3GPP TSG SA WG3 Security — S3#20 **S3-010532**

16 - 19 October, 2001

Sydney, Australia

From: **SA3**

To: **SA1, SA4, T2**

Copy: **SA2**

Title: **Initial comments on digital rights management**

Contact: Peter Howard
Email. peter.howard@vodafone.com
Tel. +44 1635 676206

SA3 have studied LSs received from S1 and T2 on digital rights management for MMS (S1-010877 and T2-010634, respectively) and from SA4 on digital rights management for streaming (S4-010534). In addition we note that since these LSs were sent, a work item on digital rights management to cover both MMS and streaming was approved at SA#13 (SP-010577). As suggested in the LSs and the work item, SA3 acknowledge that it has a role in assisting in the security aspects associated with Digital Rights Management (DRM).

As seen from the preliminary information provided in the LSs and in the work item, the security aspects of DRM are numerous and challenging. There are a large number of organisations and initiatives already dealing with DRM as listed in one of the attachments to the S4 LS (S4-010474). Therefore, before being able to assist in this work, SA3 request that the involved groups clarify to what extent 3GPP intend to standardise DRM. SA3 believe that at least three options (and combinations thereof) are possible. For each of these options the potential role of SA3 is described.

1. Standardisation of a general DRM framework (i.e. “hooks”, APIs, etc.)

   SA3’s role is expected to be minimal since the work to standardise a generic framework would not seem to involve the design or evaluation of any specific security components. However, SA3 might be able to assist in the clarification and understanding of the various security requirements that need to be addressed by security-related DRM functions that the framework must be able to access.

2. Standardisation of existing DRM solutions for 3GPP use

   SA3 could be involved in conducting security analyses of various DRM solutions to assist the selection process. Note however that this would require the necessary expertise on DRM technology (e.g. digital watermarking) to be provided in SA3 by 3GPP members.

3. Standardisation of new DRM solutions

   The design, specification and evaluation of the security components of a fully-fledged DRM solution is expected to be a large task. This would also require the necessary expertise on DRM technology (e.g. digital watermarking) to be provided in SA3 by 3GPP members.

To help analyse the problem, SA3 suggest that a separation is made between the protection of content and its associated rights during transport, and the subsequent enforcement of those rights at the user device (e.g. copy protection).

SA3 would like to inform the involved groups that it is generally impossible (at least in a cost-efficient manner) to completely eliminate the possibility for dishonest parties to override protection mechanisms. For instance, regarding copy protection, it may be possible to make abuse practically/economically infeasible for users with “regular” devices, whilst accepting that users with “rogue” or “illegal” devices may be able to “play” or redistribute content without being properly authorised to do so. It is expected that the effectiveness of DRM solutions will rely on the availability of “trusted” functionality in terminals.

SA3 looks forward to further co-operation with the involved groups on this work item.

Attachments:

S3-010419 (= S1-010877)

S3-010424 (= T2-010634)

S3-010436 (= S4-010534)

SP-010577

3GPP TSG SA WG3 Security — S3#20 **S3-010419**

16 - 19 October, 2001

Sydney, Australia

TSG-SA WG 1 (Services) meeting #12 TSG S1 (01) 877
Lake Tahoe, USA, 9-13 July 2001 Agenda Item:

Title: **LS on "Digital Rights Management"**

Source: **SA1**

To: **T2 and SA3**

Contact Person:
Name: **Tommi Kokkola**
E-mail Address: tommi.kokkola@nokia.com

SA1 have been discussing about protection of MMS message elements from unauthorised modification and forwarding.

SA1 was concerned on this issue but could not yet agree on specific requirements to MMS at this stage.

SA1 would like to invite T2 and SA3 to give further information related to "Digital Right Management" concepts. Specifically SA1 is interested in short- and long term solutions that could be used to protect MMS message elements and content in general within 3GPP system, i.e. solutions that could be applied over various transports provided by 3GPP.

3GPP TSG SA WG3 Security — S3#20 **S3-010424**

16 - 19 October, 2001

Sydney, Australia

SWG3#7 MMS ad-hoc
Braunschweig, Germany
27-29 June 2001

T2M010089
T2-010634 ***(e-approved)***

Title: MMS digital rights management

Source: TSG-T WG2

To: TSG-SA WG4

CC: TSG-SA WG1, TSG-SA WG3

Contact Person:
Name: Eskil Åhlin
Ericsson
E-mail Address: eskil.ahlin@ausystem.com
Tel. Number: Mobile +46 70 595 5177

TSG-T WG2 would like to thank TSG-SA WG4 for the comprehensive and useful information contained in the LS (tdoc S4-010429) regarding digital rights management (DRM).

