

GS1 et la lutte contre la contrefaçon

Présentation

Cette note décrit les propositions de GS1 pour contribuer à la lutte contre la contrefaçon.

Son premier objectif est d'**informer**. Un aspect majeur de la crise actuelle de contrefaçon est l'inadéquation des moyens d'inspection à la disposition des consommateurs, des distributeurs, des fabricants et des services de douane face à l'énorme flux de biens en transit. Spécialiste de la gestion des flux logistiques, GS1 suggère d'intégrer les solutions d'identification dans les dispositifs de lutte contre la contrefaçon, afin d'en améliorer la performance.

Son deuxième objectif est de **susciter des contributions**. Expert en logistique, GS1 souhaite mieux connaître les besoins des acteurs de la lutte contre la contrefaçon : directions spécialisées des grandes entreprises ; autorités de contrôle ; fournisseurs de solutions d'authentification. GS1 souhaite travailler avec ces acteurs pour définir des scénarios efficaces de lutte contre la contrefaçon, utilisant ses standards lorsqu'ils sont utiles. Ces scénarios permettraient de déployer des dispositifs combinant outils logistiques et d'authentification, approches juridiques, moyens d'action et d'intelligence des autorités de contrôle.

Utilisées seules et naïvement, les technologies d'identification de GS1 offrent une protection bien faible contre la contrefaçon : copier une étiquette avec l'identifiant d'un produit authentique vers une contrefaçon semble très simple.

Utilisées de manière cohérente, ces mêmes technologies **augmentent le coût de production de la contrefaçon** et **diminuent le coût du contrôle**, permettant d'étendre la lutte contre la contrefaçon aux biens de consommation courante. Affecter un identifiant unique à chaque contrefaçon demande un effort au contrefacteur, mais reste simple ; générer des identifiants uniques qui soient tous reconnus comme valides par le fabricant, peut être aléatoire ; générer des identifiants uniques et valides, qui soient cohérents avec les informations de localisation des produits, peut devenir statistiquement impossible. Enfin, des techniques cryptographiques largement diffusées, permettent de combattre la falsification des identifiants.

Les technologies d'authentification permettent de répondre OUI ou NON à la question : « ce produit est-il authentique ? ». Ces technologies peuvent utiliser l'identifiant comme un des éléments authentifiant ; elles peuvent également ne pas l'utiliser. Les responsables de marque gardent la responsabilité et la liberté d'adopter ces technologies d'authentification, en fonction de la nature du produit, de sa valeur et du risque encouru. Les standards GS1 cherchent à faciliter l'utilisation de ces technologies. En effet, l'identification des produits permet à un inspecteur d'orienter rapidement les requêtes d'authentification vers le fabricant et de qualifier ces requêtes de manière précise. De même, les standards GS1 d'écriture et de lecture (codes matriciels, étiquette radiofréquence) peuvent être utilisés pour transcrire des informations aidant à l'authentification. Des outils interopérables peuvent alors être diffusés pour consulter ces informations et les transmettre aux fabricants.

Afin d'illustrer cette approche, cette note propose quelques scénarios, sans souci d'exhaustivité. Certains scénarios sont déjà utilisés, hors de toute standardisation. D'autres sont en cours d'investigation. D'autres enfin apparaîtront comme nouveaux.

La lutte contre la contrefaçon devient un enjeu majeur

Les enjeux de la lutte contre la contrefaçon sont souvent rappelés dans les médias et sont bien connus du lecteur informé. Rappelons quelques éléments du rapport de l'OCDE de 2007.

- Le montant du commerce de contrefaçons atteint peut-être 200 milliards de dollars, sans inclure le commerce domestique (contrefaçon produite et achetée dans le même pays) ni les téléchargements illégaux de produits numériques ; (d'autres estimations atteignent 500 milliards de dollars, voire même jusqu'à 7% du commerce international.)
- ce montant est en croissance constante ces dernières années ;
- la contrefaçon s'étend de l'industrie du luxe aux produits de grand volume ;
- des contrefaçons apparaissent dans des circuits de distribution légitimes ;
- la santé et la sécurité du consommateur sont mises en danger par des contrefaçons de médicaments, d'aliments, de boissons, voire de produits de grande consommation (batteries, jouets) incorporant des substances dangereuses pour la santé.

