3GPP TSG SA WG3 Security — S3#23 **S3-020271**

14 - 17 May 2002

Victoria, Canada

TSG-SA Meeting #15 **TSG SA #15 (02) …**
Cheju,

TSG-SA WG 1 (Services) meeting #15 **S1-020659**
Saalfelden, Austria, 11-15th February 2002 **Agenda item: 10.7**

Presentation of Specification to TSG or WG

Presentation to:	**TSG SA Meeting #15**
Document for presentation:	**TS 22.xxx, Version 1.0.0**
Presented for:	**Information**

Abstract of document:

This TS defines the stage one description for digital rights management. Stage one is the set of requirements that shall be supported to enable digital rights management, from content packaging to secure storage and rendering.

This TS includes requirements applicable to the content authors and providers, UE and network manufacturers, which are sufficient to provide complete support of digital rights management.

Additional functionalities not documented in this TS are considered outside the scope of this TS. Such additional functionality may be on a network-wide basis, nation-wide basis or particular to a group of users. Such additional functionality shall not compromise conformance to the requirements of the rights management system defined in this specification.

Changes since last presentation to TSG-SA Meeting #14:

None

Outstanding Issues:

None

Contentious Issues:

None

3G TS 22.xxx 1.0.0 (2002-02)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital Rights Management; Proposed Stage 1 (Release 6)

Keywords
UMTS, service, streaming

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

Historically, content such as books, music, games, and videos have been delivered on paper, magnetic tape, and disks. The technology required to digitally copy and redistribute this content on a large scale prohibited the secondary market from having much affect on revenues from content sales. With large decreases in the cost of technology, e.g. storage space and recordable digital media, and greater Internet bandwidth, services like Napster and Gnutella have sprung up to allow massive redistribution of music and similar content. At the same time, the absence of protection of rights associated with this kind of content in the digital environment has so far prevented the use of Internet as a distribution channel for valuable content.

With the advent of faster wireless networks and increasingly capable user equipment, the mobile environment will soon become another avenue for distributing valuable content. This will require taking steps to establish a model for protecting the rights of the content providers when distributing digital content in the mobile environment.

This specification defines the requirements for the support of digital rights management in the wireless network. The use cases defined in section 0 should be taken into account when defining a secure, consumer-friendly rights management system.

1 Scope

This TS defines the stage one description for digital rights management. Stage one is the set of requirements that shall be supported to enable digital rights management, from content packaging to secure storage and rendering.

This TS includes requirements applicable to the content authors and providers, UE and network manufacturers, which are sufficient to provide complete support of digital rights management.

Additional functionalities not documented in this TS are considered outside the scope of this TS. Such additional functionality may be on a network-wide basis, nation-wide basis or particular to a group of users. Such additional functionality shall not compromise conformance to the requirements of the rights management system defined in this specification.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.905: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications

3 Definitions, symbols and abbreviations

3.1 Definitions

Consumer

User granted the right to access content.

Content

An image, a piece of music or a video, a book, an article, a game, an executable program or similar. Content may be delivered on its own (e.g. download or streaming of music), as part of some message (e.g. an image or music in an MMS or Email message), as part of some web content (e.g. an image in a web page), and so on.

Content Provider

An entity that distributes content to consumers. The distributor may itself be a rights holder, or may distribute content on behalf of or with permission from a rights holder.

Protected Content

Content that is subject to protection by the DRM system.

Render

To provide a visual or audio representation of content, execute content, etc.

Rights Holder

An entity owning the intellectual property rights (e.g. copyright) to content.

Super distribution

Redistribution of content from a consumer to one or more secondary recipients. Secondary recipients may, for example, receive a free sample as defined by the usage rights, or purchase new rights to render the content, and so on.

Trust

Trust is used to denote the level of trust put in a UE to uphold and enforce usage rights for protected contents.

Usage Rights

Usage rights describe how a protected content may be used, including permissions (e.g. play, view, execute), constraints (e.g. ten times, for one month), etc.

User Equipment

A consumer device used to render, purchase, move, distribute and manipulate content.

3.2 Abbreviations

For the purposes of this document the following abbreviations apply:

3G	Third Generation mobile communications technology
DRM	Digital Rights Management
EMS	Enhanced Messaging Service
HTTP	HyperText Transfer Protocol
MMS	Multimedia Messaging Service
SMS	Short Messaging Service
UE	User Equipment

4 Digital Rights Management Model

The following model that describes rights management is not definitive, and no implementation model or architecture is implied or required by it. It is solely provided to describe the functions and roles that shall be provided by the entities involved in providing the DRM solution.

