OMTP PUBLISHED

OMTP

MOBILE CONTENT SECURITY

REQUIREMENTS FOR
OMA DRM V2
ENABLED TERMINALS

VERSION:	1.5
STATUS:	Approved for publication
DATE OF PUBLICATION:	16th May 2008
OWNER:	OMTP LIMITED

CONTENTS

The information contained in this document represents the current view held by OMTP Limited on the issues discussed as of the date of publication.

This document is provided “as is” with no warranties whatsoever including any warranty of merchantability, non-infringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein.

This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based solely on this document.

Each Open Mobile Terminal Platform member and participant has agreed to use reasonable endeavours to inform the Open Mobile Terminal Platform in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. The declared Essential IPR is publicly available to members and participants of the Open Mobile Terminal Platform and may be found on the “OMTP IPR Declarations” list in the OMTP Members Area.

The Open Mobile Terminal Platform has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Defined terms and applicable rules above are set forth in the Schedule to the Open Mobile Terminal Platform Member and Participation Annex Form.

1 INTRODUCTION

1.1 DOCUMENT PURPOSE AND SCOPE

Digital Rights Management (DRM) is an enabling technology for the controlled distribution and consumption of valued media content within the mobile industry. To prevent illegal sharing of mobile content, content providers increasingly ask for content protection as prerequisite for content provisioning.

The market currently provides proprietary as well as open standard DRM solutions (e.g. OMA DRM). However, even if implementations are based on the open standard deployed in the mobile world (i.e. OMA DRM v2 standard [1]), there is still room for differences in implementations leading to usability, functionality and security issues.

To facilitate consistent and secure DRM implementations and ensure these are also acceptable from a User point of view, it is important to agree on a common set of Terminal requirements that can be used by those parties intending to deploy the OMA DRM v2 [1] solution.

As such, this document has been prepared with the intent of providing a set of agreed Terminal requirements that will help operators and Terminal manufacturers deploying OMA DRM v2 [1] to achieve consistent and User friendly implementations to support DRM-based content download service which includes peer-to-sharing across Terminals.

This document covers key areas of functionality expected by OMTP members and the specific requirements needed in Terminals to deliver services based on OMA DRM v2 [1].

Note: This document includes some requirements based on the OMA DRM 2.1 specification [2], which – as at the date of publication of this document - is still an OMA draft version.

This document does not:

- Provide a complete set of detailed functional requirements
- Replace individual operators specification, requirements and quality control levels for Terminals
- Contractually bind Terminal manufacturers

Also, this document is not to be seen as an endorsement by OMTP of the OMA DRM solution.

1.2 INTENDED AUDIENCE

The objective of this document is to provide a guide for

- Operators who intend to specify Terminal requirements in support of OMA DRM v2 [1].
- Terminal and OS manufacturers to understand key requirements in support of OMA DRM v2 [1]

1.3 CONVENTIONS

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [3].

- MUST: This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option -, though perhaps with reduced functionality. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

The requirements within this document are uniquely identified using the following format:

DRM-####(.#.#), where:

- DRM stands for Digital Rights Management

- #### is a 4 digit number uniquely identifying the recommendation
- .(.#.#) are numbers that identify sub-recommendations

2 KEY REQUIREMENTS

Whilst OMA DRM v2 [1] enables a variety of use cases, a number of scenarios have been identified as the most prominent. Therefore these shall be addressed first to ensure support in the **short term**. The initial focus will be on the support of content protection of audio and video content types as these are considered most relevant for higher value content and thus require a higher content protection solution. The use case, supporting requirements and the corresponding functional and technical requirements are detailed respectively in the following sections:

- 2.1 Support of Key Use Cases for Short Term Implementation
- 2.2 General supporting requirements
- 3 Functional And Technical Requirements for Short Term Implementation.

This task does not limit the use of unprotected content.

Furthermore, a use case dealing with the provisioning of Right Objects inside the SIM/USIM card has been included as it is considered relevant, but not realisable within the short term due to the fact that the referenced OMA SRM specification [4] is not yet at Candidate or Approved status. As such, inclusion of the use case and the supporting requirement serves to provide guidance for **mid term** support (see also sections 2.3 Support of Key Use Cases for mid term implementation and 4 Recommendation for mid term support).