TSG-T WG2 have identified a need for DRM to protect the content of multimedia messages that are being sent or received using the MMS. Further DRM in MMS is needed to provide rights ownership of the content. TSG-T WG2 welcomes the ongoing work by TSG-SA WG4.

TSG-T WG2 favours a generic DRM framework for all 3GPP defined services and for all different kind of contents and would like to see requirements from TSG-SA WG1, security considerations from TSG-SA WG3 and tools from TSG-SA WG4.

We are looking forward to a continuing fruitful co-operation with TSG-SA WG4.

Respectfully,
TSG-T WG2

3GPP TSG SA WG3 Security — S3#20 **S3-010436**

16 - 19 October, 2001

Sydney, Australia

TSG-SA4#18 meeting ***Tdoc S4 (01)0534***
September 3-7, 2001, Erlangen, Germany

TSG-SA WG 4 (CODECS) meeting #18
Erlangen, Germany 3-7, September, 2001 Agenda Item: PSS-E

Title: LS on Digital Rights Management (DRM) requirements for PSS Rel-5

Source: S4

To: S1 ad-hoc on Streaming, S1

Cc: T2, S3

Attachments: **S4-010474, S4-010482, S4-010486**

Contact person:

Name: Ofer Weintraub, Frank Hartung, Ralph Neff
Email Address: ofer.weintraub@emblaze.com, Frank.Hartung@ericsson.com, neff@pv.com

S4 kindly asks S1 to consider DRM requirements for PSS Rel-5.
Issue#1: S4 has received several contributions, including a liaison from WMF (Wireless Multimedia Forum), containing proposals for DRM requirements. These lists are quite comprehensive, but not exhaustive. However to meet the timeframe of Rel-5, S4 would like to narrow the scope and define achievable goals and solutions. Therefore, S4 would encourage S1 in defining such narrowed requirements. This most likely implies the analysis of the requirements with respect to the content to be delivered and the prioritisation of the requirements taking into account the available timeframe for finalising PSS Rel-5.

Issue#2: Specifically regarding WMF liaison it should be noted that WMF is conducting an ongoing survey of content providers, which may provide useful input to the requirements generation process. We are hopeful that such information will be available as an input to the S1 ad-hoc (possibly to become joint S1/S4 meeting) in October. Please note that WMF has posed three questions regarding the timeframe and scope of the DRM requirement work. SA4 believes that the response to these questions should be provided by S1. Please consider the three "open questions" proposed in the attached document (S4-010486) and send an appropriate response to WMF at your earliest convenience.

Date of next Plenary meeting TSG-SA WG4
03 – 07 Dec 2001 **TSG-SA WG4#19** Host: NTT DoCoMo, Venue: Tokyo, Japan.

Source: **Emblaze Systems**
Title: **Requirements for Digital Rights Management**
Document for: **Discussion/Decision**

1. INTRODUCTION

The aim of Digital Rights Management (DRM) is to digitally manage and protect the intellectual property and copyrights of content and content owners. This includes identifying the rights as well as protecting them against unauthorized or illegal use. Thus enabling authorized transfer or distribution of content according to predefined rules, which may involve commercial (payment) aspects.

Several solutions that implement aspects of DRM already exist in the market, some of which were already mentioned in 3GPP SA4 document titled *'Digital Rights Management for extended PSS in R5'*, numbered S4 (01)0357. There have also been several organizations and initiatives dealing with this subject, such as DAVIC[1], CPTWG[2] of the DVD Forum[3], OPIMA[4], the SDMI[5], ODRL[6], and MPEG (as part of the MPEG IPMP[7] effort).

The recent market trend has been to separate the actual implementations of DRM solutions from their use by applications that transfer or manipulate contents. This is typically done by attempting to standardize the interface to a generic DRM solution (e.g., in OPIMA or MPEG). As part of this trend we see solutions that involve the use of "digital rights languages" (e.g., ODRL, RealNetworks' XMCL[8], or ContentGuard's XrML[9]).

The purpose of this document is to present an aggregated list of requirements that are applicable for a DRM solution, especially in an environment in which multimedia content is transferred over networks, with real-time and streaming aspects, having end-to-end implications. It should be noted that DRM solutions "cut across" many components and aspects of a system, potentially also affecting quality, performance and interoperability.

