DLNA, DVB-CA and DVB-CPCM Integration for Commercial Content Management

Daniel Díaz-Sánchez, Member, IEEE, Fabio Sanvido, Davide Proserpio, and Andrés Marín, *Member*, IEEE

Abstract — *DLNA can be considered as a good candidate for sharing user-generated contents among household networked consumer electronics. However, commercial content sharing requires a high degree of device protection that DLNA does not provides. We propose a solution supporting acquisition and post acquisition content protection by the integration of DLNA with DVB Conditional Access and DVB Content Protection & Copy Management[1]. This article shows the design and implementation of a solution to improve commercial content management over DLNA.*

Index Terms — Conditional access system, content protection, copy management, home network.

I. Introduction

Networked electronics have dramatically increased their presence in home environments. Content distribution, a driving force in the market, besides connectivity it requires interoperability in several planes: media formats, media transmission, and content protection.

Digital Living Network Alliance (DLNA) deals with interoperability between networked consumer electronics. In 2009, market penetration was more than 5.000 certified DLNA. DLNA adopts UPnP AV [1] for service/content discovery and service configuration. Besides, it defines media formats and media transfer protocols, both missing in UPnP. That leads to an appealing scenario, where user-generated contents are shared among household devices.

Content protection relies on Conditional Access (CA) Systems and Digital Right Management (DRM) to govern content lifecycle. DVB-CA [2] systems protect contents from unauthorized access during *acquisition* (from provider's head-end to subscriber's equipment) until it is finally descrambled using key material from a subscriber module. The strong device protection in DVB-CA limits device flexibility, requiring the subscriber module plugged in the desired display device, so each device requires its own subscriber module. To overcome this limitation, we present a DLNA service that securely distributes DVB-CA key material to other display devices. Our service uses DLNA discovery, setup, and transport services to distribute protected DVB-CA messages to authorized display devices.

Due to its penetration, DLNA would be a good candidate to distribute not only user-generated contents and CA messages, as proposed, but also commercial contents. Unfortunately, DLNA does not support DRM. DLNA only supports link protection with DTCP-IP, which has some security problems [3]. It protects contents in transit from a source to a display device. Hence, contents might be accessed using software implementations of DLNA once acquired.

After acquisition, commercial contents must be handled by DRM and copy protection systems to prevent unauthorized distribution; thus, decrypted contents must not leave DVB-CA tamper proof hardware unless consumed through a secure interface as HDCP [4] or exported to any DRM system. DVB Content Protection & Copy Management (DVB-CPCM) [5] supports usage rules defining: where contents can be copied or moved; what hardware is required; how contents must be locally scrambled during transmission. Unlike other DRM systems, DVB-CPCM has more flexibility to interoperate between devices with different DRM systems.

In this article we also present a DLNA extension to use DVB-CPCM strong protection. This extension requires devices to implement both DLNA and CPCM. In our solution, DLNA discovers CPCM devices, sets up the service, and presents content information to the user, but leaves content protection to DVB-CPCM.

The remaining of the article is organized as follows. Section II describes content protection basis. Sections III, IV and V chart out DVB-CA, DVB-CPCM and DLNA specifications. Our proposal is presented in sections VI and VII, and the implementation details in Section VIII. Finally, section IX summarizes the conclusions.

II. Content Protection Basis

In content distribution, services are collections of video/audio contents bundle together in a package. Service protection ensures that subscribers are only able to gain access to services part of their subscription (acquisition). Content protection techniques avoid unauthorized copy, distribution, or manipulation of contents once acquired.

User equipment is part of the security infrastructure protecting contents. Device protection aims on avoiding attempts to hack devices and Denial of Service attacks. Device protection relies on cryptographic material stored in a tamper proof hardware to perform security tasks. In fact, DVB requires handling security functions in tamper proof hardware.

[1] This work has been partially supported by "Jose Castillejo" mobility grant that was given to Daniel Díaz-Sánchez and the ITACA project. Both of them are financed by Spanish Ministry of Education

Daniel Díaz-Sánchez is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: dds@it.uc3m.es).

Fabio Sanvido is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: fsanvido@it.uc3m.es).

Davide Proserpio is with the Telematic Engineering Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: dproserp@it.uc3m.es).

Andrés Marín is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: amarin@it.uc3m.es).

Manuscript received January 15, 2010

Devices must also be able to export contents securely to other devices.

The aforementioned security topics are grouped together in three major functional groups with some overlap among them: Conditional Access Systems, Digital Rights Management, and Copy Protection. However, the practical realization of those security functions leads to two different scenarios known as acquisition and post-acquisition.

DVB-CA Systems [2], Marlin IPTV [6], and OMA BCAST [7] are security technologies governing acquisition. DVB-CA requires a descrambler, a Conditional Access Module (CAM), and a smart card in every display device. OMA BCAST requires a smart card in some profiles. Others, as Marlin, do not make any assumption about the hardware.

After contents are acquired (post-acquisition), they must remain within the bounds of the contract until the content lifecycle ends. Contracts are enforced employing DRM and Copy Protection techniques as Advanced Access Content System (BluRay). These specifications dictate how to edit, convert to other format, redistribute, and store legally acquired contents. The foundations for any copy protection system are rights expression languages. These languages have evolved from the simplest expression of copy control indicator (CCI) fields, to the complexity of MPEG21 Rights Expression Language (REL) [8], Usage State Information (USI) described in DVB-CPCM [9], Octopus DRM [10] used in Marlin (Open IPTV forum) or OMA DRM.

III. DVB Conditional Access

DVB-CA defines a holistic approach to service protection involving content providers, distribution networks, and consumer electronics manufacturers. It standardizes content format, metadata, and protection procedures for acquisition. DVB-CA specifications have been widely adopted during the last decades. Moreover, IPTV could reuse DVB-CA seizing already deployed head-ends and consumer's hardware.