Grandes marques et services de douane sont les acteurs principaux de la lutte contre la contrefaçon. Utilisant leurs sources d'information pour cibler les contrôles, les douanes mettent en œuvre les moyens mis à leur disposition par les grandes marques pour détecter les contrefaçons. Les grandes marques assistent les services douaniers, incorporent dans leurs produits des dispositifs techniques permettant de distinguer produits authentiques et contrefaçons, finalement mobilisent leurs experts pour inspecter les biens retenus en douane.

La variété des dispositifs d'authentification et des produits sujets à contrefaçon, le secret entourant les dispositifs techniques, enfin les enjeux économiques et sociétaux, justifient un soutien à l'action des autorités, face à ce qu'il faut bien appeler une déferlante de contrefaçons.

GS1 propose son aide

Organisation internationale sans but lucratif, présente dans plus de cent pays, GS1 développe les standards permettant de fluidifier les échanges de biens dans le commerce international : identification et traçabilité (codes à barres, codes matriciels, étiquette radiofréquence), échanges électroniques. Le succès du code à barre et la dématérialisation des échanges d'information (commandes, factures, fiches produit) attestent de la capacité de GS1 à accompagner fabricants et distributeurs dans le déploiement de ces standards.

Spécialiste des standards pour le suivi des produits, GS1 contribue à la lutte contre la contrefaçon, en définissant un socle d'interopérabilité complétant les solutions d'authentification et les initiatives internationales. En collaboration avec les organismes spécialisés, GS1 définit des évolutions de ses standards vers un socle commun d'interopérabilité pour ces dispositifs de lutte contre la contrefaçon. Ce socle commun d'interopérabilité peut permettre aux autorités de contrôle d'identifier efficacement les lots suspects, puis de faire appel rapidement aux dispositifs d'authentification déployés par les grandes marques. Ce socle s'appuie sur la complémentarité naturelle des dispositifs d'authentification avec les solutions d'identification et de marquage proposées par GS1.

Par la mobilisation de son réseau présent dans plus de cent pays, en collaboration avec les organismes de lutte contre la contrefaçon, GS1 accompagne ses adhérents et les organismes concernés pour le déploiement des standards et outils techniques associés.

Des standards GS1 pour lutter contre la contrefaçon

Plusieurs technologies GS1 sont utilisables dans le cadre de la lutte contre la contrefaçon. Elles peuvent être utilisées dans plusieurs scénarios de détection, soit seules, soit avec des techniques d'authentification. Pour plus d'informations sur les standards GS1, consulter www.gs1.fr.

Les codes GS1 fournissent des méthodes d'identification homogènes pour tous les adhérents, utilisables mondialement : le code GTIN identifie *les produits* (deux unités du même produit ont le même identifiant GTIN), le code SSCC identifie *les unités physiques d'expédition* (deux palettes ont des identifiants SSCC différents, même si leurs contenus sont identiques).

Proposé récemment, le code SGTIN (« serial » GTIN) *identifie chaque unité de produit* (deux unités du même produit ont des identifiants SGTIN différents). Il permet une traçabilité unitaire des produits, pour leur localisation ou leur authentification.

Les standards de transcription GS1 (codes à barres, codes matriciels ou étiquettes radiofréquence) rendent interopérables l'écriture et la lecture d'informations sur les produits et documents associés, indépendamment du fabricant ou de l'expéditeur.

Un identifiant SGTIN peut ainsi être écrit sous la forme d'un code matriciel ou dans une étiquette radiofréquence.

Le réseau mondialisé GS1, en cours de développement, permettra l'accès aux informations disponibles sur un produit à partir de son identifiant SGTIN.

Les personnes autorisées par les fabricants pourront consulter notamment les caractéristiques du produit, son suivi logistique, ses éléments d'authentification.

Ces technologies forment un socle d'interopérabilité pour l'identification, la traçabilité, l'écriture et la lecture de l'information associée aux produits. Conçu pour être utilisé par les fabricants et les distributeurs, ce socle d'interopérabilité est mis à la disposition de la lutte contre la contrefaçon pour la lecture des informations associées aux produits. Ainsi, dès aujourd'hui, les services de douanes utilisent le code SSCC d'identification des unités d'expédition : le code SSCC permet d'associer à une unité physique un ensemble d'informations (avis d'expédition, etc.).

