests en interne de l'organisme. »*

Pour le niveau substantiel, il est estimé que *« les CAB doivent être à l'état de l'art sur le Ethical Hacking des technologies évaluées. L'objectif n'est pas de mettre systématiquement en œuvre des attaques avancées au niveau substantiel, mais de s'assurer que l'expertise et les équipements engagés sont suffisants pour estimer de façon précise le coût et la difficulté d'une attaque. Les CAB doivent automatiser au maximum ce qui peut l'être pour optimiser leurs coûts et pour concentrer leur expertise sur les analyses à valeur ajoutée. »*

PROPOSITION D'ACTION : Le cas échéant, identifier le niveau de certification (CEH, …) nécessaire pour les testeurs (tests fonctionnels ou tests d'intrusion) pour le niveau substantiel et évaluer l'impact sur les couts associés.

6. Modalités de supervision des activités permettant de s'assurer d'une homogénéité dans les travaux accomplis, et du traitement adéquat des anomalies, en lien potentiellement avec des activités de surveillance de marché

Pour le niveau substantiel, la supervision des activités des CAB est en partie assurée lors de l'évaluation périodique par l'accréditeur sur les processus de l'entité évaluatrice ainsi que par l'autorité nationale de certification.

La surveillance du marché s'entend quant à elle au sens du droit européen. Cette surveillance du marché est organisée et réalisée par les Etats membres.

Pour le niveau élémentaire, cette surveillance de marché requiert une mise en œuvre effective suivant les modalités telles que décrites dans le Règlement européen (CE) n° 765/2008[13] et la décision n° 768/2008/CE. La spécificité du volet sécurité (au sens cybersécurité) n'est - à ce stade - pas évoquée.

En matière de contrôles à effectuer, il est estimé *« qu'une autorité nationale doit être en mesure de réaliser des audits par échantillonnage des éditeurs de produits et fournisseurs de services certifiés, potentiellement en mandatant des organismes d'évaluation. »* Cela est jugé particulièrement nécessaire dans le cas d'une approche auto-déclarative.

Pour le niveau substantiel, en cas d'audit (déclenché de manière aléatoire et/ou en cas de dépassement de certains seuils), une autorité *« doit pouvoir contrôler des preuves (rapports produits par des plateformes d'automatisation de tests de sécurité, résultats d'analyse de code, fichiers de*

[13] Le Règlement (CE) n°765/2008 fixe un cadre pour la surveillance du marché des produits afin de garantir qu'ils répondent aux exigences garantissant un haut niveau de protection des intérêts publics tels que la santé et la sécurité en général, la santé et la sécurité sur le lieu de travail, la protection des consommateurs, la protection de l'environnement et la sécurité. Il fixe également un cadre pour les contrôles sur les produits provenant de pays tiers.

traçabilité des tests, certificats liés aux formations de sécurité dispensées au personnel, etc.). » Ceci imposerait donc au commanditaire d'assurer une gestion régulière d'éléments de preuve devant pouvoir être fournis à l'auditeur. Une même approche peut être envisagée pour contrôler les compétences et les processus des laboratoires d'évaluation, de même que leur capacité à protéger les données clientes.

Quelques points d'attention complémentaires sont soulevés : *« comment agir (quelles actions mettre en place) en cas de suspicion d'évaluations de complaisance ? Audits/contrôles croisés ? Une autorité nationale peut-elle auditer un centre d'évaluation dépendant d'une autre autorité pour les niveaux substantiel et élémentaire ? »*

PROPOSITION D'ACTION : Engager un travail de l'ANSSI avec les autorités sectorielles nationales et les CAB sectoriels existants sur les modalités de surveillance du marché en matière d'évaluation de la conformité (certification ou auto-déclaration).

7. Durées admissibles de validité des certificats et moyens estimés viables de maintien dans la durée de ces certificats

Il est mis en avant que *« les certificats de conformité des produits, services ou systèmes doivent clairement indiquer les risques cybersécurité maîtrisés via une liste de référence d'attaques ou un standard sectoriel reconnu et validé. »*

PROPOSITION D'ACTION : Travailler sur un modèle de certificat de sécurité mettant en avant l'état de l'art pris en compte (niveau atteint/vérifié vis-à-vis d'un référentiel d'attaques à la date de la certification).