Digital rights management capabilities are required for content such as, but not limited to, ringtones, games, books, music, and video. The purpose of digital rights management is to provide an end-to-end solution, i.e. between a content provider and a UE, ensuring that rights associated with content are enforced, thus limiting illegal access.

The complexity of any DRM solution clearly will have a direct relationship with the value of the content being protected; the higher the value of the content, the higher the means which can be justified to protect it. It can be expected that 3G terminals will be able to render both “low-value” and “high-value” content. The definition of what value to associate with which type of content, however, is a decision to be made by the content provider and is therefore

out of the scope of standardization. Nevertheless, it shall be ensured that any standardized DRM solution is flexible enough to cater for the different values content may have.

Digital rights management is not a single entity or functionality. Rather, it involves a number of different components, for example:

- Expression of usage rights.

  Usage rights express what a UE may or may not do with an content. Rights include permissions (e.g. play, view), constraints (e.g. ten times, for one month) and so on. Usage rights are always managed end-to-end – they are defined by the content provider and enforced by the UE.

- Content protection

  A DRM solution should provide some means for protecting content, (e.g. encryption)

- Trust relationships

  A DRM solution should provide some means for ensuring the establishment of a trusted relationship between the UE and the content provider.

Considering that a DRM solution consists of different components, a DRM standard should allow a content provider to deploy those components that the provider deems necessary and justifiable for the distribution of content. At a minimum, however, it will be necessary to describe the rights associated with content. The use of content protection and strong trust models should be optional for content provider.

In order to ensure a reasonable pace in the standardization of DRM existing standards for the individual DRM components should be re-used as far as possible and feasible. Further, to maximize interoperability, and to reduce terminal complexity, there should be one standardized solution for a rights description language, one solution for content protection and one solution for trust relationships as part of the 3GPP DRM standard. Options should be avoided as far as possible.

On the other hand, it needs to be acknowledged that DRM component solutions will evolve over time, and content providers may wish to deploy more advanced solutions in the future, e.g. more advanced and robust cryptographic algorithms to protect their content. Therefore, a standardized DRM solution should be extensible. However, such an evolution should occur within a tight standardization process that minimizes the number of parallel solutions existing in the market.

Distribution of content should be possible over any kind of transport; for example pull from a browser, end-to-end secure connections, streaming media, messaging (e.g. MMS, Email), local transfer (e.g. IrDA, Bluetooth), etc. There should be only one solution for digital rights management for any kind of delivery mechanisms.

A high-level model for digital rights management may be described as follows:

- Protected content, and associated usage rights, may be distributed from content providers to UEs

- The UE enforces usage rights, and prevents any unauthorised use of the content.

- If the usage rights allow, content may be distributed or moved, and accessed by the receiving UE if granted the rights to do so. The content provider may specify alternative usage rights to be applied to copies (e.g. limited ‘preview’ style rights).

- The content provider may modify or renew usage rights, e.g. when rights expire or an upgrade is requested by a user.

5 High level requirements

5.1 General Requirements

1. The DRM standard shall provide a mechanism allowing content providers to send usage rights to a UE, and to associate usage rights with content. The mechanism shall allow usage rights to be enforced.
2. It shall be possible to separate usage rules and content physically, but not logically.
3. The DRM standard shall allow usage rights and content to be delivered via the same or different transport mechanisms.
4. Usage rights shall be unambiguously bound to content.
5. The DRM standard shall impose minimal signalling and computational load.
6. The DRM standard shall be transport independent.
7. There shall be only one solution for digital rights management for any kind of delivery mechanisms and any type of content.
8. The DRM standard shall encompass the specification of at least the following three components: description of rights, content protection and establishment of trust relationship.
9. For each component one concrete mechanism shall be specified.
10. DRM shall allow content providers to use those DRM components that are appropriate for their content. As a minimum, content providers shall be able to express rights. Implementation of content protection and establishment of trust relationship shall be optional for content providers.
11. DRM shall be extensible, i.e. allow evolved DRM component solutions to be deployed. This extensibility shall occur within a tight standardisation process. Within each version of a DRM specification, if feasible, there shall be only one solution specified for each DRM component.
12. The DRM standard shall be specified as an open standard and re-use existing open standards as appropriate.
13. The DRM standard shall work reliably in environments where fragment loss (e.g. packet loss or bit errors) of information may be encountered.

