SmartRight: A Copy Protection System for Digital Home Networks

Jean-Pierre Andreaux, Alain Durand, Teddy Furon, Eric Diehl

SmartRight: A Copy Protection System for Digital Home Networks

Jean-Pierre Andreaux[1], Alain Durand[1], Teddy Furon[2] and Eric Diehl[1]

[1] THOMSON multimedia R&D France, Rennes, France

{jean-pierre.andreaux, alain.durand, eric.diehl}@thomson.net,

[2] INRIA / TEMICS, Rennes, France

teddy.furon@irisa.fr

Abstract

This paper describes the rationales supporting the design of a Copy Protection System. It reflects the experience of the Security Laboratory of Thomson in the development of SmartRight. This paper does not only account the chosen technical solutions. It also explores less technical but highly important issues such as the social, legal and commercial aspects. Hence, while carefully developing our motivations, some light is shed on the very peculiar problems raised by the enforcement of copy protection. It gives then an overview of the global SmartRight system and some technical details on its main innovative features.

I. Introduction: Context and birth of the SmartRight copy protection system

This section presents the context of copy protection dealing with legal and socio-economic aspects. This comprehensive picture shows the main actors and their relationships, the rules and some basic definitions of this field. A brief history of copy protection for DVD emphasizes the lessons from the past initiatives and the pitfalls to avoid.

A. The socio-economic aspects

In 2001, the creative industries[1] contributed more to the U.S. economy and employed more workers than any single manufacturing sector. It represented 5.24% of the U.S. Gross Domestic Product, or $535 billion and 3.5% of the total U.S. employment, or 4.7 million workers [6]. With the digital age,

[1] Theatrical films, TV programs, home video, DVDs, business software, entertainment software, books, music and sound recordings.

the artists' works, in the form of multimedia content, are stored and transmitted with a very high fidelity. This provides new business models, but it also raises an unpredictable level of piracy spoiling the creative industries. According to the Recording Industry Association of America (RIAA), the volume of sold audio CDs dropped by 5% in 2001 [7] and by 11% in the first half of 2002 [1]. The Motion Picture Association of America (MPAA) estimates that the movie industry loses $3 billion annually in potential worldwide revenue due to piracy. This does not include the losses due to Internet piracy, as they are rather difficult to estimate.

This decrease stems from three main threats. The greatest danger is the optical disc piracy made on factory production lines and in smaller scale 'CD-R labs'. The International Federation of the Phonographic Industry (IFPI) estimates that in 2001, 28% of all audio CDs sold were pirate [5]. The creative industry fights against this organized piracy thanks to collaborations with local enforcement bodies and Interpol. In 2001, over 20 millions pirate optical discs were seized. Around 42 manufacturing lines having the annual production equivalent to the CD audio market in UK, have been closed. The second threat is the online piracy in the forms of downloadable media, hard goods piracy, streaming media and online offerings of illegal circumvention devices. By some estimates, more than 350,000 movies are illegally downloaded every day and 99% of online music files are unauthorized. Here again, the creative industry is not weaponless against Internet piracy. For instance, IFPI removed over 1000 peer-to-peer (P2P) servers and 700 millions unauthorized music files [5].

This article focuses on the third source of losses, the "private copy". This problem is harder to handle than the first two ones detailed above, as it is not due to some organizations or P2P communities that deliberately infringe the law. Although content providers and CE manufacturers launched hand in hand the CD audio in the 80s and the DVD video in the 90s, the record button gives birth to a rampant dissension among the creative industries and the consumers. Consumers cheaply duplicate pristine quality content thanks to the digital technology. They do not understand that what was tolerated in the analogue age might become an act of piracy in the digital age. Whereas the number of anti-copy CD systems increases, many consumers resort to a so-called "right to space shifting" (e.g. copying CDs on portable MP3 reader) or would-be "right to backup" that they intend to exercise in an unlimited and unconditional manner. However, these practices do not clearly affect the music industry. In Germany,

a recent survey discovers that 18% of the consumers said burning CDs resulted in buying less music [5]. On the other hand, the income from sold audio CDs in 2001 increased of 5% in France, 7% in Brazil and 29% in Chile. Some explain this phenomenon by the fact that the "private copy" eases the spread of the music culture that benefits to the society and finally to the creation industries.

B. The legal aspect

All copyright systems aims at striking a proper balance between the interests of the authors and the investors and the public interest to promote learning, culture and development. The international treaties and conventions rule it through a general framework invoking copyrights, neighboring rights and exceptions [2], [3], [8] and [9]. The latter ones are situations exempting certain uses from authorization. Each national law defines its range of exception, but most copyright systems know the same types either in a limitative list or through a general provision like 'fair use' in the U.S. There is also a kind of hierarchy among the exceptions [11]. Some express fundamental rights like the exception of quotations for criticism or review. Others cover needs for public interest like collective use in libraries. The 'private reproduction' belongs to the third class of tolerated exceptions. At the time of their introduction, these tolerated acts were insignificantly prejudicial with respect to the legal and practical difficulties. . These tolerances are not rights. For instance, article 6.4 of the European Union Copyright Directive (EUCD) says that private reproduction *may* be granted under the provisions stated by Art. 5.2 (b) "*in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures*" [10]. Thus, a copy protection system may enforce the exception of private reproduction for the sake of user-friendliness but under the agreement of content provider and with respect of legal provisions.

The proper balance of rights between content owners, providers and consumers must be enforced by technical protection means. This introduces a fourth type of actors: technology providers. These are the Consumer Electronics (CE) and Information Technology (IT) industries, which embed in their products a DRM system or a CP system. DRM systems enforce various business models defined by

content providers. In particular, it implements technical means to guarantee that the consumption associated to these business models will not be tampered by dishonest users. CP systems only guarantee, if necessary, that no copy (copy-never/copy no-more) or only one copy (copy-once) can be done from a protected content. CP system does not enforce any business model. It just prevents illegal duplication.

Figure 1 sketches the actors of the content distribution chain.