It should further be noted that it may be practically impossible to satisfy **all** the presented requirements in full. An exhaustive list of today's DRM requirements may contain some inherent contradictions – for example, it may be impossible to fully control redistribution of content, while using de-facto standard formats and in the same time avoiding the use of dedicated hardware (or at least some operating

[1] Digital Audio Visual Council, see http://www.davic.org/
[2] Copy Protection Working Group, see http://www.cptwg.org/
[3] Digital Versatile Disc Forum, see http://www.dvdforum.org/
[4] Open Platform Initiative for Multimedia Access, see http://www.telecomitalialab.com/opima/ and http://www.iec.ch/opima/
[5] Secure Digital Music Initiative, see http://www.sdmi.org/
[6] Open Digital Rights Language, see http://odrl.net/
[7] There are several MPEG documents that discuss IPMP. See for example the document titled "Intellectual Property Management and Protection in MPEG Standards", numbered ISO/IEC JTC1/SC29/WG11 N3943, also available in http://www.telecomitalialab.it/mpeg/standards/ipmp/
[8] eXtensible Media Commerce Language, see http://www.xmcl.org/
[9] eXtensible rights Markup Language, see http://www.xrml.org/

system's kernel-level code[10]). Thus, there may be some sense in **prioritizing** the requirements or grouping them appropriately.

2. THE PROPOSED REQUIREMENTS

The following requirements are presented from functional point of view. This basically means the view of content owners and end-users (consumers), although some more technical aspects cannot be avoided.

One more comment should be mentioned with regards to the terminology used in documents discussing this topic: Terms like 'play' or 'use' (with respect to multimedia content) may appear with close meaning. Similarly, terms such as 'rights', 'copyrights' or 'intellectual property' are also widely used in related situations.

2.1 General Requirements

- The solution shall support **seamless** operation by the end-user (i.e., the end-user should not be bothered by DRM where not necessary).
- The solution shall support the **separation** between **identifying** rights and **protecting** them (e.g., the ability to turn off protection while still managing full right information).
- The solution shall support **separation** between **contents** and **rules** (the capability to store separately, to modify independently, and to assign different sets of rights to same content, or vice versa).
- The solution should also protect **end-user rights** (e.g., in case of content provider failures).

2.2 Functional Requirements

- **Notifying** – the system should permit users to be informed about the rights status of both content and users (e.g., don't block access without apparent reason).
- Basic **authorization** and **authentication** – the ability to prevent unauthorized usage (this is historically the "foundation" of DRM).
- **Limited usage** – the ability to block usage by various parameters (e.g., number of times content played, expiration date, etc.).
- **Partial asset protection** – the ability to apply different rules/rights to parts of a larger piece (e.g., protect streams within a session, for example for preview purposes).
- **Encryption** – the ability to scramble content while not played (e.g., against eavasedropping/interception). Note: Encryption technologies are typically used to achieve other goals, such as reliable authentication. In this specific

[10] See for example Microsoft Secure Audio Path model, http://msdn.microsoft.com/library/en-us/wmrm/htm/understandingthesecureaudiopathmodel.asp

requirement, we refer to the functional need of encrypting data if viewed by an unauthorized body.

- **Digital signature** / **fingerprinting** – the ability to later prove end-user selections or actions, in front of a 3rd party.
- **Tracking** / **watermarking** – the ability to mark content (visibly or not) for later tracking of rights or right violations. The marking should be inseparable of the content.
- **Sharing** – the ability to authorize an end-user for limited or unlimited sharing of content, or to enable him/her to forward protected contents (to be separately authorized for others).

2.3 Requirements Concerning Content Manipulation

- The ability to **prevent** unauthorized **redistribution** of contents.
- The ability to **prevent modification** of contents (even when redistribution is authorized).
- The ability to **force** the **presence** of certain content **segments** as a condition for playing it (e.g., author details or copyright information), even if content is allowed to be modified.
- The ability to automatically **"cut and paste" rights** information **together with content** segments data to which they apply. Specifically - the ability to **track** rights information in cut **parts** of an original larger piece of content.
- The ability to apply rights and tracking capabilities to a **larger** piece of content into which the original protected content is **merged**.
- The ability to **search** in a protected content should also be controlled by the DRM rules (e.g., allowed or not, with or without displaying partial search results).

