Démarches de sécurité & certification : atouts, limitations et avenir

Christian Damour

Orange Business Services
Silicomp-AQL
1 rue de la Chataigneraie
CS 51766,
35517 CESSON-SEVIGNE Cédex France
Christian.damour@aql.fr

Résumé Après une introduction à la problématique générale de la confiance en matière de sécurité des systèmes d'information (confiance que l'on peut placer dans les produits ou systèmes TI) et de la façon dont on peut garantir cette confiance et la transférer entre entités, entreprises ou individus, nous évoquons quelques-unes des démarches de sécurité applicables dans ce contexte. Puis nous faisons un focus sur les démarches de certification existantes en matière de sécurité des systèmes d'information, avec leurs différents domaines de couverture. A partir de l'exemple des Critères Communs, nous introduisons les CESTI, la certification des produits et systèmes de sécurité, ainsi que les accords internationaux de reconnaissance mutuelle des certificats de sécurité. Enfin, nous évoquons les limitations de la certification : les pièges à éviter, nos conseils et les solutions pour y remédier. Vient ensuite une conclusion sur les atouts et la valeur ajoutée, ainsi que sur l'avenir des démarches de certification.

Mots-clés : Sécurité, confiance, certification, accréditation, agrément, reconnaissance mutuelle, certificats, critères communs.

1 Introduction

En matière de sécurité des systèmes d'information, la problématique de la confiance est une préoccupation essentielle de tous les acteurs : confiance dans les produits mis en œuvre, confiance dans les offres de service des opérateurs, confiance dans le système d'information de l'entreprise et les processus mis en œuvre, confiance dans les acteurs qui sont concernés au premier chef par le niveau de sécurité global d'un système d'information. Nous en voulons pour preuve les attaques que l'on qualifie d'ingénierie sociale, consistant à identifier les acteurs clefs d'une organisation et à mettre en œuvre des moyens détournés de récupération illicite d'information sensible, de façon à préparer et à permettre la mise en œuvre d'une attaque ciblée.

L'objectif du présent article consiste à :

- poser la problématique,
- mettre en avant l'existence de démarches de sécurité et de plusieurs référentiels de certification permettant de répondre chacun à un ou plusieurs aspects la problématique,

- apporter un éclairage particulier sur le référentiel des Critères Communs[1], fondé sur notre expérience en tant que CESTI[2] :
  - identifier les atouts d'une telle démarche de certification,
  - identifier les limitations et les pièges à éviter dans le cadre de la mise en oeuvre d'un telle démarche.

2 La sécurité et la problématique de la confiance

A l'heure de la mondialisation et de la dématérialisation des échanges, la sécurité des systèmes d'information se doit de mettre en œuvre une approche globale, qui ne soit plus fondée sur une approche purement technologique, comme nous pouvons parfois être amenés à le croire.

S'agissant de sécurité, la résistance d'une chaîne est toujours celle du maillon le plus faible (même une fois toutes les précautions prises, une seule faille ou combinaison de failles suffit au pirate pour entrer) Les trois piliers fondamentaux de la sécurité sont donc à prendre compte dans leur globalité :

- le système informatique,

mais aussi :

- l'organisation, les processus, y compris la sécurité physique,
- les personnels (confiance et sensibilisation au respect des procédures).

Dans le cadre de systèmes d'information s'ouvrant de plus en plus sur l'extérieur et intégrant des solutions de mobilité avec accès à distance au système d'information de l'entreprise, les fondamentaux restent applicables, avec la logique complémentaire de protéger les activités vitales de l'entreprise et son savoir-faire, tout en facilitant l'ouverture du système d'information sur l'extérieur.

3 La sécurité : un effort permanent

Maîtriser la sécurité d'un système d'information nécessite un effort permanent dans le cadre d'une démarche de progrès axée sur la maîtrise des technologies et des processus, la sensibilisation et la communication. Il nécessite d'avoir recours périodiquement à des organismes extérieurs indépendants et de confiance à forte expertise (cabinets d'audit sécurité tels que les CESTI) et de mettre en place un processus de mesure fiable reposant sur des indicateurs (notion de tableau de bord SSI[3]).

4 Les démarches de sécurité

Améliorer le niveau de sécurité de son système d'information nécessite en tout premier lieu de connaître son besoin de sécurité :

- quels sont les éléments sensibles à protéger (classification des actifs du système d'information) ?

