Enhanced Security Architecture for Music Distribution on Mobile

Abdellatif Benjelloun Touimi[1], Jean-Bernard Fischer[2,⋆], Caroline Fontaine[3,⋆⋆], Christophe Giraud[4], and Michel Milhau[1]

[1] France Telecom R&D Div.,
2, avenue Pierre Marzin, 22 307 Lannion, France
{abdellatif.benjellountouimi, michel.milhau}@francetelecom.com
[2] Nagra France,
28, rue du Colonel Pierre Avia, 75 015, Paris, France
jeanbernard.fischer@nagra.fr
[3] CNRS/IRISA,
Campus de Beaulieu, 35 042 Rennes cedex, France
caroline.fontaine@irisa.fr
[4] Oberthur Card Systems,
4, allée du doyen Georges Brus, 33 600, Pessac, France
c.giraud@oberthurcs.com

Abstract. This paper presents the results of the French collaborative SDMO (Secured Diffusion of Music on mObiles) project, which aims at combining traditional security tools such as cryptography and smartcard with digital rights management and watermarking to reinforce the overall security of an audio content distribution service for mobile phones. The paper gives an overview of the system and of the security architecture and describes summarily the watermarking techniques employed.

Keywords: Content distribution, audio, mobile, digital rights management (DRM), smartcard, cryptography, watermarking, OMA DRM.

1 Introduction

The new generation of mobile networks and devices (2.5G, 3G and 4G) has opened up a promising market for multimedia content distribution services on mobile phones. However, before such services can be launched, the issues related to digital rights management (DRM) and the protection of copyrighted work have to be sorted out. Indeed, the existence of efficient compression formats for digital content, broadband capacity networks, and Peer-To-Peer file exchange have encouraged the piracy phenomena in the Internet world. The fear of duplicating this model in the mobile world is a major obstacle for the growth of a

⋆ Work done while at Oberthur Card Systems.

⋆⋆ This work was done when she was with CNRS/LIFL, Cité Scientifique, 59 655 Villeneuve d'Ascq cedex, France.

D. Gollmann, J. Meier, and A. Sabelfeld (Eds.): ESORICS 2006, LNCS 4189, pp. 97–109, 2006.

market for digital content distribution : if the different value chain actors (content providers, content retailers, network operators) cannot expect a fair income from their efforts, they will not enter this new market and the ultimate looser is the consumer.

To fight piracy, different approaches have been used to provide security for the distribution of audio content. Watermarking is one line of research that has been seen as very promising by the content industry to solve all their piracy ails. A lot of research has been done on watermarking during these past years [3]. However, if the technology, which consists of dissimulating information in a host signal, is mature, its applications in the real word are far from effective, especially for the protection against illegal copies. The failed experiment of the SDMI Forum in defining a system to protect copies based essentially on the watermarking technology has shown the limits of this approach [4].

The approach taken in the SDMO (Secured Diffusion of Music on mObile) project[1] aims at combining tightly the traditional security tools of cryptography and smartcard together with watermarking to strengthen the overall security of the audio content distribution service (streaming and download) for mobile phones. The main idea is to use watermarking as an active security tool to reinforce and broaden the scope of classical DRM. The project also takes advantage of the closed nature of the mobile environment, both at the network and the terminal sides, to build secure end-to-end architecture to protect audio content.

The paper first gives an overview of the protection system devised by the SDMO project for music distribution on mobiles. Section 2 describes the specifications of the system and the main usage scenarios. Section 3 describes the security architecture and analyzes how the astute interworking of cryptography, smartcards and watermarking produces a secure environment for content distribution.

2 SDMO System Description

2.1 SDMO Service and Requirements

Unlike the open Internet network, mobile networks are easier to control; indeed, the centralized and authoritarian control the operator has over his network allows for more possibilities for monitoring the traffic and possibly blocking data. Since some nodes handle all the data traffic, the usage of efficient tools to track illegal contents is really effective there. Moreover, the client in this context is well identified as a subscriber to the mobile service. This gives more means to prevent the consumption of illegal content at the end-user mobile phone.

The main objective of the SDMO project has been to define a secure audio content diffusion service in the controlled mobile world that reaches beyond to the open world of Internet. The problem was approached by first defining some ideal yet reasonable security requirements. In this context, the SDMO project defined two requirements (Figure 1):

[1] Funded by "Réseau National de Recherche en Télécommunication", the French National Research Network on Telecommunication.