2.4 Requirements Concerning Interoperability

- The ability to play **"old" unprotected content** on **current system**.
- Preventing play of **protected content** in **"old" systems**.
- The ability (at the server side) to easily **"turn off"** DRM altogether, resulting in non-serving protected material.
- Support of DRM **levels** and **optional** protective features selected by the end user (e.g., encryption).
- The solution should not strongly rely on a specific hardware **device internal id** (e.g., end user will be able to change hardware player without inherently affecting his/her rights).
- Support for common **existing** multiple content **formats**.
- Support for common **existing transport**.

- The solution shall apply the **same semantics** of rights (and especially not ignore rights altogether) for **different platforms** and/or **file formats**.
- There is a need to use **public** (known & tested) **algorithms**.

2.5 Requirements of Technical Nature

- The solution should apply all right protection features in **real-time**, while content is received by the end user (for **streaming** and **live** modes).
- The solution should **withstand loss** of fragments of information (due to communication problems).
- The **same rights** should be applied and similarly protected for the same piece of content, no matter where it currently **resides** (on disk, in memory, etc.).
- DRM processing should not affect (or have little influence on) the **performance** and **quality** of delivered content.
- The system should have some **interface** to promote **billing** and payment for royalties.
- There should be some management **tools** using standard interfaces for rights and rules management.

2.6 Requirements of Legal Nature

- The solution should not be limited in deployment and usage due to existing **export license** regulations.

3. SUMMARY

The proposed list of requirements above is by no means exhaustive. Certain organizations dealing with DRM in related environments have produced other lists in the past, overlapping the above list to some extent. In particular the list above lacks several very general requirements, which may be true for many domains (i.e., not specific to DRM). Many such requirements appear for example under the list found in MPEG-4 IPMP Call for Proposals for IPMP Technology[11] (e.g., “The solution shall support fast development of products and services”).

We believe that the list above serves as a good starting point for the TSG-SA WG4, in order to either standardize a DRM solution for multimedia content delivery in 3GPP, or provide an open framework for various DRM solutions.

END OF DOCUMENT

[11] Appears in the same MPEG document already mentioned in the beginning

3GPP TSG-SA WG4 Meeting #18
September 3-7, 2001, Erlangen, Germany

Tdoc S4 (01)0482

Source:	**Ericsson**
Title:	**DRM Requirements for PSS Release 5**
Document for:	**Discussion/Proposal**
Agenda Item:	**PSM SWG**

Introduction and background

Multimedia content is in general a valuable asset. Because of the perfect quality of digital copies and the ease of their distribution in data networks, content providers are reluctant to release premium content in digital format. On the other hand, premium content is required for attractive multimedia services in general and packet-switched streaming in particular.

It is therefore very desirable to include mechanisms for content protection into PSS, as was already proposed in the Release 4 work. The goal of content protection, also generally called Digital Rights Management (DRM), is to reduce unauthorized copies and to enable safe distribution of protected content as much as possible and feasible.

Levels of DRM protection

DRM is not a well-defined term. Several classes of DRM systems and associated copyright protection mechanisms are conceivable. The following list is not necessarily complete, but lists categories of DRM systems with different levels of protection, and different costs of deployment. These categories could be used to define the scope of the 3GPP PSS DRM standardization.

1. no protection (this is the current status of 3GPP PSS: no DRM system is included)
2. signalling of legally binding copyright information (e.g., usage rules for media content), but no technical mechanisms to enforce them
3. signalling of legally binding copyright information (e.g., usage rules for media content) and technical mechanisms to enforce them (e.g., encryption, cryptographic key management)

Besides these different classes of DRM systems there exist generic mechanisms that offer APIs and thus enable to use any DRM system. Such mechanisms have for example been standardized as part of MPEG-4 and MPEG-7 and are called ‘hooks’. A hook is an API or interface that enables to attach a DRM system, without specifying the DRM system and its functionality itself. While hooks ease the deployment of proprietary DRM solutions, they do not result in an interoperable solution, since different proprietary DRM systems are typically not compatible, even if they use the same APIs. The missing interoperability has also been recognized as a problem in the MPEG standardization. Currently, concepts for DRM modules that are loadable when required are developed in the MPEG group. However, these concepts are not mature yet. Besides the classes of DRM system stated above, hooks can be added as a further possibility for the scope of the 3GPP PSS standardization, but its associated interoperability problem should be kept in mind:

4. DRM hooks / APIs (standardized interface, no standardized DRM functionality)

(Remark: The enumerated options are in line with the options outlined in [1]

Requirements for PSS DRM Release 5

As outlined above, several different levels of DRM are possible. The standardization effort for these different levels of DRM system is also very different. In order to define suitable and feasible 3GPP DRM mechanisms it thus seems to be necessary to specify realistic requirements that the 3GPP Release 5 DRM should fulfil, and define a solution based on the requirements.