DVB-CA systems are defined across several specifications as Conditional Access, Common Scrambling Algorithm [2], Common Interface, and Common Interface Plus (CI+) [11][12]. In this section, we describe the architecture, interfaces and content acquisition process.

A. Devices architecture and interfaces

DVB-CA compliant devices need a MPEG-2 demultiplexer, CA hardware, TVs require a built-in display, and set-top boxes (STBs) require an export module that sends the content to an external display. CA hardware comprises a descrambler, a CAM, and a subscriber module. CAM and descrambler communicate using DVB-CI or CI+, as depicted in Figure 1.

A CAM implements the key distribution protocol for a given CA system provider and uses a subscriber module (typically a smart card) to handle user entitlements. The Common Interface Plus, CI+, defines how to use the descrambler's public key to open a Secure Authenticated Channel (SaC) between the CAM and the descrambler for delivering key material. As the user might infer, the CAM must be collocated with the descrambler so, in order to use a different visualization device, it is necessary to move the CAM from one device to another. Fortunately, some works, which are complemented in this article, propose a protocol to share the CAM with several descramblers through IP [13].

DVB uses MPEG-2 Transport Stream (MPEG-2 TS) for media format. MPEG-2 TS contains, besides audio and video, some data tables called Program Specific Information (PSI). These tables transport conditional access information as Entitlement Management Messages (EMMs) and Entitlement Control Messages (ECMs).

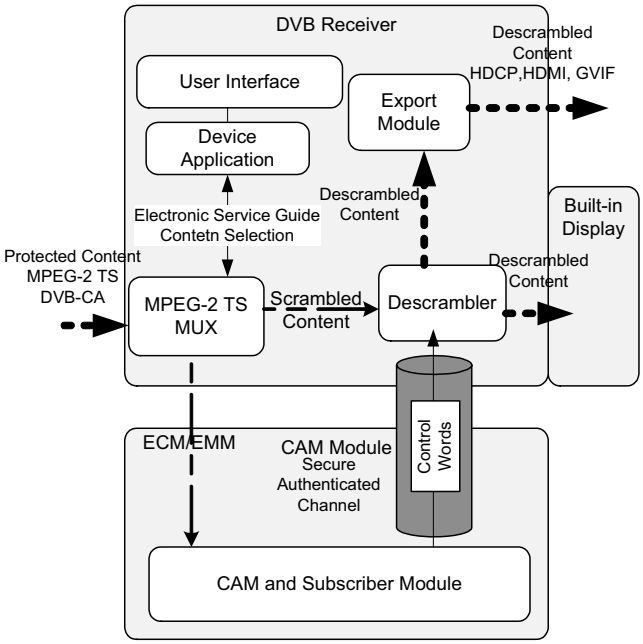

Fig. 1. DVB-CA device. The Secure Authenticated Channel (SaC) communicates the CAM and the descrambler to securely deliver Control Words. The content, once decrypted, is transferred to a built-in display (part of the device) or protected with a link protection protocol.

B. Content Acquisition

End user's hardware manages content acquisition. DVB relies on DVB SimultCrypt, which separates content encryption, content delivery and key distribution.

The provider's head-end scrambles audio and video with a hardware-generated unpredictable key called Control Word (CW) that changes frequently. DVB traditionally used Common Scrambling Algorithm (CSA) [2] for scrambling. However, new algorithms based on AES, are under development as ATIS CSA or DVB-CSAv3.

DVB does not standardize the key distribution system except for the MPEG-2 tables used for transporting that information and the descrambler-CAM interface. CWs are usually encrypted with a Service key (SK) and distributed using ECMs. Providers send EMMs containing the SK and DRM information, encrypted with a customer key CK. Hence, ECMs are common to all subscribers for the same service, but EMMs are specific to a subscriber. The service provider distributes subscription modules, smart cards or other tamper-proof devices, to decrypt EMMs and ECMs. When a user

selects a service, the demultiplexer extracts ECMs and EMMs from MEPG-2 and delivers them to the CAM module. The CAM processes them, supported by the subscriber module, and extracts CWs, conveyed to the descrambler for content decryption over a Secure Authenticated Channel (SaC).

To establish a SaC between the descrambler and the CAM for the first time, the smart card gets the descrambler serial number and sends it to the provider. Then, the provider checks the validity using known manufacturer lists. If the descrambler is trusted, the provider sends the public key of the descrambler to the card. Finally, the card generates a session key, and sends it to the descrambler encrypted with the descrambler's public key to establish a SaC channel (ElGamal authenticated key agreement).

DVB-CA scope is limited to content acquisition. During the entire acquisition process, decrypted contents never go out of tamper proof hardware. Thus, the decryption hardware, if not integrated in the visualization device, should export contents through a High-Bandwidth Digital Content Protection (HDCP, HDMI, GVIF) or a similar secure interface. Moreover, DVB defines also some specifications, as DVB-CPCM [5], to allow contents to moved, copied or exported.

IV. DVB Copy Protection Copy Management

DVB-CPCM is a post-acquisition content protection system that aims at content protection and copy management of commercial digital content in home networks. CPCM manages content from acquisition until final consumption or export according to the particular usage rules of that content. This section describes the internals of DVB-CPCM, its interfaces, the acquisition and the post-acquisition processes.

A. Devices, content protection and interfaces

CPCM devices within a household might optionally constitute the household's authorized domain (AD) that limits the content protection boundaries of a single household. Nonetheless, AD support is not mandatory.

Digital contents enter the CPCM system through an *acquisition point* to become CPCP contents. Within the CPCM system, contents can be moved, processed, stored, and copied according content usage rules. CPCM contents leave the CPCM system once consumed or exported to other systems. CPCM defines five functional entities known as acquisition point, storage entity, processing entity, consumption point, and export point [5]. CPCM devices can implement them. Figure 2 shows the conceptual diagram and functional entities of DVB-CPCM.

