# La protection de copie des contenus haute définition

**Mots clés**

Protection de copie,
Chiffrement,
Tatouage d'image

Par Éric DIEHL
*Thomson*

Afin de préserver les intérêts de l'industrie audiovisuelle, la protection de copie est indispensable. Elle est un savant mélange de cryptographie, de tatouage d'image, et de règles de conformité.

## 1. La problématique

L'avènement de la numérisation des contenus, et l'augmentation de la qualité vidéo notamment la haute définition sont de formidables facteurs de croissance pour l'industrie audio-visuelle. Mais la numérisation a également accru les risques de piratage. Le haut niveau de piratage de l'industrie phonographique illustre parfaitement ce risque [6]. Pour préserver les intérêts de l'industrie audio-visuelle, il faut mettre en place des systèmes de protection et de traçabilité efficaces.

La protection de contenus se décompose en deux problèmes distincts :

- Le contrôle d'accès
- La protection de la copie

L'objectif du contrôle d'accès est d'empêcher de voir un contenu diffusé sans en avoir payé les droits. Dans le monde de la télédiffusion (encore appelé « broadcast »), on emploie les accès conditionnels. En France deux bouquets satellites TPS et Canal+ emploient VIACCESS™ et MediaGuard™. Dans le monde IP, on emploie les Digital Rights Management (DRM). L'accès conditionnel et le DRM ont le même rôle fonctionnel. Mais leur mise en œuvre est différente. Par exemple le DRM implique la présence d'une voie de retour. Ceci n'est pas nécessairement vrai pour l'accès conditionnel. Dans tous les cas, le contrôle d'accès fait intervenir une notion de monétisation.

L'objectif de la protection de copie est d'empêcher la duplication illégale de contenu. Ainsi l'utilisateur peut être autorisé à voir un contenu, mais non pas le reproduire. C'est le cas pour certains titres DVD ou VHS qui inhibent la copie analogique. Afin d'avoir une protection totale, les deux approches sont complémentaires.

Devant l'ampleur du sujet [9], ce papier explore uniquement la protection de copie. La section 2 présente les techniques employées. La section 3 brosse un panorama des principales solutions existantes ou en cours de développement.

## 2. Les techniques

### 2.1. La gestion de copie

L'élément de base de la protection de copie est le contrôle de génération (Copy Generation Management System CGMS). Traditionnellement on emploie quatre états :

- Copie libre (Copy free) : dans cet état, la copie est autorisée sans limitation.

L'ESSENTIEL

La protection de copie s'emploie à éviter la duplication illégale de copie. Elle est un mélange de quatre « techniques ». Le chiffrement protège le contenu numérique. Le tatouage prolonge cette protection dans le domaine analogique. La révocation répond efficacement à certaines attaques. Enfin les règles de conformité complètent ce dispositif. Les systèmes de protection de copie peuvent donner une réponse réduite à un élément isolé tel que le transfert ou le stockage, ou une réponse globale.

SYNOPSIS

Copy protection attempts to avoid illegal duplication of content. It is a complex system using four elements. Encryption protects digital content. Watermark extends this protection into the analog domain. Revocation efficiently copes with several attacks. Finally, compliance rules strengthen these systems. Copy protection may apply on isolated elements such as transfer or storage or may offer a complete answer for a network.

- Copie de première génération (Copy once) : dans cet état, le contenu est copiable. La copie ainsi créée n'est pas duplicable.
- Copie bloquée (Copy no more) : dans cet état, le contenu n'est plus copiable. C'est le résultat d'une copie d'un contenu copy once.
- Copie interdite (Copy never) : dans cet état, le contenu n'est pas copiable.