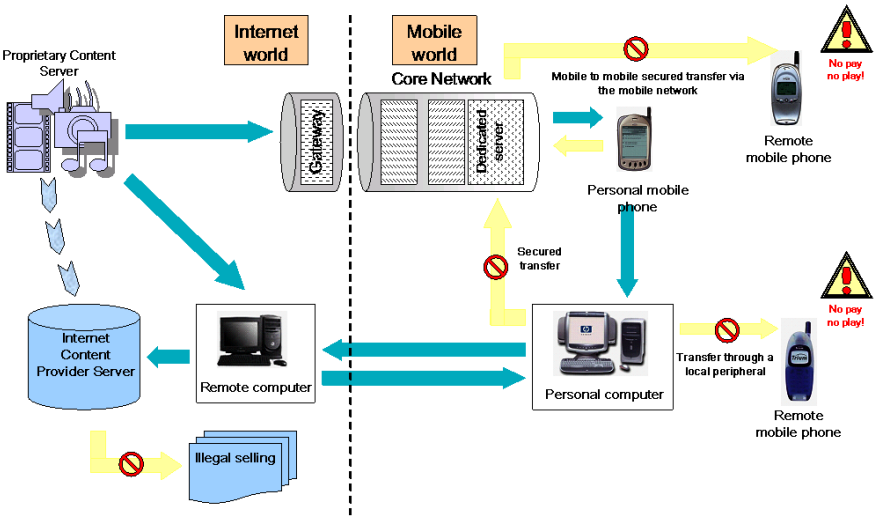

Fig. 1. Operational architecture

– *Maximizing security in the mobile domain.* This is done by prohibiting the consumption of illegal audio content on mobile devices, and the circulation thereof on the mobile operator's network. The aim here is to provide an end-to-end protection in this domain including the network and the terminal device.
– *Restricting the spread of illegal audio content in the Internet domain.* This objective is fulfilled by a constant background checking and tracing of the usage of illegal content on commercial web sites.

For a mobile operator aiming at offering and developing new services around a music catalogue, the assurance that no pirated content will circulate on his network will encourage the development of new business with the majors producing content. It is well known that the entertainment industry is very sensitive to such arguments. Checking the legality of the content during the transport through the network and in the terminal to prevent piracy is of prime importance.

To reach this purpose, SDMO intends to be a content security service provider offering the necessary tools to the actors of the content distribution value chain. In Figure 2, illustrating such a value chain, SDMO is positioned as a service for a mobile operator in agreement with an audio content provider, offering them:

– the *SDMO content preparation server*, ensuring the watermarking, compression, encryption and formatting of a music content file;
– the *SDMO Client* implemented on the mobile device allowing the playback of SDMO content and blocking illegal content;
– a *SDMO Web scrutator*;
– *SDMO Mobile network control* to stop illegal content from circulating on the mobile network.

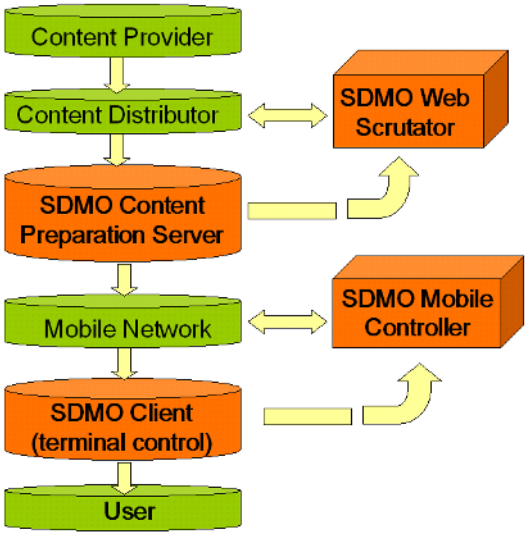

Fig. 2. The SDMO service elements and their position in the music content distribution value chain

2.2 Use Case Scenario

The project considers a classical content delivery scenario in which a mobile user buys a piece of music and acquires it from the content server. A pre-listening phase of limited duration of the audio content is possible at the same quality as the original one. Two content delivery modes are provided: download of the music file or streaming it by buying the listening rights. The usage rights are expressed and delivered in a separate licence file. The usages of the content by the user can be distinguished as follow:

