Certification européenne de Cybersécurité : bâtir un marché des TIC de confiance à 27

Chloé BLONDEAU
Experte Nationale Détachée de l'ANSSI auprès de l'ENISA

Des fondations hétéroclites

Les évaluations, labels de confiance et certifications de sécurité de produits et services TIC sont nombreux sur le marché et complexes à appréhender. Proposés par des entités privées, des organisations professionnelles ou des états, chacun y accorde sa propre définition de la confiance en y rattachant des mesures de sécurités et des processus d'évaluations spécifiques. Si quelques certifications de sécurité telle que celle des Critères Communs[1] portant sur les produits TIC s'appuient sur des normes internationalement reconnues, il y a encore peu de reconnaissance mutuelle entre les pays de l'Union européenne.

La France compte un certain nombre de schémas de certification et de qualification de produits et services TIC sous la bannière des Visas de Sécurité délivrés par l'ANSSI[2], mais ce n'est pas le cas chez tous nos voisins européens. Concernant les Critères Communs par exemple, il y a seulement 8 pays européens en mesure de délivrer des certifications au niveau national et 13 pays utilisateurs de ce type de certificats pour exiger ou justifier le bon niveau de sécurité d'un produit TIC.

Si la certification est un enjeu de confiance technologique, elle est également une problématique de marché. Hormis les cas de reconnaissance mutuelle, les industriels ne peuvent faire reconnaitre dans un pays une certification reçue dans un autre. Les efforts et les coûts de pénétration de marchés étatiques tiers ou de secteurs sensibles requérant des engagements de sécurité via la certification peuvent paraitre dissuasifs.

Au travers de la certification européenne de cybersécurité, l'Union souhaite harmoniser les niveaux de confiance qu'il est possible d'avoir dans les solutions TIC. Concrètement un certificat accordé en Europe dans le cadre du cadre européen de certification sera reconnu dans les autres pays de l'Union.

Cela implique non seulement que les contrôles techniques soient les mêmes mais que les organismes assurant les audits et évaluations ainsi que les organismes de certification suivent les mêmes procédures.

1 Common Criteria : New CC Portal (commoncriteriaportal.org)

2 Visa de sécurité | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

L'Union Européenne a ainsi mandaté l'ENISA, l'Agence de l'Union européenne pour la cybersécurité pour mener les travaux de préparation des schémas de certification européenne de cybersécurité.

Les outils européens

En 2019 le *Cybersecurity Act*[3] a permis de pérenniser le mandat de l'ENISA, l'Agence de l'Union européenne pour la Cybersécurité, et d'élargir ses missions afin de soutenir un niveau élevé commun de cybersécurité dans toute l'Europe.

Le texte détermine comment l'ENISA doit mettre en place le cadre de certification européenne et ses enjeux. Il définit le cadre de travail ainsi que les instances qui soutiendront l'ENISA dans ces travaux. Il détaille également la possibilité d'utiliser trois niveaux d'assurance dans les différents schémas ou encore la nécessité de considérer les standards internationaux existants.
D'autres législations européennes ont un impact sur le développement des schémas de certification et nécessitent une prise en compte en amont, au sein des futurs schémas de certification. Qu'elles soient existantes telles que la directive NIS2, eIDAS 2 ou en cours de définition comme le *Cyber Resilience Act* ou le *AI Act.* Ces législations peuvent, ou vont devoir, compter sur la certification européenne comme un gage de conformité lorsqu'il s'agit d'évaluer la sécurité des produits, services ou processus TIC.

En complément, dans sa communication du 18 Avril 2023[4] présentant le *Cyber Solidarity Act*, la Commission Européenne mentionne son projet d'élargissement du périmètre du *Cybersecurity Act* pour permettre la certification de « services de sécurités gérés », autrement dit de prestations de services de cybersécurité, jusqu'alors hors du mandat.

Les bâtisseurs de la certification

L'ENISA travaille avec l'écosystème en vue d'élaborer les schémas de certification. Suite à des appels publics à participation, l'agence européenne s'appuie sur des groupes de travail rassemblant les parties prenantes des secteurs concernes pour chacun des schémas.

Ces *Ad hoc Working Groups* rassemblent une vingtaine de membres statutaires, des experts ainsi que des représentants des états membres, souvent issus des différentes agences nationales de cybersécurité. Organisés parfois en sous-groupes ces acteurs apportent leur contribution à la définition des enjeux des schémas et des exigences de sécurité. Les états membres sont également consultés plus spécifiquement au travers de l'ECCG, *European Cybersecurity Certification Group.* Au-delà d'exprimer son opinion sur les schémas, l'ECCG, s'est organisé avec le soutien de l'ENISA pour adresser des sujets horizontaux aux différents schémas de certification, comme celui de la cryptographie. Jusqu'alors plutôt discutée en vue de la protection des informations classifiées, la cryptographie va ainsi faire l'objet d'harmonisation pour les solutions certifiées visant le marché intérieur.