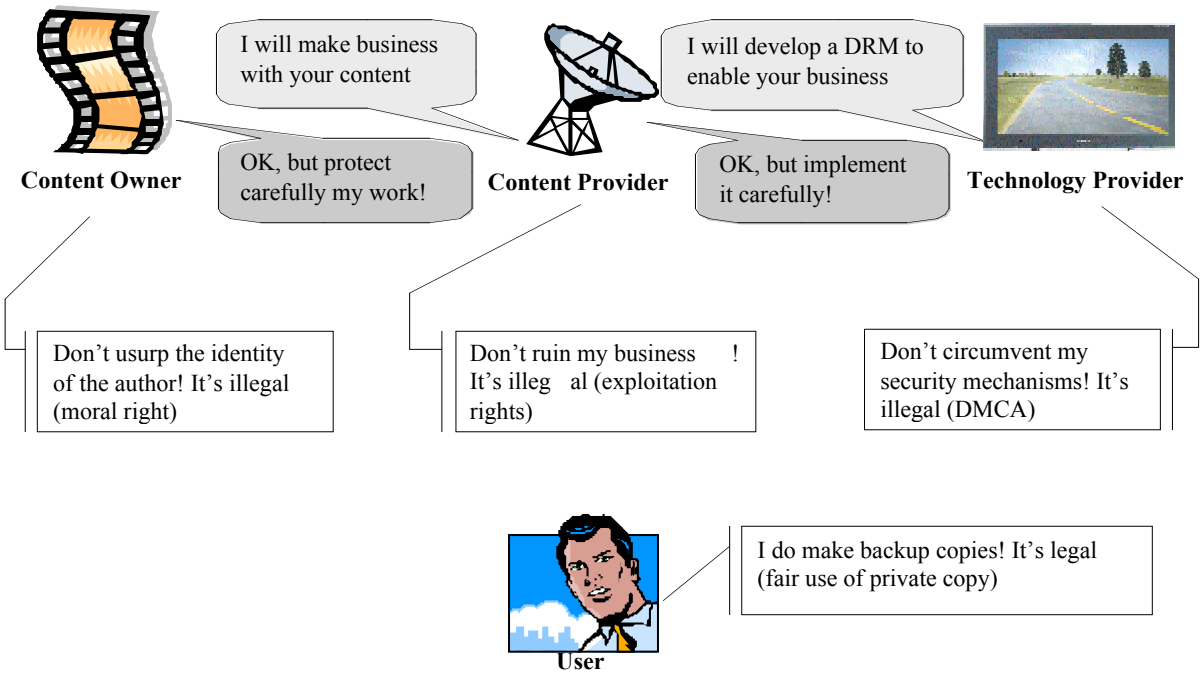

Figure 1– Balance of rights between the four actors of the content distribution chain

To conclude, the main goal of a CP system is to 'keep honest people honest' securing a fair and limited exercise of the "private reproduction" exception tolerated by content owners and providers. It prevents the 'ant piracy', i.e. individuals with very limited resources making few illegal copies for friends, relatives, or for themselves. Copy protection does not target organized piracy. However, with the fear of the average skilled hacker class, so-called 'garage piracy', the security level of CP system tends to increase. Meanwhile, new laws implementing the WIPO treaty [9] forbid the forgery of these technical barriers and they severely punish violators [10][4].

C. Lessons learnt from the past: the example of the DVD

The beginning of digital copy protection

Copy protection concerns on digital content were outlined by the motion picture industry (MP) in May 1996 with the birth of the DVD video. Many proprietary solutions already existed., But it was the first time a large dedicated forum, so-called Copy Protection Technical Working Group (CPTWG), was created in order to address the security of content stored on DVD video. MP, IT and CE industries participated in this forum and agreed in November 1996 on the first CP system called Content Scrambling System (CSS). Only CSS compliant devices could play protected content. The content is encrypted with CSS. The master key, needed to decrypt CSS-encrypted DVD videos, was delivered only to devices complying with strict implementation rules, so called compliance rules. CSS was broken in 1999.

In October 1996, CPTWG decided to study the protection of digital buses (e.g. FireWire, DVI…) between two compliant devices must be tackled as well. Many link encryption systems were proposed. Two commercial solutions were adapted. DTCP secures digital compressed content (February 1998); HDCP secureS digital uncompressed content over DVI (October 1999). An exhaustive list of the CP systems presented during the CPTWG meetings is given in [16].

Toward a global copy protection system

In 1998, the Thomson felt that piecemeal solutions using "local" CP systems (for storage, for transmission…) was the worst approach. Thomson proposed a global CP system as sketched in Figure 2. No particular distinction is made between source, storage and display devices. Another main idea was to extend the security already brought by the conditional access systems. This system was called XCA (eXtended Conditional Access) and can be considered as the ancestor of SmartRight.

II. SmartRight[2] overview

This section describes the architecture of SmartRight. First, the main requirements and features imposed during its development are provided. Then, its architecture and the chosen technical solutions are described. Some use cases and business models illustrate the behavior of the SmartRight system.