Further **mid to long term** relevant use cases will be dealt with in subsequent work (see section 5 Future work).

2.1 SUPPORT OF KEY USE CASES FOR SHORT TERM IMPLEMENTATION

2.1.1 THE USER DOWNLOADS OMA DRM V2 PROTECTED CONTENT AND PLAYS IT

In search of new content, the User browses a mobile portal. After the User has completed the selection and agreed to terms and conditions, the content and associated rights will be sent to his Terminal. The User will be able to render the content as soon as both have been fully downloaded and as long as valid usage rights are available (normal download). Alternatively, progressive download (see section 2.1.4) may be used.

2.1.2 THE USER DOWNLOADS A CONTENT ITEM AND INSTALLS IT (E.G. AS A RING TONE).

Once the User has downloaded the content, he may wish to install it for automated use (e.g. installation as a ring tone, background wallpaper, alarm tone or screensaver).

2.1.3 THE USER SUBSCRIBES TO A MUSIC/VIDEO SERVICE (RENTAL)

A Service Provider may decide to offer a service in which the User receives content and Rights Objects (ROs) in regular intervals. A User may select to have the subscription renewed automatically in which case the Service Provider (i.e. Rights Issuer) will provide the associated rights "silently", i.e. without user interaction and awareness.

2.1.4 THE USER CONSUMES AUDIO/VIDEO CONTENT WHILST DOWNLOADING IT (PROGRESSIVE DOWNLOAD)

As part of the content purchase process, the content and associated rights will be sent to a User's Terminal. The User will be able to render the content as soon as only a portion of the file has been downloaded, whilst download of the remaining file continues in the background and as long as valid usage rights are available.

2.1.5 THE USER SHARES CONTENT BETWEEN TERMINALS (CONNECTED TERMINALS)

2.1.5.1 Superdistribution

Where a User has protected content which he wishes to share with friends, he may forward this via Bluetooth®, IrDA®, messaging or other means, unless it has been delivered to the Terminal in an OMA DRM 1.0 DRM Message and therefore forwarding is not allowed. The recipient will receive the protected content, unless he is missing the rights to render it. When attempting to unlock the content (i.e. obtaining the appropriate Rights Object such that the Terminal is able to decrypt the Protected Content file for further usage), a browser session will be initiated (after User approval) and the User will be directed to the Rights Issuer Portal from which he can obtain the rights. As soon as these have been delivered successfully, content can be rendered as long as valid rights are in place.

2.1.5.1.1 Superdistribution with rewarding

When buying protected content from a Service Provider (e.g. on a web/WAP portal), the User may be asked whether she wants to be enrolled into a rewarding program set up by the Service Provider. Such enrolment allows the Service Provider to track, for rewarding purposes, the subsequent distribution of every piece of content it sells to the User without asking again for her consent.

As long as it triggers the acquisition of licenses, the superdistribution of content from the original User to others (e.g. friends) may be tracked and allows the User herself to be rewarded according to the terms and conditions of the rewarding program. The User will always be able to deny her consent for her superdistributed content to be tracked.

2.1.5.2 Domain Model – sharing content

Where a User has found a specific piece of content, the User may want to share this with other Terminals, either owned by the User (example: mobile, PC, MP3 player) or belonging to a group of friends. The User would be able to do so, where the Service Provider offers the domain model based service. To use this service, the User or the Service Provider will have to create a personal domain in which his own Terminal is registered as well as those Terminals that should be part of that domain.

As part of the service implementation, the Service Provider:

- Will need to approve the type (e.g. mobile phone, PC, music players, connected or unconnected) and the number of Terminals allowed within a domain
- May allow a Terminal to belong to multiple domains simultaneously but should carefully consider related usability issues (example: how will Users distinguish between different content downloaded to his Terminal but belonging to different domains)
- May allow Terminals to be added or deleted to a domain as requested by a User
- May allow non-subscribers to join domains as well

When purchasing the rights for the content, the User will indicate that this is meant for his domain. Alternatively, this can be set automatically by the server. The content can be rendered on Terminals, as approved by the Rights Issuer. This could be either a User's own set of Terminals or a number of Terminals owned by other subscribers. These Terminals may be either connected or unconnected Terminals[1] where Users purchase DRM Content and rights via one Terminal (example: a PC) for later use on another Terminal (example: a portable player with no wide area network connectivity). Users may then share DRM content off-line between all DRM Agents belonging to the same domain.