The CPCM functionality is encapsulated in the CPCM Instance that is the part of the CPCM device that enables interoperability between different implementations of CPCM functionality. The functionality inside a CPCM instance is split into three parts: Security Control, Content Handling, and Authorized Domain Management. Not all the functionality is mandatory for a CPCM device. Thus, the actual CPCM Instance to be used for handling a given content must conform to the Compliance & Robustness rules specified by the Content License. Unlike other DRM systems, CPCM aims on interoperate with existing DRM systems, for that reason, it supports a set of Compliance & Robustness (C&R) regimes instead of enforcing the same conditions in every device. Figure 3 depicts the CPCM device internals.

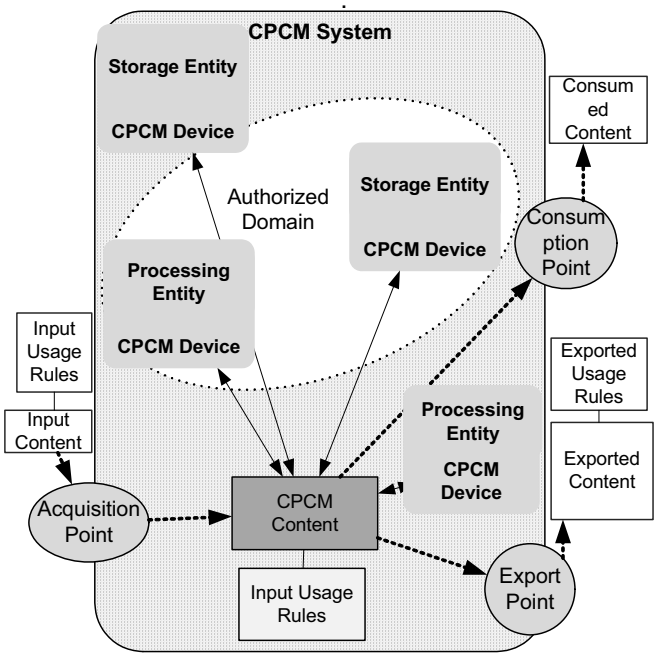

Fig. 2. CPCM functional entities and conceptual diagram. Contents become CPCM contents through and acquisition point, are exchanged among devices, and leave the system either exported or consumed.

The Security Control is responsible of storing and maintaining CPCM secret data in the host device such as: CPCM Instance certificates for establishing trust with other devices; Device Secrets to protect Content Licenses created or maintained by the CPCM Instance; and the AD Secret to protect content that is bound to an AD.

The Security Control interprets licenses to check if a device adheres to a C&R regime and to encrypt or decrypt contents. Therefore, licences must be locally encrypted and exchanged over secure channels, especially if they contain keys for decrypting content.

The Security Control handles trust management. CPCM devices establish trust by exchanging their CPCM Instance Certificates, verifying them, and checking a revocation list. Once two devices have a trust relation, they can exchange contents, if permitted by the license, by deriving a Secure Authenticated Channel (SaC) between the two CPCM instances. Unlike DVB-CA, the authentication in CPCM is mutual. The SaC key is derived with a certificate-based authenticated key agreement protocol.

The Security Control is also in charge of the Proximity Control Communications used to find out whether two CPCM devices are Local with respect to each other. The Security Control exchanges content scrambling/descrambling keys, protected content licenses and any other control information with the Content Handling.

The Content Handling part of the CPCM device includes CPCM scrambling and descrambling tools in order to satisfy the commercial content's license. It also handles exchange to/from other Content Protection Systems.

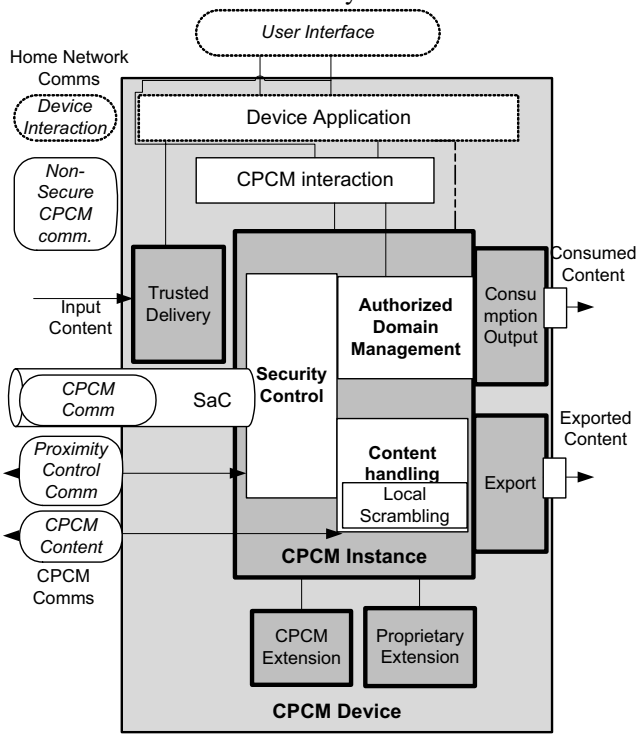

Fig. 3. CPCM Device, CPCM Instance and interfaces.

The User Interface definition is out of the scope of CPCM specifications. This interface conveys to the user information about, for instance, the authorized usage of content or an explanation of why the system prevents the user to perform an action. Regarding the device interaction, CPCM states that this interface can be any home networking protocol with a bidirectional signalling mechanism but its definition is also out of the scope of CPCM. For that reason, part of this interface is stipulated in [14] to be UPnP compliant. This interface copes with content discovery, selection, and control.