Des scénarios d'utilisation des standards GS1

Les scénarios ci-dessous illustrent la manière dont les technologies GS1 peuvent être utilisées dans le cadre de la lutte contre la contrefaçon, soit seules, soit en complément de méthodes d'authentification et de techniques cryptographiques.

Scénario 1. Vérification de l'unicité des identifiants SGTIN

Les identifiants SGTIN étant affectés de manière unique à chaque unité de produit, la présence du même identifiant SGTIN sur plusieurs unités dans un lot inspecté est un indicateur de contrefaçon.

Scénario 2. Vérification de la validité des identifiants

La plage des identifiants SGTIN affectée par GS1 à chaque fabricant est très grande (des milliards d'identifiants possibles). A tout moment, certains identifiants sont valides car ils correspondent à des produits authentiques, et d'autres sont non valides.

Chaque fabricant peut choisir la méthode d'affectation de ses identifiants. Il peut également garder secrète cette méthode. Le contrefacteur est donc dans l'impossibilité de générer des identifiants systématiquement valides. Une personne autorisée peut cependant déterminer si l'identifiant d'un produit inspecté est valide : l'identifiant SGTIN permet de déterminer le fabricant, puis l'interrogation des services du fabricant permet de vérifier la validité de l'identifiant.

Les scénarios 1 et 2 se renforcent mutuellement : les chances pour un contrefacteur d'affecter un identifiant unique *différent* à chaque produit d'un lot peuvent devenir extrêmement faibles.

Scénario 3. Vérification de la localisation attendue du produit

Le réseau GS1 est développé pour permettre notamment d'accéder aux caractéristiques et à la localisation de chaque produit, sous le contrôle de son fabricant.

Cette information de localisation peut être utilisée pour la lutte contre la contrefaçon : une incohérence de localisation est un indicateur de contrefaçon. C'est le cas, par exemple, si le produit contrôlé par les douanes est indiqué comme déjà vendu, ou bien comme stocké dans un entrepôt très éloigné, ou bien a déjà été contrôlé la veille à un poste de douanes, etc. Par ailleurs, cet indicateur de contrefaçon se renforce si des incohérences multiples sont décelées parmi les différents produits d'un lot.

Les scénarios 1,2 et 3 se renforcent mutuellement : il est très difficile à un contrefacteur de générer des identifiants différents, tous valides, et ne conduisant pas à des incohérences manifestes lors de la vérification de la localisation attendue d'un lot.

Scénario 4. Intégrité des identifiants et certification d'origine.

Les codes imprimés et les étiquettes radiofréquence sont faciles à copier et à falsifier. Ils ne sont donc pas, intrinsèquement, des éléments fiables d'authentification : un contrefacteur peut facilement copier ou falsifier des identifiants.

En utilisant des critères d'unicité du code, de sa validité ou de la localisation du produit, les scénarios 1, 2 et 3 ont montré qu'il est possible de détecter, de manière plausible mais non certaine, la falsification d'étiquettes. Par ailleurs, l'amélioration de la résistance des étiquettes à la falsification est un sujet de recherches actives, par exemple au sein du projet Européen « Bridge », ou dans le réseau international « AutoID Labs ».

Il est également possible d'utiliser des méthodes de cryptographie asymétrique pour garantir *l'intégrité des identifiants* et *certifier l'origine du produit*. Ces méthodes sont largement utilisées, notamment pour éviter la falsification des passeports récents. Tout d'abord, un « sceau cryptographique » est généré en signant les données d'identification du produit ; ensuite, ce sceau est imprimé sous la forme d'un code matriciel ou écrit dans une puce radiofréquence ; enfin, l'examen de ce sceau permet de vérifier que les données n'ont pas été modifiées depuis sa mise en place (« *intégrité* »), et de « *certifier* » qu'il a été mis en place par le fabricant ou l'expéditeur désigné.

L'origine d'un bien est une information importante pour les distributeurs comme pour les douaniers lors de l'appréciation de l'authenticité d'un produit. Pour cela, ces services utilisent souvent un document appelé « certificat d'origine ». Un « sceau cryptographique » améliorerait la fiabilité de tels certificats. De même, la conformité technique d'un produit est importante pour garantir la sécurité des personnes. Des « sceaux cryptographiques » pourraient garantir l'intégrité des certificats de conformité.