It is in the responsibility of the Service Provider to define the domain profile. Depending on his legal framework and the services he wants to offer to his customers, he needs to decide on elements such as: Maximum number of Terminals, maximum number of Terminal exchange in the domain (leave one Terminal / join another) per day for fraud detection, types of Terminals, account information and expiry dates of domains.

[1] The work of this document is focused on support of connected Terminals. Support of unconnected Terminals is considered as part of future work (see also section 4).

2.2 General supporting requirements For Short Term Implementation

Further requirements are necessary to:

- support storage and backup of protected content on the Terminal or on removable media
- support of secure implementation
- cover usability requirements.

2.2.1 Content storage and Restorage

As far as possible, a User should have the same user experience with Protected Content as with Unprotected Content for the following use cases:

- Storing Protected Content –either downloaded or received from another party- on the Terminal or on external memory where this exists
- Restoring Protected Content from external memory to the Terminal
- Moving Protected Content from one folder to another or from the Terminal to external memory where this exists.

To ensure handling of the above, the requirements will also cover the handling of Rights Objects in line with OMA DRM specifications and any implications thereof (e.g. backup of stateful Rights Objects).

2.2.2 Secure Implementation

It shall be ensured that the User or a third party is not able to manipulate the DRM implementations.

2.2.3 Ensuring Usability

With usability being one of the key success factors for adoption, the implementation shall respect the following usability principles:

- Users shall be aware of DRM but it should be as intuitive as possible.
- Users should only see DRM prompts that are absolutely necessary.
- The User experience on different domain Terminals shall be similar.
- Users shall be able to distinguish between different content products (ring tones vs. full tracks)

2.3 SUPPORT OF KEY USE CASES FOR MID TERM IMPLEMENTATION

The current section includes a use case OMTP considers relevant, but , refers to the OMA SRM specification [4] that is not yet at Approved status.

Therefore, the implementation of the following use case is recommended as soon as the aforementioned specification is raised to Approved status.

2.3.1 PROVISIONING OF RIGHTS OBJECT IN THE SIM/USIM CARD

The User can subscribe to a network operator service allowing her to store the Rights Objects for Protected Content within her SRM-enabled SIM/USIM Card. When acquiring a new mobile Terminal, the User wants to have her existing Rights Objects transferred to the new Terminal along with her account details. After plugging her SRM-enabled SIM/USIM Card into the new SRM enabled Terminal (and in any other Terminal), she is immediately able to consume the protected content for which she acquired the Rights Objects already.

3 FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR SHORT TERM IMPLEMENTATION

3.1.1 GENERAL

REQ. ID	REQUIREMENT	REFERENCES
DRM-0010	All requirements in this document related to OMA DRM v2 SHALL be in compliance with OMA DRM v2 [1]	
DRM-0020	If the Terminal supports one or more of the following content types, then it SHALL support the OMA DRM v2 [1] protection of these content types	
DRM-0020.1	Audio	
DRM-0020.2	Video	
DRM-0030	If the Terminal supports the following content type, it SHOULD support OMA DRM v2 [1] protection for the content type:	
DRM-0030.1	Images	
DRM-0035	For handling (e.g. distribution, rendering) of the supported content types, the DRM implementation SHALL NOT impose a size restriction beyond the native ability of the Terminal for unprotected content of the same type.	
DRM-0040	The DRM agent SHALL support the following permissions, constraints and elements as enabled by the OMA DRM v2 [1] permission and constraint model:	
DRM-0040.1	Permissions: play (audio/ video), display (images)	
DRM-0040.2	Constraints: unlimited, time-based (interval and datetime start / end), count, system	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0040.3	Element: Individual as defined in OMA-DRM-REL-V2.0 for binding Rights Objects to the IMSI (if the Terminal has the UICC interface).	
DRM-0045	The Terminal SHALL support the GroupID mechanism, as defined by requirement "DRM-DCF-CLI-8" of OMA DRM v2 [1].	
DRM-0050	Terminals SHALL be backwards compatible with OMA DRM v1.0 Forward Lock (FL), Combined Delivery (CD) and Separate Delivery (SD) [5].	

