REALTIME PLAYBACK OF AUDIO CONTENTS ON MOBILE DEVICE

A DISSERTATION

Submitted in partial fulfillment of the requirements for the award of the degree

of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

By

BHASKAR SINGHAL

IIT ROORKEE - CDAC NOIDA
C-56/1, "ANUSANDHAN BHAWAN"
SECTOR-62, NOIDA-201307
JUNE, 2004

CANDIDATE'S DECLARATION

I hereby declare that the work presented in this dissertation titled **"Real Time Playback of Audio Contents On Mobile Device"**, in partial fulfillment of the requirements for the award of the degree of **Master of Technology** in **Information Technology**, submitted in **IIT, Roorkee – CDAC, Noida**, is an authentic record of my own work carried out during the period from May 2003 to May 2004 under the guidance of **Maj. Gen. K. N. Singh** Chairman & MD, NextGen Media Alliances Pvt. Ltd., New Delhi.

The matter embodied in this dissertation has not been submitted by me for award of any other degree or diploma.

Date: 31st May 2004
Place: Noida

(Bhaskar Singhal)

CERTIFICATE

This is to certify that the above statement made by candidate is correct to the best of my knowledge and belief.

Date: 31st May 2004
Place: New Delhi

Supervisor:

(Maj. Gen. K. N. Singh)
Chairman & MD
NextGen Media Alliances Pvt. Ltd.

Co-Supervisor:

(Mr. V. N. Shukla)
Director (Spl. Appl.)
CDAC, Noida

ACKNOWLEDGEMENTS

The work presented in this report would not have completed without the guidance and support of many people.

In first place, I would like to thank **Prof. Prem Vratt**, Director, IIT Roorkee and **Sh. R. K. Verma**, Executive Director, CDAC Noida.

I would like to thank **Prof. R. P. Agarwal**, Course Coordinator, M.Tech(IT), IIT Roorkee and **Mr. V. N. Shukla**, Course Coordinator, M.Tech(IT), CDAC Noida.

I would like to thank my guide, **Maj. Gen. K. N. Singh**, Chairman & MD, NextGen Media Alliances Pvt. Ltd., New Delhi, for his constant support, incredible enthusiasm and encouragement. I am grateful to **Mr. Raghavendra Agarwala,** Director Technical NextGen Media Alliances Pvt. Ltd., New Delhi, for his support. I am also grateful to Mr. **Munish Kumar,** Project Engineer for the cooperation extended by him in the successful completion of this report.

Finally, I would like to extend my gratitude to all those persons who directly or indirectly helped me in the process and contributed towards this work.

(Bhaskar Singhal)
Enrollment No.-029001

CONTENTS

ABSTRACT

This Dissertation work gives an account of the Digital Rights Management System conceived and designed for NextGen Media Alliances Pvt. Ltd, New Delhi. This dissertation outlines real time playback of encrypted contents through a secured path.

The subject Digital Rights Management System has been developed as an application software and is designed to achieve a smooth and piracy free digital content delivery over the digital media i.e. Internet. Designed in consideration to the sphere of activities of Secure Digital Music Initiatives, and Open Mobile Alliance, the system facilitates searching, browsing and real time streaming of digital audio content over the internet. Further, the application module enables digital content owners to get royalty for the creative work on the digital media.

This concept of Digital Rights Management is the first of its kind being designed and implemented in India. It is aimed at effective management of digital content and their delivery over the digital media.

The Dissertation describes the above work detail.

INTRODUCTION

1.1Problem Definition

The objective of this dissertation is to implement Digital Rights Management (including Mobile DRM)[1].

In this the audio/video content will be packaged in such a way that only authorized and authenticated user can access them

This involves development of an application, which will play encrypted audio/video contents through a secured path of execution on PC as well as Mobile device/phone. Along with this every access or the download of the audio/video content over a digital media will be billed, and from the payment received from the user a royalty will be given to the content owner. Thus inhibiting piracy!!

1.2 About NextGen Media Alliances Pvt. Ltd., New Delhi

NextGen Media Alliances Pvt. Ltd. (NGMA) is an end-2-end digital rights management solutions company. Catering to a worldwide clientele, there main focus is to be able to provide digitally secured and formatted audio/ visual entertainment. They target to set new milestones in combating piracy and preventing the illegal usage of media that is the scourge of the entertainment industry, setting new platforms and pioneering new concepts in digital entertainment delivery to a demanding consumer market.

They see themselves as an 'Envision-2-Execution' firm, with cutting edge technology, committed and motivated technical and marketing teams, and a clearly defined parametric approach constituting a formidable result oriented mechanism, to ensure secure delivery solutions for digital entertainment content

NextGen Media Alliances Pvt. Ltd. (NGMA) is a pioneering, state-of-the-art digital solutions company that has integrated IT based solutions with the media industry to help secure music in the digital arena (mobile & PC), and in turn promote creativity. The management team of NGMA comprises of professionals with international experience in business management, information technology, entertainment & marketing domains.

NGMA aims to become the preferred outsourcing partner for the entertainment industry with regards to digital/electronic distribution for a worldwide market. From musicians to movie producers to television broadcast companies, NGMA's portfolio of offerings is aimed at tackling issues faced by the entertainment industry in the areas of:

- Digital Rights Management (DRM)
- E-publishing
- Copyright Infringement
- Digital Media Distribution
- Reporting/Tracking of Contents

NGMA has developed a DRM (Digital Rights Management) platform, known as the NGMA DIAS, which aims at safeguarding the rights of the original creators of the creative content. DRM is a technology that is created to secure digital contents on the internet/mobile from illegal use. It is gaining popularity the world over and NGMA is its pioneer in India. The NGMA Dias includes content owners, artists/musicians from across India who form an essential part of its value-chain. NGMA provides a single platform for secured media delivery and helps monetize media through distribution on the Internet and mobile platforms. NGMA restricts, tracks and limits usage of the contents by providing the content owners newer technology methods and secured delivery modules.

Highlights of the NGMA DIAS

- Licensing Management system
- Billing Management System
- Royalty Management System
- Advanced Search Engine
- Content Management System
- Super-Distribution

NGMA's Client & Services

Content Owners

Content Owner Registration, Content Registration

Digitization, DRM Encryption & Digital Distribution of contents

Website Creation

Network Operator

Packaged audio/visual entertainment contents

SIM Card Preloads

Handset Manufacturers

Preloads

Genre based audio/visual contents

Exclusive Applications (preloaded or WAP enabled)

Trailers/snippets of latest movie/music videos

1.3 Current Situation

The popularity of mobile terminals such as phones and Personal Digital Assistants (PDAs) is growing at an incredible rate, and with it we are also seeing a dramatic increase in the number and variety of mobile contents delivery services. While the growth of interest in mobile services is highly encouraging, problems have also arisen — namely, corruption, unauthorized copying and "wiretapping" — that threaten the continued spread and long-term success of mobile communications services.

In order to stem the tide of illegal and unauthorized access to these types of services, Digital Rights Management technology has been developed. The purpose of this technology is to enable the secure delivery of information to mobile terminals. Characteristics of mobile terminals, such as processor performance, memory capacity and user interface, have all been taken into consideration in the development of Digital Rights Management.

Unfortunately, current mobile Digital Rights Management systems are very inflexible when it comes to the architecture, terminals and contents that may be used with them, making the system less convenient for users.

- No system exists to protect the right of content owners.
- No implementation of Digital Rights Management (DRM) including Billing exists either in PC world or Mobile world
- Various Websites hosting Audio/Video contents for free.

- Free distribution of Audio/Video contents on the Internet causing entertainment industry heavy losses every day and no royalty whatsoever goes to content owner.
- Various Napster like distribution websites/player active on the Internet.

1.4 Need of an Hour!

- Implementation of Digital Rights Management (DRM) over the Internet as well as mobile world to protect the rights of content owner as well as entertainment industry all over the world.
- Development of application as well as support system which can support DRM to its full extent including licensing as well as billing.

LITERATURE SURVEY

2.1 Mobile Digital Rights Management [1]

2.1.1 Introduction

Digital Rights Management (DRM) is a technology that protects content owner rights when selling and distributing content online in a digital form. DRM also introduces new ways of selling, distributing and consuming content that can be considered as important as the prevention of piracy. With DRM, content owners and retailers can configure usage rules that allow business models such as "try before you buy", promotional previews, rentals based on play counts or expiration dates, subscriptions, and purchases of streaming or downloadable media.

While mobility presents some special requirements and limitations, it also creates new possibilities for DRM. Some of the limitations arise from the mobile devices themselves: they have limited processing power, memory, and data transmission capabilities and thus cannot use as strong and complicated encryption technologies as PCs connected to the broadband Internet. Today, key management and trust establishment in PC DRM systems are based on public key infrastructure (PKI) concepts. One of the new possibilities for DRM on mobile phones is micro billing, where fees for DRM protected content can be added to the phone bill, a technique that is not widely available for PCs.

2.1.2 Mobile DRM Today and the Future Roadmap

Downloadable content for mobile phones today consists mainly of ringing tones and logos. The mechanism used to protect the rights of content owners is called forward-lock, a hard-coded feature inside the phone that prevents the user from copying or forwarding the downloaded content outside the phone. Actually, forward-lock cannot be considered as an actual DRM system, at least an intelligent one, but it is included in this paper to describe where the technology stands today. Forward-lock does not have usage rules or any other way to describe usage rights. The concept relies solely on the hardware implementation of the terminal manufacturer (see Figure 2-1).

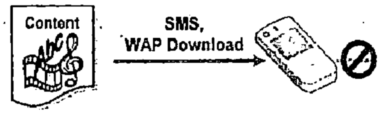


Figure 2-1. Forward-lock

FIGURE 2.1 Forward Lock

The hardware lock scheme was implemented by some manufacturers on their mobile phones before the standardization activities of the Open Mobile Alliance (OMA) Forward-lock is now one of the delivery methods for OMA DRM specification release 1 and it provides the simplest and most rudimentary standardized method for controlling content delivery for mobile phones.

Looking to the future, several topics need standardization: format of content container, content encryption, language used to express rights, delivery of content and rights to mobile device, trust establishment, and encryption key management. A single standard is crucial because several different M DRM solutions cannot be implemented due to the limited processing power and memory of the mobile devices, although phones are approaching PCs capability and function wise in the coming years.