En termes de durée de validité d'un certificat, plusieurs options sont proposées, mais toutes conduisent à fixer une durée de 1 à 3 ans.

Sont évoqués quelques principes, notamment que :

- *« un certificat ne soit applicable que sur une version majeure d'un service ou d'un produit ;*
- *la durée est portée à 3 ans si le détenteur du certificat a démontré l'existence d'un système de management des évolutions du produit, service ou système et de la prise en compte des nouvelles menaces. (Les évaluations de surveillance devront alors s'attacher à confirmer ce point pour le maintien du certificat) ;*
- *si l'éditeur peut démontrer un faible écart sur les fonctions de sécurité implémentées entre deux versions majeures (via la fourniture d'un document d'analyse d'impact), les travaux d'évaluation sur une nouvelle version pourraient être allégés. De la même manière, une re-certification pourrait être réalisée avec un niveau d'assurance plus faible (par exemple, un simple audit boite noire sur une nouvelle version, alors qu'un audit boite blanche a pu être réalisé sur la première version certifiée) ; les conditions de réévaluation devraient être conditionnées par le temps. Il est en effet important de prendre en compte le fait que des mécanismes ou implémentation de fonctions de sécurité conforme à un instant T ne soient plus*

acceptable lors de la réévaluation quelques années plus tard. Aussi l'analyse d'impact ne doit pas être limitée aux modifications ;

- *à l'inverse, si le périmètre fonctionnel a significativement évolué, une re-certification complète serait attendue. De même que pour le cas précédent, il faut tenir compte des évolutions des exigences en termes de sécurité entre deux versions relativement éloignées dans le temps ;*

- *il convient de favoriser l'usage des plateformes d'automatisation des tests de sécurité qui auraient l'avantage de pouvoir (re)produire automatiquement des certificats, à un coût réduit. »*

En complément, *« dans le cas de menaces avérées et réelles, l'autorité notifiante pourra demander aux certificateurs de s'assurer auprès des détenteurs de certificats de la prise en compte de ces nouvelles menaces. Dans le cas où ces menaces contribueraient à abaisser le niveau de confiance, le certificat sera révisé en ce sens, potentiellement restreint dans sa classification, voir si besoin suspendu. »*

Ndr : ces éléments ayant également été évoqués dans l'étude de migration du SOG-IS vers un schéma européen, l'ANSSI présente en annexe les propositions émises avec quelques autres Etats Membres.

Une mise en garde est faite sur la nécessité de définir des conditions spécifiques claires pour la maintenance de la certification, en particulier concernant le traitement de nouvelles vulnérabilités, ainsi que le traitement des mises à jour de code. *« Ceci est particulièrement important dans les verticales imposant de fortes contraintes de sécurité (safety), car il y a alors un risque élevé de conflit d'intérêt entre l'urgence du traitement d'une vulnérabilité critique et le besoin de conserver de bonnes propriétés de sécurité. »*

8. Moyens envisagés d'harmonisation des méthodes et pratiques d'analyse de risques, d'évaluation et de certification

De multiples réponses à cette question sont données au chapitre 4 concernant l'harmonisation nécessaire en termes de contenu des tests, de processus et de méthodologie d'évaluation, et de lien nécessaire entre évaluation de sécurité et évaluation métier.

A titre d'illustration, on peut souligner la proposition*, « à l'image de la CEI 62443, de convergence entre des méthodes d'analyses de risques appliquées à des systèmes critiques et des niveaux de safety (ex : SIL, AMDEC) avec des méthodes SSI (ex: Critères Communs ou CC , EBIOS), déjà utilisées dans différents secteurs (ex : familles associées à la CEI 61508), en vue d'une convergence des exigences, pratiques et livrables en commun »*, à titre d'exemple pour l'avionique, entre le duo DO 254 (hardware) + DO -178 (software) et les CC, ou pour les développements logiciels, entre ISO 15288 et CC, ISO 9126 et CC, ou encore ISO 25000: 2014 SQuaRE et CC).