### 2.2. Les briques technologiques de base

Les systèmes de protection de copie emploient quatre techniques de base :

- Le chiffrement du contenu
- Le tatouage d'image (ou watermark)
- Les mécanismes de révocation
- Les règles de conformité

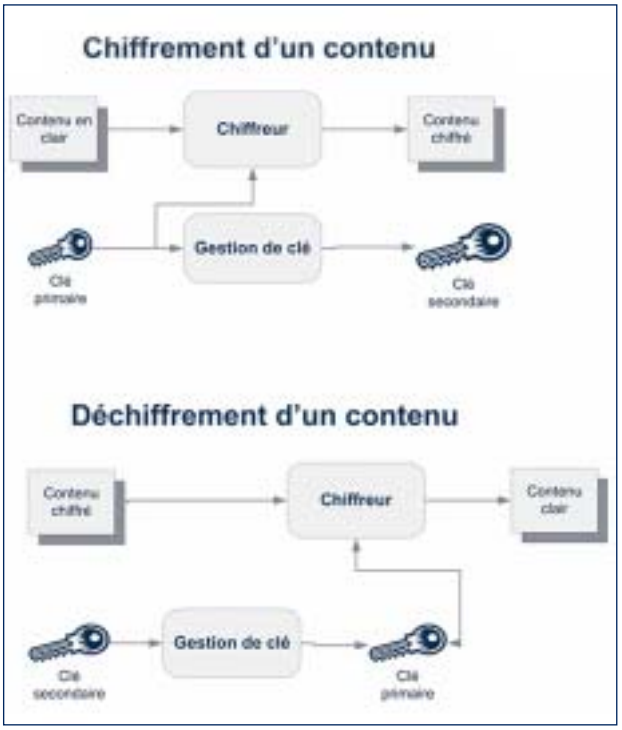


*Figure 1. Chiffrement du contenu.*

#### 2.2.1. Chiffrement

Le chiffrement de contenu applique au contenu un algorithme cryptographique de chiffrement symétrique [13]. La figure 1 illustre son fonctionnement. Le contenu est chiffré à l'aide d'une clé primaire. Pour accéder au contenu en clair, il faudra appliquer le même algorithme de chiffrement avec la même clé primaire. Il est donc indispensable que seuls les appareils autorisés aient accès à la clé primaire. C'est le rôle de la gestion de clé. La gestion de clé protège la clé primaire en lui appliquant certains processus cryptographiques. Elle fournit ainsi une information que nous appellerons clé secondaire. Seuls les appareils autorisés pourront déduire la clé primaire à partir de la clé secondaire. Chaque système de protection de copie emploie sa propre gestion de clé.

Des exemples d'algorithme de chiffrement sont DVB Common Scrambling Algorithm (DVB-CSA), AES [11], ou DES [3]. Par exemple, dans le monde DVB, tous les contenus sont chiffrés avec DVB-CSA. La clé primaire s'appelle mot de contrôle (Control Word CW). La clé primaire change toutes les 10 secondes. Le mot de contrôle est stocké dans une structure de donnée chiffrée appelée ECM (Entitlement Control Message). Les cartes à puce de l'accès conditionnel sauront déchiffrer les ECMs et donc récupérer le mot de contrôle. Les cartes à puce ne fourniront aux décodeurs le mot de contrôle que si l'usager a acquis les droits nécessaires.

#### 2.2.2. Tatouage

Le tatouage d'image permet de cacher au sein de l'image les informations de contrôle de copie [10]. Le principe du tatouage d'image, illustré à la figure 2, est d'enfouir les informations d'un message *m* en altérant légèrement l'image initiale *Co*. C'est le rôle du tatoueur. La clé de watermark lui permet de dissimuler le message dans l'image de manière déterministe. Le résultat est une image altérée *Cw* qui contient le message *m*. L'altération tient compte des caractéristiques physiologiques de la vision humaine afin d'être invisible. Un exemple rudimentaire est d'utiliser le bit de poids faible de la luminosité de certains pixels définis par la clé. Comme l'œil humain est moins sensible à la luminosité, cette altération n'est pas perceptible en théorie. Bien entendu, les tatouages modernes sont plus sophistiqués. La transmission de l'image *Cw* éventuellement introduit du bruit. Si le bruit est acceptable, la personne percevra une image « identique » à l'originale. Néanmoins, un détecteur de watermark informé, c'est-à-dire ayant la bonne clé de watermark, pourra extraire le message caché *m*. Une même image peut contenir plusieurs messages cachés.