5.2 User Requirements

1. The user experience shall not be impaired by the DRM standard.
2. The DRM standard shall permit users to be informed about the rights status of protected content.
3. The user shall be able to manage rights independently from content : e.g. he/she shall be able to delete a content, but to keep the corresponding rights (so that he/she could restore the content on the handset later without having to obtain new rights).
4. If the user change his/her UE , is shall be possible to make the already obtained rights and content available on the new UE.
5. With any received content, the user shall be able to find a reference to the location where corresponding rights can be obtained.

5.3 UE Requirements

1. The UE shall enforce any usage rights associated with protected content.
2. The DRM standard shall not prevent access to content that is not rights-protected.
3. The DRM standard must encompass removable storage. For example, if the UE stores protected content on removable media, e.g. memory cards, then the UE shall ensure that the content is protected from use by any other UE, unless access is allowed by the usage rights.

6 Usage Rights

1. The content provider shall generate the usage rights. Only the content provider may modify usage rights or remove the association between content and its usage rights.
2. The UE shall obey and enforce the usage rights.
3. Usage rights shall be stored securely.
4. The usage rights shall allow the content provider to specify different ways of handling the content (permissions) e.g. display, play, execute, copy, give etc.
5. The usage rights shall allow the content provider to specify different ways of restricting the use of content (constraints), e.g. number of times, elapsed time, alternative usage rights for copies, specific UE or group of UEs, etc.
6. The usage rights shall allow the content provider to specify, for example, the following additional information:
    - Where the content can be acquired, and where usage rights can be obtained or renewed.
7. The usage rights shall allow the content provider to specify content to be rendered on a set of DRM-enabled UEs, e.g., all devices owned by a consumer.

7 Security

1. The DRM solution shall provide a protection mechanism, allowing content providers to render content unusable to any but the intended UE.
2. The DRM solution shall provide one trust method, allowing content providers to establish a trust relationship with a UE.
3. Use of protection and trust methods should be optional for content providers.

8 Privacy

1. User information used to create the content licence shall not be disclosed without the explicit consent of the end user.
2. The user's identity shall not be disclosed to the content provider and/or to other parties without the explicit consent of the end user.

9 Charging

The DRM standard shall be able to support several charging mechanisms. The following charging mechanisms should be considered:

- Charging on a subscription basis.
- Charging on a pay before use (pre-pay) basis.
- Charging on a one-time basis for content download.
- Charging to receive streamed content.

The above list is not exhaustive.

10 Annex A (informative): Use cases

The following use cases help to describe the various aspects of the DRM standard and their impact on the consumer. Figure 1 depicts a high level view of how DRM fits into the content distribution model.

