



Provided by the author(s) and University of Galway in accordance with publisher policies. Please cite the published version when available.

Title	Techniques for securing multimedia content in consumer electronic appliances using biometric signatures
Author(s)	Corcoran, Peter M.; Cucos, Alex
Publication Date	2005
Publication Information	P. Corcoran, A. Cucos, (2005)" Techniques for securing multimedia content in consumer electronic appliances using biometric signatures", IEEE Transactions on Consumer Electronics, Vol. 51, No. 2, pp. 545-551.
Publisher	IEEE
Item record	http://hdl.handle.net/10379/287

Downloaded 2024-03-13T07:22:57Z

Some rights reserved. For more information, please see the item record link above.



Techniques for Securing Multimedia Content in Consumer Electronic Appliances using Biometric Signatures

Peter Corcoran, *Member IEEE*, and Alex Cucos

Abstract — A system is described for CE appliances which employs a biometrically auditable public key infrastructure for securing multimedia content (BAPTISM). It is based on biometrically generated key-pairs and is designed to protect the fair use rights of end-users. By taking advantage of low-cost fingerprint scanners the system can be readily incorporated into networked handheld and CE Appliances.¹

Index Terms — Biometric Authentication, Digital Rights Management, Multimedia Content & Applications, PKI Systems.

I. INTRODUCTION

Since the emergence of peer-to-peer networking and associated file-sharing services there has been significant media focus on the issue of illegal versus “fair use” copying of digital content. Much of the initial focus was on the use of newer compression formats such as MP3 which allow the size of a standard CD audio track to be reduced by a factor of 10-20 times thus facilitating the sharing of such files over a network. More recently, the increasing availability of low-cost home broadband connections and the availability of new state-of-art high-quality video codecs has further raised the issue of the copying and transcoding of DVD videos.

The dissemination of such new technologies which facilitate the copying, compression and sharing of digital content over network connections has created problems for both the music industry and Hollywood in recent years. Now whatever one's views on the copying of music & video it is quite clear that recording and movie studios and the artists, musicians and actors who work in the music and film industry require revenue in order to exist. Thus, as a society, if we value these services there is clearly a pressing need for a means to manage and account for the copying and redistribution of digital multimedia.

Quite recently the Recording Industry Association of America (RIAA) has begun to actively pursue broadly targeted legal actions against individuals who are involved in such sharing of digital content. It is worthwhile remarking that there is a contending requirement that consumers retain certain “fair use” rights to copy recordings that they have obtained legally for personal use and archival purposes. For consumers these recent legal actions introduce a new uncertainty: how can a consumer prove that they are not abusing their fair use rights

to copy music? Further, despite the assertions of the RIAA and the music industry there is evidence that allowing controlled copying and sharing of digital content can lead to market growth and improved sales. Thus, in our opinion, the challenge for content providers in today's digital age is to offer mechanisms which allow copying of digital content within the home environment combined with limited sharing of digital content to friends and family members but which restrict commercial piracy.

Ideally consumers should be able to digitally sign copies of music to authenticate the copy as a fair use copy. They should also be able to secure any copies of digital content in a manner that such content can only be used by a very limited number of specific users, such as family members or close friends. In this way consumers could proactively demonstrate compliance with recent legislation such as the Digital Millennium Copyright Act (DMCA).

The CE system described in this paper combines recent advances in biometric scanning technologies to offer a public key infrastructure solution to the issues posed by the growth in digital content sharing over broadband networks. In particular it addresses the problem of allowing consumers “fair use” rights, but at the same time restricting the illegal piracy of digital media.