Le tatouage est un savant compromis entre son invisibilité, sa robustesse aux altérations (volontaires ou involontaires) de l'image et enfin de la taille du message *m* caché.

L'intérêt majeur du tatouage d'image est qu'il survit dans le domaine analogique. Le chiffrement ne protège que les contenus numériques. Mais à la fin, les contenus numériques doivent être restitués dans le domaine analogique perdant ainsi la protection du chiffrement. Le tatouage conserve l'information de copie. Les entrées analogiques conformes détectent ce tatouage et réagissent de manière adéquate lors de la numérisation. Ainsi, un enregistreur numérique refusera d'enregistrer sur son entrée analogique un contenu qui serait marqué « copie interdite ».

Il est à noter que cet usage du tatouage d'image est différent de l'usage plus fréquent pour le traçage. Dans ce cas, le tatouage enfouit une information identifiant le destinataire original d'un contenu. En cas de diffusion

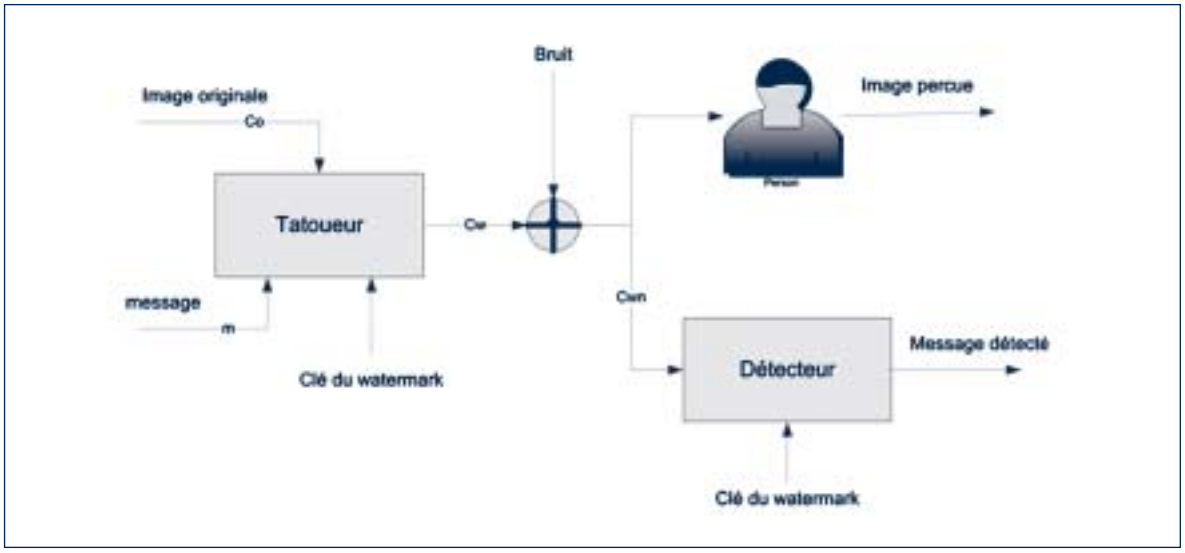


*Figure 2. Utilisation d'un tatouage.*

illégale, il est donc possible en théorie de remonter à la source de la fuite. Les tatouages successifs d'un même contenu permettent aussi d'identifier un chemin de transfert.