Req. 1. The PSS Rel5 DRM system (in the following called “the DRM system”) MUST provide mechanisms that enable content producers and content distributors to signal copyright

information and usage rules to PSS terminals.

Req. 2. Terminals and players declared compliant to 26.233 and 26.234 (“3GPP players”) MUST follow the signalled rules. They MUST NOT ignore or modify the rules.

Req. 3. Terminals and players not declared compliant to 26.233 and 26.234, but using the standard protocols and codecs (excluding the 3GPP extensions) that are defined in 26.234 (“Internet players”), SHOULD NOT be able to play protected content. They MAY be able to play unprotected content.

Req. 4. The set of possible rules MUST be flexible enough to express rules as needed for content distributor business models, like subscription or pay-per-view business models.

Req. 5. The set of possible rules MUST include the following rules

- a rule that allows/disallows storage of the media elements on the device
- a rule that allows transfer/export of the media elements to another device and playback only on that device
- a rule that allows transfer/export of the media elements to another device and sub-rules to restrict the playback (e.g., playback only on the device that the content has been exported to, playback only using the USIM of the subscriber, playback only on DRM enabled devices)
- a rule to control further copying/exporting/transfer of data exported to another device

Req. 6. It SHOULD be possible to specify separate rules for each media element in a multi-media presentation.

Req. 7. The DRM system MUST be extensible to a complete DRM system fulfilling the needs of content providers for premium content. It MUST NOT define mechanisms that block a later extension of the DRM system to provide improved protection and enforcement of the rules.

Req. 8. The DRM system SHOULD provide mechanisms that can also be used for protection of MMS content and downloaded content. There SHOULD NOT be incompatible DRM systems for MMS, PSS, and download (Note: work for a basic DRM solution has started in T2 (MMS standardization) [2] and S3 [2] [3] and should be coordinated with this effort.)

Req. 9. The DRM system SHOULD be convenient to use for the end user.

Req. 10. The DRM system SHOULD impose low signalling and computation load.

Future work

We propose to agree on a set of realistic requirements for PSS Rel5, where the set above can serve as basis for discussion, and to subsequently define a DRM solution for 3GPP PSS Rel5 that satisfies the requirements.

References

[1] 3GPP TSG-S4, Tdoc S4-(01)0357, “Digital Rights Management for extended PSS in R5”, Naantali

[2] 3GPP TSG-S4, Tdoc S4-(01)0429, “Liaison Statement in regards to Digital Rights Management” (liasion statement to S3 and T2), Naantali

[3] 3GPP TSG-S3, Tdoc S3-010293, “Reply LS on extended streaming service and user profiles”, Phoenix

TSG-SA4#18 meeting
September 3-7, 2001, Erlangen, Germany

Tdoc S4 (01)0486

Martin Hall
Chair, Application Requirements
Working Group
Wireless Multimedia Forum (WMF)
15575 Los Gatos Blvd., Suite C
Los Gatos, California 95032 USA
408-402-0566
martinh@stardust.com

WMF Document #: 0701HI110A

August 30, 2001

To: 3GPP TSG-SA WG4
Contact Person: Baruch Radin
E-mail Address: baruch.radin@emblaze.com
Tel. Number: +972 (3) 572 2111

Re: Liaison Statement on requirements for DRM

Dear Baruch,

Please find below the initial response from the WMF's Application Requirements Working Group to your request for input and cooperation on content providers' DRM requirements.

Sincerely,

Martin Hall
(on behalf of the WMF Application Requirements Working Group)

TSG-SA4#18 meeting *Tdoc S4 (01)0486*
September 3-7, 2001, Erlangen, Germany

WMF Response to 3GPP TSG-S WG4 Liaison Request

Introduction

The WMF welcomes the opportunity to coordinate work and provide 3GPP TSG-SA WG4 with input on the market requirements of content providers regarding Digital Rights Management. This document is the WMF's initial response. At the last meeting of the WMF's Application Requirements Working Group in Hawaii in July 2001, we discussed a plan for responding to your request and began the groundwork with an ad hoc task force. We are not yet complete with the work and need to better understand the timeframe requirements of your group (See Open Questions below). We had hoped to have a little more information for you but the month of August, as Europeans well know, is a difficult one to establish contact with and get information from many companies. Our plan is to consolidate requirements gathered from a number of sources as listed below and submit them as one set of requirements in a timeframe that meets your group's requirements.