Figure 2-2 portrays a MDRM roadmap for the near future. In the mobile world, DRM is in the process of being incorporated into the base operating systems and hardware instead of being a software add-on. We predict that current proprietary DRM solutions move towards standards compliance in order to take advantage of interoperability benefits and operating system and hardware support. Also, new standards based solutions are emerging (currently, for example, Nokia Delivery Server and Content Publishing Toolkit 2.0, ACCESS PCCS), Major players in the wired Internet field are also likely to enter the mobile DRM space. Microsoft has already started pushing its DRM solution into the Smartphone and Pocket PC Phone Edition operating systems. RealNetworks also offers a DRM solution, Media Commerce Suite, and works closely with Nokia in audio/video streaming.

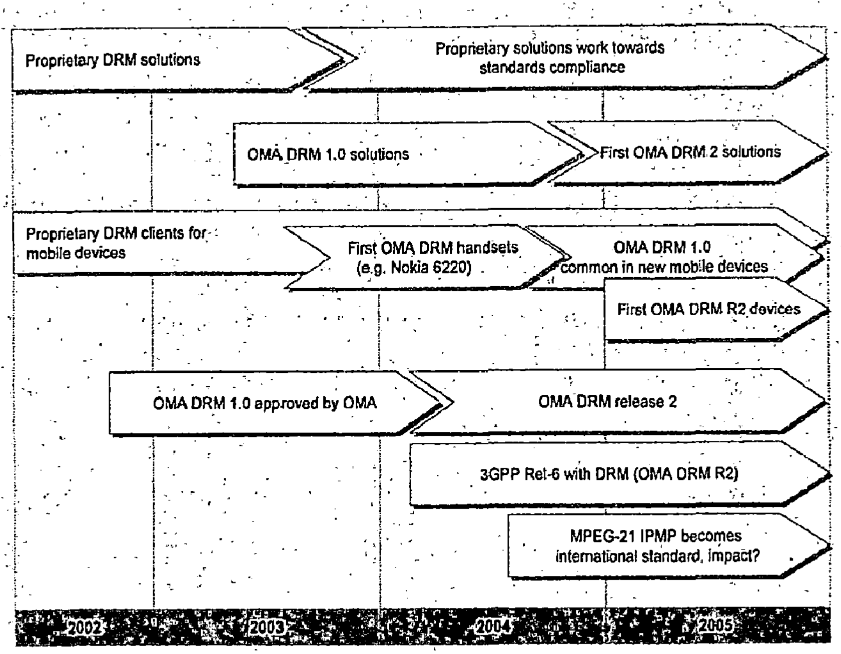

Proprietary DRM solutions
Proprietary solutions work towards standards compliance
OMA DRM 1.0 solutions
First OMA DRM 2 solutions
Proprietary DRM clients for mobile devices
First OMA DRM handsets (e.g. Nokia 6220)
OMA DRM 1.0 common in new mobile devices
First OMA DRM R2 devices
OMA DRM 1.0 approved by OMA
OMA DRM release 2
3GPP Rel-6 with DRM (OMA DRM R2)
MPEG-21 IPMP becomes international standard, impact?
2002
2003
2004
2005

Figure 2-2. Mobile DRM roadmap

FIGURE 2.2 Mobile DRM Roadmap

2.1.3 Why Digital Rights Management?

The protection and management of intellectual property rights on all digital platforms has become a major issue for content providers and carriers alike. Digital rights management (DRM) technology is being developed as companies seek to generate revenue from their digital distribution channels while controlling the access to their content. For instance, in response to the boom for illegal music file swapping on he Internet, DRM is currently being implemented by the music industry for commercial online services.

As commercial content is introduced into the mobile world, terminal manufacturers, media companies and DRM solution vendors are driving the introduction of DRM into mobile environments to enable new kinds of services. Japanese operators NTT DoCoMo and KDDI, providers of some of the earliest mobile data services, have already deployed various DRM technologies for mobile music downloading services. Users are allowed to purchase and download individual songs from selected artists, or listen to samples of them.

DRM systems can be either platform-independent, mobile-only or hybrid systems, which use mobile components for certain tasks. Whichever system is used, mobile value added service providers need to be able to protect and manage different content types like ring tones, MMS and downloadable media such as audio. General issues that must be addressed by any workable solution are security, interoperability and super distribution.

Mobile content protection technologies are already proving valuable to the industry.

Handset personalization with customized ring tones and logos has become a multi-billion euro industry thanks to simple forwarding lock mechanisms that prevent users from forwarding downloaded content. When handsets become more advanced, more sophisticated security mechanisms will be required to protect those revenues and increase them by enabling super distribution. Protection of the emerging mobile content types, such as MMS and downloadable media, will require network centric content protection solutions or more complex mobile DRM systems. Various solutions are being developed for those purposes, but still remain at early stages.

Content owners, content retailers and payment collectors fill the key roles in the DRM value chain. Most of the fixed online content retailers currently rely on credit cards for payment collection. This largely excludes young people, who are some of their best potential clients (as well as the most notorious music pirates!), from using their services.

Mobile operators could provide a solution by putting their billing solutions at content retailers' disposal. The concept has already been successfully trialled in Finland. When entirely mobile DRM systems are deployed, operators will also be able to act as multimedia content retailers. However, the content providers, such as media companies, are unwilling to release their intellectual property onto mobile platforms until there are sound protection systems in place.

Several DRM technologies compete in the fixed world and there are still no universally accepted standards. IBM, InterTrust Real Networks, Sony and others have made their technologies partly interoperable, while Microsoft wants to make Windows Media DRM a de-facto standard. It is still possible for similar standard conflicts to be avoided in the mobile space. The Open Mobile Alliance (OMA) has approved specifications for an open mobile DRM standard that is primarily adapted to MMS and ring tones etc. Leading handset manufacturers such as Nokia state that they will implement the standard in their products in the near future but other DRM technologies may still be employed for multimedia content types like audio and video.

However, leading DRM vendors such as IBM, Microsoft and Real Networks already provide solutions for both fixed and mobile platforms. Their products could possibly be used to create universal, platform-independent DRM frameworks. Existing services could also be extended to include mobile platforms. Several digital music service providers have the ability to provide turnkey music downloading services to mobile users, once handsets have the required features.

The content protection market remains fragmented both for fixed and mobile. Operators and content providers see a standard for mobile DRM as 'an absolute necessity' then mobile multimedia services reach the mass market and competition intensifies.

Before DRM-supported services can reach the mass market, a number of conditions must be met:

- Handsets supporting DRM have to become widely available and they must have intuitive user interfaces that make access to protected content as easy as possible.
- Access to mobile DRM systems must not require any complicated registration procedures.
- Limitations to certain networks or devices may be unavoidable at an early stage, but are nevertheless undesirable.
- Super distributed content should contain explicit information about charges and usage rules.
- Payments have to be collected with the help of widely available mechanisms and cause as little intrusion as possible.
- Downloading charges must be competitive in comparison to fixed-line connections.

It may be some time before all these requirements can be met. Nevertheless, there is great scope - and a pressing necessity - for implementing DRM technology in mobile environments. Content owners, service providers and operators will be able to benefit from increased business opportunities enabled with the technology and new distribution channels can be created for a range of digital content.

2.1.4 MDRM Platforms

The amount of infrastructure required depends on the DRM solution and requirements. For example, the simplest OMA DRM 1.0 Forward Lock does not necessarily require any additional infrastructure at all. A simple HTTP server is adequate if charging is not required. OMA DRM 1.0 infrastructure requirements are outlined in Table 1.

Table 1. Infrastructure required by OMA DRM 1.0

Delivery Method	**Required DRM-specific Infrastructure**
Forward Lock	None. Content can be wrapped in a DR M message and placed on a HTTP Server
Combined Delivery	Optional if dynamic rights are required, otherwise same as above.
Separate Delivery	Rights & key management
(Future PKI-based)	(Rights, key, and certificate management)

A possible OMA DRM platform operation is illustrated in Figure 2.3.

1. First the user browses and discovers interesting content, decides to buy it and clicks the 'purchase' button on a mobile portal.
2. The mobile portal generates a download order for the content.
3. The order identifies the content and contains rights and price information. The download is then returned to the client.
4. The client contacts the download server to get the actual content.
5. The download server authenticates the client.
6. Fetches the actual content from content storage.
7. Returns the content to the user.
8. At the same time the server pushes rights for the content to the client. After the content and rights have been delivered to the client, the delivery server generates charging information.

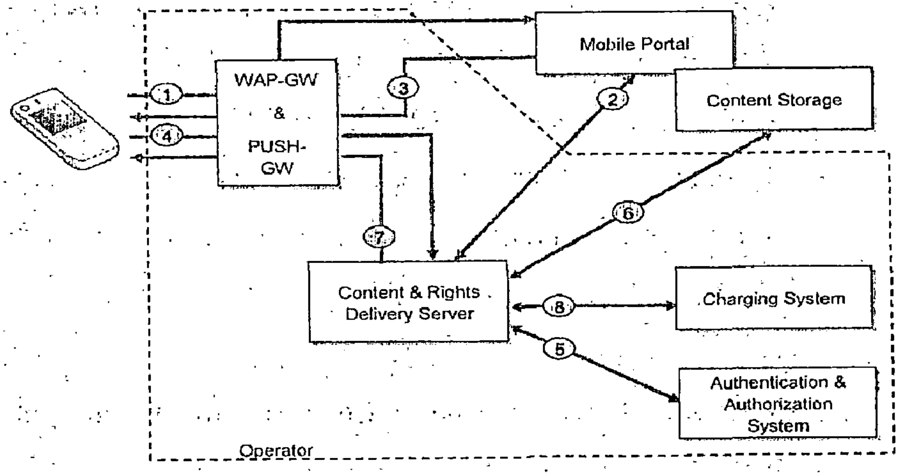


FIGURE 2.3 MDRM platform operations

2.1.5 Mobile DRM Standardization and Initiatives

The standardization forums working on MDRM are as follows

Third Generation Partnership Project

Third Generation Partnership Project (3 G P P) is a collaboration agreement between a numbers of standardization organizations established in December 1998. 3GPP's goal is to provide globally applicable technical specifications for third generation mobile communications (3G) systems.

Open Mobile Alliance

Open Mobile Alliance (O M A) was founded in June 2002 by the Open Mobile Architecture initiative and WAP Forum. OMA's goal is to introduce open standards and specifications based upon market and customer requirements for mobile industry. Among the almost 300 members are such companies as Ericsson, Microsoft, Motorola, Nokia, Openwave, Siemens, DoCoMo, Vodafone, and Sonera.