[1] Cf `http://www.commoncriteriaportal.org/public/developer/index.php?menu=2` et `http://www.ssi.gouv.fr/fr/documentation/index.html\#evaluation`

[2] CESTI : Centre d'évaluation de la sécurité des technologies de l'information : cf `http://www.ssi.gouv.fr/fr/confiance/cesti.html`

[3] Cf `http://www.ssi.gouv.fr/fr/confiance/methodes.html`

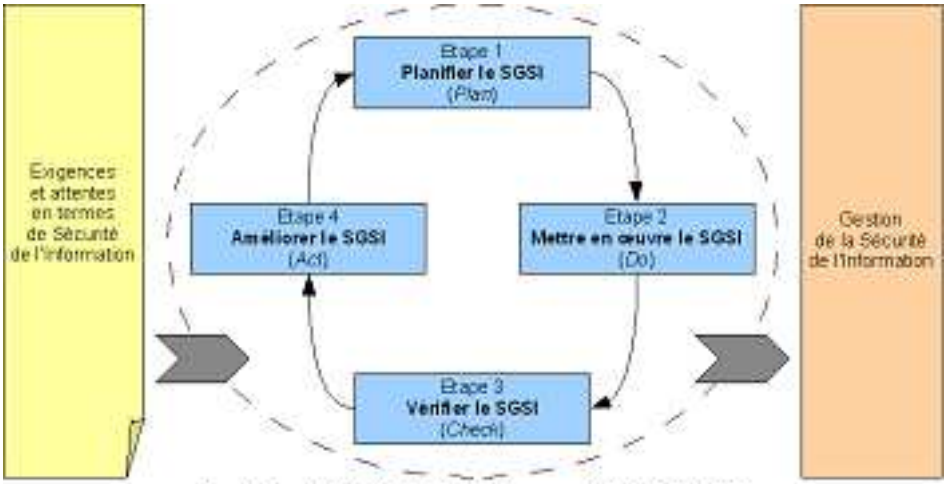

Illustration 1 : Modèle PDCA de la norme ISO 27001:2005

– contre quelles menaces internes, externes (analyse du risque : démarches telles que EBIOS[4], MEHARI[5], ...) ?

A partir de cette connaissance, il est possible de mettre en place des solutions technologiques et des processus (référentiel ISO17799[6], ISO27001) tout en gardant présent à l'esprit la nécessité de communiquer auprès des acteurs concernés de l'entreprise : mise en place de groupes de travail, d'une fonction de RSSI[7] et d'une organisation claire des responsabilités en matière de sécurité, d'une cellule interne de veille et de communication, etc.

La prise en compte de la sécurité dans les démarches de développement sur les projets internes de l'entreprise, la définition d'une politique de sécurité de l'information, la définition d'une architecture de sécurité appropriée, le choix de produits certifiés selon les Critères Communs (norme ISO15408), la définition et la mise en œuvre d'un Plan de Continuité d'Activité, la réalisation d'audits de sécurité internes et externes périodiques, sont autant de moyens qui concourent à l'amélioration du niveau de sécurité global de l'entreprise.

5 Quelques référentiels de certification

En réponse à la question de la confiance, plusieurs référentiels de certification apparaissent naturellement comme des réponses à la problématique globale :

– Le référentiel des Critères Communs ou norme ISO15408 pour les produits, systèmes informatiques, solutions et services à valeur ajoutée.
– La norme ISO27001 pour les processus et l'organisation de la sécurité.
– La norme ISO17024 et les référentiels de certification des individus.

[4] Cf `http://www.ssi.gouv.fr/fr/confiance/methodes.html`
[5] Cf `https://www.clusif.asso.fr/fr/production/mehari/`
[6] Cf `http://www.iso-17799.com/`
[7] RSSI : Responsable Sécurité des Systèmes d'Information

Tous ces référentiels ne sont pas au même niveau. Encore faut-il savoir positionner la question de la certification en deux étapes majeures :

- Quels référentiels pour la certification des technologies, des organisations et des personnes ?
- Quels référentiels pour valider l'impartialité et l'objectivité des acteurs intervenant dans les processus d'évaluation et de certification et garantir la répétabilité et la reproductibilité de leurs travaux ?

Le dénominateur commun de toutes ces démarches de certification consiste à mettre en place une organisation et des processus garantissant la confiance dans la valeur des certificats décernés. On peut citer :

- L'organisme d'évaluation (organisme indépendant et de confiance avec une expertise reconnue) qui effectue les vérifications nécessaires et délivre ses conclusions à l'organisme de certification.
- L'organisme de certification (organisme indépendant et de confiance avec une expertise reconnue) qui contrôle les travaux de l'organisme d'évaluation et décide ou non de décerner le certificat, au vu des résultats de l'évaluation.
- L'organisme d'accréditation[8] (organisme indépendant et de confiance spécialisé dans les processus et la qualité) qui contrôle que l'ensemble des processus qualité nécessaires à la bonne réalisation de leurs travaux est bien parfaitement défini et effectivement appliqué par les organismes ci-dessus.

Nota Bene : les rôles d'organisme d'évaluation et d'organisme de certification peuvent parfois être confondus. Prenons pour exemple, dans un autre domaine, le cas du contrôle technique automobile où le macaron est apposé directement par le centre ayant procédé aux vérifications, lequel a préalablement été dûment agréé par les autorités compétentes. Si nous revenons à la liste des référentiels, les normes d'accréditation des organismes d'évaluation et de certification (en France par le Cofrac) sont réparties comme indiqué dans le tableau 1) :

Domaine d'application / Portée	Organisme d'évaluation	Organisme de certification
Produits et systèmes technologiques	ISO17025 (ex-EN45001)	EN45011 / ISO/CEI Guide 65
Organisation et processus de la sécurité	ISO17021 (ex-EN45012)	
Certification des individus	ISO17024 (ex-EN45013)	

TAB. 1: Normes d'accréditation des organismes d'évaluation et de certification en France

Quant aux référentiels d'évaluation et de certification, ils sont donnés en tableau 2.