The following is a summary of the activities we have undertaken since receiving your request.

1. Created an informal task force in the AWG which identified a basic set of requirements and "open questions".
2. Investigated & reported on status of MPEG work
3. Researched status of market requirements gathering in the industry among vendors, industry forums, standards bodies etc.
4. Initiated conversation with ISMA re their requirements investigations
5. Initiated research of content providers. Electronic survey is underway via email and web.

In order to ensure we meet your request for input on requirements and to steer our work in the right direction, we respectfully request more information from 3GPP TSG-SA WG4 on your plans by answers to the Open Questions below.

The WMF would also like to take the opportunity to stress the relevance of its core operating principles, which include the need to:

1. Embrace, drive and/or enable standards-based solutions.
2. Take existing baseline technical work on multimedia streaming and messaging into account including the WMF's Recommended Technical Framework Document (RTFD) Version 1.
3. Avoid "reinventing the wheel" and to consolidate and align the work of multiple industry groups and standards bodies.

It seems that there are two options when addressing DRM standardization issues as summarized below. As referenced in "Open Questions" below, WMF is interested in which path 3GPP intends to follow regarding these options:

1. Specify only hooks as in MPEG4.
- Upside: more flexibility for vendors and carriers. Also, easier to embrace existing solutions.
- Downside: Creates potential problems for content providers and consumers who have to choose between multiple schemes and/or support multiple schemes.
2. Specify DRM in detail including the protection and licensing mechanisms.
- Upside: clear standard.
- Downside: Risk of non-uptake by major players.

Open Questions

1. What is the timeframe for 3GPP?
2. Does 3GPP SA4 intend to specify just hooks or the whole scheme?
3. Is the DRM framework/scheme being applied to streaming multimedia, MMS or both?

WMF Survey - Sample Responses to date from WMF Survey

This survey is being sent to content providers for email or web response. The URL for the survey is:
http://www.wmmforum.com/surveys/2001/drm-aug-2001.asp

Sample Response #1

This is perhaps the most significant response we've had coming from a major content provider with business interests in music, movies, television and beyond.

1. Should local storage of content at the wireless device be enabled?
C: Local storage in the wireless environment is a likely product feature. In order for the device to receive and store the highest value content in a legal and authorized manner, there must be a means of enabling and auditing robust and renewable content protection and usage control rules (i.e.; rights) within the wireless environment. Until content protection is in place, there will be reluctance on the part of some content owners to allow their high value content to flow into the wireless environment.

1.1 If yes, should stored content be capable of transfer to other devices?
C: The ability to transfer content from one device to another is a likely product feature. The explanatory statements in my answer to question 1. above also apply here.

2. Should software decoding of multimedia content be enabled at the destination device or should there be dependence on an integrated or add-on hardware component?
C: There should be dependence on an integrated hardware component that incorporates robust and renewable content protection and usage authorization technology. An add-on hardware component is unacceptable because it is an obvious piracy attack point.

3. Should the Digital Rights Management scheme adopted be compatible with other destination devices such as wired PC's?
A: Yes. It must be compatible, interoperable, and of an equal or higher level of protection and control. It also must be renewable. It need not be the same DRM scheme as the PC. When it comes to implementation decisions, there will most likely be a relationship between the quality and the value of the content allowed into the wireless environment and the strength and renewability of the wireless unit DRM implementation.

4. Should the Digital Rights Management scheme adopted be compatible with other media types (i.e. with non multimedia content)?
A: Yes. It must be compatible, interoperable, and of an equal or higher level of protection and control as those adopted for other media types. WMF is contributing to the design of a transport environment that should be designed to accommodate the widest possible range of payload types.

5. Is encryption of the delivery channel (i.e. cellular channel and/or IP protocol) enough to protect multimedia data or do the rights need to be associated with the content itself?
B. "Associate with Content" The DRM solution should be designed for the OPTIONAL triggering of the highest possible level on content protection. This would include encrypting the delivery channel, encrypting the content, and binding the rights to the content.