La mise en œuvre de ces méthodes dans le cadre de la lutte contre la contrefaçon est relativement simple, mais nécessite une coordination internationale pour l'échange de certificats cryptographiques : GS1 pourrait aider à sa mise en place. Des détails techniques de ce scénario sont disponibles en annexe 1 et 2.

Les scénarios 1, 2, 3 et 4 se renforcent mutuellement : il est virtuellement impossible à un contrefacteur de générer des identifiants différents, valides, cohérents pour leur localisation, dont l'intégrité et l'origine sont garanties par la cryptographie. Par ailleurs, ***ces scénarios combinés peuvent être mis en œuvre pour un coût unitaire quasi-nul*** : des opérations logicielles et l'impression d'un code matriciel suffisent.

Scénario 5. Authentification des produits

Combinés, les scénarios 1, 2, 3 et 4, rendent virtuellement impossible la production de faux identifiants, mais n'empêchent pas le transfert d'une étiquette ou la copie d'un code matriciel. Ce transfert ou cette copie sera peut-être détecté selon un des scénarios 1, 2 ou 3, mais cette détection ne prouve pas, en général, la contrefaçon. Ainsi, seuls ou combinés, les scénarios 1, 2, 3 et 4, ne permettent pas de garantir l'authenticité d'un produit. Des techniques d'authentification complémentaires deviennent nécessaires.

Les dispositifs d'authentification sont variés : hologrammes, techniques optiques visibles ou cachées (UV, micro-impressions), matérielles (ADN, fil spécial tissé), électromagnétiques, cryptographiques, etc. Cette variété offre au fabricant le choix de la méthode qui convient le mieux à son produit et au risque encouru. La responsabilité de la preuve d'authenticité ou de contrefaçon appartient au fabricant. Ainsi, les services de douanes peuvent parfois rester dans l'ignorance de l'ensemble des techniques utilisées.

GS1 propose d'utiliser l'identifiant du produit pour accéder à l'« information d'authentification », propriété du fabricant. Cela permet à un tiers extérieur au fabricant de déterminer la procédure d'authentification à suivre. Les premières étapes de cette procédure peuvent être accessibles à ce tiers extérieur, mais sa conclusion se fait en général sous la responsabilité du fabricant, par les experts de la marque.

La combinaison des scénarios 1, 2, 3, 4 et 5 apparaît très efficace. Les scénarios 1, 2 et 3 fournissent des indicateurs de contrefaçon sur des bases logistiques. Le scénario 4 garantit l'intégrité et l'origine de l'identifiant. Cet identifiant permet d'accéder à l'information d'authentification qui permet de valider, ou non, l'authenticité du produit.

Cette efficacité est obtenue tout en garantissant au fabricant la liberté du choix d'une méthode d'authentification, ainsi que le contrôle de l'information d'authentification. Par ailleurs, les services de contrôle disposent d'outils homogènes pour lire les identifiants et pour consulter les fabricants afin de vérifier l'authenticité du produit.

Scénario 6 *Criminalisation de la contrefaçon ?*

La crise de la lutte contre la contrefaçon est non seulement une crise logistique et une crise d'authentification, mais elle est également une crise d'ordre public.

Légalement, la contrefaçon est une atteinte à la propriété intellectuelle. Passible de la juridiction civile, elle est poursuivie à la demande des ayants-droits. Certains ayants-droits adoptent une politique de tolérance « zéro » et font saisir tous les lots détectés de contrefaçons. D'autres appliquent un « seuil » d'action. De nombreux ayants-droits font détruire tous les lots de contrefaçons ; quelques uns poursuivent systématiquement les contrefacteurs en justice. De fait, les contrefacteurs sont rarement poursuivis et n'encourent que des peines minimales. Cette situation favorable n'a pas échappé aux réseaux criminels qui y trouvent une activité lucrative et peu risquée.

Certains experts prônent la criminalisation de la contrefaçon, sa qualification au pénal. Cette qualification permettrait aux autorités judiciaires de poursuivre les contrefacteurs de leur propre initiative, et justifieraient l'augmentation des peines encourues.