Moving Picture Experts Group

The Moving Picture Experts Group (M P E G) was established in January 1988. MPEG is a working group inside the International Organization for Standardization (I S O) and it defines global standards for the compression, decompression, processing, and coded representation of moving pictures and audio. MPEG uses the term Intellectual Property Management and Protection (1 P M P) for DRM and it is incorporated in the M PEG-4, MPEG-7, and MPEG-21 standards. MPEG-4 can be described as a standard for multimedia for the fixed and mobile web, MPEG-7 as a standard for the description and searching of multimedia content, and MPEG-21 as a multimedia framework targeted for bringing together the existing elements of delivery and consumption of multimedia content. IPMP Extensions for MPEG standards should be available in 2003 according to the MPEG work plan.

2.1.6 The Future: DRM System with Trust and Security Model [8]

From a security point of view, the current mobile DRM standard, OMA DRM 1.0, is quite lightweight. The rights object or the content encryption key (CEK) is not protected. The device or the DRM Agent is not authenticated prior to issuing rights. All this makes it relatively easy to circumvent the DRM protection.

The next release of OMA DRM is believed to include a more sophisticated trust and security model. Typically, such a model is based on public key infrastructure (PKI) concepts, although other methods are also possible. In PKI, trust and key management is based on public key cryptography, certificates, digital signatures and trusted third parties (certification authorities)[7]

In a more advanced system, each DRM Agent and/or device has a proof of its compliance, and this proof is presented to the rights issuer before the rights and the CEK for the content are issued. Also, it is possible for the device (user) to authenticate the rights issuer in a similar way. The rights object and the corresponding key are bound to the device so that it is useless in any other device. Therefore, the rights can be delivered using any delivery method, not only WAP PUSH. The system also makes it possible to revoke compromised devices so that no new content (rights) is issued.

Naturally, more advanced security makes the system more complicated. In the case of PKI, each device needs a private/public key and a certificate in tamper-resistant storage. It is also necessary to authenticate any DRM Agent (for example media player) that tries to access the sensitive information. Also, on the server side, more infrastructure is needed. Software implementers, device manufacturers and content providers (rights issuers) need mutual trust, which in a PKI system is implemented as a trust hierarchy. This means certification authorities, certification procedures, and mechanisms for delivering the information on compromised devices and software (for example, certificate revocation lists).

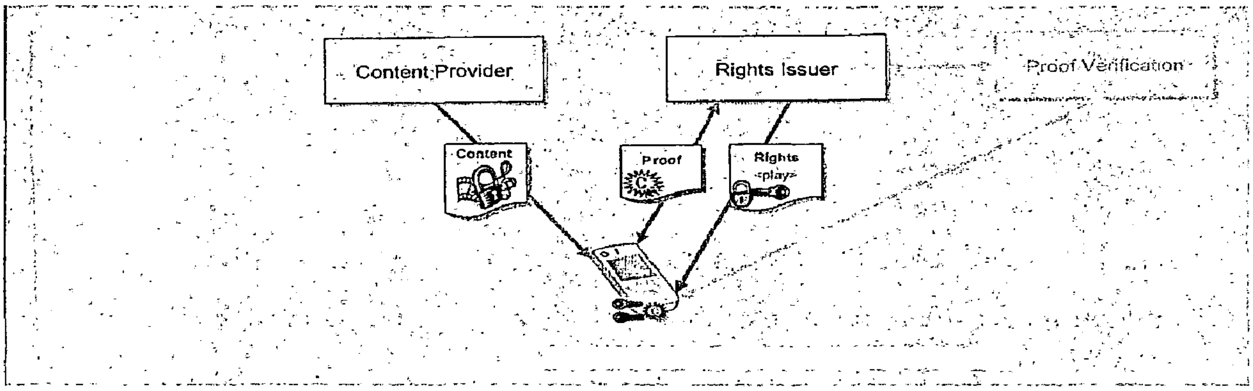


FIGURE 2.4 PKI Base DRM Systems

Content delivery in a PKI based DRM system (Figure 2.4) is quite similar to the separate delivery case. However, in this case the device's compliance is checked before the rights are granted. Also, the rights are protected (for example, encrypted with the device's public key).

2.2 Secure Digital Music Initiative (SDMI)[2]

The Secure Digital Music Initiative (SDMI) is a forum that has brought together more than 200 companies and organizations representing information technology, consumer electronics, security technology, the worldwide recording industry, and Internet service providers.

SDMI's charter is to develop open technology specifications that protect the playing, storing, and distributing of digital music such that a new market for digital music may emerge.

The open technology specifications released by SDMI will ultimately:

- Provide consumers with convenient access to music both online and in new emerging digital distribution systems,
- Enable copyright protection for artists' works, and
- Promote the development of new music-related business and technologies.

SDMI is not producing a single format, technology, or design. The SDMI frameworks allow a variety of competing technologies and download formats to be used within its system.

According to the SDMI forum any application must have following features to implement DRM.

2.2.1 Watermarking of Contents

Watermarking of contents means that whenever a content is played on any DRM compliant player, that content will be marked by a key so that if the same file illegally copied by someone else or illegally distributed is played on another player, it will report an error message and also indicate to the content owner that the content has been Illegally copied.

Thus inhibiting illegal copying and distribution.

2.2.2 Individualization of Player

Individualization of player means that every player is unique i.e. for every player a unique identification key exists which will allow the content publishers, providers, and owners to implement watermarking of contents, and also to maintain the identity and authenticity of the user.

2.2.3 Disabling Digital Output

Disabling digital output of the sound card is very important since even after following the secured audio path model the contents can be captured from that digital output port.

Which can then be further reproduced in any digital format, thus not solving the overall cause of the system.

The **DRM Kernel Component** provides two basic features that protect the integrity of encrypted music.

First, the DRM client and the DRM kernel component are in communication when a music file is played. This communication between components prevents anyone from tampering with the encrypted signal or from inserting false information.

Second, the DRM kernel component does not decrypt the music signal until all remaining components are authenticated. That is, before decrypting content and passing it to the next system component, the DRM kernel component verifies that each remaining component in the path to the sound card (each component that can access the content) is signed with a certificate from Microsoft. The absence of a signature can indicate that the component is a false driver or in some other way suspicious. So, if any of the remaining component fail validation test by the DRM kernel, the signal is halted. Otherwise, if all components pass validation, the DRM kernel component decrypts the music and passes it to the next component.

Microsoft digitally signs drivers that pass the Windows Hardware Quality Lab (WHQL) tests to assure consumers that they are using the highest-quality drivers. This practice is standard and guarantees the authenticity of component because the signature cannot be forged, nor can the code be modified without destroying the signature. Drivers included with Windows ME are updated and signed. Drivers that are not signed for use with Windows ME cannot play packaged files that require both Secure Audio Path and signed drivers.

Secure Audio Path is a feature of Windows Millennium Edition and is an improvement to the digital rights management (DRM) model. In the current digital rights management model (used by Microsoft and all other DRM systems on the market today), when packaged digital music is played, the encrypted content passes to the digital rights management client. The DRM client verifies that the player and the component developed with the Microsoft® Windows Media™ Format Software Development Kit (SDK) is valid. If they are valid, the DRM client decrypts the content and sends it to the player, which then sends it to the audio components. At this point, the decrypted music is available to applications and plug-ins that can intercept the music, leaving it susceptible to tampering. The content is then passed to other system components until it reaches the sound card and is played.

In the Secure Audio Path model, the player does not decrypt the content. Instead, it is passed in an encrypted state until it reaches system components in the computer kernel. Before decrypting and passing the content on to any other components, a DRM kernel component verifies that all remaining components in the path to the sound card are valid and authenticated. When this verification is completed, the content is decrypted and the music is played.

In the Secure Audio Path model, applications cannot be used to modify packaged music in any way. For example, when an application is used to intercept a music signal, the signal sounds like random noise. As a result, applications used to modify signals (such as an equalizer) cannot change the sound of the music.

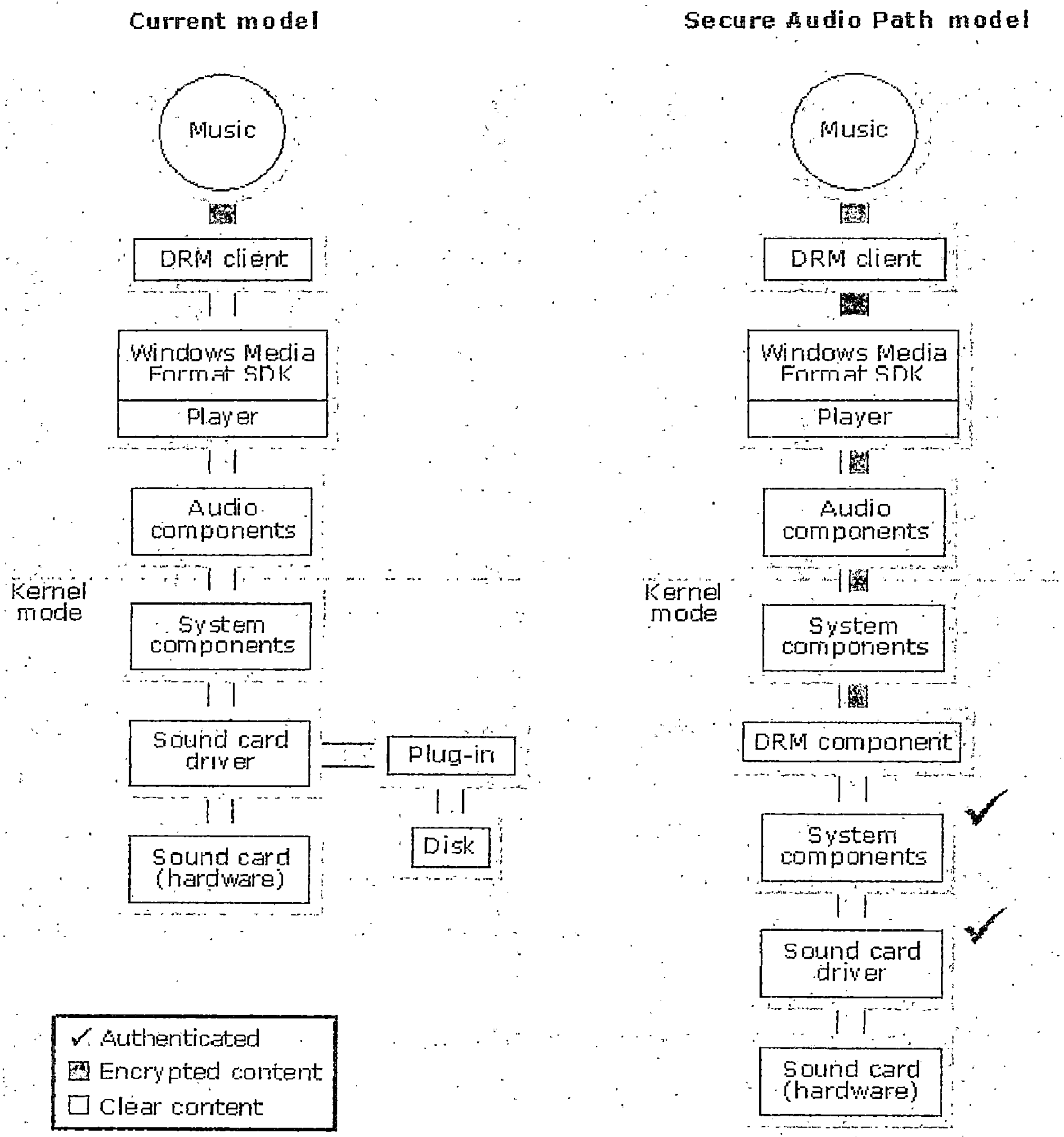


FIGURE 2.5 Secure Audio Path Model

Some applications are used to view a music signal. For example, some applications display flashing lights in time with the music signal, but do not modify it. To accommodate the use of such applications, a small part of the music is decrypted and passed in clear form with the encrypted content. The resulting signal is very poor (worse than telephone quality) but suffices for applications used to view signals.