- *Locally at the terminal device*: in that case, any use (play, copy, ...) is constrained by the usage rights granted in the licence;
- *Redistribution*:
  - *through the mobile network*: the user can transfer the audio content to another mobile phone. The content should not be played by the new user device before paying the corresponding rights. In the case of pirated content, it should not be played on mobile devices neither be circulating in the mobile network. A rigorous control of the content should be placed in some core network nodes.
  - *through the device peripherals (Infrared, Bluetooth, memory stick, ...)*: the mobile user can also transfer this content to and from his own personal computer via a peripheral. From there on, it becomes easy to transfer the content to other remote computers. It is also possible for this content to be placed in some web sites on Internet; for this reason, the content provider

servers should be continually examined in order to verify that they are not retailing illegal content. Another possible strategy consists in prohibiting such type of transactions by locking the device peripherals.

In the case of content exchange between two mobiles terminals, the *Mobile Network Controller* has the task of filtering illegal content.

2.3 SDMO Content Format

The audio content is compressed in MPEG-4 AAC-LC (Low Complexity profile) format at 24kbps bit rate. This audio codec is recommended by 3GPP as an audio codec for Packet Switch Services in the mobile network [1]. The resulting compressed bitstreams are encrypted using the AES-128 CBC algorithm, then put into 3GP file format for streaming or downloading. This file is associated with a licence in OMA DRM REL v2 format (based on ODRL language) indicating the usage rights and restrictions as well as the necessary decryption keys and the content identifier [8]. Such format, including the content and the licence, is called SDMO DRM format. To allow the detection of illegal content, two types of audio content are distinguished in the framework of SDMO system:

- *Controlled content*: necessarily in SDMO DRM format (*i.e.* encrypted and wrapped with SDMO DRM header + a separated licence) or another format provided by a legal distribution service.
- *Uncontrolled content*: in any format not associated with a DRM service.

With this distinction, a content can be (i) encrypted and in SDMO DRM format and hence it is controlled, (ii) or in clear and hence either free or pirated. In the latter case, the content was encrypted and the cryptographic protection has been circumvented; this is the situation where the watermark comes into play to distinguish between legal and pirated content.

3 Security

3.1 Separating Security Contexts

Analysis. The security of a mobile phone is relatively low, especially since the trend is towards more open operating systems. Mobile phones are more and more like PCs and are prone to the same ills: viruses, Trojan horses, etc. Moreover, the user might be inclined to deliberately load hacking programs in order to access protected content without payment of the licences. That is why the keys and the cryptographic algorithms are usually stored in the USIM (Universal Subscriber Identity Module), the smartcard which is in the mobile phone.

For a system relying on the super-distribution model, where the same content is always encrypted with the same key, the biggest threat is the compromise of the content key. If that occurs, it is easy to give everyone access to the content key, while still using the original ciphered content.

In order to prevent this threat, one has to provide a means to protect the content until the moment of the audio rendering. However, since the content is in compressed format, the decompression operation requires the deciphering of the content. Ideally, these two operations, deciphering and decompression, should be performed in a tamper-proof environment, the smartcard in our case. However, due to the limitation of the smartcard in terms of processing power, the file has to be (for the time being) decompressed in the mobile phone.

It is a classical paradigm, often seen in PayTV applications, to have the smartcard deliver the content keys to the decoder in order for it to decrypt the video stream. There, the keys are changed very frequently, so that intercepting the content keys by hacking a decoder and distributing them to would-be pirates is not a good solution, as by the time the key arrives at the destination, a new key is already in use. However, this model does not stand for a content that has a long lifetime, like in the distribution of musical content destined to be stored and played at will. If the key is compromised, not only is the content available in clear, but the pirates can use the legitimate content (*i.e.* encrypted content) for free and even sell the keys.

Solution. In the SDMO project, the smartcard is used to separate the security contexts of the SDMO distribution architecture and the SDMO player system. Indeed, the smartcard is the secure holder of the licence, and thus of the coveted file encryption key `ContentKey`. If the key were to be sent to the mobile phone to decrypt the file, it would be easy to hack one phone to recover the content key and then distribute it. So the simple solution is to have the smartcard decrypt the file internally.