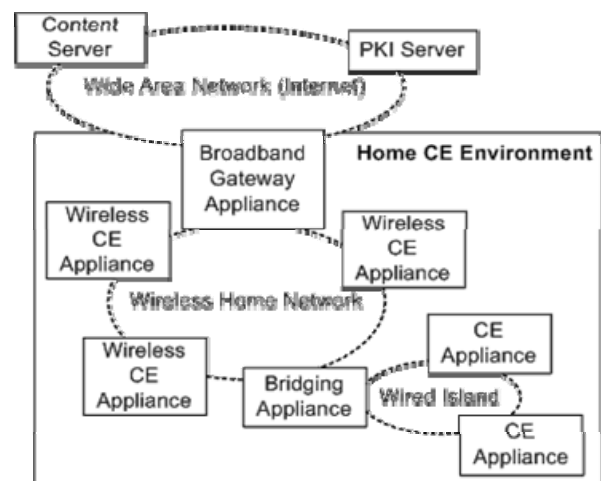


Fig 1: The Emerging Home Network Infrastructure

This CE system is particularly amenable to incorporation in embedded devices, notably networked A/V appliances, where a fingerprint scanner could be incorporated into the record & playback subsystem and access to a public key repository is provided over the network. Further, it offers an original and unique approach to the problem of copyright protection and content management in the digital age facilitating the return of responsibility for legal use of digital content back into the hands of the end user, while at the same time empowering him with means to authenticate his legally owned content and to

¹This work is supported under the Technology Development Phase of the Enterprise Ireland Commercialization Fund.

Peter Corcoran is with the Dept. Electronic Engineering, National University of Ireland, Galway (e-mail: peter.corcoran@nuigalway.ie)

Alex Cucos is with the Consumer Electronics Research Group in the Dept. of Electronic Engineering, National University of Ireland, Galway (e-mail: cucos@wuzwuz.nuigalway.ie)

copy it in a restricted manner for the sole use of friends and family.

II. SYSTEM OVERVIEW

The system described in this paper combines recent advances in biometric sensing technologies, specifically in fingerprint scanning and voice recognition, to offer a public key infrastructure solution to the issues posed by the growth in digital content and the problem of allowing consumers "fair use" rights, but at the same time restricting the illegal piracy of digital media. It offers an improved means of user authentication for public key technology through the use of unique biometric authentication.

A. Main System Components

The system comprises two principle components:

- (i) a software/firmware client-side engine designed for incorporation in a consumer electronic appliance and
- (ii) a server-side engine which implements and supports the public-key storage and management functions.

The client-side aspects of the system further comprise:

- (i-a) a biometric data analysis subsystem capable of generating a unique and repeatable digital signature which can be associated with an end-user of the system;
- (i-b) a public/private key-pair generator which can create unique key-pairs based on the aforementioned digital signature;
- (i-c) permanent storage for private keys;
- (i-d) a recording and/or rebroadcast subsystem which encodes digital content using at least one public key, and may also digitally sign the content using an end-user's private key;
- (i-e) a playback subsystem which can decode digital content secured with an end-user's public key;
- (i-f) a network subsystem or data I/O subsystem which allows public key data to be imported and exported.

B. Advantages of the Baptism System

Among the principle benefits offered by BAPTISM we note:

1) No centralized private key infrastructure

Because of this it is thus very difficult to reverse-engineer the system private keys in order to break the underlying security mechanism. In essence each CE appliance can have its own unique private key so that there is a very large number of private keys to be reverse-engineered.

2) Bit-copying of secured data is not possible

Many DVD pirates simply bit-copy the original media using specialized equipment. Once they have a valid bit copy it is trivial to mass-produce pirate copies of a new DVD. With BAPTISM key-secured data each consumer will get a unique, personalized copy of the digital multimedia content and bit-copying is no longer practical.

3) Facilitates limited copying and sharing of content

Restricted copies of digital multimedia can be made by end-users for their friends and family. To do this they simply locate the public keys of the person(s) they wish to make a media copy for and the recording engine will sign the media with their private key and encode the data with the public key of the recipient. Note the fact that the media is permanently and irrevocably signed with a user's private key acts as an disincentive to abuse of the recording facility and the fact that the media copy can only be used by a single recipient further restricts its value in the black market.

For these reasons we believe that the system offers an original and unique approach to the problem of copyright protection and content management in the digital age. It facilitates returning much of the responsibility for legal use of digital content back into the hands of the end user, while at the same time empowering the end user with means to authenticate their legally owned content and to copy it in a restricted manner for the sole use of friends and family. This will also provide consumers with an affirmative defence against potential legal actions arising from claims of abuse of "fair use" rights. Because the system adds value in these ways for consumers it offers advantages over more centralized content protection systems such as the CSS system used to secure digital content on DVDs.

As with any such system there will be individuals who seek to abuse the system, but with the approach adopted by the BAPTISM system it is significantly more difficult to "crack" the system because this requires breaking into the secured data of individual users rather than the secured data of a corporate entity.