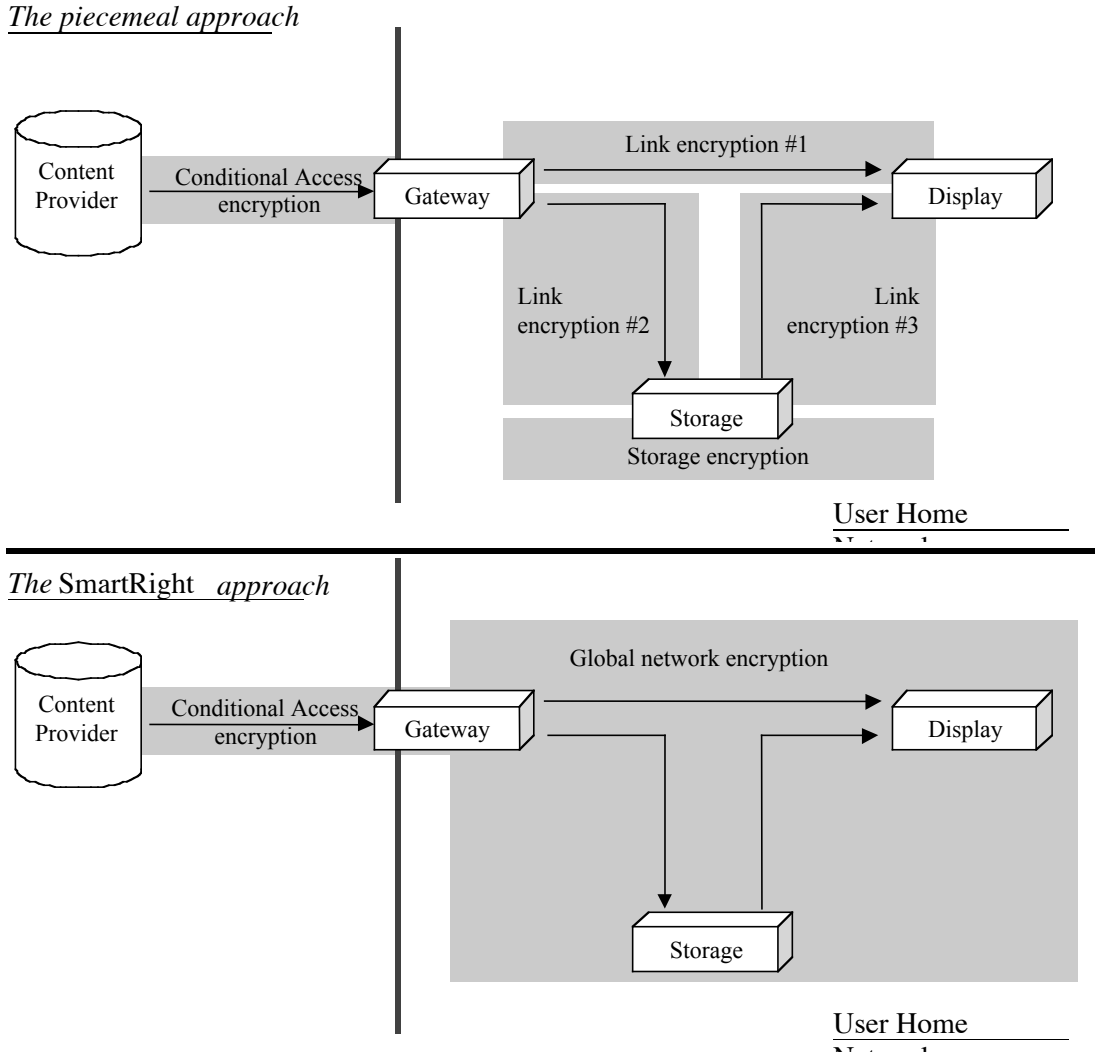

Figure 2 – The SmartRight alternative to the multiple copy protection systems approach.

[2] SmartRight was first designed by Thomson, with the help of world-class technology partners: Canal+ Technologies, Gemplus, Micronas, Nagravision, Pioneer, SchlumbergerSema, SCM Microsystems, STMicroelectronics.

A. Main features

End-to-end protection

SmartRight's philosophy is to prevent any break in the chain of content protection. To that end, digital content is kept scrambled as required throughout the home network while stored or transferred from one device to another and until it is played for the consumer on a rendering device such as a TV set.

Universality

SmartRight makes no assumption on the format of the content it receives. It accepts content from any kind of digital source, including free-to-air broadcast and pre-recorded content.

Interoperability

SmartRight is separate from, and complementary to, all currently available Conditional Access (CA) and DRM systems. It defines a common syntax for SmartRight content to ensure interoperability, and defines an API with current CA and DRM systems.

SmartRight can be used with any current and future bi-directional digital interface, such as FireWire, or Wi-Fi.

SmartRight's end-to-end protection may coexist and interoperate with all currently existing CP systems. To that end, inbound and outbound rules have been defined between the SmartRight system and other coexisting content protection systems on the same digital home network, to enforce the rules associated to the content.

Renewability

Any commercial security system will be broken [17]. Renewing the security scheme is therefore a must-have feature for any serious design. Thus, SmartRight uses renewable security modules. CE devices will be equipped with removable modules such as smart cards.

Personal Private Network

SmartRight introduces the innovative concept of personal private network (PPN), which is composed of a set of devices, owned by a given person or household. It is not limited to a given location and does not require any permanent connection, which means it supports multiple homes and mobile devices. Consequently, a user can access all his content on any device belonging to his PPN.

Nevertheless, to ensure the protection of rights associated to the content, a SmartRight device belongs to only one PPN at a given time, and two different PPNs cannot interoperate. The number of rendering devices within a same PPN is limited. The absence of such limitation would actually allow to share a unique, global PPN over the Internet.

Business model enabler

SmartRight facilitates the creation of a wide range of innovative business models, including any time- or event- related business model that may be supported by digital devices connected to a PPN. SmartRight provides a secure environment for the consumption of content in accordance with such business models. All content usage rules are determined and managed by the CA and DRM systems that deliver content to the home network.