Additional comment:
The standards effort should also address the design and rapid implementation of distinct DRM layers in the wireless environment. Layering will allow manufacturers to create devices for specific single or multiple layers of content, providing the consumer with more wireless device and content choices. The layers should span from unsecured public domain data to highly secured movie content delivery and banking transactions. Parameters should include authentication (ex. yes or no), encryption (ex. yes or no), time-based usage rules (ex. becomes unusable after X days), quality-based usage flags (ex. low resolution that plays on all units, high resolution that only plays on compatible units), and the ability to virally distribute the content when it is bound with the usage rules.

There is an immediate need for these standards for ringtones for cell phones, downloadable games, and MP3 files.

Sample Response #2

1. Should local storage of content at the wireless device be enabled? Yes, but we must be realistic to reality of bandwidth and prohibitive cost of adding storage to wireless.

1.1 If yes, should stored content be capable of transfer to other devices?
C. Yes, but from a Server to Client model, not the Device itself.

2. Should software decoding of multimedia content be enabled at the destination device or should there be dependence on an integrated or add-on hardware component?
A. Software

3. Should the Digital Rights Management scheme adopted be compatible with other destination devices such as wired PC's?
A. Yes

4. Should the Digital Rights Management scheme adopted be compatible with other media types (i.e. with non multimedia content)?
A. Yes

5. Is encryption of the delivery channel (i.e. cellular channel and/or IP protocol) enough to protect multimedia data or do the rights need to be associated with the content itself?
A. Channel Only

Other Standards Bodies/Industry Organizations

MPEG-4

MPEG-4 work on Digital Rights Management goes by the name "Intellectual Property Management and Protection". For an overview of the technical side of the IPMP framework, see also WMF Document Number 0701HI111 accompanying this letter.

In April 1997, a "Call for Proposals for the Identification & Protection of Content in MPEG-4" was issued. This enabled requirements to be gathered that led to the definitions of two pieces of technology:
1. Identification of Intellectual Property
2. Protection Mechanisms

In July 2000, a new call for proposals was issued to address the following requirements:

[ISO/IEC JTC1/SC29/WG11 N3543, MPEG Requirements Group, Call for Proposals for IPMP Solutions, July 2000, Beijing MPEG meeting]

1. The solution shall support access to and interaction with content while keeping the amount of hardware to a minimum. There shall be no duplication of similar devices to interact with similar content from different sources. To a lesser extent, the same applies to software. Examples of interaction with content are playback, copy, edit, create and so forth.
2. The solution shall support easy interaction with content from different sources without swapping of physical modules; that is without requiring action on the part of the end user. Addition of modules is acceptable if it requires a one-time action, if the device supports it, and if the cost is reasonable.

3. The solution shall support conveying to end users which conditions apply to what types of interaction with the content. An example is payment for playback.
4. The solution shall support protection of user privacy. Note: In many countries legislation requires that no user information shall be disclosed without the explicit consent of the end user.
5. The solution shall support service models in which the end user's identity is not disclosed to the service/content provider and/or to other parties.
6. The solution shall support the preservation of user rights. Notes: 1) For instance, the solution shall support preservation of user rights in such events as the provider going out of business. **2)** It is believed that an important requirement of end users is that their rights to interact with the content not be revoked for alleged misuse when the burden of disproving misuse is entirely on the end user. However, MPEG does not currently see any implications for these requirements.
7. The solution shall support the content and the end user's rights to interact with it to survive common accidents, e.g. an operating system crash, or a flat battery.
8. The solution shall support MPEG-4 terminal mobility, e.g. end users should be able to use the same device in different locations.
9. The solution shall support content mobility across MPEG-4 terminals, e.g. end users should be able to move to a different terminal and keep their rights to interact with the content. Note: Assuming easy access to the content, this mainly applies to the portability of the rights to interact with it.
10. The solution shall support content and the end user's rights to interact with it to survive changing to a new version of similar hardware or software. Note: Assuming easy access to the content, this mainly applies to the renewability of the rights to interact with it.
11. The solution shall support content and the end user's rights to interact with it to survive changing to a different type of MPEG-4 hardware. Note: Assuming easy access to the content, this mainly applies to the survivability the rights to interact with it.
12. The solution shall support transferring, temporarily or permanently, content and the rights to interact with it to another party.
13. The solution shall enable content owners to control which of their assets are available when, where and under what conditions.
14. The solution shall support persistent security over time and renewability of that security.
15. The solution shall support the flexible expression of different business models/rules, which might yet be unknown and which may change over time, markets and geography. Note: Some business models are envisaged to involve 'super distribution', in which content and rights to interact with it are passed along from one user to another
16. The solution shall enable content owners to change business rules whenever and however they wish.
17. The solution shall support implementations that are cost effective with regard to the value of the content to be managed and protected.
18. The solution shall support fast development of products and services.