#### 2.2.3. Révocation

Aucun système de sécurité n'est inviolable. Un bon système de sécurité doit survivre à une attaque. Deux stratégies sont utilisées pour révoquer des appareils corrompus :

- La liste de révocation : les appareils reçoivent une liste des appareils corrompus. Un appareil conforme ne peut interagir qu'avec un appareil n'appartenant pas à cette liste. Les appareils du parc installé doivent avoir la liste la plus à jour.
- Broadcast encryption [12] ; récemment une nouvelle famille de gestion de clés est apparue. Une autorité centrale livre un jeu de clés pour chaque appareil. L'émetteur définit la liste des appareils pouvant accéder au contenu. Le broadcast encryption crée une structure de données appelée Key Block. Un appareil appartenant à la liste trouvera la clé primaire en appliquant un calcul mathématique avec son jeu de clés et la Key Block. Les appareils n'appartenant pas à la liste ne trouveront pas la clé primaire en appliquant le même calcul mathématique. Par cette méthode, la gestion de clé fait à la fois la protection de la clé primaire et la révocation. En d'autres termes, le contenu définit l'ensemble des appareils qui pourront l'accéder. Le broadcast encryption évite ainsi l'envoi d'une liste de révocation.

Malheureusement, la révocation ne répond pas à toutes les attaques. Certaines peuvent éventuellement contourner le mécanisme de révocation. Dans ce cas, la seule réponse efficace est le remplacement complet de toute la solution soit par le chargement d'une nouvelle version logicielle, ou par le remplacement d'un module de sécurité amovible (carte à puce…).

#### 2.2.4. Règles de conformité

Les règles de conformité permettent d'imposer le respect de certaines contraintes. Ces règles définissent le comportement des appareils. Par exemple, elles peuvent imposer la présence de détecteur de tatouage sur une entrée analogique. Certains systèmes de protection de copie assument qu'un enregistreur recevant un contenu marqué « copie interdite » refusera d'enregistrer. Les règles de conformité nécessitent un contrat légal. Elles sont souvent annexées à l'accord de licence technologique.

## 3. Les familles de solution

### 3.1. Les protections pour unités de stockage

L'objectif est d'empêcher de dupliquer illégalement un contenu stocké. Les attaques classiques sont de deux types :

- Accéder au contenu stocké par un système pirate
- Faire une copie parfaite bit à bit

La réponse classique à la première attaque est le chiffrement. Seul des appareils conformes ont les secrets nécessaires à la gestion de clé. L'hypothèse de sécurité est qu'un appareil non-conforme n'est pas capable de la reproduire. Cette hypothèse par exemple s'est révélée fausse avec le système de protection du DVD (Content Scramble System). Les logiciels pirates reproduisent la gestion de clé du CSS.

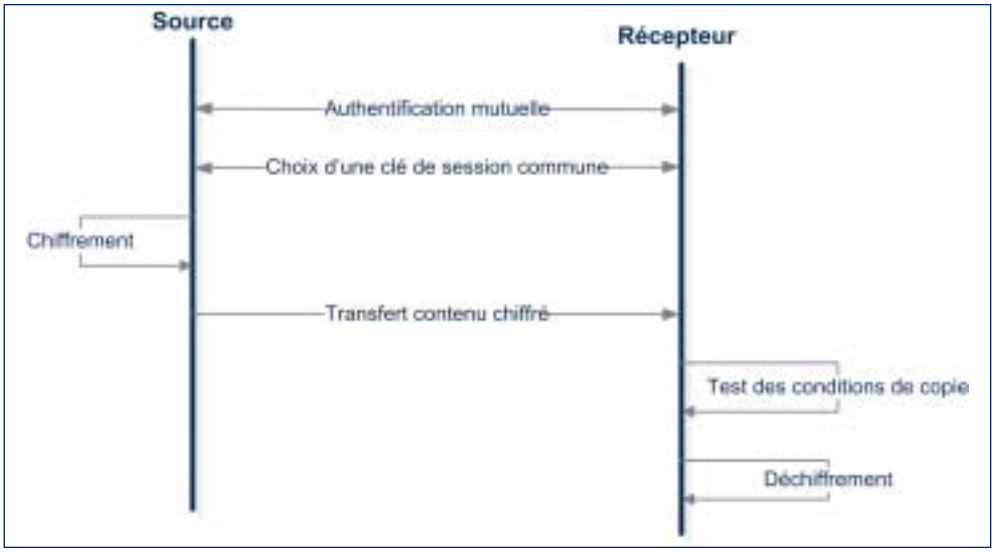


*Figure 3. la protection de copie sur bus.*

La réponse à la copie parfaite a typiquement trois solutions :