In order to avoid the clear content to appear on the smartcard-to-mobile interface, the smartcard and the mobile phone set up a local secure channel, *i.e.* they set up a local session key which is updated from time to time, e.g. for each new musical content or at each start-up. Thus, after decrypting the content with the key `ContentKey` stored in the licence, the smartcard re-encrypts it with the local session key in order to send it to the player for further decryption, decompression and audio rendering.

Now, if a mobile phone is hacked and its keys are compromised, it does not affect the whole system and may not lead to massive piracy where content keys are distributed to be used to decrypt original content files.

A simple key establishment protocol. To allow session key establishment, every USIM card contains a common SIM-Player Authentication key `SimPlayerAuthKey` which is stored in the smartcard in a secure environment (as for `UserKey`). On the other hand, each SDMO player is personalized with an individual key `PlayerKey` and its certificate, consisting simply in the `PlayerKey` encrypted with AES using the key `SimPlayerAuthKey`.

During the first step of the session key establishment, the Player generates a 16-byte random challenge and encrypts it with its key `PlayerKey`. This value concatenated with the Player certificate is sent to the USIM. The latter is able

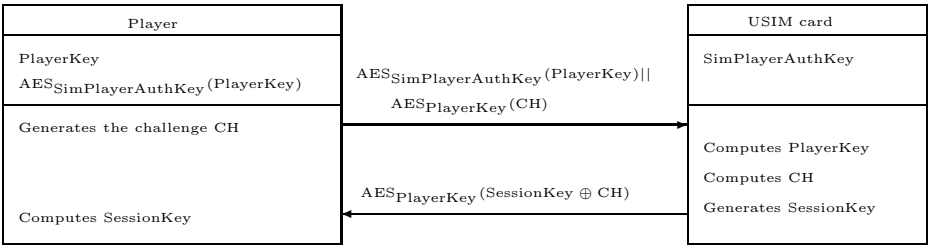

Fig. 3. The session key establishment protocol

to decrypt the Player certificate in order to recover `PlayerKey` which is used to decrypt the challenge.

Secondly the USIM generates a 16-byte session key `SessionKey` which is XORed with the challenge; the result is encrypted by using `PlayerKey` and is sent to the Player.

Finally the Player recovers the session key by decrypting with his key the value sent by the card and by XORing the resulting value with the challenge.

In order to avoid a zero session key attack which can be mounted by a hacking card by sending in the last step the encrypted challenge received at the first step, we prohibit session keys equal to zero. Figure 3 summarizes the session key establishment.

As players are not tamper-proof devices, hackers may succeed in recovering a couple (Player key, Player certificate) and propose programs that authenticate themselves to the USIM and thus gain access to the content in clear. To counteract this kind of piracy, a revocation list is maintained in the data base of the SDMO server in order to blacklist the keys from hacked Players and is send to the USIM with the licences.

The question now is: is this enough to ensure reliable mutual authentication and good session keys? In our setting, where the basic premise is that the smartcard is secure, the session key is unilaterally chosen by the smartcard. A more complex authentication, such as SSL, would be time consuming and would not take advantage of the dissymmetry in the tamper-proof character of the smartcard versus the mobile. Clearly, a pirate could set up a connection with a card by sending a random message and would thus establish a secure channel for which he does not know the key, which is useless in our case as the only thing that will happen is that he will have the content encrypted with an unknown key, meaning he gained nothing.

3.2 Adapting OMA ROAP Security Context for Smartcards

In order to protect the musical content, the first level of protection in SDMO involves a classical DRM architecture, more precisely the OMA (Open Mobile Alliance) DRM v2 architecture [6].

The goal for OMA is to provide an open system, where any device of any kind can connect to any server and negotiate a licence. In the SDMO architecture, the only device that is supposed to enter in communication with the server is the user's smartcard. This smartcard has been personalized in order to fulfil this mission, with applications and data, especially keys, that permit access to the server.

Our goal has been to make the most out of the tamper resistance of the smartcard in order to simplify the protocols and the computation power needed, yet still remaining compatible with OMA DRM v2 protocols [7] and licence formats [8].