2.3 Open Mobile Alliance (OMA)[3]

Downloading content to a mobile phone has been big business for years, with most mobile users at some time or another downloading icons or ring tones. Analysts at Jupiter Media Metrix have stated that in 2001, users in Europe have spent 590 Million Euros on content for their mobile phones. Nokia and other companies have launched Java-enabled phones for the mass market, creating an even bigger potential mobile content market. With the availability of content types today such as Java applications and MIDI ring tones, as well as phones with multimedia capabilities, the whole business of content downloading is set to boom. Digital rights management protects the rights of all in the supply chain and offers them an extension to the current model of distributing and selling their content. Content owners need to know they will be paid for the use of their content, operators need to be able to bill fairly for content and the whole issue of how to control content distribution must be addressed.

The Open Mobile Alliance (OMA) has tackled these issues with the standardization work of the OMA download, which includes:

1. Applying Digital Rights Management (DRM) to content and its distribution,
2. Enabling controlled (i.e. reliable) delivery of generic content objects.

DRM will prevent illegal distribution of media objects and provide new business models such as preview, super distribution, gifting, rights updates and more. For example, a user can download a MIDI ring tone or game to his mobile for a day or a week, and be given the option to buy refreshed rights after his original rights have expired.

2.3.1 Benefits of DRM

For content providers, DRM will provide new opportunities and distribution channels. Such benefits will encourage developers to produce more applications and high quality content, safe in the knowledge they will be paid properly for their work. DRM will benefit users who will have a wider range of high quality content for consumption, preview capability and more flexible ways of paying for content such as subscription, super distribution and refreshing rights for earlier downloaded content. Higher usage of content download services means higher data traffic and revenue per user for operators. Operators can build on the existing content download services and attract more downloads with the variety of business models. DRM technology allows content to be distributed in a controlled manner. Market demands may otherwise lead to "do-not-forward" any type of content policy, as is already the case with the existing business today.

2.3.2 The OMA proposal for DRM

The new OMA DRM version 1.0 standard will govern the use of mobile-centric content types, whether it is received by WAP download or MMS. This is the world's first mobile DRM standard. OMA DRM version 1.0 was officially approved in October 2002. The standard provides three DRM methods:

Forward-lock -intended for the delivery of news, sports, information and images that should not be sent on to others. This applies often to subscription-based services. The device is allowed to play, display or execute, but it cannot forward the media object. The content itself is hidden inside the DRM message that is delivered to the terminal. A DRM message contains a media object and an optional rights object. In the forward-lock method, the DRM message contains only the media object.

Combined Delivery – enables usage rules to be set for the media object. This method extends Forward-lock by adding a rights object to the DRM Message. Rights define how the device is allowed to render the content. Rights can be limited using both time and count constraints. This method enables the preview feature.

Separate Delivery – protects higher value media and enables super distribution, which allows the device to forward the media, but not the rights. This is achieved by delivering the media and rights via separate channels, which is more secure than combined delivery. The media is encrypted into DRM Content Format (DCF) using symmetric encryption, while the rights hold the Content Encryption Key (CEK), which is used by the DRM User Agent in the device for decryption.

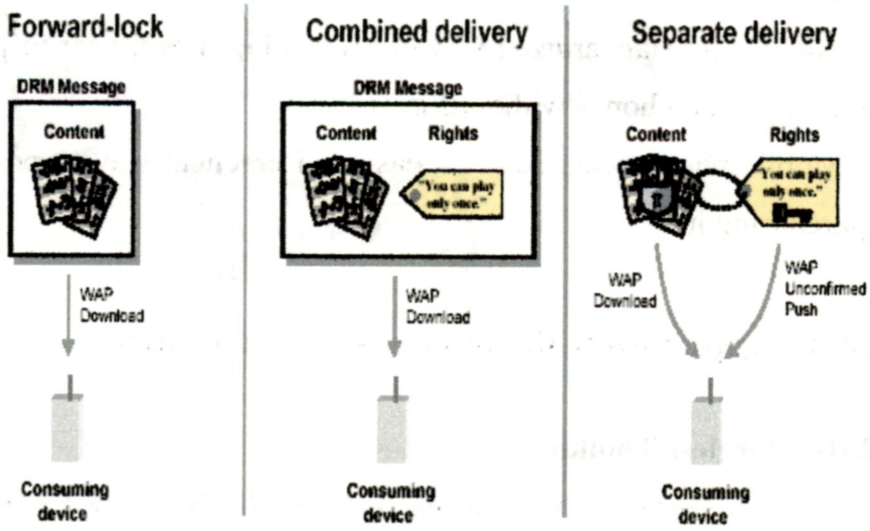


FIGURE 2.6 OMA Delivery Methods

Super distribution is an application of Separate Delivery that also requires a Rights Refresh mechanism that allows additional rights for the media. Recipients of super distributed content must contact the content retailer to obtain rights to either preview or purchase the media. Thus, the separate delivery method enables viral distribution of media maximizing the number of potential customers while retaining control for the content provider through centralized rights acquisition.

2.3.3 The way forward

The next phase of DRM technology should enable increased security to ensure authenticity and integrity of both content and rights. Higher security is important to protect applications as they become more sophisticated and hence, higher value. Examples of such content include high quality music, Symbian applications, audio and video streams. This will enable protection, content backup, distribution and adaptation to new value chain configurations.

Nokia is committed to the OMA DRM work and plans to have terminals and servers compliant with this new OMA standard. The standardization work in OMA Download includes both Digital Rights Management and Over-The-Air Download of Generic Content.

The version 1.0 concentrates on having an early-stage simplified MDRM standard that can be implemented rapidly. The standard is developed mainly to solve two problems.

- There is no standardized way of preventing illegal peer-to-peer content delivery that exists on phones without forward-lock.
- Mobile phone users have no easy and practical way to preview content before purchasing it.

2.4 Mobile Application Development Environment

2.4.1 J2ME Wireless Toolkit

The *Java*^{TM} *2 Platform, Micro Edition, Wireless Toolkit User's Guide* describes how to install, configure and work with the J2ME^{TM} Wireless Toolkit and its components.

The J2ME Wireless Toolkit supports the development of Java applications that run on devices compliant with the Mobile Information Device Profile (MIDP), such as cellular phones, two-way pagers, and palmtops.

2.4.1.1 Overview

The J2ME Wireless Toolkit supports a number of ways to develop MIDP applications. You can carry out the development process by running the tools from the command line or by using development environments that automate a large part of this process.

The KToolBar, included with the J2ME Wireless Toolkit, is a minimal development environment with a GUI for compiling, packaging, and executing MIDP applications. The only other tools you need are a third-party editor for your Java source files and a debugger. For more information on the Ktoolbar.

An IDE compatible with the J2ME Wireless Toolkit provides even more convenience. For example, when you use the Sun ONE Studio 4, Mobile Edition, (formerly ForteTM for JavaTM) you can edit, compile, package, and execute or debug MIDP applications, all within the same environment.

This section describes the phases of MIDP application development outside of editing, and how the toolkit contributes to these phases. The phases are illustrated in the following diagrams.

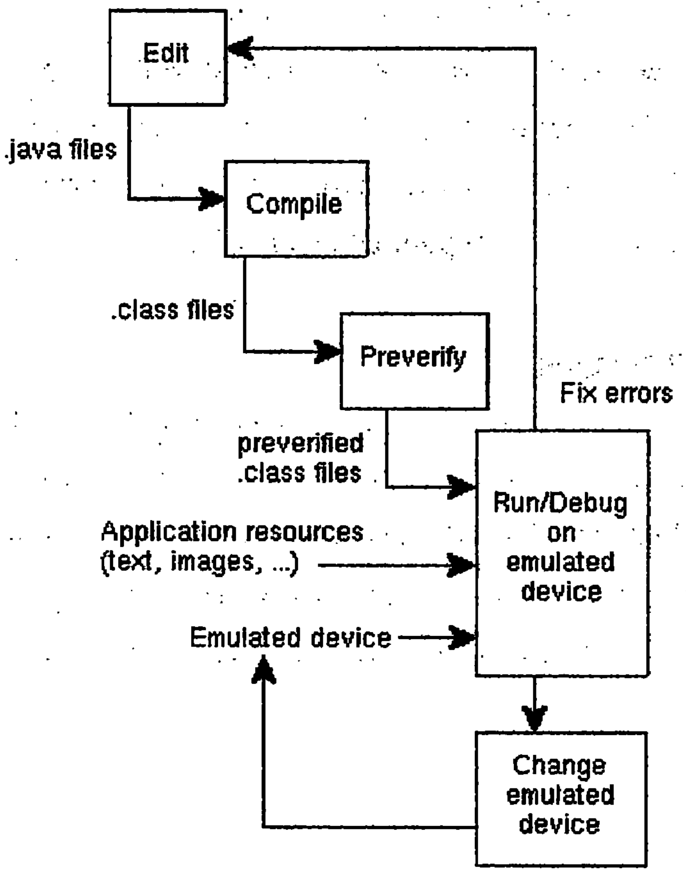


FIGURE 2.7 – Developing and Testing an Application

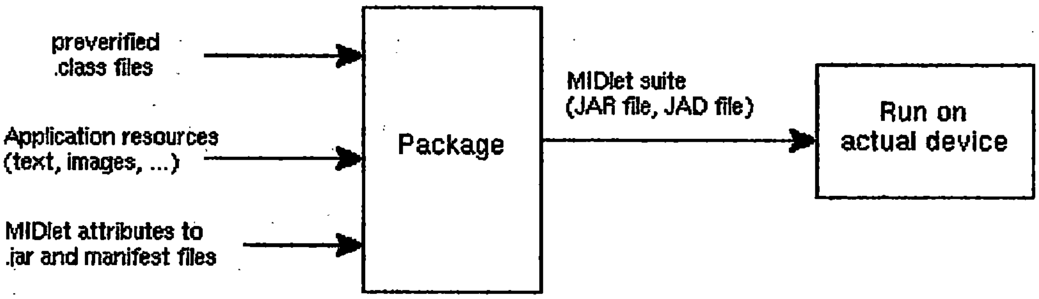

preverified .class files
Application resources (text, images, ...)
MIDlet attributes to .jar and manifest files
Package
MIDlet suite (JAR file, JAD file)
Run on actual device

FIGURE 2.8 – Packaging an Application

2.4.1.2 Compilation and Prefabrication

When you use KToolbar or a toolkit-compatible environment, such as the Sun ONE Studio 4, Mobile Edition, the environment compiles your source files for you, using the Java 2 SDK, Standard Edition (J2SETM SDK) compiler.