- Un contenu marqué « copie interdite » sur un support enregistrable est considéré comme illégal. Un appareil conforme ne le restituera pas.
- La diversification du contenu ; dans ce cas, le contenu est lié cryptographiquement à l'identité du support. Traditionnellement la gestion de clé prend comme paramètre supplémentaire un identifiant unique du support. Ainsi la clé secondaire devient unique pour chaque support.
- Certaines parties du disque enregistrable ne peuvent être gravées, ni modifiées par l'enregistreur. Dans ce cas, le schéma de protection de copie utilise cet espace afin d'empêcher une copie bit à bit en *y* plaçant des données critiques.

Dans les systèmes en cours de développement, on peut citer deux solutions : Blu-Ray Disc Copy Protection System (BD CPS) pour le Blu-ray DVD [2], et Advanced Access Content System (AACS) [1]. Les deux systèmes emploient le broadcast encryption pour la gestion de clés et AES pour chiffrer le contenu. Le disque contient deux types d'informations : le contenu chiffré en AES avec une clé primaire et les informations nécessaires pour calculer la clé primaire. Parmi ces informations se trouve la table de révocation RKB (Revocation Key Block). Chaque lecteur a un jeu de clés uniques. La table de révocation est construite de telle sorte que tous les lecteurs n'ayant pas de clés révoquées retrouvent une même valeur en utilisant cette table. Par contre, un appareil ayant une clé révoquée trouvera une autre valeur. La bonne valeur sert à chiffrer la clé primaire. Seuls les appareils non révoqués peuvent trouver la clé primaire qui chiffre le contenu du disque Ainsi chaque disque transporte sa propre liste de révocation.

### 3.2. La protection de copie pour bus

Le premier objectif est d'empêcher que l'appareil récepteur puisse faire une copie illégale. Le second objectif est d'éviter de pouvoir faire une copie en espionnant la transmission d'un contenu.

La solution est le chiffrement du contenu lors du transfert entre les deux appareils. Les deux appareils s'authentifient mutuellement. Cette authentification garantit qu'ils sont conformes. Car seuls les appareils conformes ont les secrets nécessaires pour s'authentifier. Ces secrets sont délivrés par une autorité de certification. Une fois authentifiés, ils établissent une clé commune de session. L'émetteur chiffre le contenu à envoyer avec cette clé commune. Le récepteur déchiffre le contenu reçu avec cette même clé et agit en conformité avec l'état du contenu. Les règles de conformité définissent le comportement espéré du récepteur.

Il est important de comprendre la différence entre la protection de copie d'un bus et sa sécurisation. En effet, la sécurisation d'un bus n'assure que la confidentialité et l'intégrité du transfert. Elle répond donc au second objectif. Ainsi, IPSec permet de garantir la sécurité du contenu lors de son transfert sur un bus Ethernet [3]. Mais IPSec ne garantit pas qu'un contenu marqué « copie interdite » ne soit pas copié par la cible. Le test des conditions de copie n'est pas défini par IPSec. Le premier objectif n'est pas rempli. Mais la protection de copie définit en plus le comportement des émetteurs et récepteurs selon le mode de copie.