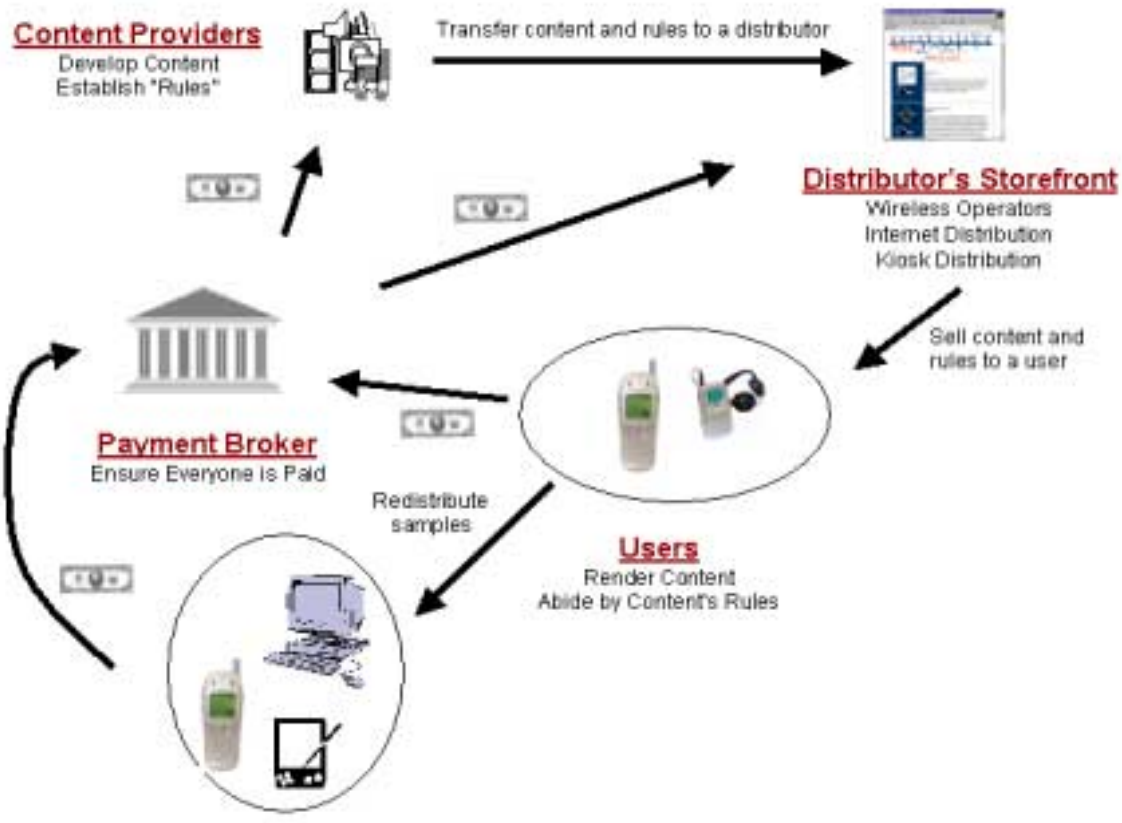

Figure 1 DRM and Content Distribution

Acquiring usage rights

When Alice wants to buy a song, she will simply browse a website with the UE and find the song she wants. The content provider may allow Alice to preview the available songs. After deciding on a song, she specifies which type of payment option she wants for the song. She chooses to buy the song, which gives her the right to play the song whenever she wants.

Content delivery

Once a song is downloaded, it can be accessed by Alice's UE according to associated usage rights. In either case, the new song title will be added to Alice's content list and Alice can play the song on her UE. Memory limitations on a UE may force Alice to keep some of her content in some other physical storage device, e.g. a memory card or a network store. The UE ensures that protected content is encrypted before storing it in this way. Alice may be made aware of which music is local and which is stored remotely by using a separate listing or special marks on local songs. If Alice knows that she wants to listen to certain songs many times, she may want to store these songs locally on the UE.

Alice and the content provider may employ any of the following means to download content to her UE:

- Downloaded from the server, POS, or kiosk and stored on a UE
- Streaming from the server, POS, or kiosk to one or more UEs
- Delivered using SMS, EMS, or MMS
- Delivered over-the-air, via a local connection or personal area network, or using other transport mechanisms

Content usage

Alice downloads the content to her UE, but would also like to play it on another DRM-enabled UE that she owns. The usage rights may allow her to transfer the song to the other UE and render it, according to the content usage rules.

While Alice is at work, the battery goes flat on her UE. After recharging her UE, she is able to access content saved in non-volatile memory, or backup copies saved on a memory card or in a network store.

A week later, Alice purchases a new UE. If usage rights allow, Alice may transfer her purchased content and play it on her new UE.

Super distribution

Depending on a song's usage rights, Alice may have the right to make copies and send them to other people. The copies may have another set of usage rights than Alice's original; perhaps only allowing limited access to the content while full access can be purchased from the content provider. If Alice's UE is capable of establishing a short-range ad-hoc network, transferring contents is made easier, and can rapidly lead to more content distribution and possibly increased content sales.

The samples that Alice distributes may consist of just a 20 or 30 second clip of a main portion of the song. Or, she may be allowed to distribute the song with the usage rights only allowing the song to be played one time. After the initial play, the user would have to purchase rights from the content provider to play the song again. Other types of sampling may also be possible.

Gifting Rights

Alice really likes the song and decides she wants to send it to Susan also. Alice contacts the content provider with her UE and pays to have content delivered to Susan. Susan receives the song, and is able to listen to it using the rights paid for by Alice. Alternatively, Susan may receive a notification that the song has been gifted to her and she can download it at her leisure.

Other Services

Additionally, other services may be provided within the DRM model. Examples include, but are not limited to:

- Trust services
- Authentication services
- Payment brokers
- Content bank (network storage of downloaded content)
- Rights locker (network storage of usage rights)

The content provider may run such services itself, or they may be provided as generic services by communication service providers.

11 Annex B (informative): Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	Work Item