B. Architecture

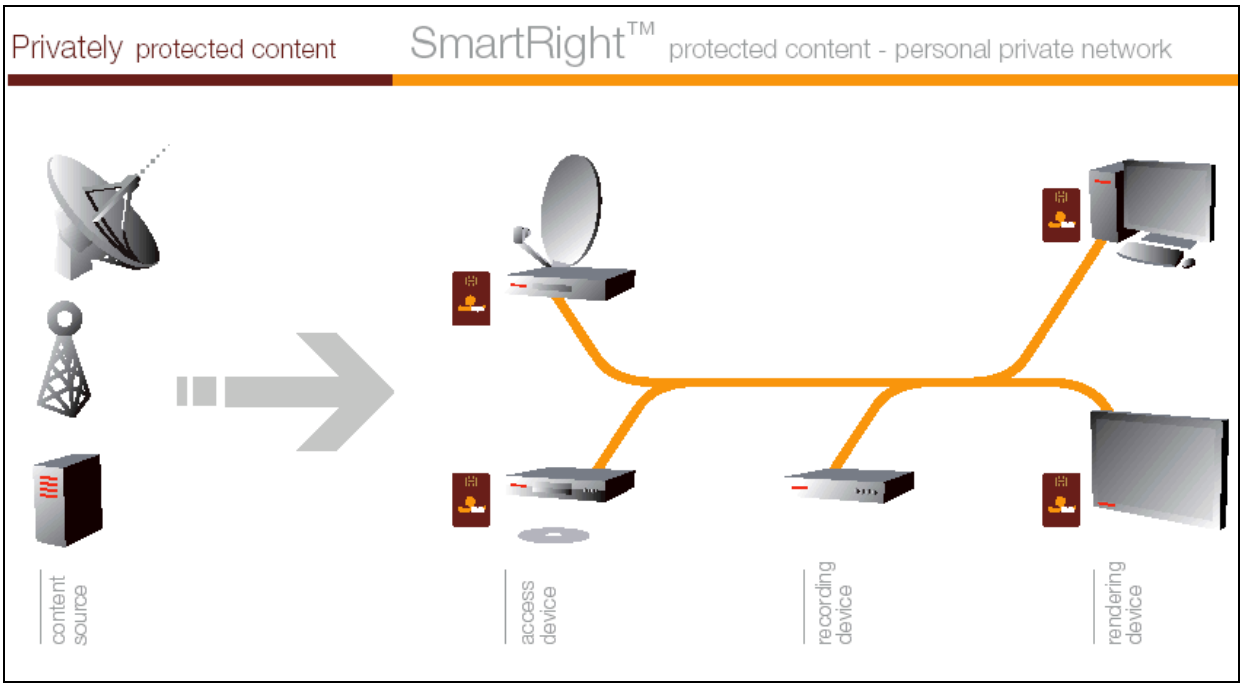

Figure 3 – SmartRight environment and architecture

Environment

Figure 3 shows the environment of the SmartRight system. There are two domains of protection:

In the first domain (on the left side), pre-recorded encryption, private CA systems or DRM systems protect content while delivered to the home,

In the second domain (on the right side), the SmartRight system protects content after it enters the home and until it is rendered or exported.

Devices

SmartRight-enabled devices may play three roles:

Acquisition role. In this role, the device is a gateway for protected content coming from outside the home network. Distribution means include broadcast, broadband, pre-recorded media, or proprietary DRM systems,

Presentation role. The device renders SmartRight protected content or exports content to proprietary CP systems,

Storage role. The device records content carried over the home network. Since SmartRight protected content is scrambled, it remains protected while stored.

SmartRight-enabled devices may combine several roles, such as acquisition and presentation roles (e.g. an Integrated DTV), or as storage and acquisition roles (e.g. a set top box with embedded personal video recorder).

Cards

To ensure high-level protection and renewable security, SmartRight uses removable security cards. Theses cards hold keys and perform secure cryptographic processing. Within the SmartRight architecture, the card associated to the access role is called converter card, and the card associated to the presentation role is called terminal card.

C. SmartRight use cases

Every piece of content entering the SmartRight PPN is associated to one scenario. The three possibilities are view-only, private-copy and copy-free.

Usage rules for view-only content are:

It is possible to render it while it is delivered at home,

It is not possible to render it if it has been stored,

It is not possible to render it in a different PPN.

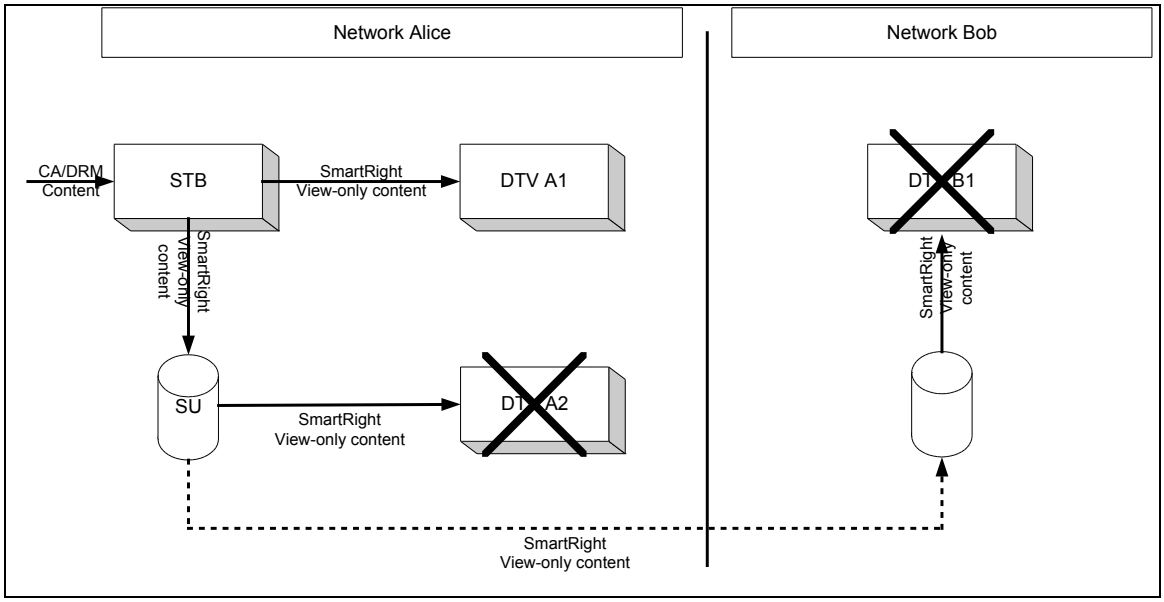

Figure 4 – View-only usage rules

Usage rules for private-copy content are:

It is possible to render it while it is delivered at home,

It is possible to render it even if it has been stored,

It is not possible to render it in a different PPN.