19. The solution shall support implementations into devices that have a long life cycle, i.e. at least five years.
1. Implementation of the solution shall be based on currently available technology.
2. The solution shall not impose policies. Note: Imposing policies is the legitimate domain of content, service and application providers, and governments.

ISMA

We are in discussion with the Internet Streaming Media Alliance to coordinate our requirements gathering with efforts they have underway. We expect to have more information from them in the next one to two weeks.

SDMI

The Secure Digital Music Initiative is focused on developing specifications for protected digital music distribution. The SDMI membership includes a number of significant content providers whose requirements are presumably reflected in public specifications issued by SDMI. At the time of writing it is not clear whether content providers requirements were formally collected, documented and made public by SDMI. We are undertaking more work to determine what formal requirements work, if any, was conducted by SDMI.

Proprietary Solutions

Since a number of companies have undertaken frameworks or technology solutions that address DRM requirements, we feel it's also important to be at least aware of directions these companies have taken. Please note that this research is note yet complete.

Companies we feel it's important to be aware of include, but are not limited to:

Intertrust
Reciprocal
ContentGuard
SealedMedia
Nokia
Entrust
IBM (Electronic Media Management System - EMMS)
Microsoft
RealNetworks (RealServer iQ for streaming; MusicNet solution for downloadable files)

SealedMedia

Requirements identified in a SealedMedia White Paper
http://www.sealedmedia.com/solutions/whitepapers/en-busus.pdf

- Robust, persistent content protection
- Publishing power, agility & control
- A painless consumer experience
- Rapid, low-risk implementation and ease of use

- Scalability
- Win-win pricing

Nokia

From Nokia presentation to W3C, Jan 2001
"Nokia - Position Paper
W3C Workshop on Digital Rights Management"
http://www.w3.org/2000/12/drm-ws/pp/nokia-durand.html

Our specific requirements for a DRM solution, are

- Efficiency. Makes efficient use of limited resources of mobile device
- Support for multiple delivery channels (broadcast, streaming, superdistribution)
- Support for a variety of devices
- Interoperability between various content provider's DRM systems
- Ease of use. That it will not adversely affect the usage patterns of consumers
- Cost effectiveness.
- Support for relative, emerging standards.
- Support for flexible rights management (metered, pay per view, loaning)

From a Nokia perspective, these requirement areas cover Music, Publishing, Video, Software and Games.

3GPP TSG-SA Meeting #13 ***Tdoc SP-010577***
Beijing, China, 24-27 September 2001 **Agenda 8.9**

Source: Motorola, Nokia, Siemens, Vodafone

WID on Digital Rights Management (DRM)

Work Item Description

Title

Digital Rights Management (DRM)

1 3GPP Work Area

	Radio Access
	Core Network
X	Services

2 Linked work items

Multimedia Messaging Service(MMS), streaming

3 Justification

Services and capabilities specified by 3GPP allow "content" (including, but not limited to data, text, audio, or video) to be delivered (by a variety of means, including streaming, downloading) and played or stored for future use on the mobile. Delivery methods may include forwarding onward from the device. It is essential to create a solution that will respect the intellectual property rights as specified by the rights holders.

4 Objective

Specify a framework that will support an interoperable, uniform, high volume market for the distribution of protected content. Expression and enforcement of rights and rules is an essential component of this distribution capability (so called Digital Rights Management, DRM).

5 Service Aspects

In order for protected distribution of content to be acceptable to consumers, it must be transparent and non-intrusive.

6 MMI-Aspects

Beyond the scope of standardization.

7 Charging Aspects

Charges may accrue accessing and downloading content (though the exact charging models to be used are beyond the scope of standardization), however some aspects related to charging may need to be standardized.

8 Security Aspects

Security of downloadable and or streaming content must be preserved, i.e., it must not be possible to "play" unauthorized copies.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		x			x
No			x		
Don't know	x			x	

10 Expected Output and Time scale (to be updated at each plenary)

The WI is being targeted for Release 6. Additional details will be provided after initial investigations are complete.

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11 Work item raporteurs

Nokia

12 Work item leadership

TSG SA1, (supporting WGs – TSG SA4, TSG SA2, TSG SA3, and TSG T2).

13 Supporting Companies

Motorola, Nokia, Siemens, Vodafone, Materna

14 Classification of the WI (if known)

x	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)