Les solutions commerciales les plus connues sont Digital Transmission Copy Protection (DTCP) et High Definition Copy Protection (HDCP) [7]. DTCP protége

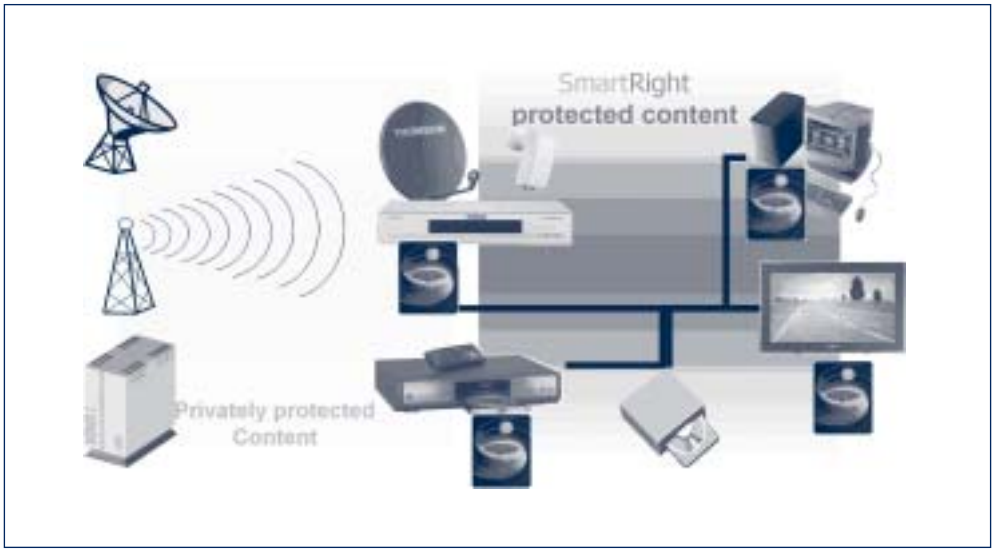


*Figure 4. L'environnement SmartRight.*

les contenus compressés sur Ethernet, IEEE1394, USB, ou MOST [5]. HDCP protège les contenus non compressés sur Digital Video Interface (DVI), ou High Definition Multimedia Interface (HDMI).

Nous allons examiner plus en détails le protocole HDCP. Comme indiquée par la figure 3, la première étape est l'authentification. L'émetteur HDCP vérifie que le récepteur est bien autorisé à recevoir du contenu protégé HDCP. Selon un principe similaire au broadcast encryption, chaque entité a une table de 40 clés privées (notée KSV) et un identifiant unique. L'émetteur A envoie son identifiant $A_{KSV}$. Le récepteur B renvoie son identifiant $B_{KSV}$. L'émetteur A vérifie que $B_{KSV}$ n'est pas révoquée. Le récepteur doit avoir les listes de révocation les plus récentes. A ce stade, l'émetteur a vérifié que le récepteur est du type HDCP. Ils vont maintenant établir une clé commune $K_M$. Pour ce faire, chacun utilise sa table KSV et l'identifiant de l'autre pour la calculer. Ainsi, chacun peut trouver $K_M$ sans qu'elle n'apparaisse sur le bus. Seuls les appareils ayant une table valide peuvent trouver cette clé. A et B vont calculer une valeur $R_0$ à partir de $K_M$. B renvoie sa valeur calculée à A qui vérifie quelles sont égales. A ce stade, A a la preuve que B est authentifié et qu'ils ont une même clé de session. La transmission chiffrée peut débuter. Le chiffrement est un basique chiffrement de flux (stream cipher en anglais). L'opération XOR est effectuée bit à bit entre le contenu et la sortie d'un générateur pseudo aléatoire. Le récepteur B effectue la même opération. Il faut noter que dans le cas de HDCP, il n'y a pas de test des conditions de copie car les règles de conformité imposent que le récepteur ne peut pas enregistrer le contenu reçu.