3.1.2 DOWNLOAD

REQ. ID	REQUIREMENT	REFERENCES
DRM-0060	A Terminal SHALL support the following download mechanisms when downloading DCF and Rights Object(s):	
DRM-0060.1	OMA Download v1.0 (using CD as specified in OMA DRM v2, section G3.2 and OMA DRM v2, section 11.3.1.3. [1])	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0060.2	OMA Download v1.0 [6], using SD as specified in OMA DRM v2, section 11.3 [1]: Depending on whether the Rights Object or the DCF is sent first using OTA, the Terminal SHALL support the following download processes: • Where the Rights Object is to be sent first, a first Download Descriptor (DD) SHALL be sent with a ROAP Trigger (co-delivery method) to download the Rights Object. The DD SHALL contain a "nextURL" element which the Terminal SHALL use to download the DCF (possibly using a second DD). • Where the DCF is to be sent first, a first Download Descriptor (DD) SHALL be sent to download the DCF. The DD SHALL contain a "nextURL" element which the Terminal SHALL use to download a Rights Object Trigger (possibly using a second DD with co-delivery method). In each case, if a subsequent DD is used then: • if there is no "nextURL" element in the subsequent DD then the terminal SHALL close the browser application (if it was automatically launched by another application). • otherwise the terminal SHALL navigate to this nextURL.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0065	A Terminal SHALL support the following download mechanisms when downloading DCF only: • HTTP File downloads, as defined by RFC2616 [7] • OMA Download v1.0 [5]. If a subsequent DD is used then: - if there is no “nextURL” element in the subsequent DD then the terminal SHALL close the browser application (if it was automatically launched by another application). - otherwise the terminal SHALL navigate to this nextURL.	
DRM-0070	A Terminal SHOULD support the following download mechanisms (when downloading either the Rights Object only or when downloading DCF and Rights Object):	
DRM-0070.1	OMA Download v2.0 [8]	
DRM-0080	The Terminal SHALL present the User with an accurate indication of progress during the download (e.g. a progress bar displaying the percentage of content still to be downloaded).	
DRM-0080.1	In case of OMA Download v1.0 [5] using CD or OMA Download v2.0 [8], this indication SHALL end after the receipt of both files, i.e. the DCF and the Rights Object. The Terminal SHALL only display a single progress indication for the complete download process.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0080.2	In case of OMA Download v1.0 [5] using SD as specified in OMA DRM v2 section, 11.3 [1], • The Terminal SHALL NOT provide a further notification (e.g. textual message) to the User after downloading and installation of a Rights Object (RO) specifically informing on this other than the general download message as specified in requirement DRM-0120. • The Terminal SHALL display a single progress indication for the DCF download process. • The Terminal SHOULD only display a single progress indication for the complete download process. Should this be not possible, the Terminal MAY display a cycling timer (e.g. hour glass) during the RO download.	DRM-0120
DRM-0080.3	If implicit ROAP protocols are required (see OMA DRM v2 section 5.1.7, [1]), the progress indication SHALL encompass these implicit ROAP protocols, i.e. the Terminal SHALL present only one progress indication to the User. Should this (i.e. requirement DRM-0080.2) not be possible, the Terminal MAY display a cycling timer (e.g. hour glass) during this ROAP process.	DRM-0080.2
DRM-0090	The Terminal SHALL be able to receive ROAP Triggers via the co-delivery of an OMA Download v1.0 Download Descriptor as specified in OMA DRM v2 section 11.3.1.2 [1].	
DRM-0100	The Terminal SHALL support the User Consent Whitelist as specified in OMA DRM v2 section 5.1.8 [1] to ensure there is no User interaction for any ROAP protocol.	
DRM-0100.1	It SHALL be possible to populate this Whitelist at manufacturing time.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0100.2	The Terminal SHALL not enable the User to modify this Whitelist.	
DRM-0100.3	Where a Terminal supports OTA Device Management, it SHOULD be possible to securely update the Whitelist OTA.	
DRM-0110	The Terminal SHALL clearly indicate to the User during the download process where the DCF can be accessed later on. For example, the file location (whether on the Terminal or external memory and also the respective folder) could be indicated as part of the progress bar or at the end of the download process. This information SHOULD be such that it is understandable to the User and in line with general related UI used by the Terminal[2].	