Domaine d'application / Référentiels	Référentiels
Produits et systèmes technologiques	Critères Communs (norme ISO15408)*
Organisation et processus de la sécurité	Norme ISO27001**
Certification des individus	CISSP, ISO27001 Lead Auditor, etc.

TAB. 2: Référentiels d'évaluation et de certification (* Voir le registre international des certificats Critères Communs : `http ://www.commoncriteriaportal.org/public/consumer/index.php ?menu=4` ; ** voir le registre international des certificats ISO27001 : `http ://www.xisec.com/`

[8] En France le Cofrac (COmité FRançais d'ACcréditation) : `http://www.cofrac.fr/`

6 Les Critères Communs : référentiel de certification

Dans le domaine des produits, systèmes informatiques, solutions et services à valeur ajoutée, les Critères Communs constituent un référentiel complexe, difficile à appréhender, mais ayant démontré une réelle efficacité, et possédant de nombreux atouts.

Ce référentiel présente les qualités suivantes :

- Il est générique dans ses applications à tout type de produit ou système (logiciels, matériels, systèmes, réseaux, solutions complexes à haute valeur ajoutée), mais souvent fustigé pour sa complexité et les difficultés d'appréhension que cela engendre.
- Il garantit la confiance dans les résultats à travers le recours à des organismes dont la compétence et l'indépendance sont reconnus.
- Il est normalisé à l'échelle mondiale.
- Il fait l'objet d'une reconnaissance internationale des certificats. Un certificat émis dans un pays a la même valeur dans tous les pays au monde signataires des accords.

Les Critères Communs sont génériques. C'est là un atout considérable qui en fait un standard de fait dans de nombreux domaines d'application : les cartes à puce, la Défense nationale, l'OTAN (niveau EAL3) et dont l'application s'étend jusqu'à des firewalls, des sites industriels de conception et de production de cartes à puce, des services de VPN d'opérateurs de télécommunications, des solutions de signature électronique par transposition en droit français de la Directive européenne n ° 1999/93/CE sur la signature électronique.

Le processus de qualification au niveau standard et les Profils de Protection rédigés sous l'égide de la DCSSI en sont une illustration. Ils concourent à faciliter la mise en œuvre des Critères Communs et à en faire un standard de fait dans l'industrie, en visant à permettre la comparaison du niveau de sécurité entre les produits/solutions du marché.

En outre, l'un des objectifs de la DCSSI est de faire normaliser par l'Afnor (Association Française de Normalisation) ces mêmes Profils de Protection. De ce fait, ils pourront être cités comme des textes de référence applicables dans le domaine des appels d'offres publics (conformément au Code des Marchés Publics).

Bien au delà de cela, le gouvernement français, sous l'égide de la DGME/SDAE (Direction Générale de la Modernisation de l'Etat / Service du Développement de l'Administration Electronique) met en place, avec le concours de la DCSSI un Référentiel Général de Sécurité (RGS) fondé principalement sur la PRIS V2 (ou Politique de Référencement Intersectorielle de Sécurité, Version 2.1 [9]).

Ce référentiel vise à standardiser le niveau de confiance que peuvent avoir les administrations françaises dans différents services de sécurité (confidentialité, identification, authentification, signature, horodatage,...) et à définir les processus de vérification associés, lesquels s'appuient le plus souvent sur la certification selon les Critères Communs et des Profils de Protection.

7 Le Schéma Français d'évaluation et de certification et les accords de reconnaissance mutuelle des certificats

Un exemple d'application du référentiel de certification de la sécurité que constituent les Critères Communs est le Schéma Français d'évaluation et de certification.

Ainsi, le Cofrac accrédite les CESTI selon la norme ISO17025.

[9] Cf `http://synergies.modernisation.gouv.fr/rubrique.php3?id_rubrique=285`

La DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) intervient à la fois en tant qu'organisme national de certification et en tant qu'organisme national en charge de l'agrément des CESTI.

En outre, la DCSSI dispose d'un manuel qualité tant pour ses activités de délivrance de certificats selon les Critères Communs que pour celles d'agrément des CESTI : Manuel qualité du centre de certification version 1-0 et des procédures associées (Source `http ://www.ssi.gouv.fr/fr/documentation/index.html#evaluation`).

Les CESTI conduisent leurs travaux d'évaluation :

- Selon un référentiel qualité approuvé (leur Manuel Qualité d'Evaluation et les procédures associées soumises à l'approbation du Cofrac et de la DCSSI à l'occasion d'audits périodiques).
- Avec le référentiel des Critères Communs et sa méthodologie d'évaluation associée.
- Sous le contrôle de la DCSSI qui approuve l'ensemble des travaux réalisés et délivre le certificat de sécurité à l'issue d'une conclusion favorable des travaux d'évaluation conduits par le CESTI.