III. SYSTEM ARCHITECTURE

The main architecture of the BAPTISM PKI infrastructure is illustrated in **Fig 2.** below. At the heart of the system described in this paper is the use of biometric identification of the user. This can be readily implemented in an unobtrusive and cost effective manner using recent developments in fingerprint sensing technology. However the system might equally well employ face recognition or voice analysis technology to achieve the same result of a repeatable biometric signature linked to an individual consumer.

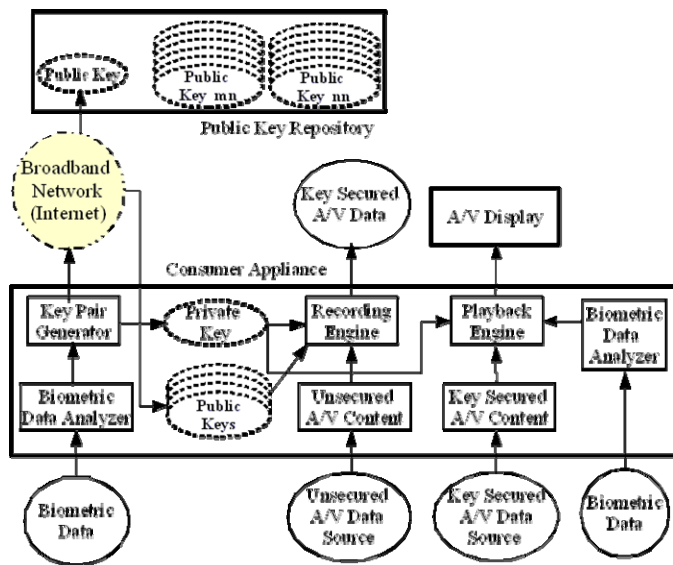


Fig 2: Core Elements of Baptism Public Key Infrastructure

A. System Initialization

When the system is initially configured for use a user must first activate the CE appliance with their biometric signature, generating an immutable public/private key-pair. The user first presents the necessary biometric input which is analysed to confirm that the data constitutes a unique and repeatable digital signature. This signature is then used to generate a unique public/private key pair within a *key-pair generator* subsystem.

This “master” private key is stored locally and can only be transferred outside the appliance in special circumstances. This is an important aspect of the system described herein because, if the “master” private key were readily accessible then, data signed or secured by the end-user associated with that key could be easily compromised. Note that additional key-pairs can be created for different family members. However the first key-pair created is the “device master” and is an important aspect of device initialization.

The associated public key can be transferred outside the appliance via a means of data output such as a network connection, or alternatively by removable data storage such as a smart card or computer memory card. We expect that next-generation CE appliances will be network enabled, thus this data export is achieved through a broadband network connection to the Internet. Thus the associated public key is transferred to a public key server where it is available to anyone who wishes to generate key-secured content for the owner of the key.

The public key may, optionally, be stored locally with the public keys of family members and friends. These locally stored public keys are those most commonly used by the end-user and may be employed to prepare copies of digital content which is only accessible to the owners of those keys. Keeping a local copy serves to simplify user interface aspects of this process as the end-user of the appliance can simply scroll

through the locally stored public keys. If a key is not stored locally then a search for that person's public key must be initiated on the network. This is a more involved process and requires a more sophisticated user interface.

The “master” private key is retained internally by the CE appliance and is used to sign copies of multimedia content recorded by the CE appliance and to decrypt key-secured multimedia content which has been encoded using the consumers public key.

B. Normal Operation (Media Recording)

Once the appliance is initialized it can be used to record and playback key-secured multimedia content in a manner with is completely transparent to the end-user.

Unsecured A/V content may be input to the appliance in a number of ways: (i) streamed from a broadband network connection; (ii) directly from removable optical media such as DVD or CD inserted into an optical drive, or (iii) from terrestrial or satellite receivers incorporated into the appliance. Once an unsecured source of content is selected it may be recorded by the key-encoding engine onto a local hard disk or optical media.

Note that this recorded content is not a copy of the original A/V content, but rather an encoded copy which can only be accessed by providing a suitable public key to a decoding engine.

In default mode the recording engine will encode content with all of the public keys which have associated private keys stored on the appliance. Optionally, the device may also require the input of a valid biometric signature prior to initiating content recording.

C. Normal Operation (Playback)

The playback of encoded media is initiated by firstly selecting the multimedia content for playback. Normally, if the content was recorded on a particular appliance then it can be automatically played back on that appliance or on a local TV set or display appliance. Alternatively, if the content was encoded using the public key of a 3rd party appliance then that content can be transferred to the 3rd party appliance and can also be played back on that appliance.