PROPOSITION D'ACTION : Lancer avec l'industrie une étude sur les convergences des méthodes, processus, outils, et exigences des domaines de la *safety* et de la SSI.

En complément, pour faciliter l'harmonisation entre les parties prenantes de la certification, il est proposé qu' *« au plan national, en complément de l'animation du niveau élevé, l'ANSSI ait un rôle*

d'animation et de coordination des CAB (Voir point suivant). » et *« qu'au plan international, une coordination et une information mutuelle sur les méthodologies de tests existent. »*

Il est noté qu'au-delà de l'animation, *« mettre en place des moyens de contrôle efficaces est un prérequis pour assurer une véritable harmonisation des méthodes et des pratiques, pour éviter la course au CAB le moins exigeant, et pour éliminer le risque de distorsion de concurrence liée aux certifications de sécurité. »* Ce point est susceptible de relever des activités de revue par les pairs, mais pas uniquement (la surveillance du marché évoquée au chapitre 6 en est également un pilier potentiel).

Enfin, un poids important est donné à *« la nécessité d'homogénéiser au niveau européen, par schéma, via des référentiels (*l'exemple de SecNumCloud est donné*) ou autres « profils », les spécifications techniques de besoin et les méthodes associées d'évaluation et d'analyse de risques ainsi que les modalités de certification qui préciseraient notamment :*

- *les fonctions de sécurité exigées/recommandées à implémenter ;*
- *les configurations de sécurité exigées/recommandées ;*
- *les exigences/recommandations de sécurité, associées ;*
- *les mesures de durcissement à mettre en place ;*
- *les mesures d'hygiène à mettre en place. »*

9. Besoins identifiés d'accompagnement de la montée en puissance des acteurs par l'ANSSI et l'écosystème existant (CESTI), et détermination des informations pertinentes qui pourraient être échangées (guides, vulnérabilités par exemple) avec l'ANSSI dans le fonctionnement d'un schéma

Tout d'abord, il est estimé que *« la communication sur les schémas existants doit continuer, via l'ensemble des publications de l'ANSSI, afin d'être mieux connus dans les secteurs d'activité, pour permettre la compréhension des acteurs industriels qui veulent aller dans cette démarche, et une meilleure appréhension des schémas futurs. »* En complément, la proposition est faite de *« publications annuelles sur des retours d'expérience chiffrés, notamment sur le rapport coûts/bénéfices), à destination notamment des nouveaux acteurs. »*

Ensuite, *« l'ANSSI et ses CESTI doivent être des acteurs actifs des schémas de certification[14]. Le savoir-faire et l'expérience acquise doivent bénéficier à l'ensemble du marché européen, même si à l'inverse, des laboratoires spécialisés et pointus doivent pouvoir devenir CAB même s'ils ne sont pas CESTI aujourd'hui. »*

Il est rappelé qu'outre son rôle de certificateur dans le schéma actuel national de certification, l'ANSSI joue un rôle majeur dans l'animation de l'écosystème : organisation des échanges techniques de type

[14] En particulier, en termes de prise en compte de retour d'expérience, de support en formation et de soutien sur les méthodes et outils préconisés.

inter-CESTI, participation au JHAS, … permettant un partage des bonnes pratiques et du référentiel technique d'évaluation (outils, attaques, méthodologie, etc). Ces actions permettent une harmonisation des pratiques entre les différents laboratoires et mettent en place une mutualisation de la veille dans le domaine.

Il est ainsi estimé que *« ce rôle est à renforcer dans le nouveau schéma avec une ouverture des inter-CESTIs ou la mise en place d'une coordination particulière aux nouveaux organismes certificateurs, sous la forme, par exemple, de collèges dédiés aux différents niveaux d'évaluation ou aux domaines spécifiques pour sauvegarder la confidentialité des informations critiques (à l'image de l'organisation actuelle avec des réunions spécifiques aux CESTIs hard et soft). »*

Nota : il est remarqué que *« La France, parmi certains autres états, a mis en place un schéma actuel de certification avec une technicité et une pertinence reconnue internationalement. Cette technicité bénéficiant aux acteurs nationaux (laboratoires mais aussi industriels utilisateurs de la certification) doit être maintenue dans la mesure du possible, l'ANSSI, en tant que représentant national, devra œuvrer au maintien de cette technicité dans les nouveaux schémas. »*

PROPOSITION D'ACTION : Engager, sur la base du retour d'expérience national (InterCESTI) et international (JIL et ses sous-groupes) la réflexion sur l'organisation de l'animation des CAB, mettant en avant les valeurs techniques soutenues par la France.