Toute cette organisation a pour finalité une maximisation de la confiance que l'on peut attendre dans les résultats de ces travaux, sans omettre de mentionner les accords de reconnaissance mutuelle des certificats signés entre de nombreux pays au monde (par les gouvernements de ces pays).

A cette fin nous évoquerons les accords européens :

- SOG-IS[10] (Senior Official Group – Information Security) qui permettent une reconnaissance des certificats tous niveaux confondus entres les pays signataires.

Et les accords mondiaux :

- CCRA[11] (Common Criteria Recognition Arrangement) qui permettent une reconnaissance des certificats entres les pays signataires, pour les niveaux EAL1 à EAL4.

A cette occasion, nous ferons le point des pays signataires du CCRA et mentionnerons la distinction entre :

- Les pays dits « producteurs de certificats » qui ont mis en place un processus et une organisation reconnue par leurs pairs (i.e. les pays qui sont déjà reconnus en tant que tels) sous l'égide d'un organisme national de certification nécessairement placé sous tutelle de l'autorité gouvernementale qui est signataire des accords de reconnaissance mutuelle.
- Les pays dits « consommateurs de certificats » qui ont seulement rejoint en tant que signataire du CCRA à des fins de reconnaissance des certificats émis par les pays « producteurs de certificats ». Ce statut est généralement temporaire, le temps de devenir « pays producteur de certificat ». Une fois un processus et une organisation ad'hoc mises en place, l'organisme de certification national du pays candidat à cette reconnaissance de « pays producteur de certificat » passe par un audit réalisé par des représentants d'organismes de certification nationaux de pays ayant déjà acquis le statut. Le processus dont fait partie cet audit est appelé « shadow certification ».

8 Limitations de la certification : les pièges à éviter, conseils et solutions

Malgré de nombreux atouts, la certification selon les Critères Communs comporte de nombreuses limitations intrinsèques qu'il vaut mieux connaître, afin d'en optimiser l'utilisation, que ce soit :

[10] Cf `http://www.ssi.gouv.fr/fr/confiance/mra.html`

[11] Accords de reconnaissance mutuelle ou CCRA (Common Criteria Recognition Arrangement) : `http://www.commoncriteriaportal.org/public/consumer/index.php?menu=3` ; voir aussi : `http://www.ssi.gouv.fr/fr/confiance/mra.html`

- Lorsqu'en tant que développeur d'un produit de sécurité, je suis candidat à une certification selon les Critères Communs de mon produit.
- Lorsqu'en tant qu'utilisateur final, je cherche à comparer les offres des différents éditeurs de produits de sécurité.

Outre l'identification des spécificités et limitations de ce référentiel, nous verrons quelles précautions prendre pour choisir en connaissance de cause son produit de sécurité certifié et savoir s'il répond à la problématique de sécurité du système d'information au sein duquel il est prévu d'être déployé, quels conseils s'appliquent lors de la mise en œuvre du produit certifié, et quelles sont les offres des CESTI pouvant permettre d'éviter les pièges et de se préparer le cas échéant à un processus de certification de son produit de sécurité, de son système informatique ou de son offre de service de sécurité en tant qu'opérateur de télécommunications.

Parmi les spécificités et limitations de la certification selon les Critères Communs, évoquons :

- Sa complexité entraînant souvent des difficultés d'appréhension qui est liée à sa généricité, mais les CESTI ont mis en place une offre de formation aux Critères Communs et à l'évaluation, de préparation à l'évaluation et d'accompagnement des développeurs candidats à une évaluation / certification. La contrainte majeure reste qu'un même CESTI ne peut intervenir en accompagnement et en évaluation auprès du même client, pour des raisons évidentes d'indépendance (il ne peut être juge et partie).
- Sa forte dépendance au produit/système faisant l'objet du certificat : les évolutions ultérieures du produit/système ne sont pas prises en compte par défaut. Cette limitation peu impactante dans le cas d'une carte à puce Romée qui est figée lors de sa fabrication, s'avère dimensionnante dans le cas d'un produit logiciel dont l'éditeur diffuse des évolutions tous les 3 mois, ou dans le cas de patchs logiciels édités avec la même fréquence (parfois davantage).
- La notion de périmètre d'évaluation ou de portée du certificat qui offre la possibilité de restreindre la portée du certificat à un sous-ensemble du produit et des fonctionnalités/services de sécurité qu'il implémente.
- Les notions de Profil de Protection et de Cible de Sécurité qui permettent de comparer les produits et de connaître la portée réelle d'un certificat ainsi que ses conditions de validité.
- L'intantanéïté de la validité du certificat (une photographie à l'instant « t » du produit/système) et l'absence de garantie qu'il reste valide dans la durée après son émission. En effet, l'état de l'art des attaques peut évoluer après la délivrance d'un certificat ainsi que les outils disponibles : nouvelles failles de sécurité découvertes quotidiennement par les pirates[12], nouvelles techniques d'attaque, nouvelles heuristiques et nouveaux algorithmes de calcul d'attaques découverts par la recherche, évolution de la puissance de calcul des ordinateurs qui double tous les dix-huit mois conformément à la Loi de Moore, etc. En outre, comme évoqué plus haut, le produit lui-même peut être amené à évoluer dans le temps et les versions ultérieures d'un produit ne sont pas couvertes par défaut par le certificat d'origine.
- La notion de niveau d'évaluation (EAL1 à EAL7 dans le cas des Critères Communs) dont découle une résistance plus ou moins grande du produit à des attaques. Le niveau d'évaluation visé détermine le potentiel d'attaque d'un attaquant auquel le produit est censé résister. Plus le niveau d'évaluation est élevé, plus les investigations réalisées par le CESTI ont été poussées et plus élevée est la résistance du produit à des attaques. En tout état de cause, il faut garder présent à l'esprit que la sécurité (et donc la confiance) est toujours une notion relative. Un produit certifié n'est pas garanti sans faille de sécurité, mais avec une confiance d'autant plus