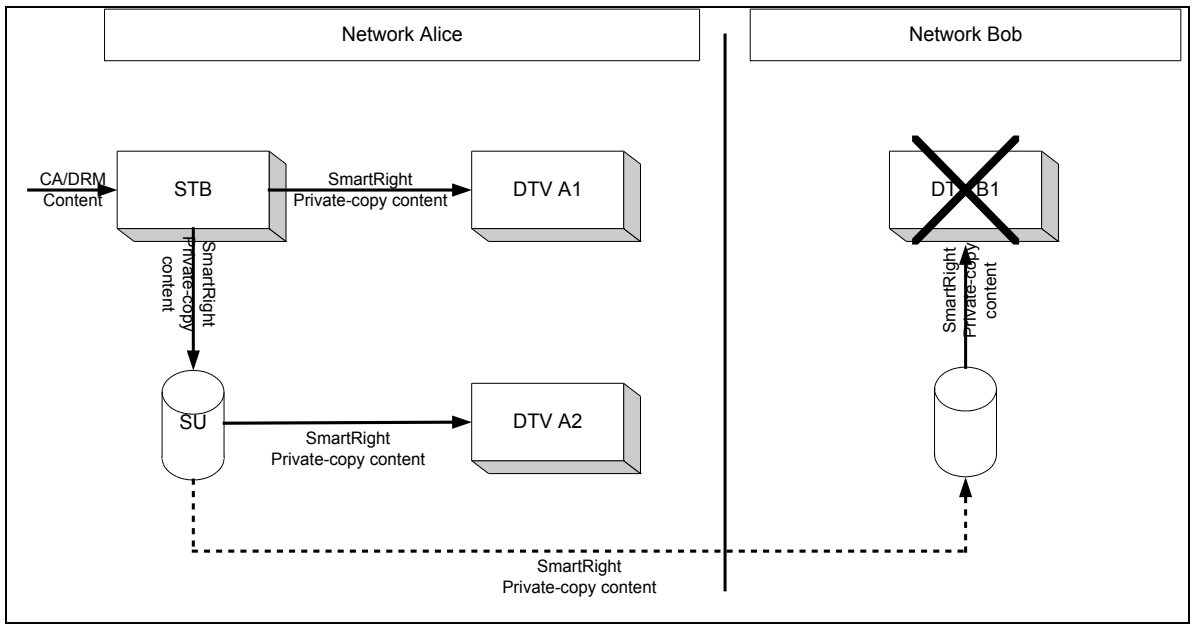

Figure 5 – Private copy usage rules

Usage rules for copy-free content are:

It is possible to render it while it is delivered at home,

It is possible to render it even if it has been stored,

It is possible to render it in a different PPN.

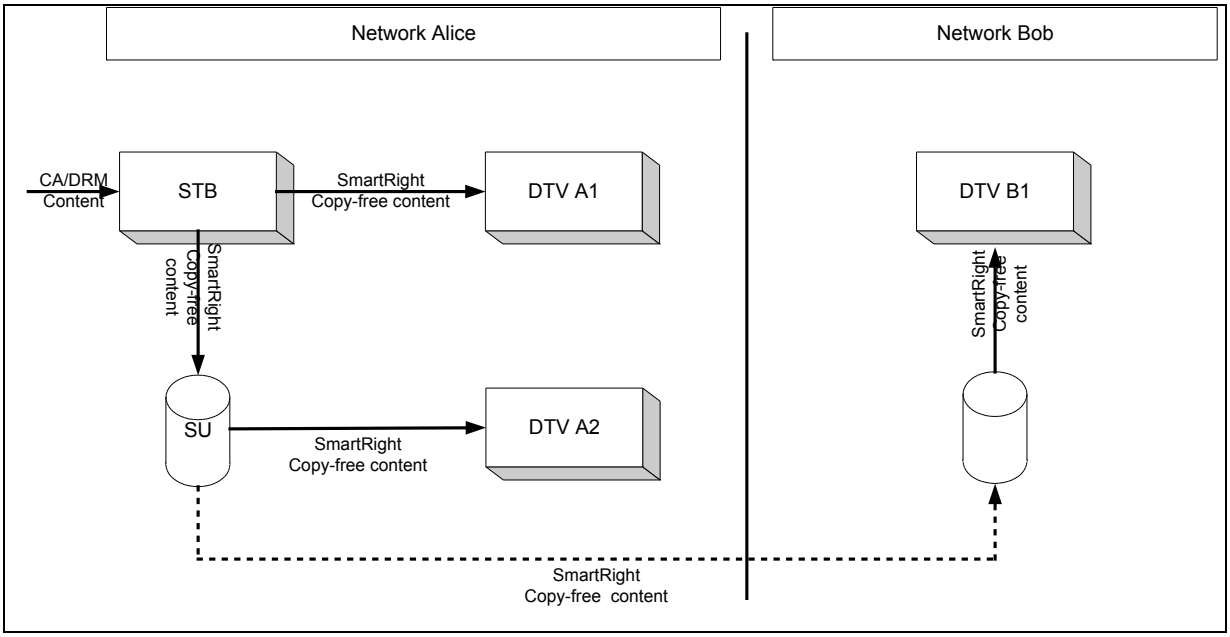

Figure 6 – Copy-Free usage rules

D. Business models on top on SmartRight

CA and DRM use view-only and private-copy to enforce their business rules. One example, the "Pay twice and keep it" model will illustrate it.

Pay twice then keep it

In this model, the broadcaster proposes at least two offers:

The offer "Basic", the customer pays for accessing content once without being able to record it,

The offer "Premium", the customer pays for accessing content program twice with being able to record at the second access time.

If the customer buys content with the offer "Basic", then the associated rules of the content in the PPN will be view-only.

If the customer buys content with the offer "Premium", then the associated rules of the content in the PPN will be view-only for the first access, and private-copy for the second access.

III. SmartRight in detail

This section details the protocols and algorithms managing the PPN. They have been designed to comply with user-friendliness and CP requirements.

User-friendliness requirements are:

No master device: the PPN management shall be distributed so that the user does not need to buy and maintain a dedicated device to run it,

Untethered clusters support: Untethered clusters belonging to one person or family (main household, summer home, …) shall belong to the same PPN,

Install and play: the installation of a device on a PPN shall be fully transparent to the user,

No remote authority: the PPN management shall not require the presence of a return channel to a remote authority,

User privacy: no personal information about the customer or content accessed by the customer shall leak.

CP requirements are:

PPN control: PPN management shall prevent devices from belonging to several PPN or shall prevent PPN interconnections. Furthermore, it shall restrict the PPN size,

Private-copy enforcement within a PPN: Private-content from a first PPN shall not be consumable in any other different PPN,

View-only enforcement within a PPN: recorded view-only cannot can not be played back,

End-to-end Protection: content shall be descrambled only when needed, i.e. in the presentation device

E. Personal Private Network management

Removable secure cards manage the PPN. All terminal cards of a same SmartRight PPN share a secret key named network key (K_N). This section describes this key management.

Transition between Virgin, Progenitor and Sterile terminal cards states:

A SmartRight terminal card may have three states. A terminal card that holds no network key (i.e. it is not yet installed on a PPN) is said Virgin. A terminal card that holds one network key (a terminal card

knows at most one network key) and is able to transmit its network key to a Virgin terminal card (during its installation on the PPN) is said Progenitor. Finally, a terminal card that holds one network key but may not transmit it to another terminal card is said Sterile.