If no suitable private key is available locally to decode the content then the appliance can optionally display the public keys which have been used to encode this content. A user must next initiate a private key transfer from an external device. This procedure is described in more detail in section VI below.

Note that activating either of the record or playback functions requires that the user has recently provided their biometric signature to activate the encoding or decoding processes. It is not expected that this would be required every time the appliance is used, but there would certainly be a requirement that a valid signature were provided occasionally – for example, on initial device activation or at least once every 24 hours.

IV. SYSTEM IMPLEMENTATION

In this section we describe the practical implementation of an initial prototype of BAPTISM.

A. Reference Platform (Hardware & OS)

An embedded x86 architecture platform provides an ideal hardware platform for system prototyping. Such systems are readily available in compact form factors and provide most of the system peripherals and relevant I/O subsystems. Such a reference platform can support content streaming over both wireless and wired networks and additionally provides optical drives, 1394 and USB2 connectivity and hardware support for certain MPEG functions. Output modes include VGA, S-Video and SPDIF digital audio. Additional support for TV or satellite tuners can be readily added using two available PCI slots.

We chose to adopt the latest version of the *Fedora Core Linux* distribution for our OS reference [1]. In addition to the standard system packages a wide variety of compatible 3rd party packages is available and excellent tools now exist to support the resolution of package interdependencies. Thus it is a relatively straightforward process to set up a well supported multimedia A/V platform with support for many state-of-art audio and video transcoding packages.

B. PKI Implementation

Implementing a full multi-server PKI infrastructure which is publicly accessible over the Internet is a non-trivial undertaking [2]. Fortunately we do not require such a full implementation in order to set up a working proof-of-concept. This can be readily implemented on a local area network by employing the OpenPGP Key Server software [3] compiled to run on a standard desktop server configured according to our OS reference platform.

C. Client-Side Software Development

Software for the embedded client is somewhat more complex and must combine elements of (i) a biometric analysis subsystem; (ii) a key-generation engine; (iii) I/O subsystems for access to multiple sources of multimedia content and for key export; (iv) a content recording system; and (v) a content playback subsystem. All of these elements must be functionally integrated and may need to interoperate with a higher-level multimedia application such as a networked PVR.

The python scripting language [4] was chosen for most of the prototyping work. It facilitates rapid development and is well supported with encryption libraries [5, 6]. We have also created a python wrapper for the open-source videolan project [7] to provide advanced multimedia streaming support for the playback and recording subsystem. A further advantage of Python is that it supports integration of production code with portable ANSI-C/C++ modules for time-critical sections [8].

1) Recording Engine

Our prototype system allows two modes of operation. In manual mode a recording or playback operation must be

actuated from a user-interface module but the system may also be placed in an automatic mode. In this latter case a recording of any CD or DVD which is inserted into the optical drive is automatically initiated. This process includes the encoding of the inserted media with all locally registered key pairs. In this automatic mode the system does not require authentication, but the recorded content will no longer be accessible from the hard disk unless a playback event is actuated which incorporates the correct biometric authentication of one of the registered key pairs.

2) Playback Engine

This also features a manual and an automatic mode of operation. In the manual mode each playback event should be authenticated with a signature corresponding to a locally registered private key. However, as this may prove tedious the system also incorporates a mode with actuates the playback engine for a fixed period of time from a single authentication. Playback will be restricted to content which is encoded with that particular key, however the user may browse and select encoded content without any restrictions for a fixed time period.

3) Biometric Analysis Subsystem

We have investigated the use of fingerprint scanning technologies, speaker recognition techniques and face recognition as part of the BAPTISM system. Fingerprint scanners, in particular, are now available at pricing levels commensurate with the requirements of CE applications. However there are still many complications involved in determining repeatable biometric signatures from such sensors. As our investigations in this area are still in progress we will not detail them here but leave that to a future publication.

V. SECURED CONTENT SERVICE TO END USERS

The BAPTISM system may be equally well employed by content providers. Examples of potential services which could be offered to consumers include key-secured DVDs and network based video-on-demand (VOD) services. An illustrative implementation of such a service is shown in **Fig 3**.