After compiling the sources, the development environment passes the generated class files to the Preverifier. This tool rearranges bytecodes in the classes to simplify the final stage of bytecode verification on the CLDC virtual machine. It also checks for the use of virtual machine features that are not supported by the CLDC.

2.4.1.3 Running and Debugging

When you use KToolbar or a toolkit-compatible environment such as the Sun ONE Studio 4, Mobile Edition, you can run and debug applications within the environment using the Emulator, which simulates the execution of the application on different target devices. The Emulator enables you to approximate the experience a user has with an application on a particular device, and to test the portability of the application across different devices.

2.4.1.4 Packaging

MIDP applications, or MIDlets, are packaged into a MIDlet suite, a grouping of MIDlets that can share resources at runtime. The following diagram illustrates how a MIDlet suite is organized.

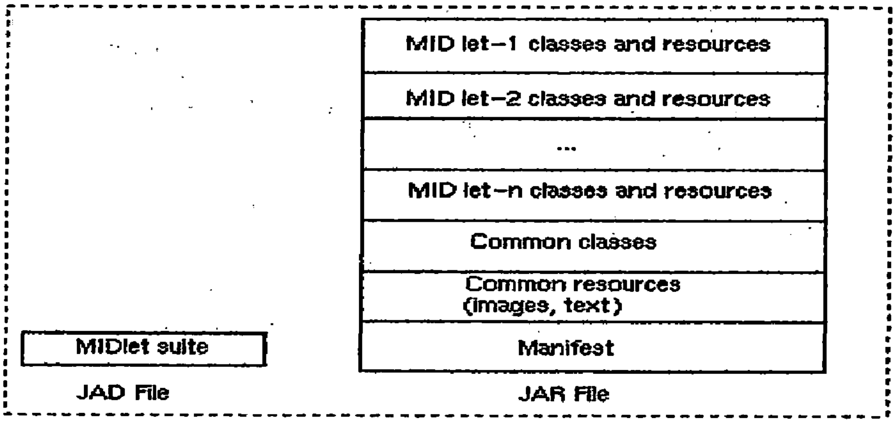

MID let-1 classes and resources
MID let-2 classes and resources
...
MID let-n classes and resources
Common classes
Common resources (images, text)
MIDlet suite
Manifest
JAD File
JAR File

FIGURE 2.9 – MIDlet Suite Components

More formally, a MIDlet suite includes:

- A Java Application Descriptor (JAD) file.

This file contains a predefined set of attributes (denoted by names that begin with "MIDlet-") that allow application management software to identify, retrieve, and install the MIDlets. All attributes appearing in the JAD file are made available to the MIDlets. You can define your own application-specific attributes and add them to the JAD file.

- A Java Archive (JAR) file.

The JAR file contains:

  - Java classes for each MIDlet in the suite.
  - Java classes shared between MIDlets.
  - Resource files used by the MIDlets (for example, image files).
  - A manifest file describing the JAR contents and specifying attributes used by application management software to identify and install the MIDlet suite.

Development environments such as KToolBar and the Sun ONE Studio 4, Mobile Edition automate the packaging of MIDlet suites. To package MIDlet suites from the command line, you need the J2SE SDK JAR tool to create JAR files, and a text editor for creating JAD files.

2.4.1.5 Packaging Obfuscated Source Code

An additional feature of the J2ME Wireless Toolkit is the ability to build an obfuscated package. You are required to obtain a code obfuscator plug-in to use this feature. The JAR file for the code obfuscator should be placed in the *j2mewtk.dir*\bin directory.

Obfuscation removes extraneous class information, such as local variable names. Classes, methods, interfaces, and such are renamed so as to make them ambiguous. An obfuscated package protects your project files from decompilation and reverse engineering. In addition to protecting your source code, the obfuscation process reduces the size of the classes resulting in smaller JAR files. The details of how code is obfuscated is dependent on the specific code obfuscator you choose to use.

When creating an obfuscated package, preverification is done after the code has been obfuscated rather than immediately after compilation.

2.4.2 Nokia Developer's Suite for J2ME

Nokia Developer's Suite for J2ME™ allows content creation for MIDP versions 1.0 and 2.0. It provides you with tools for creating MIDlet classes, creating and signing Application Packages (MIDlet Suites), emulating and deploying MIDlets and converting audio files to resources used by the MIDlets.

To create content for MIDP-2.0 profile, you should use Series 60 MIDP Concept SDK Beta 0.3, Nokia edition. For MIDP-1.0 MIDlets, use Nokia 7210 MIDP SDK 1.0 SDK. In this context, using an emulator refers to setting the desired SDK as the default SDK

In addition to content creation tools, help tools also exist for setting up the Nokia Developer's Suite for J2METM environment, which includes the content creation tools, SDKs/emulators and working directories.

The stand-alone installation of Nokia Developer's Suite for J2METM does not include tools for editing, compiling or debugging the MIDlet classes, you must use third party tools and a Java™ SDK for these purposes. The other option is to install Nokia Developer's Suite for J2METM integrated with an IDE such as Borland JBuilder or Sun ONE Studio, which provide the tools for editing, compiling and debugging MIDlets.

2.4.3 Mobile Media Application Program Interface

Many multimedia types and formats exist in today's market and new types and formats are being introduced all the time. There are also many diverse methods to store and deliver these various media types. For example, there are traditional storage devices (such as disk file systems, CDs and DVDs), wired protocols (UDP, HTTP, etc.) and wireless protocols (WAP, etc.).

J2METM devices range from cell phones with simple tone generation to Personal Digital Assistant and Web tablets with advanced audio and video rendering capabilities. To accommodate diverse configurations and multimedia processing capabilities, an API with a high level of abstraction is needed.

2.4.3.1 What is Mobile Media API?

The Mobile Media Application Programming Interface (MMAPI) provides support for multimedia applications on Java-enabled devices. The devices on which the media can be run can range from simple cellular phones to more sophisticated devices, such as PDAs and set-top boxes that support advanced sound and multimedia capabilities. This API allows simple access and control of time-based media, such as audio and video, and is both scalable and extensible to support more sophisticated multimedia features.

This API is an optional package, which can be implemented and used on most Java enabled devices. It can be run on a profile, such as MIDP, which is intended primarily for small, resource-constrained devices such as cellular phones, pagers, personal organizers, mobile Internet devices, and so forth. It can also be implemented to run on a configuration, which specifies the minimum required complement of Java technology components and libraries for small-connected devices. Examples of configurations and platforms on which the API can be implemented are the Connected, Limited Device Configuration (CLDC), the Connected Device Configuration (CDC), Personal Java™, JDK™, and J2SE™.

This flexible API has been designed to run with any protocol and format. For example, the API does not specify that transport protocols, such as HTTP or RTP (Real-time Transport Media), or media formats such as MP3, MIDI, or MPEG-4, have to be supported. However, the API contains all the functionality needed to support these protocols and many more. It allows API implementers and Java profile creators to choose which formats they will support.

2.4.3.1.1 Basic Concepts: Protocol and Content Handling

Basically, multimedia processing can be broken into two parts:

- Handling the data delivery protocol
- Handling the data content

Protocol handling refers to reading data from a source (such as a file, capture device, or streaming server) into a media processing system. Content handling usually requires processing the media data (parsing or decoding, for example) and rendering the media to output devices such as an audio speaker or video display.

Two high-level objects are used in this API:

DataSource and Player.

Each object encapsulates the two parts of media processing:

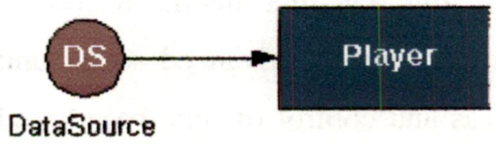


FIGURE 2.10 Protocol Handling

- DataSource for protocol handling
- Player for content handling

A DataSource encapsulates the protocol handling. It hides the details of how the data is read from source--whether the data is coming from a file, streaming server or proprietary delivery mechanism. DataSource provides a set of methods to allow Player to read data from a DataSource for processing.

A Player reads from the DataSource, processes the data and renders the media to the output device. It provides a set of methods to control the media playback and basic synchronization. Players also provide some type-specific controls to access features for different media types.

Finally, a factory mechanism, the Manager, creates the DataSources and Players and connects them together. The Manager permits custom DataSources and Players to be added so that new protocols and content types can be supported.

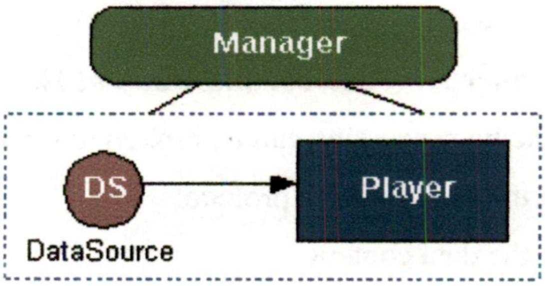


FIGURE 2.11 Factory Mechanisms

2.4.3.1.2 API Details

The createPlayer method is the top-level entry point to the API:

Player Manager.createPlayer(String urlString)

The urlString fully specifies the protocol and the content of the data:

<protocol>:<content location>

The Manager parses the URL and creates a DataSource to handle the data delivery protocol based on the specified protocol. The DataSource derives the content type from the data. The Manager then takes this content type and creates a Player to handle the presentation of the data. The resulting Player is returned for use by the application. The Player provides general methods to control the data flow and presentation, for example:

```
Player.realize()
Player.prefetch()
Player.start()
Player.setMediaTime(long time)
```

Fine-grained control is an important feature of the API; therefore, each Player also provides type-specific controls with the getControls and getControl methods:

```
Control[]Player.getControls()
Control Player.getControl(String controlType)
```

Since different types of media will yield different types of controls from its corresponding Player, the getControls and getControl methods can expose features that are unique to a particular media type. For example, for the MIDI type, you can get back a MIDIControl from the Player's getControl method.