[12] Cf `http://vigilance.aql.fr/`

importante que le niveau d'évaluation atteint est élevé, l'on peut dire que le produit possède statistiquement peu de chances de comporter des failles de sécurité non identifiées, donc qu'il apporte une confiance certaine. En outre, la résistance d'un produit à des attaques n'est jamais infinie. Plus les moyens dont dispose l'attaquant pour mener à bien son attaque sont importants (temps, expertise, outillage spécifique, connaissance du produit, collusion avec un utilisateur ou un administrateur, etc.), plus élevées sont ses chances de réussir son attaque et aucun produit de sécurité ne possède une résistance infinie. Tout est une question de moyens à mettre en œuvre par l'attaquant pour mener à bien son attaque. Cela correspond à la notion de potentiel d'attaque d'un attaquant introduite dans les Critères Communs.

Pour pallier certaines des limitations ci-dessus (et **contribuer au maintien de la validité d'un certificat dans le temps**), la DCSSI a défini les processus de :

- « Surveillance des produits certifiés »[13].

et de :

- « Continuïté de l'assurance des produits certifiés »[14].

Ces deux processus s'appliquent tous deux postérieurement à la date d'émission d'un certificat initial. Ils constituent tous deux une alternative à la ré-évaluation du produit (i.e. une nouvelle évaluation complète du produit selon les Critères Communs dans une version postérieure à celle qui a été initialement certifiée). Ces processus sont mis en œuvre spécifiquement à la demande du développeur du produit et consistent respectivement à :

- Charger un CESTI de surveiller l'apparition de nouvelles failles de sécurité pouvant remettre en cause la validité du certificat. Tant que de telles failles de sécurité n'ont pas été identifiées par le CESTI et tant que le produit n'évolue pas dans le temps, la validité du certificat initial peut donc être prolongée par la DCSSI.
- Mettre en place chez le développeur du produit, un processus de nature à prendre en compte les évolutions dans le temps du produit (pourvu que ces évolutions restent mineures), à s'engager à faire évoluer la documentation du produit, à surveiller l'absence d'impact de ces évolutions sur le niveau de sécurité du produit et à en apporter la preuve à un CESTI à l'occasion d'un audit annuel de processus. Dans ces conditions, la validité du certificat initial peut donc être prolongée par la DCSSI, tant que de nouvelles failles de sécurité n'apparaissent pas dans le produit ou tant qu'une évolution majeure du produit ne survient pas, qui ne ne permettrait plus d'acquérir de certitude que son niveau de sécurité est maintenu, sans un ré-examen complet de la nouvelle version du produit par un CESTI (ré-évaluation qui implique une sortie du processus de continuïté de l'assurance).

Voici maintenant nos **conseils à un utilisateur final d'un produit de sécurité** (RSSI par exemple) qui cherche un produit de sécurité répondant à son besoin de sécurité spécifique, à intégrer au sein de son système d'information.

- Rechercher le Profil de Protection sur Internet (document public facilement accessible en général[15]) et/ou demander la Cible de Sécurité du produit à l'éditeur, ou se la procurer dans sa version publique auprès de l'organisme de certification (exemple : `http://www.ssi.gouv.fr/fr/confiance/certificats.html` ou `http ://www.commoncriteriaportal.org/public/consumer/index.php?menu=4`).

[13] SUR-P-01 Surveillance des produits certifiés. Source `http://www.ssi.gouv.fr/fr/documentation/index.html\#evaluation`

[14] `MAI-P-01` Continuité de l'assurance des produits certifiés. Source `http://www.ssi.gouv.fr/fr/documentation/index.html\#evaluation`