In this implementation a content provider receives a request from a consumer for access to some multimedia content they will also be provided with a public key for the customer or a means to locate such key from a public key repository. The content provider can next proceed to access the original content from their local data infrastructure and to encode and copy the data onto a DVD which can then be mailed to the consumer. Alternatively, for a VOD service the requested multimedia content is encoded and streamed over the network to the consumer. All content generated by a content provider service must be signed with the company's private key which allows for future auditing of DVDs.

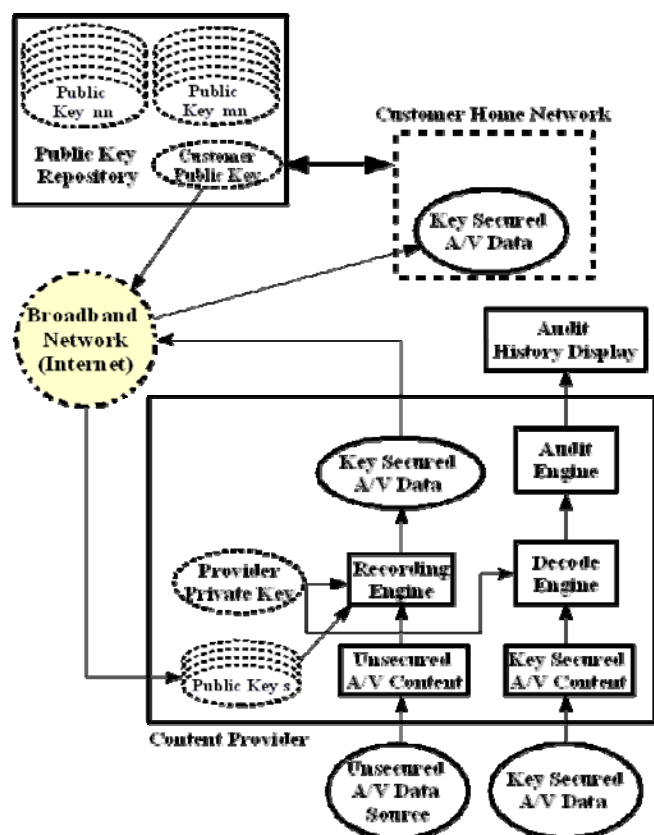


Fig 3: Content provider service using BAPTISM

A key benefit of this method of content distribution is that every DVD is unique to a single consumer and can only be used by that consumer. This effectively prevents bitcopying of a DVD for the simple reason that each DVD is uniquely encoded with the public key of a biometrically verifiable consumer's signature. Another interesting side-effect of the BAPTISM system is that it provides a unique means for individual artists to directly distribute their works digitally without a need to enter into contracts with a large music publisher.

This embodiment also allows a content providers to perform an audit trail on digital content they have released. Such content will be signed by their private key and, as the originator of the content, this will allow them to test and extract audit information from copies of the original digital content data. This process is also illustrated in Fig 3.

It is assumed that some key secured audio/video data has been obtained and is to be processed for audit. This data is loaded into the content provider's system and is then processed by an enhanced decode engine which can extract data regarding the public keys with which the digital content has been encoded and the private key with which the content copy was signed. Note that only the originator of the master copy of the content can perform such an audit. This information is passed into an audit engine which determines the form of content licensing which was purchased by the customer for this content and determines if a licensing violation has occurred. The audit engine will access various customer databases and IT subsystems of the content providers system during this

processing step. Finally an audit history report for this particular digital content can be generated and displayed to an operator, or alternatively, stored for future reference.

VI. PRIVATE KEY EXCHANGE

One advantage of the BAPTISM system architecture is that the system's private key can be embedded in the firmware of consumer appliances. Assuming that reasonable security precautions are taken in the hardware subsystems of said appliances it will be difficult to tamper with the system's private keys.

It is true that an attacker could determine the means used to create keys and publicly provide access to a "cracked" key pair. However it is simple to remove such key pairs from the official public key servers used by the system. We also remark that BAPTISM employs an opt-in approach; thus a user chooses to adopt the technology because they wish to demonstrate that they are not abusing their rights to copy digital content.

Another important issue which is raised in the context of private keys, is that it is desirable that an end user of the BAPTISM system can have a single private key associated with their biometric signature. This is more a convenience to the end-user who would like to be able to play the same movie or music on ALL of their consumer appliances. Thus it is desirable that each appliance does not create its own unique private key, but can access, instead, a single master private key. This capability is incorporated in the design of the BAPTISM system and we will now describe how it can function within a home networking environment without compromising the security of the master private key.

