1.4-3

Biometrically Auditable Public Key Infrastructure Technology for Secure Multimedia Content

Peter Corcoran, *Member, IEEE*, Alex Cucos and Thomas Grossman,
Dept. Electronic Engineering, National Univeristy of Ireland, Galway.

***Abstract*--A system for signing and tracing the use of digital content based on biometrically generated key-pairs is described. The system is designed to protect the fair use rights of end-users and can be readily incorporated into networked CE Appliances..**

I. INTRODUCTION

The CE system described in this paper combines recent advances in biometric scanning 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 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.

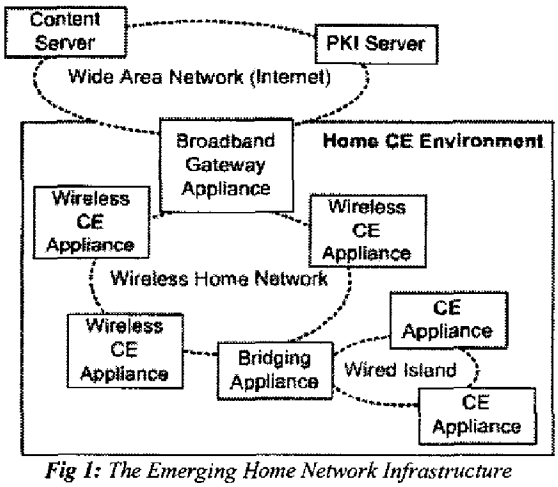

Fig 1: The Emerging Home Network Infrastructure

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

II. System Overview

The main architecture of the invention 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.

When the system is initialized a user must 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 analyzed 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.

The 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 private key were readily accessible then, data signed or secured by the end-user associated with that key could be easily compromised. 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.

Where a broadband network connection to the Internet is available the associated *public key* is then exported to a public key repository 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. Keeping a local copy serves to simplify the process of making a secure copy 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.

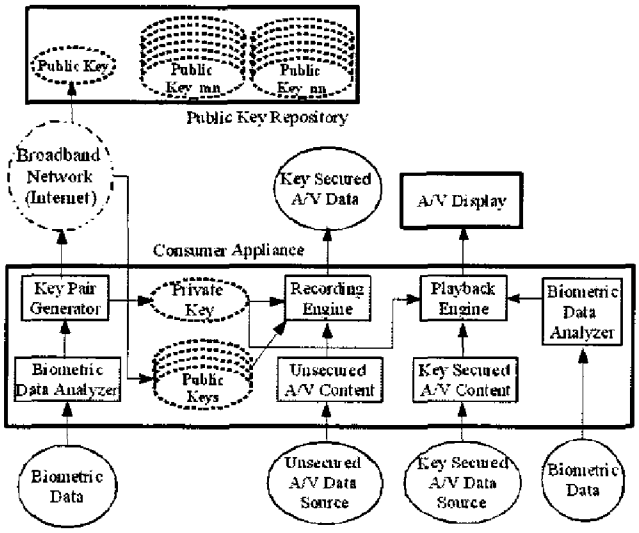

Fig 2: Core Elements of Baptism Public Key Infrastructure

0-7803-8838-0/05/$20.00 ©2005 IEEE.

III. Secured Content Service to End Users

The present invention public key infrastructure 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.

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 is that present invention 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.

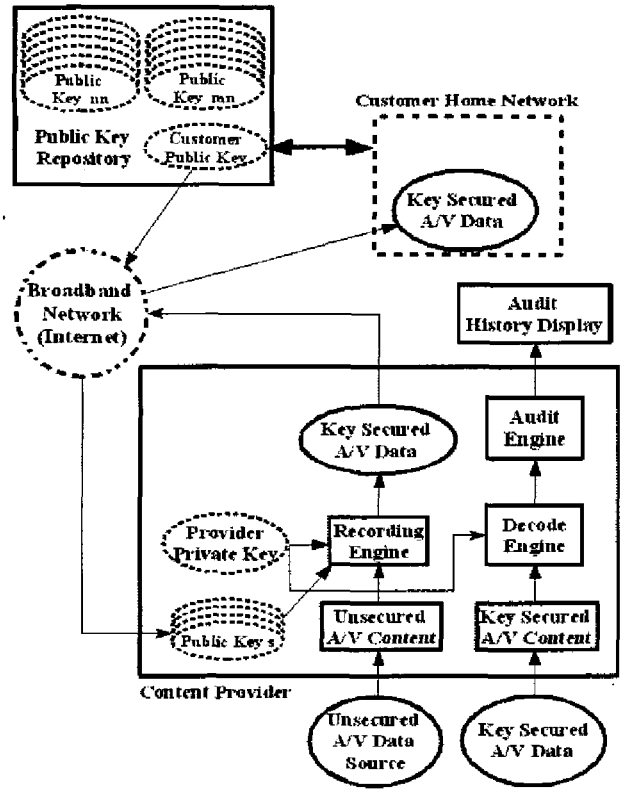

Fig 3: Content provider service using BAPTISM

IV. Private Key Exchange

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 makes a local network broadcast that it is prepared for key transfer.

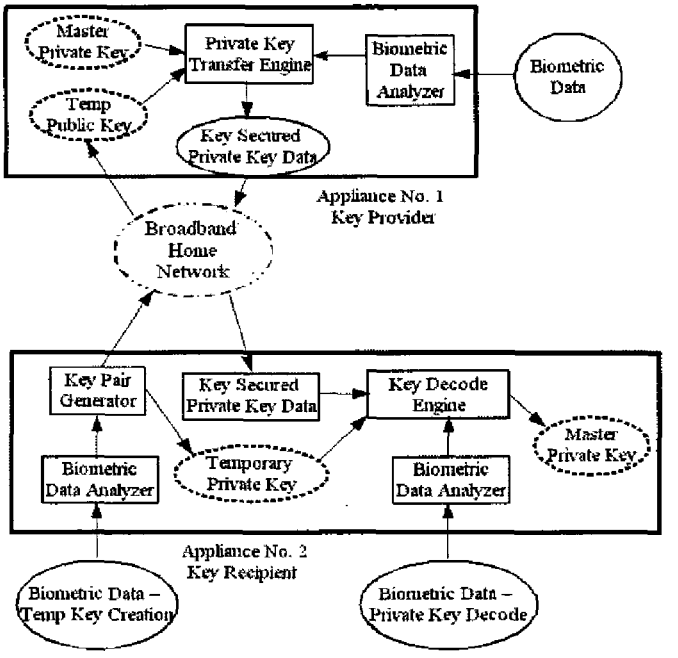

Fig 4: Secured Private Key Exchange Mechanism.

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 termporary public key to the transferring appliance. 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.

V. Conclusions

As there is no centralized key infrastructure it is difficult to reverse-engineer private keys. In essence each CE appliance can have its own unique private key so there is a very large number of private keys to be reverse-engineered. Further, because each consumer will get a unique, personalized copy of the original content bit-copying is no longer practical. The system also allows consumers to make restricted copies of digital multimedia for their friends and family. Note the fact that the media is irrevocably signed with a user's private key is a strong incentive against copyright abuse.

Acknowledgment

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