En complément, au niveau national, pour mieux aborder les marchés sectoriels, il est jugé souhaitable *« que l'ANSSI mette en place un ou plusieurs groupe(s) de travail impliquant les éditeurs de produits, les fournisseurs de services, les autorités sectorielles (ANSM, ASIP Santé, …) et les organismes d'évaluations.*

Les objectifs d'un tel groupe de travail seraient :

- *de proposer de nouveaux schémas d'évaluation à l'ENISA ;*
- *de proposer des profils de protection pour certaines catégories de services et de produits ;*
- *de définir les opérations d'évaluation à mener pour chaque schéma, étant donnée la criticité des produits et services concernés ;*
- *d'encourager le développement de référentiels de bonnes pratiques, d'états de l'art et de guides de références ;*
- *de stimuler l'écosystème des éditeurs d'outils d'analyse de sécurité pour qu'ils convergent vers les besoins des schémas ;*
- *de définir un cadre méthodologique commun et borné pour que chaque laboratoire ait les mêmes modalités et conditions d'exécution des prestations.*

Ce groupe pourrait également être en charge de la *« création d'une nomenclature commune des vulnérabilités pour que tous les certificats et les acteurs parlent de la même chose. ».* La mise en place de CERT pour les domaines d'activité en lien avec les différents de schémas de certification (exemple :

pour les vulnérabilités et menaces spécifiques au domaine de la santé, création d'un CERT-SANTE) est également évoquée.

PROPOSITION D'ACTION : Engager la réflexion sur l'organisation nationale de l'animation des communautés sectorielles.

Enfin, il est suggéré que *« l'ANSSI priorise son action vis-à-vis des acteurs ou des produits issus de secteurs industriels qui ne bénéficient pas de certification de sécurité actuellement (aéronautique, automobile, médical, énergie) »*.

Ndr : Ces demandes confirment des actions déjà partiellement engagées par l'ANSSI, sous pilotage de sa division coordination sectorielle (COS).

10. Outils qui permettraient d'automatiser les activités, et compétences nécessaires pour le développement et l'exploitation de ces outils

Pour le niveau d'évaluation élevé, tel qu'il se pratique aujourd'hui dans les Critères Communs ou la CSPN, la compétence de l'évaluateur est très largement utilisée. Il doit imaginer de nouvelles techniques d'attaques, ou, au minimum, adapter la mise en œuvre des attaques connues aux particularités du produit en ciblant généralement les contre-mesures existantes. Cette exigence génère des difficultés pour évaluer l'objectivité et la reproductibilité de l'évaluation entre divers laboratoires, voire entre divers évaluateurs d'un même laboratoire. Les exigences sur les systèmes qualités, l'agrément en sus de l'accréditation, le contrôle des travaux par l'ANSSI sont des éléments mis en place pour limiter (mais pas annuler) cette variabilité.

Il est estimé que *« pour les niveaux inférieurs, dans le contexte d'une pratique industrielle et systématisée (ou très large), ces méthodes sont sans doute inapplicables. Il semble souhaitable d'avoir recours à un outillage et des méthodologies formalisées.*

Le développement d'outils ne doit pas être juste un accélérateur pour la réalisation des tests, ce doit être un prérequis. Il ne s'agit pas de raccourcir le temps requis avec la disponibilité d'un outillage, mais d'inclure certains tests dans l'évaluation uniquement s'ils sont outillés. »

Comme exemple d'outils, on peut citer :

- les outils de scan de vulnérabilités et de test de mots de passe par dictionnaire ;
- les outils de tests de conformité des interfaces (par exemples : outil P-SCAN de CEA Tech/Bureau Veritas - LCIE ; outil NESSUS utilisé par CNPP…)

PROPOSITION D'ACTION : Etablir les spécifications des outils envisageables pour mener les évaluations et analyser l'offre disponible.