The ROAP protocol defined by OMA DRM v2 uses a 4-pass registration protocol in order to authenticate a device and set up a security context, *i.e.* a shared session key that will be used to secure the subsequent communications. This protocol makes heavy use of public key infrastructure in order to certify the device and thus is very demanding in computation for both server and device. This is an issue when the user's device is a mobile phone, since public key cryptography demands intensive computations and is accordingly power hungry. Moreover, it is difficult to store and manipulate secret keys inside a mobile, because it is not a secure computing environment, opening the door to key compromising and account hacking. That is why the keys and cryptographic algorithms are stored in the USIM.

Looking at the ROAP protocol, it appears that once the device is registered to the server, there is no further need to run through the registration again as long as the security context is not compromised. So that if the keys are well protected, as in a smartcard, there is no need to ever register again once the first security context is established. Furthermore, there is only one security context per couple server-device, so that, in a system like SDMO where the server is unique, each smartcard has only one security context to manage. Therefore, this once-in-a-lifetime registration protocol can occur before the smartcard is issued to the user in the secure environment of the personalization process of the smartcard. The protocol can then be simplified to the extreme: the shared key is simply generated by the SDMO server and stored both in the smartcard and in the users account database on the server. From that moment on, no one will have access to the shared key outside of the SDMO licence server and the SDMO application in the smartcard.

With regards to security, one gets thus the full security of the OMA DRM v2 ROAP protocol without the hassle of public key cryptography and with the added security that no operation involving the keys is performed outside a secure environment. OMA specifies the AES as the algorithm to use in case of symmetrical encryption cryptography, so we choose the 128-bit AES in Cipher Block Chaining mode with an initial value set to zero.

Our scheme works as follows. In preparation of the system, the SDMO licence server manages a secure database of users accounts, whereas each user is issued an ID and a key. For each of the users, a smartcard is personalized with his specific data: `UserID` and `UserKey`, according to the ROAP (Right Acquisition

Object Protocol) registration protocol [7]. From there on, the user's smartcard and the SDMO licence server can communicate securely by using the shared `UserKey` with the ROAP protocol. This key cannot be compromised as it is stored in the server and in the smartcard only, both secure environments, and the key never leaves these.

Each content file is encrypted with its particular key `ContentKey` according to OMA DRM specifications [5]. Once the content is encrypted, it has no intrinsic value any more without the corresponding key; so the encrypted file can be freely distributed by any means, and in particular using super-distribution. The file is encapsulated in an OMA DRM envelope, so that the content identifier `ContentID` can be easily recovered. On the system side, the final step is to store both `ContentID` and `ContentKey` in a secure database managed by the SDMO licence server.

When a legitimate user wants to play a file, he purchases the right to do so from the SDMO licence server which downloads the corresponding licence containing the key `ContentKey` into the user's smartcard, using the ROAP protocol with the security session (based on `UserKey`) established at the smartcard personalization.

3.3 Improving Security on the Local Link with Watermarking Techniques

Let us first remark that an audio file can be transferred through any interface, like the radio (operator's network), Bluetooth or Infra-Red. This does not have any impact on the lawfulness of the download. For example, a legally purchased audio file can be temporally stored on a memory card or a computer in order to free space on the mobile phone. The crucial information at the terminal level is to know if the hardware should render the file or not. So, the right question is: "Has the use of this file *originally* been protected by SDMO?"

- If no, we assume that it is a content which can be played freely.
- If yes, we have to check that a licence has been purchased before playing.

It is difficult to find a technical solution based only on cryptographic tools to such a question, especially because of the "originally" term. Due to the fact that the decompression process has to be performed on a content in clear, cryptographic protection is of no use after this step. So that there are several means for a pirate to either recover the content in clear or to play pirated content:

- hack the keys of one player and replace the player's software by its own
- monitor the buffers of the player and read or write data on the fly
- insert a pirate software on the interface of the software modules of the player or of the audio rendering hardware

Hence, we decided to supplement the encryption based security with the embedding of a watermark signal, which remains imperceptible but present in the whole audio signal, even when it is converted to an analogical format and played.

The captured signal still contains a watermark, and the use of such a pirated content can be detected. On the content server side, the watermark is embedded before the encryption and DRM encapsulation.