The CPCM Interaction is also out of the scope of CPCM specifications and handled by the Non-Secure CPCM Communications interface. This interface is responsible of obtaining information about the authorized usage of any content that can be accessed by the device and to request access to a CPCM contents under the control of the device.

Regarding content transmission, CPCM describes how to create a SaC for License delivery and how to use Local Scrambler to protect contents prior delivery. Nevertheless, CPCM first phase specifications addresses CPCM for content encoded and transported by linear transport systems in accordance with [15], which does not support the transmission over IP protocols, although a later phases will support transmission over RTP as stated in [16].

B. Content Acquisition

Input content enters the system from a trusted source incorporated to the CPCM system at an Acquisition Point. The trust between the source and the CPCM Instance is the result of the mutual approval under the control of C&R regime. Moreover, it can be achieved via a CPCM extension that mutually establishes trust with the CPCM instance. CPCM specifications describe several Acquisition Points as a DVB-CA system collocated at the device. In this case, the content license is extracted from EMMs and ECMs, the content is descrambled and introduced in the system, locally scrambled, for post-acquisition management.

CPCM is designed to be interoperable with other DRM systems. It can accept contents from other DRM systems whenever they are able to generate a CPCM compliant content license from the original content. Unlike other DRM systems, it also countenances several C&R regimes instead of tying every device to the same set of conditions. This freedom benefits interoperability among DRM systems. Moreover, CPCM can export contents to other DRM systems. Unfortunately, DVB has defined no C&R regime until today, thus it is not possible to evaluate interoperability in detail.

C. Post Acquisition

When a CPCM device (client) requests contents from other CPCM device (host), the server checks the AD credentials, if both devices are part of an AD, so they already have a trust relation; or establish trust by exchanging CPCM Instances certificates. Then, the host checks the Content License to find out if the client device complies with the C&R regime. If the content can be delivered to the client, the host sends the License to the client over the SaC and starts delivering the content to the client. The client extracts descrambling information from the license and descrambles the content for consumption, storage, or processing.

V. DIGITAL LIVING NETWORK ALLIANCE

The objective of DLNA is to achieve interoperability between devices using industry standards. From users' perspective, DLNA provides the means to move digital contents among devices through the home network without complex configuration wizards. DLNA selected TCP-IP for network connectivity and UPnP, HTTP, HTML, XML and SOAP for device discovery, device and service description, device control and presentation. DLNA does not characterize devices enforcing the use of dedicated hardware as DVB-CA or DVB-CPCM do. It just defines devices by the role they play in the consumer environment.

A. Devices and Interfaces

DLNA adopts UPnP fundamental device model [1]. These specifications define three functional components: Media Server (MS), Media Renderer (MR), and Control Point (CP). A device might implement several functional components, for instance, a DLNA media player combines CP and MR functionalities. Devices in DLNA expose services that provide actions. These services can be controlled via state variables or events. Control Points discover and control other devices on

the network; they coordinate operations among devices that yield to the desired result.

UPnP AV facilitates the discovery and configuration but it does not define how contents are transferred. DLNA goes beyond UPnP defining mandatory Media Formats, as MPEG-2 for video or JPEG for pictures, and Media Transport protocols as HTTP or RTP. DLNA certified devices must support the mandatory formats. However, other media formats might be supported to the discretion of the manufacturer.

Regarding Media Management, DLNA incorporates UPnP forum AV and printing technology as the basis of DLNA Media Management. The services provided by this technology are Content Directory, Connection Manager, AV Transport, and Rendering Control. Content Directory is a mechanism for every content server to advertise its contents creating a uniform directory. Connection Manager determinates how content can be transferred between two devices matching capabilities between servers and renderer devices. The AV Transport service enables control over the playback of video and audio streams. The rendering control service is intended to provide control points with the ability to query and/or adjust any remote attribute. AV transport uses protocols over TCP-IP for transferring media between devices, however, other out of band transfer protocols or interfaces can be used. In fact, DLNA adopts HTTP as the mandatory Media Transport protocol but supports RTP.

B. Link Protection

The efforts of DLNA on content protection focus on link protection technologies that protect the transfer from a source device such as a MS to a display or MR. DLNA devices must implement DTCP-IP [3] for link protection.

DTCP specifications define a cryptographic protocol to protect sensitive contents from illegal coping, intercepting or tampering as it traverse transmission links such as IEEE 1394 or any other high performance digital bus. DTCP-IP is a specific adaptation of DTCP for IP. DTCP-IP embeds in the content stream a Copy Control Information (CCI), which is a two-byte flag that specify how contents can be duplicated.

In DTCP-IP, devices first authenticate each other and derive a key. Then, content flow is encrypted using M6 baseline cipher with a 56-bit key. DTCP over IP employs stronger ciphers and full authentication. Full Authentication relies on Elliptic Curve Digital Signature Algorithm (EC-DSA) for signing and verification. It also employs the Elliptic Curve Diffie-Hellman (EC-DH) key exchange algorithm to generate a shared authentication key. However, DTCP-IP is vulnerable to some well-documented attacks even if digital signatures and DH are used. In [17] four different common attacks are taken into account to analyze DTCP robustness. Considering the existence of one malicious device that can intercept, modify and insert messages in the communication between two legitimate devices, three of these attacks, reflection, Winer, and Lowe's attack, have led to an authentication failure that make impossible the legitimate transmission. Moreover, the last attack identifies a possible identity mismatching. In this attack a malice device with a valid certificate can use a variation of Lowe's attack for retransmit sensitive content stream from the source device A to a third unauthorized device B. Apart from this receiver mismatch attack, a replacement of the sender's identity is also possible.

C. Content Acquisition and Post Acquisition

DLNA does not support the concept of content acquisition as CPCM does. Unlike CPCM, that requires the client device to comply with a C&R regime, DLNA requires only the media format and transport to be supported by both devices. DLNA does not define a DRM system at this moment. The only kind of protection offered by DLNA is link protection.