Fig 4 shows how secured exchange of a private key may occur over a local home network:

(i) To initiate the exchange the user must biometrically activate a private key transfer engine in the appliance which holds the master private key. If the private key selected for transfer matches the activation signature then the appliance broadcasts on the local network that it is ready for key transfer.

(ii) To complete the key exchange the user must activate in receive mode the private key transfer engine of the receiving appliance. This (i) generates a temporary local key-pair, (ii) locates the transferring appliance on the local network and (iii) exports the temporary public key to the transferring appliance.

(iii) The transferring appliance next encrypts the master private key with the temporary public key it has received from the receiving appliance and then transfers the encrypted master private key to this receiving appliance.

Note that all network transfers of temporary public keys and encrypted private keys are made over SSH, further proofing the system against eavesdropping.

Despite the complexity of the security mechanisms described above, the workflow for the end user is relatively simple – they activate transfer mode on the first appliance using their fingerprint as activation code; they then verify themselves by fingerprinting a second appliance and the key transfer sequence is completed. In this way a single private key can be shared by all CE appliances in the home network (or by mobile devices which are brought into the home environment) and a single public key for all appliances can be used by the consumer.

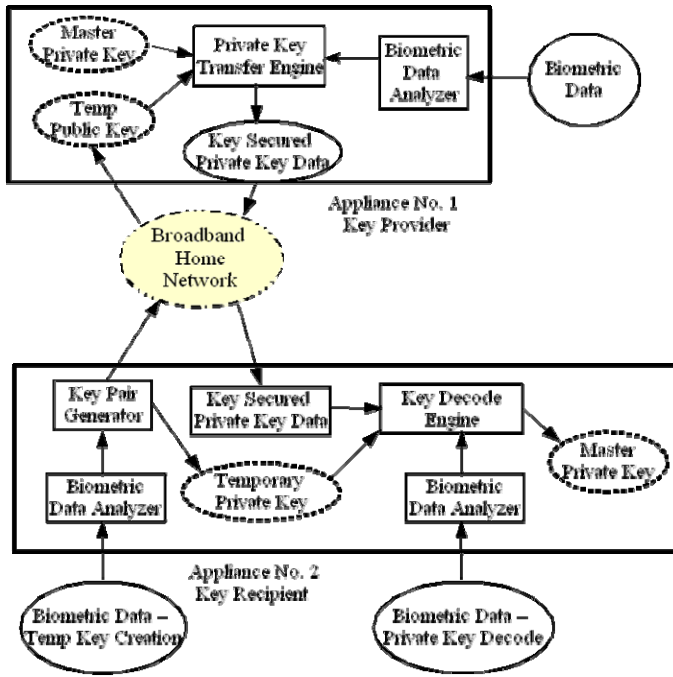


Fig 4: Secured Private Key Exchange Mechanism.
pubs/transactions/auinfo00.pdf.

VII. DATA REBROADCAST OVER A WIRELESS HOME NETWORK

The problem addressed in this embodiment is the potential copyright infringement which may occur if a user is rebroadcasting audio or video content over a wireless home network. In principle this could be construed as an instance of 'fair use', but as other persons in an adjacent dwelling could also access the rebroadcasted music or video there is a genuine cause for concern on the part of the copyright holder. By adopting the use of BAPTISM to filter WLAN content rebroadcasts this concern can be readily addressed. To employ BAPTISM in such a rebroadcast scenario the data stream should be encoded at source, prior to rebroadcast, with the public key of the owner(s) of the data. If the data is already in the form of a key-secured data stream this encoding step is not needed. At the receiving appliance the biometric signature of the owner of the data is required in order to unlock the data stream using the relevant private key. Typically the rebroadcasting and receiving appliances would share the same private key which would be securely transferred between appliances using the method described in the next section of this disclosure document.

A detailed overview of WLAN rebroadcast employing the BAPTISM infrastructure is given in Fig 5. It incorporates many similar aspects of the present system described earlier. This implementation represents another very interesting potential application for the BAPTISM technology and as it is transparent across any IP enabled network it could also be employed for WLAN rebroadcasting of secured content.