Cette criminalisation pourrait s'appuyer sur des techniques mentionnées ici. Par exemple, la falsification d'éléments d'authentification ou de sceaux cryptographiques pourrait être passible de poursuites au pénal, comme est poursuivie la falsification de billets de banque. Si les conditions techniques, juridiques et politiques étaient réunies, certains scénarios décrits ici pourraient aider à la détection de ces falsifications.

Conclusion

Les scénarios exposés ici illustrent l'utilisation des technologies développées par GS1 dans des dispositifs complets de lutte contre la contrefaçon. Des variantes de ces scénarios sont déjà utilisées, indépendamment des codifications et des standards de GS1. D'autres scénarios font l'objet d'études avancées pour valider leur pertinence.

Ces scénarios peuvent être déployés de manière concertée ou indépendamment les uns des autres, permettant ainsi une grande flexibilité aux différents acteurs.

La standardisation de certains de ces dispositifs **apporterait des gains économiques importants**. En effet, le développement de standards permet la mutualisation d'outils homogènes et à large distribution, conçus pour de multiples utilisateurs et dont le prix est nettement plus faible que celui de produits et de solutions spécifiques. Enfin, l'utilisation de techniques cryptographiques conjointement aux standards d'écriture et de lecture de GS1 permet le déploiement de certains scénarios **à un coût unitaire quasi-nul**, tout en offrant un bon niveau d'indication de contrefaçon.

L'utilisation des codes et des standards de transcription de GS1 dans des dispositifs de lutte contre la contrefaçon, permettrait de bénéficier, pour la protection des marques, d'investissements déjà réalisés ou bien justifiés par d'autres applications.

Enfin, les PME sont aujourd'hui souvent démunies pour lutter contre la contrefaçon de leurs produits. En effet, de nombreux outils actuels étant d'une complexité et d'un coût trop importants. Le développement d'un socle d'interopérabilité cherche à offrir à ces entreprises des moyens de protection pour leurs produits, à un coût acceptable.

Demande de commentaires

Afin d'orienter ses travaux, d'améliorer et de valider ces scénarios, GS1 souhaite recevoir vos commentaires et contributions. Si vous le souhaitez, nous pourrions vous inviter à participer à un groupe de travail visant à élaborer des propositions techniques précises.

Vous pouvez faire parvenir vos commentaires et contributions à l'adresse suivante :

Laurent Vieille
Chargé de mission « anti-contrefaçon ».