[15] Cf `http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5`

- En prenant connaissance de ces documents ainsi que du rapport de certification associé, identifier :
  - Si le produit dispose bien des fonctionnalités/ rend bien les services de sécurité répondant à son besoin.
  - Si l'ensemble de ces fonctionnalités/services de sécurité (ou au moins le sous-ensemble répondant à son besoin) entre bien dans la portée du certificat. Bien noter que pour tout service ou fonction de sécurité hors périmètre, le certificat n'apporte aucune confiance.
  - Si la version certifiée du produit de sécurité (mention obligatoire dans la Cible de Sécurité, le certificat et le rapport de certification) correspond bien à la dernière version commercialisée par l'éditeur. A défaut, être conscient que seule la version certifiée du produit présente les garanties liées au certificat.
  - Si le produit fait l'objet d'un processus spécifique constituant une garantie complémentaire de confiance dans le niveau de sécurité qu'il atteint postérieurement à la date de délivrance du certificat : processus de « Surveillance des produits certifiés »[16] et de « Continuïté de l'assurance des produits certifiés »[17], ré-évaluation dans une version ultérieure éventuellement en cours.
  - Si les hypothèses sur l'environnement d'exploitation du produit et sur son utilisation (restrictions éventuelles présentes dans le Cible de Sécurité et ayant présidé à la délivrance du certificat) sont compatibles avec l'usage que l'on veut en faire dans le cadre d'une intégration à son système d'information.
  - Si le produit a en outre fait l'objet d'un processus spécifique (de type qualification au niveau standard/renforcé/élevé et d'une analyse de la résistance de ses mécanismes cryptographiques) par la DCSSI (dans le cas d'un produit évalué et certifié en France uniquement).
  - Si le produit a fait l'objet d'un autre processus spécifique de validation de ses mécanismes cryptographiques (s'il comporte de tels mécanismes) quand il a fait l'objet d'une évaluation et d'un certificat délivré à l'étranger (FIPS140-2 ou FIPS140-3 aux Etats-Unis, Canada, Royaume-Uni, Australie, Nouvelle-Zélande), etc.
- Une fois un ou plusieurs produits identifiés comme cible du besoin de sécurité initial, comparer les produits en question sur la base :
  - De leur adéquation au besoin de sécurité initial.
  - Du niveau de sécurité attesté par chaque certificat (niveau EAL1 à EAL7 dans le cas des Critères Communs) dont découle une résistance plus ou moins grande du produit à des attaques.
  - Du périmètre sur lequel porte le certificat.
  - De la date d'émission du certificat : plus le certificat est ancien, plus le risque d'obsolescence est élevé, sans qu'aucune métrique évidente ne puisse en apporter la certitude, autre que la mise en place d'un processus formalisé de gestion du risque, à partir des vulnérabilités résiduelles identifiées en sortie du processus d'évaluation.

Note Bene : En cas de non utilisation d'un référentiel commun de type Profil de Protection, il est certains cas où les produits ne seront pas comparables du point de vue de leur niveau de sécurité. Par exemple, parmi deux produits certifiés sur des périmètres différents, vaut-il mieux retenir un

[16] SUR-P-01 Surveillance des produits certifiés. Source `http://www.ssi.gouv.fr/fr/documentation/index.html\#evaluation`

[17] MAI-P-01 Continuité de l'assurance des produits certifiés. Source `http://www.ssi.gouv.fr/fr/documentation/index.html\#evaluation`

produit certifié au niveau EAL4 sur un petit périmètre ou bien un produit certifié au niveau EAL2 sur un périmètre plus vaste ?

Enfin, voici quelques **conseils à un développeur d'un produit de sécurité** qui cherche à savoir si un tel processus présente un intérêt pour lui et pour le produit/solution qu'il développe et comment il doit s'y prendre pour lancer un tel processus.

Nous identifierons les questions qu'il doit se poser et tenterons d'y répondre :

- Quel objectif pour une telle certification : marketing/avantage concurrentiel, obligation de conformité réglementaire, standard de fait/exigence du marché, exigence d'un ou plusieurs clients spécifiques, autre raison (amélioration du niveau de sécurité de son produit et/ou de ses processus internes de développement par exemple) ?
- Quel niveau viser ?
- Quel périmètre de mon produit/système soumettre à la certification ?
- Dois-je viser ou non un processus de qualification ?
- Dois-je viser une conformité à un Profil de Protection existant ? Cela me facilitera-t-il la tâche ?
- Dois-je me faire assister par un CESTI ?
- Comment faire le choix d'un CESTI qui évaluera ma solution ?
- Faut-il que je fige une version de mon produit/système pendant la durée du processus d'évaluation ?
- Quel impact du processus d'évaluation et de certification de mon produit sur mes locaux, mon organisation, mes processus et méthodes de développement ?

9 Conclusion

Le marché de la certification de la sécurité est promis à un brillant avenir, compte tenu des enjeux :

- mondialisation et dématérialisation des échanges,
- mutations technologiques majeures en cours (solutions de mobilité, convergence voix-données-images, vers le tout communicant en tout lieu et à tout moment...
- accroissement et morcellement de l'offre en matière de sécurité des systèmes d'information sans pour autant que les utilisateurs ne puissent y voir clair dans les compétences réelles, ni la confiance qu'il peuvent avoir dans les individus, les organisations et les technologies qui leurs sont proposées,
- enjeux économiques et stratégiques avec une augmentation inéluctable de la dépendance des organisations vis-à-vis des technologies de l'information et l'accroissement concommittent de l'impact potentiel des attaques réussies,
- montée de la criminologie informatique tant en interne qu'en externe (fortement liée à l'intérêt d'une attaque réussie qui augmente).