La question du modèle économique de production et de diffusion des outils est peu évoquée, mais on note une proposition de *« framework outillé en open source, international, sous responsabilité d'une communauté fédérée par une autorité unique (ex : ENISA), pour gérer les certifications et le référencement des preuves associées ; ce framework permettrait une automatisation de traitements, relances et de production de statistiques. »*

On note également l'intérêt de *« laisser l'écosystème offrir des solutions de tests disponibles dans le cloud, ou prenant la forme de logiciels ou d'appliances virtuelles/matérielles. Le mode d'utilisation (par les éditeurs ou bien uniquement par les laboratoires d'évaluation) doit également être ouvert, mais cadré par des exigences communes aux différents laboratoires. »*

11. Identification des schémas existants réutilisables ou à créer

En matière de certification, de multiples schémas existent actuellement. Ils ont été initiés par des initiatives soit gouvernementales, soit liées à des associations professionnelles.

Sont cités en exemple Cyber Essentials, Cyber Essentials + et ISA Secure :

CYBER ESSENTIALS

Pour contribuer à renforcer les capacités de sécurité de l'information d'organisations de toutes tailles, le gouvernement britannique a élaboré une stratégie en dix étapes et un programme de certification en deux étapes, dont Cyber Essentials (CE) est le premier maillon. La certification Cyber Essential (CE) est une condition préalable à la conclusion d'un contrat avec le gouvernement britannique et permet à une entreprise de démontrer qu'elle dispose d'un niveau de compétence de base en matière de cyber sécurité, c'est une approche accessible et pour un coût limité.

L'organisation identifie les systèmes les plus susceptibles d'être attaqués par un agresseur peu qualifié et met en œuvre un ensemble de contrôles recommandés afin d'assurer une protection de base. Ces contrôles des systèmes d'information comprennent notamment des pare-feux à la frontière du réseau et des passerelles Internet, une configuration sécurisée, le contrôle d'accès, la protection contre les logiciels malveillants et la gestion des correctifs logiciels.

Une fois ces contrôles mis en œuvre, l'organisation remplit un questionnaire détaillé en ligne puis le soumet à une évaluation indépendante par l'intermédiaire d'un des portails Web d'accréditation CE, tels que APMG ou CREST. Un expert en sécurité de l'information d'un organisme de certification tiers examine le questionnaire et confirme si le niveau de mise en œuvre requis pour recevoir la certification CE a été atteint. Le certificat est posté en ligne et l'organisation peut afficher le logo CE sur ses documents de vente et de marketing.

CYBER ESSENTIALS PLUS

Lors de la seconde étape appelée Cyber Essentials Plus (CE+), l'organisation fait l'objet d'un audit indépendant mené par un auditeur, expert en cyber sécurité de l'information qui vérifie que ses systèmes et contrôles répondent aux exigences du programme CE+.

Cette étape implique généralement des tests plus intensifs, y compris des tests de pénétration, une analyse de la vulnérabilité et une visite des installations hébergeant les services.

La certification Cyber Essential (CE+) s'inscrit dans une approche de gestion des risques de l'information et de la cyber sécurité plus complète.

Plusieurs points sont jugés intéressants sur ces deux schémas :

- *« la disponibilité des certificats sur un espace internet en libre accès ;*

- *l'exigence de tests de pénétration pour le niveau Cyber Essentials + ;*

- *la démarche progressive pilotée par le niveau de risque ou de menace. »*

ISA Secure

ISA Secure est une méthode d'évaluation applicable pour des produits, des installations industrielles et des processus d'entreprise. Le référentiel normatif utilisé pour cette évaluation, est la norme IEC 62443 qui a été développée à l'origine par le groupe ISA (International Society of Automation).

Le schéma de certification proposé par ISA Secure est détenu par l'ISCI, il requiert une accréditation par un organisme accréditeur national.