laurent.vieille@gs1fr.org

GS1 France

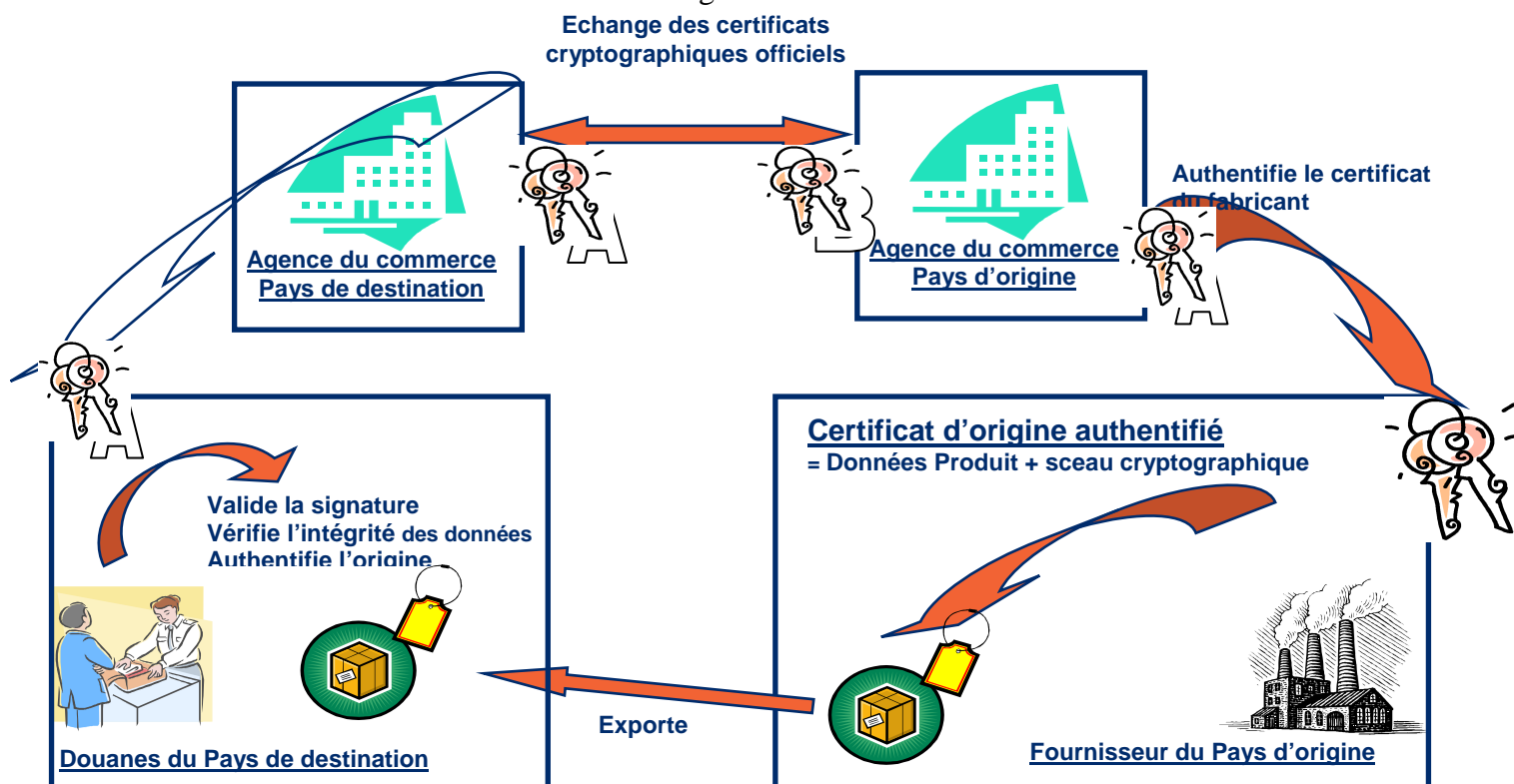
www.gs1.fr

Annexe 1 – Détails du scénario 5 : Vérification d'intégrité et certification d'origine

Cette annexe décrit un dispositif utilisant des techniques cryptographiques asymétriques pour la vérification de l'intégrité des données d'un produit et pour la certification de son origine. Ces techniques sont largement déployées sur les réseaux informatiques ou pour éviter la falsification des passeports dits « passeports électroniques ».

A titre d'illustration, la lutte contre la falsification des passeports fonctionne de la manière suivante. Les données d'état civil et la photographie de la personne sont signées par un certificat cryptographique de l'état émetteur ; le résultat de cette opération, appelé « sceau cryptographique », est associé au passeport. Les techniques cryptographiques asymétriques garantissent que seul l'émetteur peut avoir généré un tel sceau : *l'origine du passeport est certifiée*. L'utilisation du sceau permet aux autorités de contrôle de pays tiers de vérifier que l'état civil et la photographie n'ont pas été falsifiés: *l'intégrité des données est vérifiée*.

Figure 1.



La figure 1 illustre l'utilisation de ces techniques cryptographiques asymétriques à la protection des données d'un produit, ainsi qu'à la certification de son origine. De nombreuses variantes étant possibles, ce schéma est donné à titre d'illustration.

- Chaque pays participant désigne une autorité habilitée, une « agence nationale du commerce ». Cette agence nationale reçoit des *créances cryptographiques* selon un schéma agréé : une *clé privée* et un *certificat cryptographique*; la clé privée reste

secrète¹ ; le certificat cryptographique est public et contient notamment l'identification du pays et une *clé publique* appariée à la clé privée. Les agences nationales du commerce s'échangent leurs certificats cryptographiques selon un protocole sécurisé, qui pourrait s'inspirer de la « valise diplomatique ».