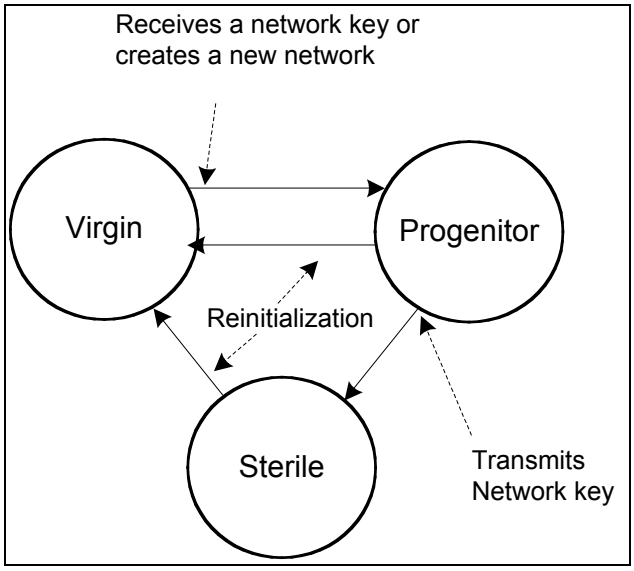

Figure 7: State transitions of terminal card

Handling of the current network size

A SmartRight PPN can have at most one Progenitor terminal card. This terminal card handles the network size. Before transmitting key to a Virgin terminal card, it decrements the current network size. After the removal of a terminal card from the PPN, it increments the current network size.

Terminal cards mode

Each terminal card "connected" to a same PPN cluster run in one of the three following modes:

operational mode: the device performs content management operations,

blocked mode: the device does not perform any content management operation,

key distribution mode: the device performs PPN management operations and may perform content management operations at the same time. Protocols and operations running during this mode are depicted in *Figure 8*.

Key distribution overview

For the sake of convenience, the terms Virgin, Progenitor and Sterile will refer respectively to Virgin terminal cards, Progenitor terminal cards and Sterile terminal cards.

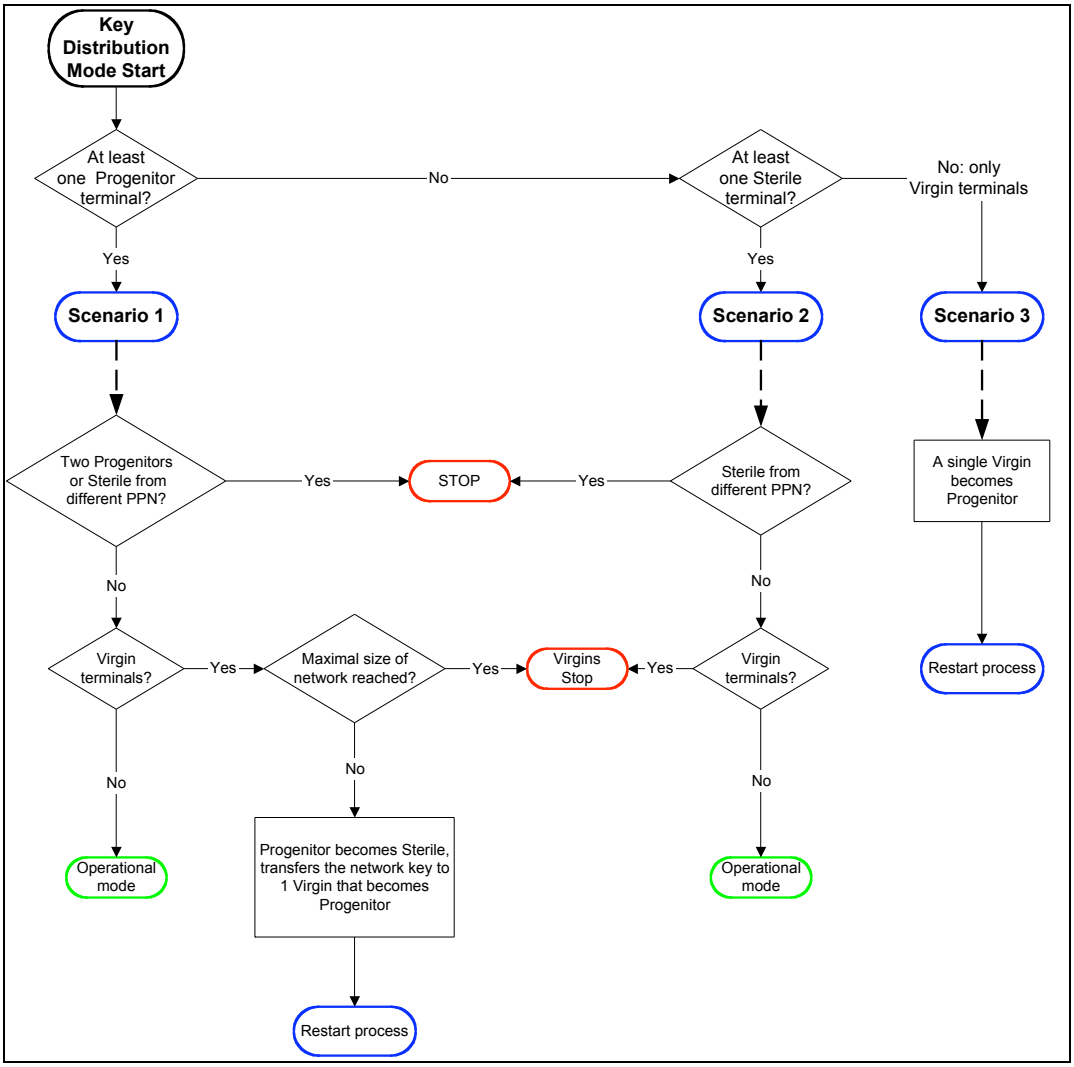

Figure 8 - key distribution protocol

Each time a device is connected to a PPN cluster or switched on or that a card is inserted in a connected device, all the cards of that PPN cluster enter the key distribution mode. They first exchange messages to identify the state of the possible other present terminal cards:

If there is at least one Progenitor, the different terminal cards check that there is only one present Progenitor and that every other Sterile (if any) belong to the same PPN as the Progenitor. If not, they enter blocked mode. Else, Sterile enter operational mode. The Progenitor checks if there are some present Virgins. If not, or if the maximal network size is reached, it enters operational mode (and Virgin, if any, enter blocked mode). If yes, the Progenitor updates the current network size, becomes Sterile and transmits the network key and the current network size to one of the Virgin (others enter blocked mode). This one

becomes Progenitor and launches a new key distribution protocol. Network key transfer is secured using usual PKI techniques based on a Root Authority.