DESIGN & IMPLEMENTATION

The objective of developing this application is to protect the rights of content owner thus inhibiting piracy along with implementing solution, which won't harm the revenue generation of network operators via super distribution.

Hence it basically enables mobile user download music right from his/her Mobile device. The dissertation application started with gathering resources that were needed to program for Mobile devices, which are listed below. After the requirements phase was over, the main task was to successfully establish a network connection of the Mobile device/emulator with the NGMA Server. Following that the goal remained as to implement successfully the HTTP connections with the HTTP firewall/servers of NGMA along with the addition of billing module i.e. user has to pay for each download and a part of that goes to content owner. The various system requirements for the above-mentioned phases are mentioned below:

3.1 Platform Used

Following is the description of the tools, languages and platform used in the development of this application.

Tools:	J2ME Wireless Toolkit Version 2.1(Beta), Mobile Emulator
Language:	Java Micro Edition
Platform:	Java Virtual Machine (JVM)

3.2 Requirements

- Java Enabled Mobile Phone with Polyphonic Support
- NGMA Server
- Mobile emulator
- Wap Support/Http ver 1.1 Support

3.3 Design Details

The components involved in the whole system are as follows

3.3.1 Licensing Management System (LMS)

The LMS issues well-defined licenses for purchasing entertainment content and maintains their record. This system comprises of the Master License Server (MLS) and Local License Server (LLS). There are more than one Local License Servers (LLSs). These license servers are environment-specific, i.e., the allocation of these license servers depends upon the environment of the player. The LLSs are allocated by the MLS. The MLS transfers the request to the LLS corresponding to the environment of the player. The main function of these LLSs is to provide the license to the player for playing the content. Functions of the Master License Server (MLS):

Transfer of Request

The MLS identifies the environment of the player and then transfers the request to the LLS corresponding to that environment.

Maintains the Record

The MLS keeps the record of all the licenses generated against each content and for each player/user.

Functions of the Local License Server (LLS):

When the billing process is complete, the Billing Server sends the message to the MLS, which then checks the environment of the player and accordingly forwards the request to the corresponding LLS.

Now the LLS, on the basis of the request and content IDs, generate the key-ID or the license-ID for that content.

After the generation of License, the License Server sends this license to the Session Manager, which then forwards the same to the player. Without this license-ID the user cannot access the content that he has purchased.

3.3.2 Billing Management System

All requests for purchase of content are directed to the Master Billing Server (MBS), which then transfers them to Local Billing Servers (LBSs) depending on the mode of payment. The processing of credit/prepaid cards for the purchase of content is done by the Local Billing Server (LBS).

Functions of the Master Billing Server (MBS):

Transfer of Request

When the request for the purchase of content comes in, it is forwarded to the MBS, which identifies the mode of payment and amounts the content/s and transfers the request to the corresponding LBS.

Maintains the Record

The MBS maintains the record of all the bills with respect to the purchase of each content.

Forwards the request to the Royalty Server

When the bill payment is cleared against the content, the MBS pushes the message to the Royalty Server. Functions of the Local Billing Server (LBS):

- The LBS checks the validity and processes the credit/prepaid cards and generates the invoice of the purchased contents.
- After the billing, it pushes the acknowledgement to the MLS.
- It also maintains the record of all invoices generated.

3.3.3 Royalty Management System

RMS is the database that stores most vital information about content owners. It keeps record of assigning royalties that are due to an artiste, producer, or association after a purchase is finalized, i.e., upon receipt of payment for the requested/ provided content.

Functions of the Royalty Server:

- The money generated through the sale of contents is divided by the Royalty Server on the basis of pre-decided percentage shares of each participant of the value-chain.
- It generates reports for stakeholders on the basis of content/s sold.
- It gets information from the Master Billing Server, the Master License Server and the Session Manager and synchronizes the same.

3.3.4 Advanced Search Engine

Basic functionality of the Advanced Search Engine is to search for the copyright contents over the web and then list those websites and IP addresses which host those contents illegally.

Functions of the Advanced Search Engine (ASE):

Creation of Extensive Database:

An extensive database of the entire valid URL across the web is created which web sites the crawler to access all the web sites across the world can use.

Web Crawler:

Basic function of the web crawler is to crawl through the "string sums" listed in our database and find all the unlisted sites and add them to our database.

Content Focused Searcher:

Basic function of the Content Searcher is to search our listed and related content(s) in the listed websites of our database and form a list of websites having our content. After this, a priority wise list of the web sites is made wherein the content is searched the next time.

3.3.5 Content Management System

The Content Management System (CMS) stores all information related to contents. It is like a warehouse that keeps record of licensing and billing of all contents. It also has record of contents purchased by each player and the time they are purchased. The CMS comprises of the Master Content Management System (MCMS) and the Local Content Management System (LCMS).

Functions of Master Content Management System (MCMS):

Search:

The MCMS searches contents from the database on the search criteria given by the User.

Transfer of request to the LCMS:

When the user is ready for the purchase of content, the MCMS searches the database to find the LCMS on which the particular Content is. Once found, the

MCMS transfers the request to that LCMS followed by the message push to the Master Billing Server.

Record Maintenance

It maintains the record of the content(s) purchased by each player with the date of purchase of content(s).

Functions of the Local Content Management System (LCMS):

- When the request for content reaches the MCMS, it is routed to the LCMS corresponding to that content. The network provider/ISP/digital distributor does this.
- After this, the LCMS initiates a search for the requested content in the database, which once found, is encoded into the requested format.
- The content is also encrypted with a content-key, so that the user can access it only after he/she has obtained the license for the same.
- The content is then delivered to the Session Manager, which then forwards it to the player.

3.3.6 Super-Distribution

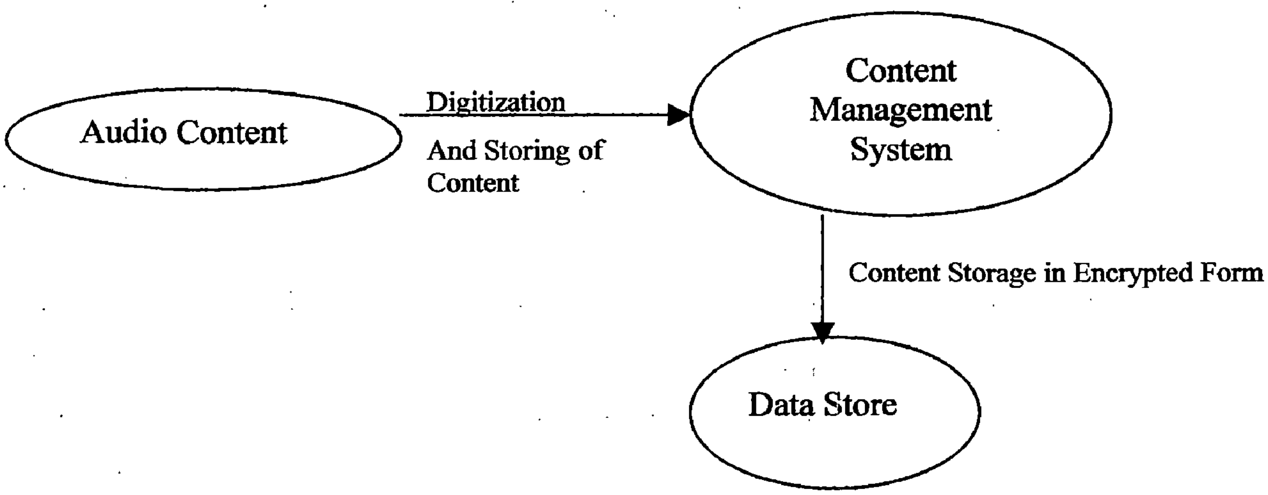
Super-distribution is the process where in one user forwards the content to another user and the Sender is billed for the content. We provide the super distribution facility for mobile contents enabling content owners and other stakeholders to get their fair share of revenue.

3.4 Implementation Details

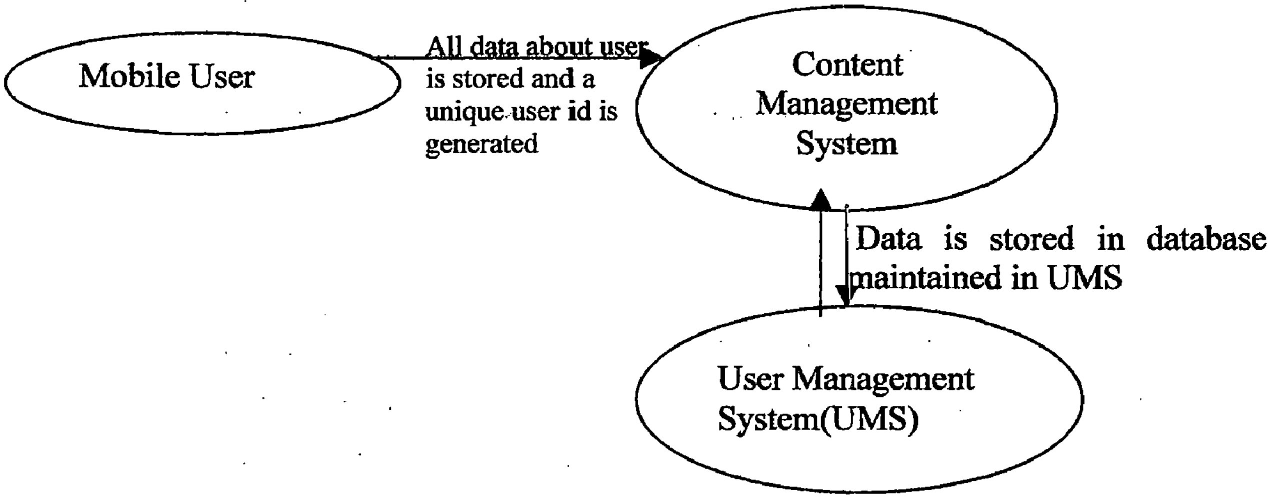
The step-by-step procedure is as follows:

Step 1: Content Registration

In this step the audio content in any format is entered into the content management system and the content is digitized. Also in this content owners are registered with the system and a unique ID is given to them as well as there content.