- Un fabricant demande son agrément auprès de l'agence nationale du commerce de son pays et reçoit en retour ses propres créances cryptographiques : une clé privée et un certificat cryptographique. Ce certificat est authentifié par l'agence nationale du commerce, ce qui lui permet d'être accepté par les autres pays participant.
- A l'aide de sa clé privée, le fabricant signe les informations du produit : ces données « produit » incluent en particulier son identifiant SGTIN. Le « sceau cryptographique » produit par cette signature est apposé au produit, avec les données « produit », par exemple sous la forme d'un code matriciel.
- A la réception du produit, les autorités de contrôle du pays de destination lisent les données « produit » et le sceau cryptographique à partir du code matriciel. Ils vérifient l'intégrité des données et l'origine du produit de la manière suivante :
 - L'identifiant SGTIN du produit permet de retrouver le certificat cryptographique du fabricant, par exemple grâce à un service en ligne.
 - En utilisant le certificat du fabricant avec le sceau cryptographique apposé au produit, les autorités de contrôle vérifient que les données « produit » n'ont pas été modifiées.
 - De plus, en cas de doute sur le certificat cryptographique du fabricant, les autorités de contrôle ont les moyens de vérifier son authenticité à l'aide du certificat cryptographique de l'agence commerciale du pays d'origine.

Ces techniques de cryptographie asymétrique permettent de vérifier que les *données « produit »* transcrites sur un code matriciel n'ont pas été modifiées. En effet cette vérification échoue si les données « produit » visibles dans le sceau ne sont pas celles qui ont été utilisées lors de la signature. Elles permettent également de certifier *leur origine*. En effet, cette vérification ne réussit qu'en utilisant le certificat public du fabricant.

¹ De nombreuses solutions sont possibles pour garder ce secret. Par exemple, des solutions largement disponibles consistent à générer et stocker cette clé privée dans un matériel sécurisé (carte à puce, clé USB sécurisé, « Hardware Security Module »), sécurisé par mot de passe et/ou des données biométriques (empreinte digitale).

Annexe 2 – Algorithmes de signature et de vérification

Cette annexe décrit les protocoles de génération de sceaux cryptographiques par signature, de vérification de l'intégrité des données et de certification de leur origine.

La figure 2 illustre l'opération de signature de données « produit ». Premièrement, les données « produit » sont transformées en une forme simplifiée « canonique » par une opération appelée « hachage ». Cette forme canonique est conçue pour être signée par la clé privée du fabricant, fournie par l'Agence Commerciale du pays d'origine. Le « sceau cryptographique » résultant est transcrit sur le produit avec les données produit.

La figure 3 illustre la vérification de signature par les autorités de contrôle. Premièrement, les données « produit » présentes sur le produit sont « hachées » pour obtenir leur représentation canonique. En parallèle, le sceau cryptographique présent sur le produit est décrypté à l'aide de la clé publique du fabricant, pour obtenir la représentation canonique d'origine. Les propriétés cryptographiques garantissent que ces deux représentations canoniques sont identiques seulement si les données présentes sur le produit lors du contrôle sont identiques à celles présentes initialement, lors de la génération du sceau cryptographique.

Figure 2 : génération du sceau cryptographique d'origine

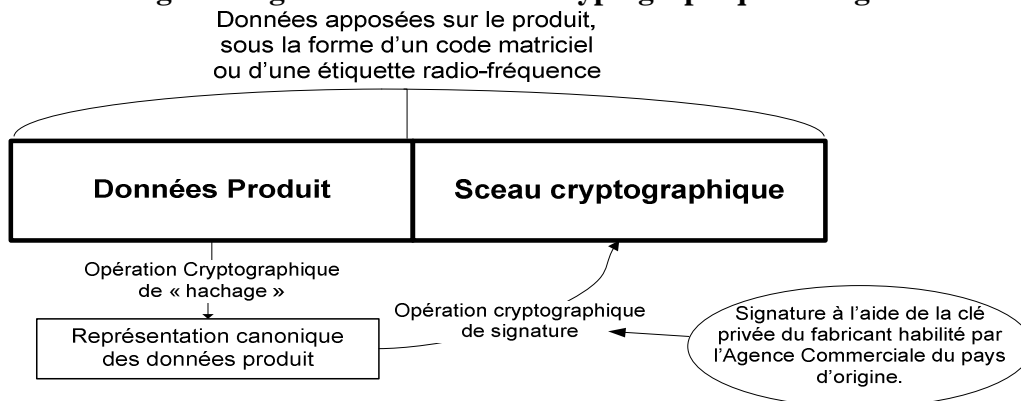


Figure 3 : vérification de l'intégrité des données et de l'origine du produit