VI. DLNA EXTENSION FOR DVB-CA KEY DELIVERY

Nowadays, display devices are commonly equipped with a descrambler and a CAM. Moreover, some of them are equipped with network interfaces and DLNA support. Devices with DLNA and DVB-CA support can access user-generated contents offered by other household devices through the home network. However, they require a CAM to be plugged in the slot for acquiring commercial contents even if there is a CAM already plugged in household device they can communicate with.

In this section, we describe our DLNA extension to deliver DVB-CA Control Words to other descrambler-equipped devices. In this way, display devices can acquire commercial contents even if the CAM is located in other device. Our work is based on the Home Key Management System (HKMS) depicted in [13]. This solution defines security mechanisms to register the CAM sharing service with the provider, to register additional descramblers and to establish a SaC over the home network. However, the system setup might be difficult to handle preventing it to be widely adopted. For that reason, we designed and developed a solution that makes the HKMS interoperable with DLNA discovery and media transport services.

A. The Home Key Management System

The HKMS relies on a Secure Channel Proxy (SCP), an advanced descrambler that distributes key material to several descramblers over the home network. The SCP logic can be implemented in software but a descrambler is needed for security operations. Moreover, the descrambler must be able to establish several Secure Authenticated Channels in parallel.

The HKMS requires the SCP to be authenticated by the provider. Moreover, every additional descrambler must be authenticated when used for the first time. This is necessary to avoid a rogue SCP to redirect key material to unauthorized descramblers.

To register the SCP with a provider, the Subscriber Module, typically a smart card located in the CAM, gets the serial number of the descrambler that will act as SCP. The smart card sends the serial number to the provider protected with a keyed Message Authentication Code (MAC), a nonce and a

time stamp to prevent reply attacks. The provider checks the validity of the descrambler acting as SCP, computes a secure response (RES), and sends it to the smart card. RES contains a session key, called $K_{SCP,}$ and a nonce encrypted with both the card key and the SCP public key. To prevent security problems, the nonce is different for the card and the SCP. The provider sends also a DRM object governing the service, and it might require a payment for the service. The card sends the encrypted K_{SCP} to the SCP. If the descrambler and the card are legitimate, they would be able to decrypt the nonce and the K_{SCP}. After that, the nonces are sent back to the provider, protected with a MAC, for verification. The K_{SCP} will be used to establish a SaC between the CAM and the SCP.

Registering a new display device to consume CWs from the SCP requires the new descrambler to create a SaC channel with the SCP. The SCP sends the serial number of the new descrambler to the card. The card then sends the serial number to the provider for verification. If it is a valid descrambler, the provider returns its public key. Then the card sends the public key to the SCP that derives a key and establishes a secure channel with the descrambler.

When the service is active, the smart card uses the DRM object received during the SCP setup to determinate, for instance, the validity period and the maximum number of simultaneous emissions.

B. Architecture

The HKMS gateway might be either a Set Top Box (STB) or any other device equipped with a descrambler. The gateway has access to commercial contents using DVB-CA. It has a network interface, a CAM, and a descrambler that acts as the SCP. Figure 4 shows the architecture of the HKMS gateway. The gateway must implement a DLNA Digital Media Server (DMS) to send SaC messages and, optionally, scrambled content to client devices.

Clients are DLNA certified display devices (equipped with a descrambler). Figure 5 shows the architecture of the display device. To use the HKMS, every display device must implement a DLNA Digital Media Controller (DMC) and a Media Rendered (DMR). .

C. The Digital Media Server

The gateway implements a DLNA Digital Media Server. It advertises an UPnP device description that includes the model name, serial number and a URL for presentation.

Once the SCP has been registered with the provider, the Device Application publishes a service for client descrambler setup. This service description contains two commands, *init* and *getEncryptedSaCKey*, both require the descrambler's serial number as parameter. The *init* command triggers the HKMS additional descrambler registration with the SCP. The *init* command returns an operation result that can be "success" or an error code. After a successful *init* command, the display device can invoke the *getEncryptedSaCKey* command to receive the SaC key encrypted with descrambler's private key.

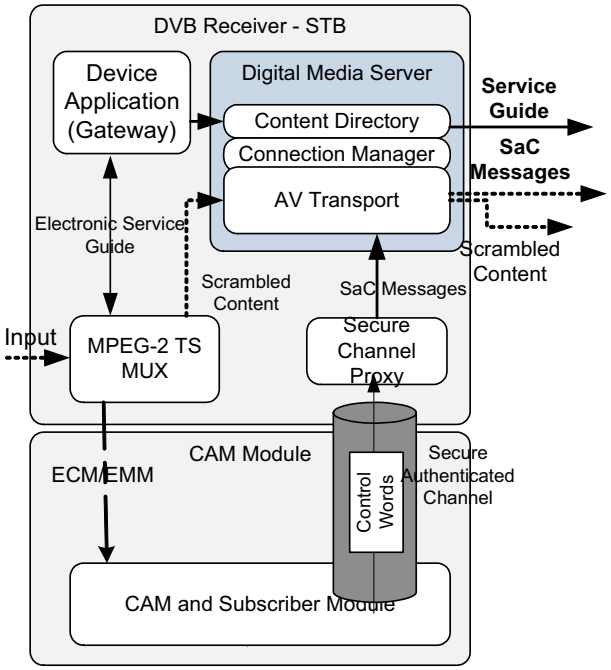

Fig. 4. Conditional Access Module sharing over DLNA. The figure shows a STB implementing a DLNA DMS that transport Secure Authenticated Channel Messages over DLNA to deliver keys to a remote descrambler.