Toutefois, la prise en compte de la sécurité à tous les niveaux dans les organisations, et la reconnaissance de l'intérêt des démarches de certification de la sécurité, passe par une amélioration d'une niveau de maturité des organisations, et donc par :

- une prise de conscience des enjeux associés,
- le déblocage des budgets sécurité correspondant aux enjeux, en considérant la sécurité davantage comme une assurance contre des dommages potentiels qu'à travers une logique classique de rapport entre un gain financier à court terme et un investissement réalisé (ROI),
- la meilleure connaissance des atouts et limitations des référentiels de certification de la sécurité.

En effet, nous voyons encore trop souvent la certification de la sécurité utilisée comme un pur argument marketing sans que pour autant l'on ne se préoccupe de savoir ce qui se cache derrière. Cela donne lieu à des griefs à l'encontre de la certification et à des arguments contre son coût, l'opacité du processus, etc. ; ce qui occulte encore trop souvent les bénéfices que l'on peut en retirer. Toutefois, il est évident que d'autres voies existent pour vérifier le niveau d'expertise, la confiance et l'indépendance, encore faut-il savoir s'il est encore possible à chacun de se forger sa propre opinion (au risque d'être subjectif), ou bien s'il ne vaut pas mieux s'appuyer sur des structures existantes dont c'est le métier pour se faire une opinion (lequelles apportent a minima une objectivité certaine dans les qualifications qu'elles décernent et permettent une échelle de comparaison des offres).

Parmi les meilleures pistes de développement de la certification de la sécurité, rappelons :

- Le domaine de la carte à puce dans lequel l'impact d'une faille de sécurité découverte après la distribution des cartes est considérée à juste titre comme ayant un impact suffisamment important (au pire, nécessité de rappeler l'ensemble des cartes pour les faire repasser par le site de personnalisation, voire nécessité de fabriquer de nouvelles cartes corrigeant la faille avec le risque de ne pas pouvoir faire supporter le surcoût au porteur de la carte, et impact extrêmement négatif d'un tel rappel sur l'image de marque du fabriquant et/ou de l'émetteur).
- Le domaine de la Défense nationale et de l'OTAN dans lequel c'est en pratique le seul référentiel reconnu comme apportant le niveau de confiance requis, et pour des raisons réglementaires.
- Le domaine de la signature électronique qualifiée (avec effet juridique de renversement de la charge de la preuve) correspondant à la transposition en droit national de la Directive européenne n ° 1999/93/CE sur la signature électronique.
- Les travaux du gouvernement français autour du Référentiel Général de Sécurité (RGS) et de la PRIS V2 (ou Politique de Référencement Intersectorielle de Sécurité, Version 2.1).
- Les travaux de la DCSSI autour de la rédaction, de la certification et de la normalisation par l'Afnor de Profils de Protection, dans la perspective de pouvoir les citer comme des textes de référence applicables dans le domaine des appels d'offres publics (conformément au Code des Marchés Publics).
- La mise en place par la DCSSI des processus de qualification aux niveaux standard, renforcé et élevé s'appuyant sur le processus d'évaluation et de certification selon les Critères Communs et bientôt la qualification au niveau élémentaire. Ces processus conduisent à la constitution et à la diffusion d'un catalogue de produits qualifiés[18] à l'attention originellement des administrations et organismes publics, mais dans lequel tout organisme privé a intérêt à choisir des produits de confiance.
- Les prévisions d'agrément des CESTI par la DCSSI dans le domaine de l'expertise des mécanismes cryptographiques ; lesquels disposeront alors de compétences reconnues dans ce domaine.

[18] Cf `http://www.ssi.gouv.fr/fr/politique_produit/catalogue/index.html`

Références

Outils méthodologiques pour la sécurité des systèmes d'information **Source :** `http://www.ssi.gouv.fr/fr/confiance/methodes.html`	
Identification	**Référence, origine et source**
EBIOS	**EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) ***Résumé :*** *La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI.* *Le référentiel EBIOS est composé d'un ensemble d'outils pour découvrir la méthode, s'yformer, la pratiquer et contribuer à son développement communautaire.* Source : `http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html`
PSSI	**PSSI (Politique de Sécurité des Systèmes d'Information)** ***Résumé :*** *La PSSI reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration...) en matière de sécurité des systèmes d'information (SSI).* *Le guide PSSI a pour objectif de fournir un support aux responsables SSI pour élaborer une politique de sécurité du ou des systèmes d'information (PSSI) au sein de leur organisme. Il est décomposé en quatre sections :* *o l'introduction permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ;* *o la méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ;* *o le référentiel de principes de sécurité ;* *o une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires...).* Source : `http://www.ssi.gouv.fr/fr/confiance/pssi.html`