### 3.3. La protection du contenu dans le domaine autorisé

Récemment une nouvelle approche de la protection de copie est apparue tenant compte des futures réseaux domestiques numériques. Ainsi, le DVB Copy Protection group a défini le concept de domaine autorisé. Le domaine autorisé est l'ensemble des appareils appartenant à une même famille. Il comprend les appareils du domicile, de la résidence secondaire et les appareils portables. Au sein de ce domaine, les appareils doivent pouvoir accéder aux contenus de manière transparente. Un des avantages de ces systèmes est la notion de copie privée. Au sein d'un même domaine, il est possible de faire un nombre illimité de copies. Mais ces copies ne sont utilisables que dans ce domaine. Une implémentation efficace de la copie à usage privé est donc possible.

Deux systèmes proposent une protection de copie pour le domaine autorisé : SmartRight et xCP. SmartRight utilise une approche proche de l'accès conditionnel avec des cartes à puce. xCP utilise le broadcast encryption.

Une des difficultés majeures de la protection de copie pour domaine autorisé est la gestion du dit domaine. Le domaine autorisé est en constante mutation. De nouveaux appareils viennent s'y ajouter. Les appareils portables ne sont pas connectés en permanence. De plus, il faut limiter la taille du domaine à une valeur raisonnable. La gestion doit être transparente pour l'utilisateur. Il ne serait pas acceptable que l'utilisateur soit indûment gêné par la protection de copie. Il faut respecter la vie privée de l'utilisateur. Cette liste n'est pas exhaustive.

Dans le cas de SmartRight [8], les contenus arrivent au réseau domestique, protégés par des systèmes propriétaires tels que Accès Conditionnel ou DRM. Le système

SmartRight prend le relais au sein du réseau domestique. Les contenus sont chiffrés par exemple en AES. Seuls les téléviseurs vont les déchiffrer. La clé de chiffrement (ou clé primaire de la figure 1) est protégée par une clé de réseau commune à tous les appareils d'un même réseau domestique. Les cartes à puce établissent et gèrent la clé de réseau commune ainsi que la protection des clés de chiffrement. Aussi une carte du domaine autorisé d'Alice ne peut pas déchiffrer de contenus du domaine autorisé de Bob. En effet, elle n'a pas la clé de réseau de Bob et elle ne peut donc accéder à la clé primaire.

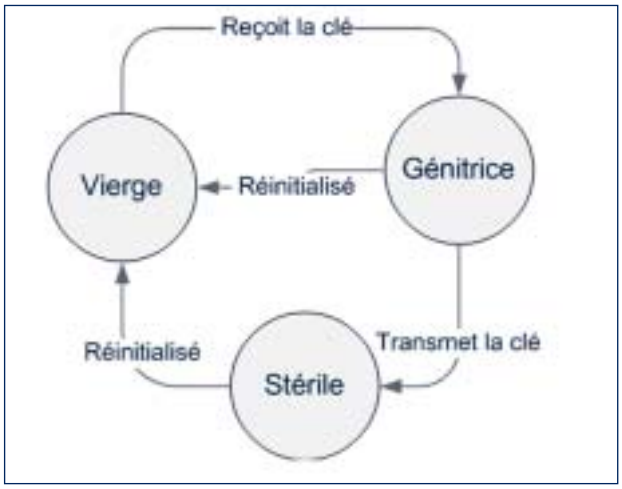


*Figure 5. Les états des cartes à puce SmartRight.*

Nous allons décrire sommairement la manière dont SmartRight propage la clé de réseau dans le domaine autorisé (voir figure 5). Les cartes à puce sortant de l'usine sont dans l'état vierge. Elles ne connaissent pas la clé de réseau. Lors de la création du réseau, la carte vierge génère aléatoirement une clé de réseau. Elle passe dans l'état géniteur. Si une carte génitrice rencontre sur le réseau une carte vierge, elle lui transmet de manière sécurisée la clé de réseau. Elle passe alors dans l'état stérile. Une carte stérile ne peut plus transmettre la clé de réseau. La carte vierge qui a reçu la clé de réseau devient la carte génitrice. Afin de limiter la taille du domaine autorisée, le nombre de transferts géniteurs est borné. Si des cartes appartenant à des domaines distincts sont mis en relation, elles se bloquent et refusent de déchiffrer les contenus. Cette gestion de clé offre les caractéristiques suivantes :

- La taille du domaine autorisé est bornée.
- Les domaines autorisés sont isolés et ne peuvent échanger des contenus.
- La gestion du domaine autorisé respecte la vie privée des utilisateurs car elle ne fait pas intervenir de tierce partie.
- La gestion du domaine autorisé est transparente pour l'utilisateur.