The Device Application receives the Electronic Program Guide (EPG) from the MPEG-2 demultiplexer and builds an UPnP service description for every DVB service in the EPG. For every DVB service, the Device Application adds a service type, a URL for downloading the service description, a URL for control and a URL for eventing. We used a vendor specific service type (DVBSaCSetup) to avoid collisions with other services.

The service description for each DVB service contains an identifier extracted from DVB PSI tables and two commands: *start* and *stop*. The descrambler's serial number must be sent as a parameter when invoking any of these commands. The service type for the service description is also vendor specific (*DVBSacSvc*). When a display device invokes the start command, the DMS selects the DVB service through the Device Application, which implements Gateway functionality. The demultiplexer sends ECMs for the selected service to the SCP for decryption.

The Device Application instructs the SCP to encrypt control words for the appropriate descrambler according to the serial number. The *start* command returns "success" or an error code. If the service has been successfully selected, CWs are encrypted as if they were transmitted over a SaC, but published as event variables. Thus, in order to receive CWs, the Digital Media Controller at the display device must subscribe to the state variable using the UPnP General Event Notification Architecture (GENA). The *stop* command deselects the service and removes the state variable when invoked.

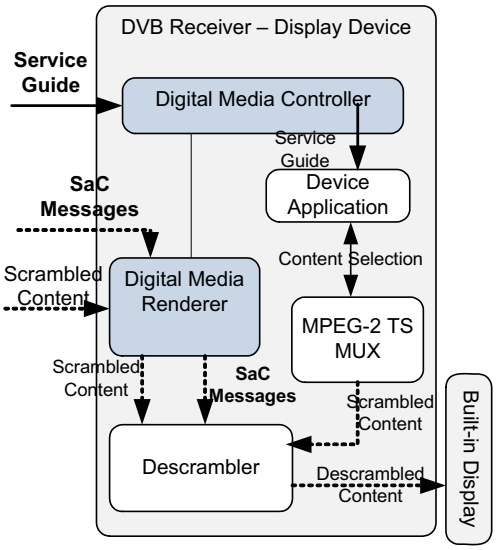

Fig. 5. The figure shows the architecture of a display device that can receive DVB-CA key material over DLNA.

If the display device has no access to the scrambled content, it can request not only CWs, but also scrambled content to the STB. The media type used for scrambled content delivery is MPEG-2 that is compliant with DLNA. Our software supports both HTTP and RTP for scrambled AV Transport.

D. The Digital Media Controller and Renderer

Display devices willing to access to commercial content key streams from the Gateway must implement a DLNA Digital Media Controller (DMC) and a Digital Media Rendered (DMR). The DMC finds content offered by the DMS and matches it to the rendering capabilities of the DMR.

When a user selects a protected content, the Device Application looks for an appropriate CAM in the device. If the CAM is absent, the Device Application requests discovered services to the DMR. The Device Application searches for a DLNA service with the same DVB service identifier. Figure 6 outlines the message exchange.

If the display device has access to the scrambled content, the DMR invokes the DVBSaCSvc *init* command, subscribes to the state variable that contains SaC messages, and pushes CWs to the Device Application upon reception. The Device Application tunes the appropriate channel and acts as a virtual CAM feeding the descrambler with the appropriate CWs.

If the display device has no access to the scrambled content, the DMC passes the control URL of the DVBSaCSvc to the DMR with an *AVT::SetTransportURI* message. The DMR will establish a content stream flow from the DMS upon reception of an *AVT::Play* message in order to receive scrambled content from the Gateway. Finally, the DMR sends the scrambled content to the descrambler while the Device Application sends CWs to the descrambler.

VII. DLNA Extension for DVB-CPCM Interworking

DLNA provides an easy and cost-effective solution to share contents among devices through the home network. As mentioned before, DLNA provides optional protection during content delivery using DTCP-IP. DLNA would be appropriate to share commercial contents over the home network due to its penetration; however, the link protection of DLNA is not enough to ensure commercial content protection. DLNA does not prevent contents from being tampered once acquired. The reason is that DLNA does not make any assumption about the target device. Thus, software devices can be used to gain unauthorized access to protected commercial content.

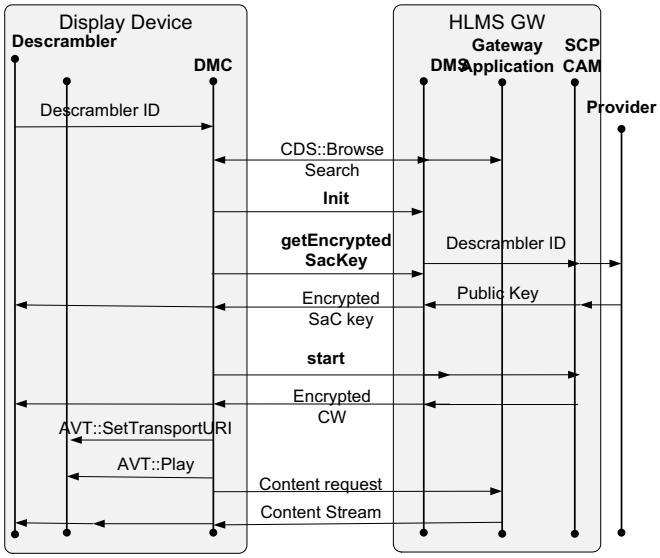

Fig. 6. The figure shows a possible message for descrambler setup and exchange during a session.

Unlike DLNA, CPCM defines a robust system to protect and manage contents with a comprehensive license language, several robustness regimes, secure device architecture, and strong content protection that requires tamper proof hardware. However, CPCM relies on plain UPnP for discovery and service setup leaving user interaction, device interaction and media transport protocols poorly defined. CPCM first phase specifications does not support the transmission over IP protocols, although a later phase will support transmission over RTP as stated in [16].