If there is no Progenitor but at least one Sterile, all Virgins enter blocked mode and they can not be installed. The Sterile check they all belong to the same PPN. If so, they enter operational mode, else, they enter blocked mode.

If there are only Virgins, a new PPN is created after user confirmation. A Progenitor is chosen amongst the present Virgins and other Virgins enter blocked mode. The Progenitor picks at random the PPN network key and sets the current network size to the maximum network size. A new key distribution protocol is then launched.

Some additional protocols are defined as well to reinitialize Progenitor or Sterile and to enable the mobility (among the PPN terminal cards) of the Progenitor state.

Access devices and associated converter cards do not know the network key. SmartRight design actually respects the public key paradigm where the secret needs to be only in the decryption place. Access devices deliver content to the PPN. They only need to know encryption keys. Recording devices neither know the network key. They are pure bit-buckets. Neither access devices nor recording devices are in the current network size account.

F. Content management

Access devices turn proprietary-protected content into SmartRight- protected content. The access device replaces the rules embedded into the content, for instance a CA Entitlement Control Message, with a SmartRight License called LECM (Local Enforcement Copy Management). If the content is not scrambled using a regular scrambling algorithm[3], it is descrambled (if needed) and re-scrambled using Control Words generated by the converter card.

Handling of the LECM in the converter card

The converter card builds the LECM. It embeds information about the content protection (usage rules, authorization to export the content to another domain…), and the Control Words needed to descramble the content. LECM integrity is fully ensured for private-copy and view-only content. LECM

confidentiality is partially guaranteed for private-copy and view-only content. In these cases, Control Words and other secret information are encrypted while usage rules remain in the clear.

LECM is protected by a secret key called LECM key (K_L) that is randomly chosen by the converter card. This key is used to encrypt the confidential part of the LECM. The clear part of the LECM embeds as well the encryption of K_L by K_N (we will write $E\{K_N\}(K_L)$). Hence, any terminal card belonging the right PPN will be able to recover K_L since it knows K_N. It will then be able to decrypt the confidential part of the LECM. To ensure integrity, a digest of the LECM computed before the encryption of the confidential part is appended. The alteration of the clear part of the LECM is thus not possible.

Handling of the LECM Key

Converter cards obtain $E\{K_N\}(K_L)$ using public key cryptography techniques. During key distribution mode, they obtain the certificate of one terminal card from the PPN. They pick then at random K_L, encrypt it using terminal card public key and send the result to the terminal card. The latter retrieves K_L using its terminal private key. It re-encrypts then K_L using K_N and sends back the result to the converter card.. This is the way how the converter card knows $E\{K_N\}(K_L)$ without having K_N.

Handling of the LECM in the terminal card

Copy-free

For copy-free content, the Control Word is not encrypted. The content may be descrambled thus in any PPN and at any time.

Private-copy

For private-copy content, the confidential part of the LECM (encrypted by K_L) contains the Control Word while the clear part contains $E\{K_N\}(K_L)$. Thus, any terminal card from the relevant PPN will be able to recover the Control Word then the content. Any other terminal card will not be able to correctly decrypt the confidential part of LECM and subsequently the Control Word. Stored content can be played at anytime since LECM embeds all information the terminal card needs to access the Control Word. This is how SmartRight enforces private-copy usage rule.

---

[3] Triple DES in the US, DVB-CSA in Europe.

View-only

For view-only content, the converter card picks at random two additional specific keys. The first one, K_C, is used to super encrypt the Control Word. The result of that super encryption together with the second key K_A constitutes the LECM confidential part. When the terminal card decrypts the confidential part of the LECM, it recovers K_A and the super encrypted Control Word. It picks then at random a challenge and sends it to the converter card. The converter card computes a digest of that challenge using key K_A and sends back the result together with key K_C. The terminal card checks the digest and, if it is correct, recover the plain Control Word using key K_C. The converter card erases then K_A and K_C. If the user tried to store the content, when playing it back, the terminal card will choose and send a new challenge. Neither the converter card (that has already erased K_A) nor the storage unit (that never knew K_A) can compute the right digest. The terminal card will thus refuse to play the content even if it receives the correct K_C (recorded by the user). The knowledge of K_C without the network key is useless to recover the Control Word. Sending K_C in the clear does not thus open any security hole.

For more elaborated content consumption rules or business model, the converter card delays the erasure of K_A and K_C. For instance, to allow time-shifting for half an hour, the erasure will be delayed of thirty minutes. The converter card will thus be able to reply to the challenge during the allowed time-shifting window. For a play twice content, the erasure will be only made at the second play.

G. Analogue hole handling

This section presents the use of watermarking in CP systems and, in particular, its integration in SmartRight. It does not detail the watermarking technique itself.

As explained above, SmartRight enforces usage rules and manages devices in the PPN with highly secure cryptographic protocols. The weakest link of the delivery chain is now the analog link. Video has to be rendered on a display. Audio has to be spoken by loud speakers. Pirates, as dishonest users, can play content, record the resulting analogical signal, digitize them, and distribute the files. This threat is called the analog hole.

The current technical answer is watermarking. The watermark signal carries data invisibly embedded in multimedia content, which survives to the analog path. At the playback, this information may allow detection of illegally recorded contents. The problem for CP experts is the integration of the watermarking primitive in the global system architecture. The typical issues are what information the embedded bits represent, when content is watermarked, and in which device the watermark is decoded.

In past approaches (e.g. CPTWG), the embedded data describe the kind of content, i.e. the use case of its consumption. Videos are watermarked at the content source, and the hidden data are decoded at the end of the distribution chain by the user's devices. This approach brings severe drawbacks when mapped on advanced business models. For instance, recording devices have to change the watermark signal to allow further on the distinction between original materials such as 'copy once' and their copy labeled 'copy no more'. A second pitfall is that, assuming use cases of section II, servers must have two different versions of each piece of content with the information 'view only' or 'private copy' embedded in. Customers of the "Basic" offer receive the first version whereas the second version is streamed to the customers of the "Premium" offer.