In order to overcome the security hole at the decompression step, we use a watermarking technique whereby the content is identified by a specific identification number, `WmID` (*SDMO Watermark Identifier*). This number is recovered in the rendering module, at the very last moment before actual rendition of the signal.

The system works as follows. When the content file is prepared for distribution, the `WmID` is computed and inserted as a watermark in the signal, then the file is ciphered with the `ContentKey`. The `WmID` is stored in the content database along with the `ContentKey`. When a user asks for a licence, the `WmID` is added in an specific ciphered field of the licence. When the mobile starts playing a content file, the `WmID` is transmitted to the rendering module via a secure link (that has been set up in the same manner as on the smartcard-to-mobile interface). Thus, the rendering module simply extracts the watermark of the content currently playing and compares it to the content it is supposed to be playing. As long as they coincide, rendition goes on. As soon as there is a discrepancy, rendition stops independently of the player software. In order to be able to play free non-SDMO content, as long as no watermark is detected, rendition is performed.

So a normal execution works as follows. The encrypted file is delivered to the player and its licence is delivered to the USIM (file and licence can be sent separately). When the user select the content to be played, the player sends the file to the USIM. Upon receiving the header of the file, the smartcard checks the licence (key and usage rights), decrypts the content and sends a new version of it to the player, encrypted with the session key. At the same time, it sends an encrypted command containing `WmID` to the rendering module. The player decrypts the content, decompresses it and sends it to the rendering module. The hardware starts rendering the content and checks the watermark on the fly.

When a user wants to play an audio file illegally, several cases can occur.

- The USIM does not contain the licence corresponding to the content. The file will not be decrypted by the smartcard.
- The player is not a SDMO player. It will not get a session key from the USIM card and will not be able to decrypt the content.
- The file is pirated (it was originally protected by the DRM system, but the DRM protection has been stripped off and the file decrypted); however, it still contains a SDMO watermark. The player will decompress the content, but the hardware module will stop render it as soon as the watermark is detected.

If the file is not encrypted and does not contain a SDMO watermark, it is considered as a legal clear content. Thus, the player will decompress it and the hardware module will render it since no watermark is detected.

3.4 Improving Security in the Network with Watermarking Techniques

Given the insertion of the SDMO Watermark Stamp, bound to the content in a discrete way (without any additional signaling bit), an appropriate probe can check the content in the mobile network and will be able to discriminate between SDMO pirated content and non-pirated content and act in an appropriate way.

As the SDMO Watermark Stamp has to be checked at the network level, it has to be just one bit indicating that the signal is legal or not. This test must be simple, fast enough and robust.

Several cases can occur:

- If a content moving through the mobile network is encrypted (in SDMO DRM format), then no watermark check has to be performed as the content is in a protected format.
- If a content is not encrypted, a watermark check has to be performed. If the audio signal carries the SDMO Watermark Stamp, it is a SDMO pirated content that has been decrypted or "captured" somehow (e.g. in the vicinity of the digital to analogue conversion). The network should take action, for example block the pirated content, reject it or report some information to the provider for further use.
- If the content is not encrypted and does not carry the SDMO Watermark Stamp, then the content is assumed not to be pirated and can transit through the mobile network.

3.5 Specifications of the Watermarking Techniques

We considered two kinds of watermarks, both hidden in the audio files in an imperceptible and robust way: a *SDMO Watermark Stamp* and a *SDMO Watermark Identifier*. The first one can be extracted to prove that the file has been pirated and is used for network control; the second one gives an identifier which is compared during audio rendering with the one extracted from the licence in the terminal.

The main specifications of these watermarks, resulting from the network and the terminal requirements, are given in Table 1.

Table 1. SDMO watermarks properties

Specifications	SDMO Stamp	SDMO Identifier
Capacity (bit)	1	32
Duration (seconds)	15	15
Desired bit error rate	10^{-5}	10^{-5}
False alarm rate	10^{-7}	10^{-7}