TDBSSI	**TDBSSI (Tableau De Bord SSI), Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information.** ***Résumé :*** *Un TDBSSI permet de disposer, aux différents niveaux décisionnels, de pilotage et opérationnels, d'une vision synthétique de la situation de la sécurité, que ce soit dans ses dimensions techniques ou fonctionnelles (couverture des risques, qualité de la politique de sécurité, suivi des audits, des actions et des alertes. . .).* *Il constitue en effet un outil de synthèse et de visualisation indispensable pour suivre toutes les actions liées à la SSI. Il contribue à contrôler que la stratégie définie dans la politique de sécurité est mise en œuvre par les niveaux de pilotage et opérationnel, et à la remontée d'informations pertinentes jusqu'aux décideurs.* Source : `http://www.ssi.gouv.fr/fr/confiance/tdbssi.html`
DSIS	**DSIS (Développement de Systèmes d'Information Sécurisés),** Version 1.1, Guide à l'usage des réalisateurs - 5 janvier 1994 - DISSI/SCSSI. Source : `http://www.ssi.gouv.fr/fr/confiance/dsis.html`
Défense en profondeur	**Mémento sur le concept de la défense en profondeur appliqué aux SI**, SGDN/DCSSI, Version 1.1 – 19 juillet 2004 Source : `http://www.ssi.gouv.fr/fr/confiance/documents/methodes/mementodep-v1.1.pdf`
Maturité SSI	**La *plaquette* et le *guide* relatifs à la maturité SSI** **Plaquette Maturité SSI :** Positionner son organisme en 9 questions. Source : `http://www.ssi.gouv.fr/fr/confiance/documents/methodes/maturitessi-plaquette-2005-04-19.pdf` **Guide : Positionnement d'un organisme en matière de maturité SSI :** Approche méthodologique, SGDN/DCSSI, Version du 26 octobre 2005. Source : `http://www.ssi.gouv.fr/fr/confiance/documents/methodes/maturitessi-methode-2005-10-26.pdf`
Archivage électronique sécurisé	**Archivage électronique sécurisé :** *les analyses préalables, les documents introductifs, les documents d'aide à l'élaboration du référentiel :* Le cahier des charges pour un système d'archivage électronique, SGDN/DCSSI, V.2006-05-16. La politique et les pratiques d'archivage, SGDN/DCSSI, V.2006-07-24. La grille d'audit, SGDN/DCSSI, V.2006-07-24. Source : `http://www.ssi.gouv.fr/fr/confiance/archivage.html`

Normes et standards de référence pour la certification	
Identification	**Référence complète**
ISO 17025	**NF EN ISO/CEI 17025 :2005,** Septembre 2005, Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais, AFNOR, Indice de classement : X 50-061.
EN 45011	**Norme NF EN 45011,** Mai 1998, Exigences générales relatives aux organismes procédant à la certification de produits, AFNOR, Indice de classement **:** X50-071
ISO 17021	**ISO/IEC 17021 :2006,** Conformity assessment – Requirements for bodies providing audit and certification of management systems, 2006-08-31. ***Abstract :*** *ISO/IEC 17021 :2006 contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (e.g. quality management systems or environmental management systems) and for bodies providing these activities. Certification bodies operating to this International Standard need not offer all types of management system certification.* *Certification of management systems is a third-party conformity assessment activity. Bodies performing this activity are therefore third-party conformity assessment bodies.* *ISO/IEC AWI 17021-2, Part 2 : Requirements for third party auditing of management systems, 2006-11-28, Status = Under development.*
ISO 17024	**ISO/IEC 17024 :2003,** Conformity assessment – General requirements for bodies operating certification of persons, 2003-03-28. ***Abstract :*** *ISO/IEC 17024 :2003 specifies requirements for a body certifying persons against specific requirements, including the development and maintenance of a certification scheme for personnel.*
ISO 19011	**NF EN ISO 19011,** Décembre 2002, Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental, AFNOR, Indice de classement : X 50-136.
ISO 17799	**ISO/CEI 17799 :2005(F),** Juin 2005, Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information, deuxième édition du 15-06-2005.

ISO 27001	**ISO/CEI 27001 :2005(E), Octobre 2005,** Information technology - Security techniques - Information security management systems - Requirements / Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences, première édition du 15-10-2005.
Critères Communs CCV2.3 également Norme ISO 15408	**Common Criteria for Information Technology Security Evaluation** CCMB-2005-08-001, Part 1 : Introduction and general model, Version 2.3, August 2005. **Common Criteria for Information Technology Security Evaluation** CCMB-2005-08-002, Part 2 : Security functional requirements, Version 2.3, August 2005. **Common Criteria for Information Technology Security Evaluation** CCMB-2005-08-003, Part 3 : Security assurance requirements, Version 2.3, August 2005. **Common Criteria, Common Methodology for Information Technology Security Evaluation,** CCMB-2005-08-004, Evaluation Methodology, Version 2.3, August 2005. Source : `http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2`
CC V3.1 rev1	**Common Criteria for Information Technology Security Evaluation** CCMB-2006-09-001, Part 1 : Introduction and general model, Version 3.1 revision 1, September 2006. **Common Criteria for Information Technology Security Evaluation** CCMB-2006-09-002, Part 2 : Security functional components, Version 3.1 revision 1, September 2006. **Common Criteria for Information Technology Security Evaluation** CCMB-2006-09-003, Part 3 : Security assurance components, Version 3.1 revision 1, September 2006. **Common Criteria, Common Methodology for Information Technology Security Evaluation,** CCMB-2006-09-004, Evaluation Methodology, Version 3.1 revision 1, September 2006. Source : `http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2`