The key idea underlying the integration of the watermarking primitive in the SmartRight system is that there is no need to embed information related to the kind of content, as its management is already perfectly tackled by the above-mentioned cryptographic protocols. Hence, the past approach is discarded. We indeed combine robust watermarking with content scrambling. Protected content is watermarked and scrambled. A piece of content that would be in the clear and watermarked would necessarily be illegal. Display devices check this condition before rendering digital content.

The following comparison of the associated trust model, the complexity and the resistance to malicious attacks only concerns the watermarking primitive.

In the first approach, the trust model expects that all devices of the PPN comply with good behavior. This puts security assumptions on the gateway, rendering and recording devices. Unfortunately, this is wrong when dealing with non-compliant recording devices. In our approach, detection occurs at rendering rather than at reception. Thus, the system does make no assumption on the receivers and recording devices. This reduces the number of security requirements. Therefore, the second trust model is simpler.

In the first approach, watermark's payload is meaningful, whereas, in SmartRight, the watermark has no payload. Impairing the payload modifies the behavior of the primitive. First the decoding of hidden bits requires more complexity than the detection of the presence of a watermark signal. Moreover, there is no need to implement the watermark embedding functionally in any devices. Protected content is watermarked in the studio whatever its consumption use case. The detection functionality is only implemented in the display devices. Secondly, theoretical studies have shown a trade-off between non-perceptibility, payload and robustness. Thus, reducing payload to the minimum guarantees a better resistance to any malicious attack against the watermark technology itself. For instance, asymmetric watermarking techniques [14] and the JANIS method [15] have shown higher security levels than the classical spread spectrum watermarking method.

IV. Conclusion

With the advent of digital age, copy protection becomes a major issue for all the actors of the video chain. Copy protection is necessary to protect content owner rights. But copy protection must also respect consumers rights. SmartRight system replaces the current piecemeal solutions by a unique global solution that protects the whole home network. This approach allows the introduction of two new features of a copy protection system: renewability and Personal Private Network. Renewability allows to survive inevitable hack. This should be of value for content owners and manufacturers. Personal Private Network allows content owners to tolerate consumers' private use similar to analogue age without the risk of mass uncontrolled distribution.

This paper disclosed an original key management that allows a limited number of principals to securely share a common secret key without the need of a central authority. This security scheme may be useful in secure networking.

References

[1]. Market data pages of the website http://www.riaa.org

[2]. Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms, 6th of September 1952.

[3]. Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, 26th of October 1961.

[4]. Digital Millennium Copyright Act, October 1998, available at www.loc.gov/copyright/legislation/dmca.pdf

[5]. IFPI Music Piracy Report, June 2002, available at http://www.ifpi.org/site-content/antipiracy/piracy2002.html

[6]. S.E. Siwek, Copyright Industries in the U.S. Economy: The 2002 Report, April 2002

[7]. IFPI, World Sales 2001, executive summary available at http://www.ifpi.org/site-content/statistics/worldsales.html

[8]. Agreement on Trade-related Aspects of Intellectual Property Rights (TRIP), April 1994.

[9]. WIPO Copyright Treaty and Performances and Phonograms Treaty, adopted by the Diplomatic Conference, December 1996.

[10]. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, Official Journal L 167, pp 10-19, also available at http://eucd.info/directive-2001-29-ce.pdf

[11]. T. Maillard and T. Furon, Towards Digital Rights and Exceptions Management Systems, submitted to EURASIP Journal on Applied Signal Processing.

[12]. Digital Transmission Content Protection white paper, available at http://www.dtcp.com/data/wp_spec.pdf

[13]. High-bandwidth Digital Content Protection specifications, available at http://www.digital-cp.com/data/HDCP10.pdf

[14]. T. Furon and P. Duhamel, An Asymmetric Watermarking method, IEEE trans. On Signal Processing, vol. 51, num. 4, April 2003.

[15]. T. Furon, Watermarking for copy protection, PhD. Thesis, Ecole Nationale Supérieure des Télécommunications de Paris, March 2002.

[16]. A. Eskicioglu, J. Town and E. Delp, Security of digital entertainment content from creation to consumption, Signal Processing: Image Communication, 18:237-262, 2003.

[17]. R. Anderson, Security Engineering, Willey Computer Publishing, 2001

Biographies

Jean-Pierre Andreaux

Jean-Pierre Andreaux was born in 1973. He received his DEA (First degree in a PhD program) in applied mathematics from the University of Limoges, in 1996. He is now working on cryptographic protocols and algorithms with Thomson Corporate Research in France. His research interests are primarily in the area of the copy protection and the security of home networks.

Alain Durand

Alain Durand was born in 1972. He graduated from Ecole Nationale Supérieure de Techniques Avancées (ENSTA) in 1995. He received the same year his DEA in computer science from the University of Paris VII. From 1997 to 1999, he worked in Oberthur Smart Cards as a cryptography implementer. He joined then the security laboratory of Thomson Corporate Research in France. His research interests are mainly the content protection and the secure protocols.

Teddy Furon

Teddy Furon was born in 1974. He graduated from Ecole Nationale Supérieure des Télécommunications (ENST Paris) in Digital Communication engineering in 1998 (DEA STN). He received his Ph.D. degree in 2002 in signal and images processing engineering. From 1998 to 2001, he worked in the security laboratory of THOMSON multimedia. From 2001 to 2002, he was a postdoctoral fellow at the TELE laboratory of the Université catholique de Louvain-la neuve. He is currently a researcher at the TEMICS project in Institut National de Recherche en Informatique et Automatique (INRIA). His research interests are in the area of watermarking, steganography and security analysis through signal processing techniques. He co-chaired special sessions on watermarking at IEEE MMSP 2001 workshop and at EUSIPCO 2002 conference.

Eric Diehl

Eric Diehl was born in 1962. He graduated from Ecole Nationale Supérieure d'Electronique et Radio-électricité de Grenoble (ENSERG) in 1985. In 1987, he joined LEREA, a subsidiary of

THOMSON. He worked on CDI, Pay TV, home networking, User Interface and security. Since 1999, he leads the security laboratory of THOMSON Corporate Research. The current primary interest of this team is content protection, and security of networks. He filed more than 60 patents in the fields of security, Pay TV, and User Interface.