Au travers du SCCG, le *Stakeholder Cybersecurity Certification Group* mis en place par la Commission Européenne et composé d'un échantillon représentatif du marché de la cybersécurité, le secteur privé est aussi consulté afin d'orienter la stratégie de développement des schémas et la définition des sujets prioritaires.

3 Règlement (UE) 2019/881 du parlement européen et du conseil (règlement sur la cybersécurité) EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)
4 Cybersécurité : vers un renforcement des capacités de l'UE à des fins de coopération opérationnelle effective, de solidarité et de résilience https://ec.europa.eu/commission/presscorner/detail/fr/IP_23_2243

Les organisations européennes et internationales de normalisation tels que l'ETSI et le CEN-CENELEC ainsi que l'EA, l'agence européenne d'accréditation sont également parties prenantes des travaux.

L'avancement des travaux

L'Agence de l'Union européenne pour la cybersécurité a entamé les premiers travaux de certification en novembre 2019 avec le lancement du groupe de travail pour la transformation du schéma SOG-IS des Critères Communs portant sur les produits TIC en un schéma européen : EUCC. Ce schéma comporte deux niveaux d'assurance : substantiel et élevé. La proposition de l'ENISA sur ce schéma est en passe de devenir un acte d'exécution de la Commission Européenne. Par la suite commencera une période de transition. L'ENISA a engagé des premiers travaux sur la stratégie de maintenance du schéma.

EUCS, *European Cybersecurity Certification scheme for Cloud Services*, est le schéma de certification portant sur les services Cloud. Ce schéma proposera trois niveaux d'assurance et s'inspire en partie des schémas nationaux existants tel que SecNumCloud ou encore le schéma allemand C5. Un des sujets qui fait débat et donne beaucoup d'exposition médiatique aux travaux, est l'intégration d'exigences garantissant une immunité aux législations non européennes pour le niveau le plus élevé.

Les travaux portant sur la certification 5G ont démarré en novembre 2022. Une première phase a permis d'analyser les systèmes d'évaluation et de certification industriels existants, en particulier ceux de la GSMA, et leurs mises à jour nécessaires pour se conformer au *Cybersecurity Act*. Un premier projet de schéma devrait être disponible pour consultation publique vers la fin de l'année 2023.

En parallèle de la rédaction des schémas, l'ENISA organise des pilotes sur tout ou partie des exigences proposées dans les projets de schémas en vue de tester l'applicabilité des mesures et leur cohérence. Ainsi ces pilotes ont pu porter sur la transition entre une certification SecNumCloud et un niveau élevé du futur EUCS ou encore sur le processus d'accréditation pour les futurs organismes d'évaluation et de certification dans le cadre de EUCC. De manière plus horizontale, des pilotes portent également sur le processus de remontées de vulnérabilités et de communication entre les différents acteurs dans le cas d'une vulnérabilité sur une solution certifiée.

Afin de répondre aux futures législations, aux évolutions règlementaires et d'anticiper la question de la certification des nouvelles technologies, l'ENISA développe des études de faisabilité. L'Agence européenne étudie ainsi la possibilité de, soit réutiliser des schémas existants, soit d'identifier les nouvelles méthodes d'évaluation. A ce jour deux études de faisabilité sont en cours, une portant sur l'EUID *Digital Wallet* et l'autre sur l'intelligence artificielle.

Et après la livraison des schémas ?

L'application des schémas de certification revient aux états membres et aux autorités nationales de certification de cybersécurité désignées. En France, ce rôle est détenu par l'ANSSI.

Ces dernières auront la responsabilité de surveiller le marché, notifier les organismes d'évaluation de conformité souhaitant évaluer et certifier. Ce sont elles qui certifieront ou délègueront pour le niveau élevé des schémas.

L'ENISA de son côté contribue à la maintenance et à la mise à jour des schémas de certification. Elle développe ainsi les guides qui permettront une

interprétation harmonisée des exigences, des processus et des modèles de documentations nécessaires à la conduite des évaluations.

L'Agence européenne soutient le nouveau marché créé *via* la certification avec le développement d'un site internet dédié. En façade, celui-ci aura pour mission de promouvoir et de suivre l'historique des certificats émis à travers la publication d'un catalogue, de diffuser les documents nécessaires à la certification ainsi que les informations en vue de guider le marché en amont et tout au long du cycle de vie des certificats.

En coulisses, il permettra aux organismes certificateurs d'émettre des certificats avec une identification unique et un label ainsi que des tenir à jour les informations de ces derniers.

L'ENISA tend également à accompagner l'écosystème vers la certification en organisant une conférence rassemblant annuellement une communauté toujours plus grande.