DLNA and DVB-CPCM can complement each other to bring a better solution for commercial content sharing over the home network. DVB-CPCM can take benefit from the DLNA device interoperability, in the service interaction plane, and its market penetration, whereas DLNA can take profit of DVB-CPCM device protection and its interoperability between DRM systems.

In this section, we describe our solution for DLNA and DVB-CPCM integration starting with an overview of the architecture followed by a detailed description of every module.

A. Architecture

Figure 7 charts out the architecture of a device with DLNA and DVB-CPCM functionality. The device implements a Digital Media Server (DMS), a Digital Media Controller (DMC), and a Digital Media Renderer (DMR). The device coordinates the DLNA modules through a CPCM proprietary extension called *DLNA Manager Extension*.

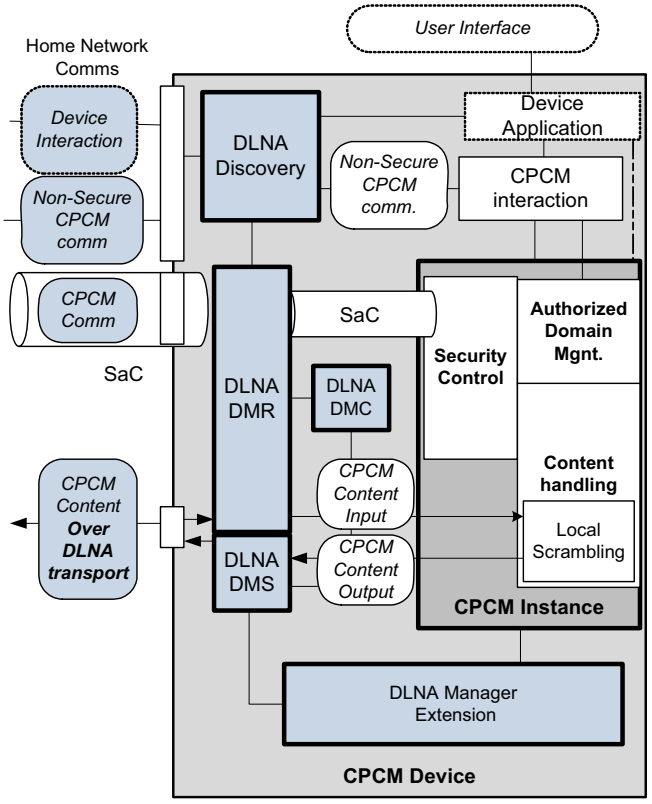

Fig. 7. DLNA DVB-CPCM device simplified architecture. The device implements a DMC, a DMR and a DMS. CPCM communications are carried over DLAN AV transport or as evented variables.

The sole objective of the *DLNA Manager Extension* is to coordinate interactions between CPCM instances and DLNA components. This extension provides discovery services, device interaction, presentation, and encapsulation for moving locally scrambled contents over DLNA AV transport protocols. The *DLNA Manager Extension* has no access to CPCM contents since they are handled entirely by the CPCM instance, it just provides service discovery and transport services to CPCM.

B. DLNA Modules

The *DLNA Manager Extension* controls the interaction between the CPCM Instance and the DLNA modules. It provides service descriptions for Device Interaction, CPCM Communications, and for each CPCM content item available at the CPCM Instance.

The DLNA Discovery module handles service discovery on behalf of the DLNA modules. It advertises services offered by the CPCM device and discovers services offered by other devices. The services offered by a DLNA CPCM device are *Authorized Domain Management*, *Trust Establishment*, *Secure Authenticated Channel*, and *Content Delivery*.

The *Authorized Domain Management* (ADM) is handled by the DMS and the DMR. It is in charge of providing commands to join an existing Authorized Domain (AD), to create a new AD, to leave an AD and to discover new ADs. The DMS receives invocations from devices to perform ADM operations, checks the commands for errors or missing parameters, extracts information from the SOAP call, reformat the command adequately for CPCM and delivers it to Authorized Domain Management module of the CPCM instance through the CPCM Interaction interface. Thus, the DMS performs adaptation from DLNA to CPCM.

The *Trust Establishment* service is managed by the Security Control. The DMS receives invocations from other devices and provides transport and adaptation. The aim of this service is to assist CPCM during the exchange of CPCM instance certificates to derive a trust association.

The *Secure Authenticated Channel* service provides transport services for establishing a SaC and exchanging SaC messages between two trusted devices. Security Control manages the service and the DMC provides transport and adaptation between DLNA and CPCM. The transport mechanism used to deliver SaC messages depends on how frequently the Local Scrambling Algorithm changes the CW. SaC messages can be delivered as events or directly through an AV transport channel. Moreover, this channel might be used to securely deliver content licenses.

The *Content Delivery* service is managed by the Content Handling module and involves the DMR, the DMS, and the DMC. If the CPCM device acts as the source, it advertises its contents through the DLNA Discovery module. The service description for a CPCM content item comprises, among other DLNA information, the required CPCM Compliance & Robustness regime. If the client device complies with the required regime, the Content Handling module sends content to the client device while the security control delivers SaC messages to the client device using an AV transport protocol or event variables. The DLNA Manager captures the protected content and sends it to the DLNA DMS module that encapsulates it over an adequate AV transport protocol.

If the CPCM device acts a client, it discovers contents and generates an appropriate presentation. When a user selects a content, the DMC coordinates the DMS at the server device and the DMR at the client device. If both devices have a trust relation, the DMR invokes the *Secure Authenticated Channel* service to negotiate the content delivery. The DMR at the client device communicates with the DMS to find out whether the device meets the Compliance & Robustness regime demanded by the license or not. If the client device is eligible to receive the content, the DMC invokes the DMS of the server device to receive the content license. After that, the DMC requests the content to the DMS and redirects it to the DMR for rendering. The DMR unwraps CPCM contents transported using DLNA media transport and sends them to the CPCM Instance for either processing, storage or consumption.