Chaque partie de la norme comporte une liste fournie d'exigences techniques, dont la conformité est évaluée sur la base de la preuve amenée par l'organisme audité. La nature de ces preuves est variée, par exemple :

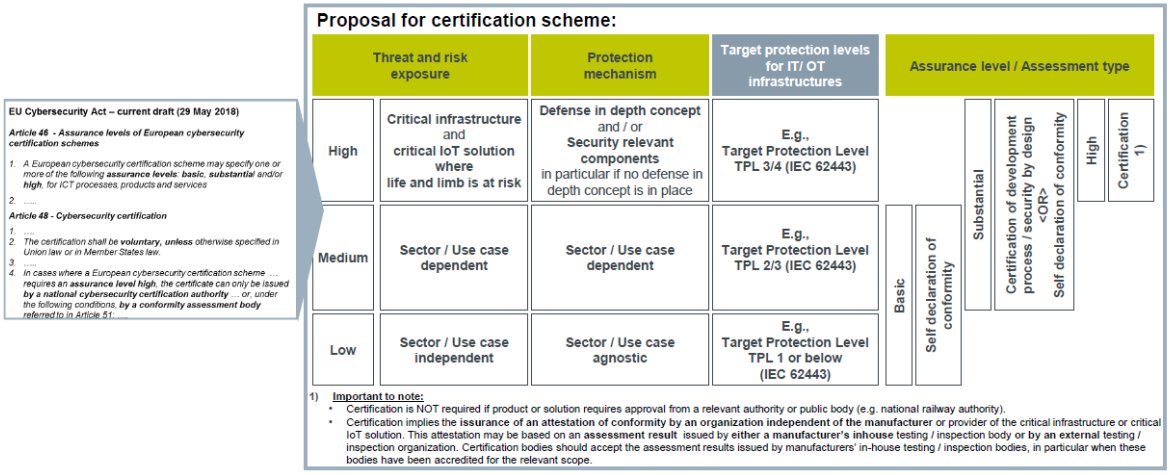
- Politique et Procédures
- Manuels utilisateur
- Manuels produit
- Rapports de tests
- Documents sur les outils de sécurité utilisés
- Rapports d'activités
- Enregistrements d'événements
- Rapports d'audits
- Checklist
- Copie d'écran
- Rapport d'incidents
- Traces (Log) fournies par le produit/la solution
- Historiques gérés par le produit/la solution

L'évaluation globale clause par clause est complétée par un test de robustesse des interfaces du produit. Ce test consiste à solliciter les interfaces réseaux du produit (*flooding, fuzzing*) et à vérifier que les fonctions déclarées importantes sont préservées et restent opérantes.

Après acquittement d'une redevance, quelques laboratoires à travers le monde (CSSC, Exida, TUV Rheinland) ont été reconnus par ISA Secure et sont aptes à délivrer des certificats sur quatre parties essentielles de la norme IEC 62443 (2-3, 3-3, 4-1, 4-2). La certification sur la base de l'IEC 62443 (ISA Secure ou autre) est internationalement reconnue dans le monde industriel.

Une proposition de correspondance entre les niveaux de l'IEC 62443 et les niveaux de certification du *Cybersecurity Act* est faite dans la figure ci-après.

Proposal for a certification scheme aligned with the assurance levels of the EU Cybersecurity Act



SESIP

Ce schéma SESIP[15] (*Security Evaluation Scheme for IoT Platforms*) s'intéresse aux technologies sous-jacentes de l'IoT, qui définissent les fonctions de sécurité de base, et a pour vocation la certification d'objets connectés reposant sur des technologies elles-mêmes certifiées, permettant ainsi de simplifier le processus de certification de ces objets sans sacrifier leur niveau de sécurité.

Sont cités également des exemples de schémas de certification « métier » intégrant le volet cyber sécurité :

Certification NFA2P pour les centrales d'alarme et les transmetteurs d'alarme

Le dispositif mis en place permet d'attester, par l'apposition du logo « @ » à la marque de certification NFA2P, du respect des exigences relatives à la sécurité informatique applicables aux centrales d'alarmes et aux transmetteurs d'alarme, en cohérence avec le niveau de sécurité physique et électronique applicable (niveaux 1, 2 ou 3 en fonction de la classe de risque associée au produit selon le référentiel de certification produit).