Il est important de noter que la protection de contenu pour le domaine autorisé est auto-suffisante. En effet, elle répond à la fois à la problématique de la protection des unités de stockage et de la protection des bus avec un système unique. Les autres approches demandent de combiner différents systèmes.

## 4. Conclusions

La protection de copie est indispensable pour préserver les intérêts de l'industrie audio-visuelle. Des solutions techniques apparaissent. La couverture de la protection varie allant de la protection du support physique jusqu'à une protection globale contrôlant la copie sur l'intégralité d'un réseau domestique.

Les recherches dans le domaine de la protection de copie doivent s'orienter vers deux axes. Le premier est commercial. Il faut trouver de nouveaux modes de protection de copie qui réconcilient les intérêts des ayants droit et des utilisateurs. Le second axe est technique. Un des défis les plus importants est la renouvelabilité du système de protection de copie une fois déployé.

## Références

[1] http://www.aacsla.com/.
[2] http://www.blu-ray.com/.
[3] http://www.ietf.org/html.charters/ipsec-charter.html.
[4] "*Data Encryption Standard*", NIST, 1991, FIPS 46-3, available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.
[5] "*Digital Transmission Content Protection white paper*", disponible à http://www.dtcp.com/data/wp_spec.pdf.
[6] "*Commercial Piracy Report 2004*", juillet 2004, disponible à http://www.ifpi.org/site-content/library/piracy2004.pdf.
[7] "*High-bandwidth Digital Content Protection specifications*", rev 1.1, 2003 disponible à http://www.digital-cp.com/data/HDCPSpecificationRev1_1.pdf.
[8] J.P ANDREAUX, E. DIEHL, A. DURAND, T.FURON, "*SmartRight a copy protection scheme for Digital Home Networks*", IEEE Signal Processing, mars 2004.
[9] P. CHANTEPIE, M. HERUBEL, F. TARRIER, "*Mesures techniques de protection des oeuvres et DRMs, janvier 2003, Ministère de la culture et communication*", disponible à http://www.ddm.gouv.fr/rubrique.php3?id_rubrique=88.
[10] I. COX , M. MILLER, J. BLOOM, "*Digital watermarking*", Morgan Kaufmann Publishers, 2002.
[11] J. DAEMEN, V. RIJMEN, "*The Design of Rijndael AES The advanced Encryption Standard*", SPRINGER, 2002.
[12] S. FIAT, M. NAOR, "*Broadcast encryption, in advances in cryptology*", Crypto '93, Lecture Notes in Computer Science 773, pp. 480-491.
[13] B. SCHNEIER, "*Applied cryptography*", 2nd edition, John Wiley, 1996.

## Les auteurs

**Eric Diehl** est né en 1962. Il est diplômé de l'Ecole Nationale Supérieure d'Electronique et Radio-électricité de Grenoble (ENSERG 85). En 1987, il rejoint Corporate Research THOMSON. Il y a travaillé sur le CDI, la télévision à péage, les réseaux domestiques, les interfaces utilisateurs et la sécurité. Depuis 1998, il dirige le laboratoire sécurité de THOMSON Corporate Research. Ce laboratoire s'intéresse particulièrement à la protection des contenus le long de la chaîne de l'image. Le système SmartRight est une émanation de cette équipe.
Il a déposé plus de 65 brevets dans les domaines de la sécurité, télévision à péage et interface utilisateurs. Il est l'auteur de multiples publications.