VIII. CONCLUSION

A novel PKI based on biometric signatures has been described. The system is designed to support the recording and

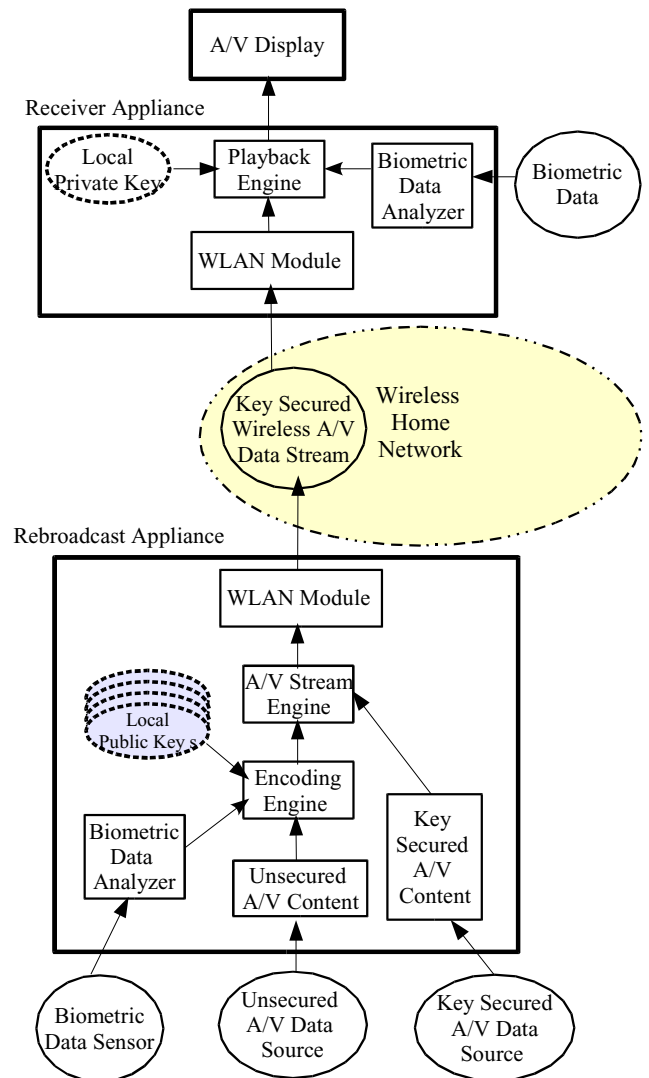


Fig 5: WLAN rebroadcast using BAPTISM.

playback of personalized digital content on CE appliances using low-cost fingerprint scanning technology to provide a means of generating and authenticating a user's private key. Although the IT infrastructure to support this system architecture has been largely implemented there remain some issues with regard to the repeatability and reliability of the biometric scanning technologies which are proposed. These issues and some proposed solutions will be considered in detail in future work.

ACKNOWLEDGMENT

The support of *Technology Development Fund* of Enterprise Ireland for this research work is acknowledged.

REFERENCES

- [1] <http://fedora.redhat.com/>
- [2] *The Open-Source Public Key Infrastructure Book* available online at: <http://ospkibook.sourceforge.net/docs/OSPki-2.4.7/OSPki-html/ospki-book.htm>
- [3] <http://sourceforge.net/projects/pks/>
- [4] <http://www.python.org>
- [5] <http://www.freenet.org.nz/ePyCrypto/>
- [6] <http://www.amk.ca/python/code/crypto.html>

- [7] <http://www.videolan.org>
[8] <http://swig.sourceforge.net/>



Peter Corcoran received the BAI (Electronic Engineering) and BA (Math's) degrees from Trinity College Dublin in 1984. He continued his studies at TCD and was awarded a Ph.D. in Electronic Engineering for research work in the field of Dielectric Liquids. In 1986 he was appointed to a lectureship in Electronic Engineering at NUI, Galway. He is also director of IP for FotoNation Ireland Ltd. His current research interests include embedded systems

applications, home networking, digital imaging and wireless networking technologies.



Alexandru Cucos received his B.S. degree in Electronic Engineering from "Transilvania" University from Brasov, Romania, in 1997. At the same university he received in 1998 M.S. degree in Electronic Design Automation. He received a M.Eng.Sc. degree in electronic engineering at National University of Ireland, Galway in 2001. Currently he is a senior research engineer working in the Consumer Electronics Research Group at National University of Ireland, Galway. His

research interests include network streaming of multimedia content, embedded systems design, communication network protocols, and biometric sensing techniques.