[15] La version est disponible publiquement sur https://trustcb.com/iot/sesip/ , et les premières évaluations pilotes vont démarrer dans les premiers jours de 2019.

Certification A2P pour les serrures de bâtiment

Le dispositif mis en place permet d'attester, par l'apposition du logo « @ » à la marque de certification A2P, du respect des exigences relatives à la sécurité informatique applicables aux serrures connectées, en cohérence avec le niveau de sécurité physique et électronique applicable (niveaux 1, 2 ou 3 en fonction de la classe de risque associée au produit selon le référentiel de certification produit).

Certification CNPP Certified pour les caméras de vidéosurveillance et les enregistreurs vidéo numériques

Les référentiels techniques applicables dans le cadre de ces certifications imposent que les produits respectent l'exigence d'un niveau de sécurité informatique supérieur ou égal à 1. Il est proposé au demandeur de valoriser le niveau de sécurité informatique obtenu par le produit lors des essais sur le certificat CNPP Certified. Ce dispositif est applicable à toute évaluation de la conformité d'un produit de sécurité / sûreté présenté sous le modèle « objet connecté ».

Enfin, d'autres exemples sont cités *« qui peuvent servir d'inspiration :*

- *les schémas Mifare et Felica, représentatifs au niveau organisationnel (un laboratoire peut être évaluateur ou certificateur) ;*
- *les schémas FIPS et PCI DSS, représentatifs pour leurs modalités d'évaluation des experts et leurs modalités d'audit (le schéma PCI DSS propose 12 points de contrôles particulièrement pragmatiques). »*

Au-delà de l'inspiration, *« la nécessité d'établir des liens avec les porteurs/leaders internationaux des schémas de certification (à titre d'exemples : UL2900, OWASP, GSMA IoT security, IIC guidelines, PCI certifications, IEC 62443), pour la reconnaissance des certificats UE hors UE »* est affichée comme un critère de succès de la certification européenne. *« Ces liens doivent permettre de partager des exigences communes (besoins, suites de tests…). »*

12. Règles attendues de protection des activités liées à l'évaluation et à la certification de sécurité

De manière générale, il est jugé que *« toutes les activités d'un CAB liées à un produit tiers doivent être strictement protégées. La confidentialité des informations liées à un produit doit être scrupuleusement respectée. Des mesures spécifiques doivent être mises en place pour minimiser l'impact d'une faille de confidentialité du laboratoire ou du CAB. »*

Plus précisément, est évoqué *« l'intérêt des laboratoires pour que les règles actuelles en vigueur soient maintenues pour le niveau élevé : sauvegarde du savoir-faire des laboratoires, confidentialité de certains savoir-faire critiques (ne pas diffuser des techniques permettant d'attaquer des produits sur le marché). ».* Il est en complément évoqué que *« les règles attendues de protection pourraient être similaires à celles régissant les activités des PASSI »*.

Il est à noter que quelques voix se font entendre pour mettre en avant que pour les travaux d'évaluation au niveau élémentaire, et ceux au niveau substantiel qui se cantonneraient à une analyse boite noire d'un produit ou d'un service*, « il ne semble pas nécessaire d'imposer ce niveau de*

protection du niveau élevé. Pour ces travaux, il est tout de même attendu le suivi d'un minimum de règles d'hygiène (contrôle d'accès, stockage et transmission sécurisées, etc.). » Cependant, elles ne remettent pas en question le sujet de la gestion propre des vulnérabilités.

PROPOSITION D'ACTION : Organiser la publication des vulnérabilités en bonne intelligence avec les offreurs et les règles applicables aux CERTs et préserver le contrôle réglementaire des 0-days, y compris pour les niveaux substantiel et élémentaire.

Les CAB doivent également être protégés des pressions pouvant influencer les résultats des évaluations. *« Les règles de confidentialité et de responsabilité de l'ISO 17065 doivent s'appliquer pleinement. »*

En complément, le schéma français actuel de certification définit l'activité d'évaluation comme un engagement de compétences et de moyens et n'implique pas la responsabilité des laboratoires dans le cas d'une faille détectée après la certification *: « cet aspect doit être maintenu dans le cadre des nouveaux schémas »*.