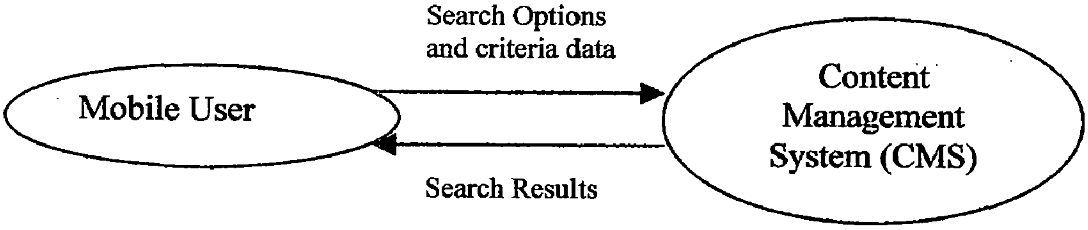


Step 2: User Registration


Mobile User
All data about user is stored and a unique user id is generated
Content Management System
Data is stored in database maintained in UMS
User Management System(UMS)

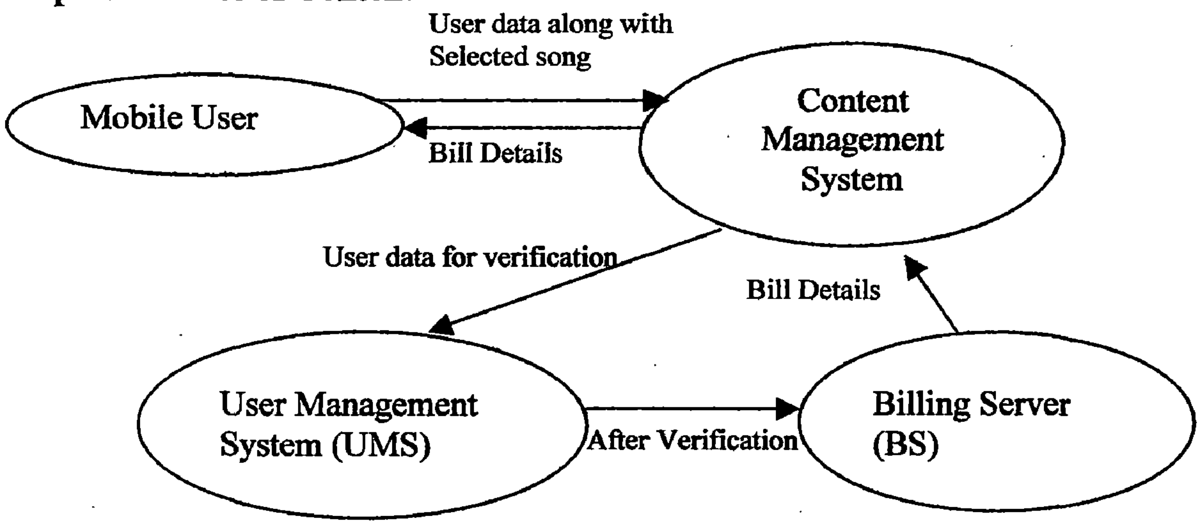
In this step user is registered into the system so that he can make use of the service. User enters user name, password and other necessary information and after processing (storage) data user management system generates user id and returns it back to user for future use.

Step 3 Searching of Contents


Search Options and criteria data
Mobile User
Content Management System (CMS)
Search Results

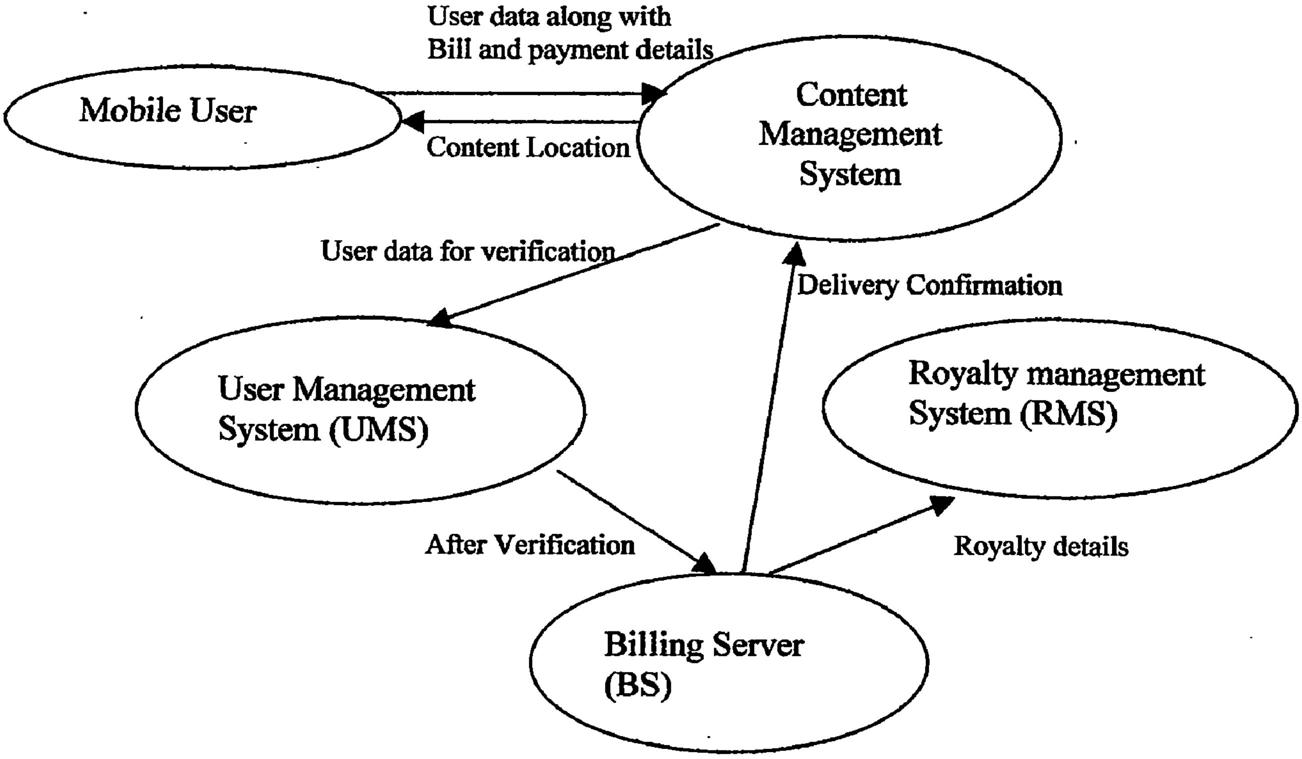
In searching of content, user selects the either of the three given option (song name, album name, artist name) and submit the keyword, content management system searches in its databases and send the result back to the user for further action.

Step 4 Purchase of Content



For purchasing contents user selects the song and send the user details to the CMS. Then CMS sends the user details to UMS for verification. Once user is verified, Billing Server generates the bill and sends to the CMS, which sends the bill details to user for further work.

Step 5 Payment of Content



RESULTS AND DISCUSSIONS

4.1 Work Completed

- Study of DRM Standards and Initiatives.
- Framework of the application is designed.
- Application interface with basic functionalities like billing user and searching contents is completed on PC.
- Application with searching functionality and billing module along with real time playback of audio contents from the web server is completed on Mobile
- Individualization of NGMA player being implemented.

4.2 Comparison

Comparison with two DRM systems that exist for mobile phones presently

- **Over-the-air delivery: forward lock mechanism**

  Over the air delivery has a drawback that it is implemented by forward lock mechanism, which cause loss to network operators since user are not able to send there content to other users thus affecting the overall network usage. The design implemented in this dissertation overcomes this by the use of separate delivery concept of OMA, i.e. encrypted content and rights to play/copy that are sent separately, thereby user can send content to other user but other user cannot play that content till it get the rights from the authorized server. Hence it maintains network usage as well as royalty option for content owner.

- **Via PC: Internet DRM managed by the PC**

  Internet DRM has one major drawback that it generally doesn't have any billing involved. Whole of the contents are not registered and hence are illegal. The dissertation design overcome this by involving a very strong billing module and content registration along with artist registration thus transparency is maintained throughout the process of acquiring content and selling them to user.

The main thing in the design discussed is to get maximum for all i.e. network operators should get maximum network usage and content owners should get the revenue of there work.

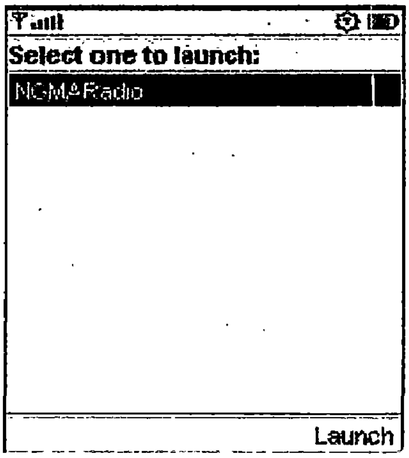
- DRM is not only for protecting content, but also a new way to sell and distribute content
- Everyone in the content value chain will benefit from a good DRM system

4.4 Future Work

- Working towards disabling digital output
- Enhancing the system by the use of Key Based Security System.[6]

4.5 Screen Shots of Mobile Application

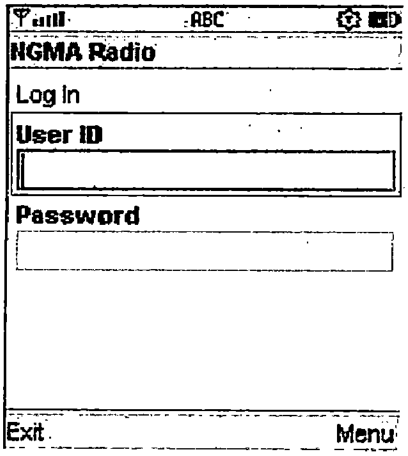
Figure 4.1 Application Start



Select one to launch:

NGMA Radio

Figure 4.2 User Login



NGMA Radio

Log In

User ID

Password

Figure 4.3 Select Option Login/Register

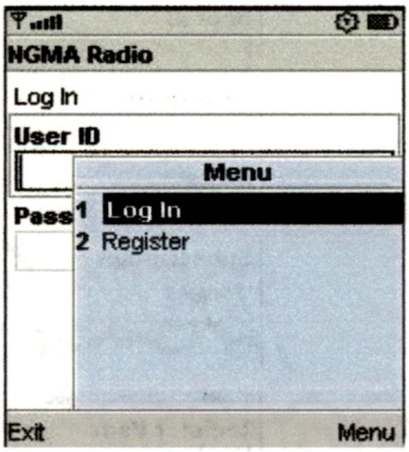
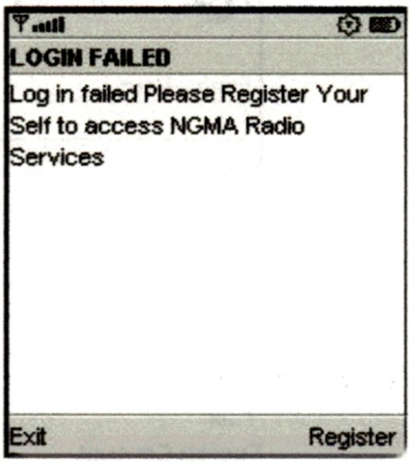
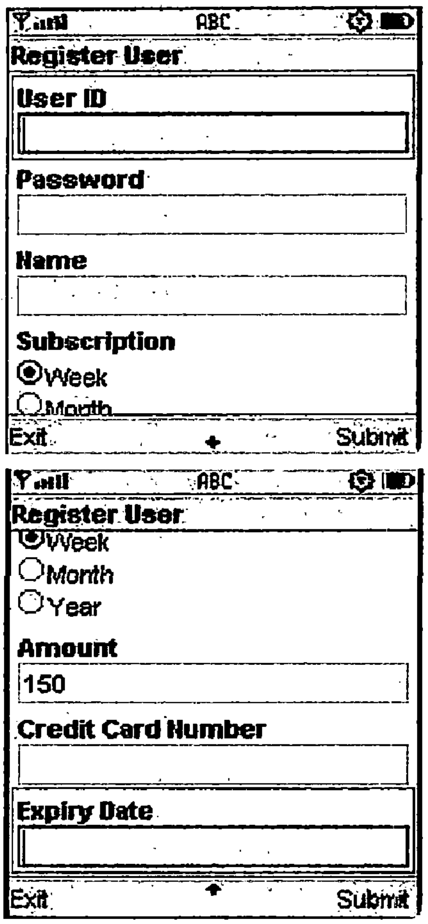


Figure 4.4 User login Fail



Log in failed Please Register Your Self to access NGMA Radio Services

Figure 4.5 User Registration form



Register User

User ID

Password

Name

Subscription

● Week

○ Month

Register User

● Week

○ Month

○ Year

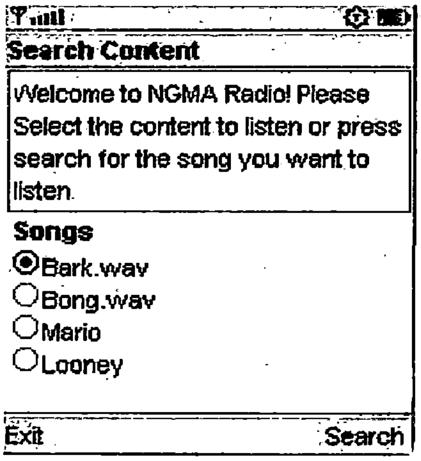
Amount

150

Credit Card Number

Expiry Date

Figure 4.6 Live Radio Content Select Form



Search Content

Welcome to NGMA Radio! Please Select the content to listen or press search for the song you want to listen.

Songs

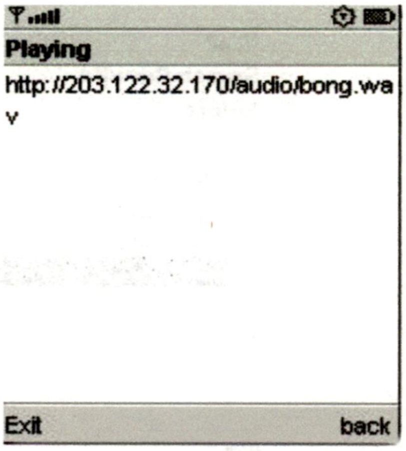
● Bark.wav

○ Bong.wav

○ Mario

○ Looney

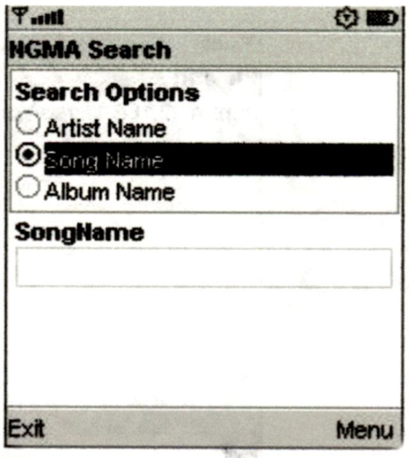
Figure 4.7 Playing Live Radio



Playing

http://203.122.32.170/audio/bong.wav

Figure 4.8 Search Form with Search options



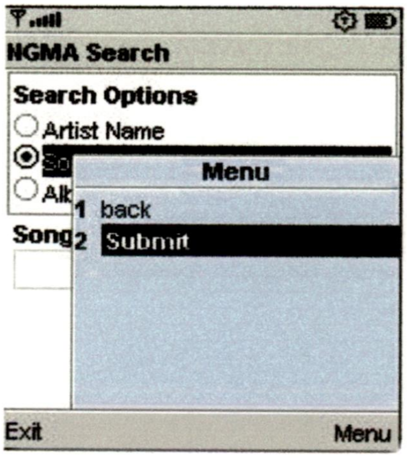
NGMA Search

Search Options

○ Artist Name
● Song Name
○ Album Name

SongName

Figure 4.9 Sending Request



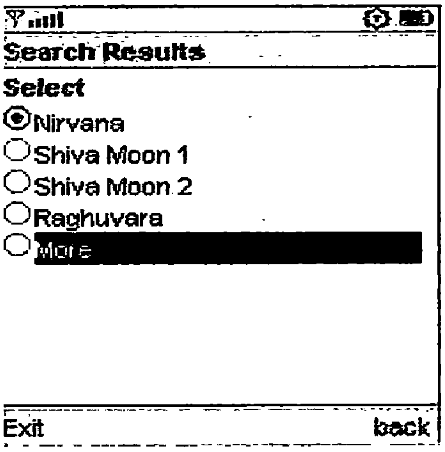
NGMA Search

Search Options

○ Artist Name
● So
○ Alk

Song

Figure 4.10 Display of Search Results on User Mobile Screen



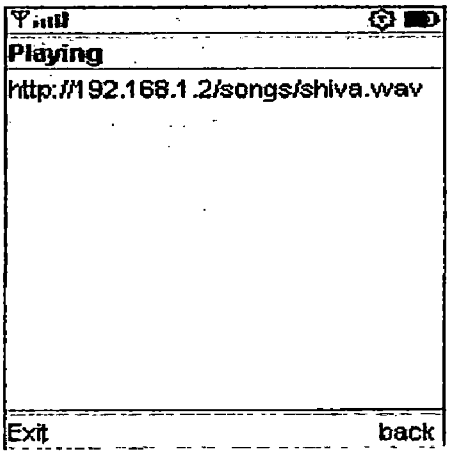
Search Results

Select

● Nirvana
○ Shiva Moon 1
○ Shiva Moon 2
○ Raghuvara
○ More

Exit back

Figure 4.11 Streaming the content from its IP



Playing

http://192.168.1.2/songs/shiva.wav

Exit back

CONCLUSION

Digital Rights Management is the key to protect content owner rights while at the same time enabling completely new ways for distributing content among friends and communities. This super distribution capability-seems to have a lot of potential in the mobile world. Although content services on the Internet have not yet taken off on a major scale, people are already used to the super distribution of content (jokes, pictures, music, video clips, etc.) using email and other services. In the mobile world, where one has the possibility of using operator's monthly subscription bill to aggregate micro transactions, people are thought to be willing to pay for polyphonic ringing tones, java games, screen savers, etc. This DRM protected commercial content could be downloaded from content servers, by MMS, or by super distribution from one's friends.

MDRM is becoming a reality - for example Nokia have committed to the OMA standard and has announced their first products (delivery server, content publishing toolkit) and client devices (Nokia 6220, available in the second half of 2003) that implement the OMA DRM 1.0 specification. In addition to Nokia, also other companies (for example, ACCESS, OM DSecure) are bringing OMA DRM solutions to the market and mobile operators, for example Vodafone, are embracing OMA DRM.

The development towards a more sophisticated MDRM system has already started at OMA. This system presumably has a trust and security model, for which one well-known solution is the public key infrastructure (PKI) based approach. The next OMA DRM release is expected in the late 2004 - early 2005 range, and first products some time after that.

Appendix A

ADDITIONAL RESOURCES

Initiatives, Forums and Associations:

3GPP	www.3qpP.orq
MPEG	mpeq.telecomitalialab.com
OMA	www.openmobilealliance.orq
XrML	www.xrml.orq
ODRL	www.odrl.net

Definitions, acronyms and abbreviations:

3G	Third Generation Mobile Communications Technology
3GPP	Third Generation Partnership Project
DRM	Digital Rights Management
HTTP	Hypertext Transfer Protocol
IPMP	Intellectual Property Management & Protection. MPEG's definition for DRM
MDRM	Mobile Digital Rights Management
MMS	Multimedia Message Service
MPEG	Moving Picture Experts Group
ODRL	Open Digital Rights Language
OMA	Open Mobile Alliance
PKI	Public Key Infrastructure
SMS	Short Message Service
WAP	Wireless Application Protocol
XrML	eXtensive rights Markup Language

REFERENCES

[1] Jukka Helin, Sonera Corp., Media Lab 2002, "Implementing and Capitalizing on DRM Structures for Mobile Content". IIR's 5th Mobile Data & Internet Services Summit

[2] Dr. Mathew, 2002, Secure Digital Music Initiative Version, 1.0, Jan 2002

[3] E. Levinson, OMA-Download-DRMCF-v1_0-20020708-p, Proposed Version 08-July-2002

[4] Secure Digital Music Initiative 's portable device specification and Phase I watermark, version 1.0, Mar 2002

[5] Sissel Henriette Larsen, 2003, "Mobile Content Market & Mobile Digital Rights Management". ETSI Workshop, Mobile Commerce Transactions.

[6] Dr. Kim, Hong Sun, 2003, "M-Commerce & Security". SecureSoft.

[7] Ahmet M. Eskicioglu, John Town, Edward J. Delp, 2003, "Security of Digital Entertainment Content from Creation to Consumption".

[8] Griffith Jones, 2003, "DRM in a Wireless World", OFTA 2-days Technical Workshop: Bridging the Gap - Development of Mobile Multi-media, Value-added and Content Applications in the New Era.