VIII. PROTOTYPE IMPLEMENTATION

Every module of our solution has been developed in software. We developed a display device using a modified VideoLan implementation. The display device, which mimics a TV, has an input module to acquire contents carried over MPEG-2 Transport Streams, a Common Interface Plus (CI+)

module and a virtual CAM. This display device was extended using "uShare", an UPnP and DLNA Media Server for Linux, to deliver key material over DLNA.

To accomplish the testing phase, we developed a DVB-CA compliant header modifying VideoLan with an Open Source implementation of DVB Common Scrambling Algorithm.

Regarding the DVB-CPCM device, we implemented a trusted delivery module to acquire content, a CPCM instance and the DLNA Manager Extension. We used DVB Common Scrambling Algorithm for simulating DVB-CPCM Local Scrambling algorithm. We tested part of our software in an ARM development board with successful results. Thus, we believe it can be deployed in state of the art consumer electronics.

IX. Conclusions

We have designed and prototyped a robust solution for sharing commercial contents in the home environment. We accomplish this objective with a twofold contribution: a DLNA extension to distribute DVB-CA key material to descrambler equipped display devices and a DLNA extension that interoperates with DVB-CPCM. DLNA provides discovery, content transport, and configuration services and its media transport mechanisms are used as a transport protocol among tamper proof hardware. DVB content protection messages are the payload of DLNA messages. Thus, our solution takes the best of both systems: the simplicity and penetration of DLNA and the strength of DVB-CA and DVB-CPCM systems.

References

[1] Contributing members of UpnP Forum, "UpnP Device Architecture Version 1.1", *UpnP Forum*, October 2008.

[2] European Telecommunications Standards Institute, "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems", *European Telecommunications Standards Institute*, ETR 298, October 1996.

[3] The 5C, "Digital Transmission Content Protection (DTCP) Specification", Vol. 1, Revision 1.51, 2007.10, *The 5C*, February 2005.

[4] Digital Content Protection LLC , "High-Bandwidth Digital Content Protection System", Revision 1.3, *Digital Content Protection LLC*, December 2006.

[5] European Telecommunications Standards Institute, "Content Protection and Copy Management Specification; Part 2: CPCM Reference Model", ETSI TS 102 825-2 V1.1.1, *European Telecommunications Standards Institute*, July 2008.

[6] Marlin Developer Community, "Marlin Broadband Architecture Overview for Marlin Adopters", *Intertrust* ,2007.

[7] Open Mobile Alliance (OMA), "Mobile Broadcast Services Architecture", Candidate Version 1.1, OMA-AD-BCAST-V1_1-20091013-C, *Open Mobile Alliance,* 2009.

[8] Xin Wang , "MPEG-21 Rights Expression Language: enabling interoperable digital rights management", *IEEE Multimedia*, vol. 11, no. 4, pp. 84-87, December 2004

[9] European Telecommunications Standards Institute, " Content Protection and Copy Management Specification; Part 3: CPCM Usage State Information", ETSI TS 102 825-3 V1.1.1, *European Telecommunications Standards Institute*, July 2008.

[10] Marlin Developer Community, "The Role of Octopus in Marlin", *Intertrust* ,2006.

[11] European Telecommunications Standards Institute, "Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification", TS 101 699 V1.1.1, *European Telecommunications Standards Institute*, November 1999.

[12] CI Plus LLP, "CI Plus Specification, Content Security Extensions to the Common Interface", V1.2, *CI Plus LLP*, 2009.

[13] D. Díaz-Sánchez, A. Marín, F. Alménarez, A. Cortés. "Sharing conditional access modules through the home network for Pay TV Access", *IEEE Transactions on Consumer Electronics*, Vol. 55, Issue 1, pp. 88-96, 2009

[14] European Telecommunications Standards Institute, "Content Protection and Copy Management Specification; Part 9: CPCM System Adaptation Layers", ETSI TS 102 825, V1.9.1, *European Telecommunications Standards Institute*, Sep. 2009.

[15] European Telecommunications Standards Institute, "Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream", ETSI TS 101 154 , V1.1.1, *European Telecommunications Standards Institute*, July 2008.

[16] European Telecommunications Standards Institute, "Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols", ETSI TS 102 005 , V1.3.1, *European Telecommunications Standards Institute*, July 2007.

[17] H. Tian, Y. Wang. "Security Analysis of the Digital Transmission Copy Protection Specification". *Security and Management Conference,* pp. 134-137, 2006.

BIOGRAPHIES

Diaz-Sanchez, Daniel (M'07) received a Telecom. Eng. degree from Univ. Carlos III de Madrid in 2002. He graduated as Master Telematic Engineering (2004) and obtained his PhD (2008) from Univ. Carlos III of Madrid. He works as researcher and teacher at Universidad Carlos III. His research topic is distributed authentication, authorization and content protection.

Sanvido, Fabio received a Telecom. Eng. degree from Univ. degli studi di Trieste in 2008. In the same year he began a Master of Telematics Engineer in Univ. Carlos III de Madrid where he currently works as researcher for the telematic department since 2008. His research interests includes advanced authentication methods and security in New Generation Networks..

Proserpio, Davide received a Telecom. Eng. degree from Technical University of Milan in March 2008. In September 2008 he started his MsC studies in the Univ. Carlos III of Madrid. He is currently combining his studies with a position as researcher in Telematic Department. His research topics include New Generation Network (NGN) and Advanced Authentication Mechanisms.

Marín López, Andrés (M'07) received a Telecom. Eng. degree and PhD from the Technical Univ. of Madrid in 1992 and 1996 respectively. He lectures in Computer Networks and Ubiquitous Computing in the Univ. Carlos III de Madrid, as an associate professor. His research interests include ubiquitous computing: limited devices, trust, security services, and security in NGN.