PROPOSITION D'ACTION : S'assurer d'un cadre de responsabilité pour les acteurs de la certification de cybersécurité se basant sur les ISO/IEC 17065/17025/17021 (régissant les aspects confidentialité, impartialité et gestion des conflits d'intérêt).

13. <u>Tout autre thème jugé pertinent</u>

Pour soutenir la proposition d'action vis-à-vis de la certification des briques open source, il est *« préconisé d'aborder spécifiquement ce sujet dans les nouveaux schémas, et de publier un guide dédié à destination des communautés, avec notamment les problématiques afférentes : financement, interaction avec les communautés. »*

L'ANSSI, qui finance annuellement de multiples évaluations de briques et logiciels open source en vue de leur certification, et soutient financièrement les projets associés de certaines communautés, ne peut que partager cette idée, et peut largement faire part de son retour d'expérience.

Annexe 1 : Liste des contributeurs à l'AMI

Activus

Amossys

Bureau Veritas

CEA Tech

CNPP

COFRAC

Eshard

Eurosmart

Gemalto

LNE

NXP Semiconductors

Red Alert Labs

SCASSI

Serma

Siemens

ST

Trusted Labs

Contact ANSSI : Franck Sadmi, 01 71 75 89 30, franck.sadmi@ssi.gouv.fr

Annexe 2 : Propositions en matière de gestion de la durée de vie des certificats pour la transition du SOG-IS vers un schéma européen

Ndr : Reproduction des éléments donnés en SOG-IS MC aux membres du SOG-IS, à la Commission Européenne (DG Connect), et à l'ENISA.

To handle the needs for both a) Monitoring compliance of certificates and b) Dealing with undetected cybersecurity vulnerabilities, the proposal is to adopt the following:

- CABs to establish an administrative validity of certificates, as defined in the draft CCRA document: certificate will be published for 5 years.
- CABs to work on improving evaluation methods, so that the assurance gained during the initial certification process retains some of its validity on forthcoming updated versions (e.g. by evaluating the patch mechanisms on the product and patch processes from the developer), where evidence can be provided that those updates are issued according to a defined set of requirements.
- Developers to commit to:
    - performing an impact analysis of all changes over the course of the product's lifecycle, including fixes for errors and vulnerabilities, and functional modifications[16] to the product;
    - monitoring CVEs and other published security vulnerabilities that may apply to the certified product, and submitting an impact analysis where necessary to their CAB , to demonstrate that actions taken allow to maintain the security level;
    - a responsible and public communication on analysis resulting from the previous points, including liaising with the CAB and its national CERT – part of the international CERT community - for the publication, where necessary, of a specific CVE associated to the product;
    - handling complaints received from their clients and responding to them with appropriate measures.

Comment#1: in order to allow the certificates to cover the corrected versions of a certified product, this might imply that the certificate is established for the evaluated version x.y1 and all following minor versions x.y2… based on the permanent monitoring process.

Comment#2: part of these requirements might be covered by a better use of existing flaw remediation requirements from the Common Criteria (ALC_FLR.x).

[16] Functional modifications should only remain minor; otherwise a new certificate should be issued for the associated new product.

- CABs to proceed to a periodic[17] review of certificates, based on a security assessment[18] from an ITSEF that takes into account the impact analysis of accumulated changes from the previous evaluation and an updated State of the Art, in order to confirm[19] the security certificate.
- CABs to withdraw certificates in the following cases:
    - evidence that the developer does not respect its commitments;
    - a security reassessment has led to a FAIL verdict and no correction may apply.

[17] The applicable period (and associated sponsorship rules) is to be defined by the risk owners who consume certificates.

[18] The security assessment will most probably require redoing some evaluation tasks, depending on the impact analysis on the one hand, and the evolution of the State of the Art of attacks (for the specified security level) on the other hand.

[19] In case the assessment is successfully passed the validity of the certificate could be extended; if the initial requirements are no longer met, it could lead to issuing a new certificate with a scope reduction (either on functionality or assurance), or to withdrawing the certificate.