Table 2. BER performances of the SDMO watermarking algorithms

	Spread Spectrum Scheme		Scalar Costa Scheme	
Attack/Compression	Condition	BER	Condition	BER
Without attacks		0		0
White Gaussian Noise	SNR = 40 dB	$4 \cdot 10^{-5}$	WNR = 39 dB	$3 \cdot 10^{-6}$
	SNR = 25 dB	$5.1 \cdot 10^{-3}$		
Level adjustment	Gain = +6 dB	$1.2 \cdot 10^{-6}$	Gain = +10 dB	$1.2 \cdot 10^{-5}$
	Gain = −6 dB	$2.5 \cdot 10^{-6}$	Gain = −10 dB	$2.3 \cdot 10^{-3}$
Cropping	Rate = 10^{-5}	$3.7 \cdot 10^{-6}$		
	Rate = 10^{-4}	$7.4 \cdot 10^{-4}$		
De-synchronization			1 to 10 sample/s	$3.17 \cdot 10^{-6}$
Compression	AAC@24 kbit/s	10^{-3}	AAC@24 kbit/s	10^{-5}

The watermark payload was set to 32 bits every 15 seconds, to prevent listening to a significant part of the audio content in case of unauthorized listening.

The watermarking detection key stored in the terminal could be compromised. The use of an asymmetric watermarking algorithm is hence recommended at the level of the terminal. However, the actual state of the art of asymmetric watermarking shows that no algorithm is robust enough. As the watermark robustness is the most important criterion, we decided to use a symmetric algorithm and maximize key's security in the terminal. Two different blind symmetric watermarking technologies have been explored and developed: algorithm based on *time domain Spread Spectrum* [2] and on *Scalar Costa Scheme* [10, 11]. As it is not the purpose of this article to detail these techniques, we will only expose their behavior. We considered robustness according to ordinary or malicious transformations (noise addition, filtering, cropping, de-synchronization, ...), and of course took into account the AAC compression step.

The performances of the two algorithms have been also evaluated in terms of BER against different attacks (see Table 2).

4 Conclusion

This paper presents the SDMO system and its specifications aiming to maximize the audio content security in the mobile domain. This objective is reached by defining an end-to-end security architecture involving both the terminal and the network in a complementary way. Such architecture uses watermarking in close relationship with cryptography, rights management and smartcard in the terminal.

The implementation of the proposed architecture has shown how flexible the SDMO specifications are when combined with an existing DRM standard like

OMA DRM v2. According to this security domain, the SDMO Content protection solution must be seen as an added value security tools.

Acknowledgements

This work was funded by the French ministry of industry through the RNRT project SDMO. The authors would like to thanks all the project participants from Laboratoire Signaux et Systèmes (LSS), Laboratoire d'Informatique Fondamentale de Lille (LIFL), France Telecom Research and Development Division, Orange, Faith Technology and Oberthur Card Systems.

References

1. 3GPP TS 26.234. "Transparent end-to-end Packet-switched Streaming Services (PSS); Protocols and codec". Release 6, 2005.
2. C. Baras, N. Moreau. "An audio Spread Spectrum data hiding system with an informed embedding strategy adapted to a Wiener filtering based structure". In Proceedings of IEEE International Conference on Multimedia and Expo, Amsterdam, July, 2005.
3. M. Barni, F. Bartolini, "Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications", Marcel Dekker Ed., February 1, 2004.
4. S. Craver, J. Stern, "Lessons learned from SDMI", Workshop on Multimedia Signal Processing, October 3-5, 2001, Cannes, France.
5. Open Mobile Alliance, Content Format, Candidate Version 2.0, OMA-TS-DRM-DCF-V2_0_20050901-C.
6. Open Mobile Alliance, DRM Architecture, Candidate Version 2.0, OMA-TS-DRM-AD-V2_0_20050908-C.
7. Open Mobile Alliance, DRM Specifications, Candidate Version 2.0, OMA-TS-DRM-DRM-V2_0_20050915-C.
8. Open Mobile Alliance, Rights Expression Language, Candidate Version 2.0, OMA-TS-DRM-DRM-V2_0_20050825-C.
9. RNRT SDMO Project, `http://www.telecom.gouv.fr/rnrt/rnrt/projets/res_02_74.htm`
10. A. Zaidi, R. Boyer, and P. Duhamel, "Audio Watermarking under Desynchronization and Additive Noise Attacks". IEEE Transactions on Signal Processing, vol. 54, no 2, February 2006, pp. 570–584.
11. A. Zaidi, J. Pablo Piantanida, and P. Duhamel, "Scalar Scheme for Multiple User Information Embedding". Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2005, Philadelphia, USA, March 17-23.