[2] It is the assumption that the User Experience for content downloads should be as much as possible the same, regardless whether Content is Protected or not.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0120	If both DCF and RO are downloaded: • the DCF SHALL automatically be stored in the default folder[3] as selected by the Terminal or in a folder chosen by the User • the RO SHALL be stored in the RO repository, • the content SHALL NOT be automatically decrypted and/or rendered. • The Terminal SHALL present the User with a notification of the completed download, providing him with the option to render the content or continue browsing. • If the User selects to render the content, the Terminal SHALL start the relevant rendering application. Otherwise the User SHALL be taken back to the browser or the application that initiated the download. For a recommended prompt, see section 3.1.12, requirement DRM-0690.	DRM-0690
DRM-0120.1	The Terminal SHALL insert all Rights Objects (excluding stateful Rights Objects and excluding Parent Rights Object) in the DCF as soon as possible and before the DCF leaves the Terminal. The Terminal MAY take this action immediately after download or after first rendering, however this SHOULD NOT impact the performance of the Terminal. See also DRM-0620.	DRM-0620

[3] As defined by the operator and/or implemented by the vendor.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0130	In case of a download failure of either the DCF and/or the Rights Object, the Terminal SHOULD display an appropriate error message including the reason (e.g. "No network" for network disconnection for instance, "Cancelled by user" or "Download error" for the other cases) and SHALL provide the User with an ability to go back to the application that initiated the download (e.g. a browser). This application may enable the User to initiate a re-download or to learn more about the issue or how to proceed.	
DRM-0140	The Terminal SHALL ensure that its DRM capabilities can be fully identified by the Rights Issuer portal via the following three mechanisms: - HTTP header (DRM version, Accept Headers), - the ROAP DeviceDetails extensions and - the UAProf.[4]	

[4] The assumption is that the Terminal uses its default browser. Where a User downloads a different browser to the Terminal or makes use of an alternative download agent (e.g. podcast client), this new application may not be able to declare the OMA DRM Agent capabilities native to the Terminal via HTTP header and UAProf.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0150	When the Terminal initiates a ROAP exchange in order to unlock a DCF (by using silent URL, RI URL from DCF or RI URL from RO): • if there is no “nextURL” element in the DD delivering the ROAP Trigger and there are no other ongoing downloads, the Terminal SHALL automatically close the browser application (if launched) after this ROAP exchange has been completed. • If there is a “nextURL” element in this DD, then the Terminal SHALL navigate to this nextURL. Whilst unlocking the DCF, the Terminal SHALL present the User with appropriate information. For a recommended prompt, see section 3.1.12, requirement DRM-0730.	DRM-0730
DRM-0151	When a Download Descriptor contains an “install notify url", the Terminal SHALL NOT display information to the User concerning notification process of Download Descriptor.	

3.1.3 RENDERING OF PROTECTED CONTENT

REQ. ID	REQUIREMENT	REFERENCES
DRM-0155	The Terminal SHALL first consume the Rights Objects stored on the Terminal RO Repository with algorithm defined in OMA DRM v2 REL §5.9 [1]. If there is no valid Rights Object on the Terminal RO Repository in local repository for DCF, the Terminal SHALL install all (valid) Rights Objects included in the DCF. The Terminal SHALL select a Right Object with algorithm defined in OMA DRM v2 REL §5.9 [1]. If there is no valid Rights Object included in the DCF, the Terminal SHALL get Rights Object by using rightIssuer URL, preview URL, SilentUrl (as specified in OMA DRMv2 [1]).	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0160	The Terminal SHALL allow the DRM Agent to launch the browser in accordance to the OMA DRM v2 specification sections 5.2.2 and 5.3.5 [1].	
DRM-0171	The Terminal SHALL be able to handle DCFs in parallel to support at least the following cases : • the User plays a protected audio file in the background whilst viewing a protected image[5] in the foreground • the player SHALL be able to render a playlist of protected audio files with no noticeable delay between the playback of successive files • the player renders a protected audio file and the Terminal rings with a protected audio file. The player is automatically on pause during the call and the requirement DRM-0230 is verified.	DRM-0230
DRM-0175	The Terminal default file manager SHALL be capable of recognising the DCF and the content type, and providing the User with information about the content (metadata) and associated rights.	
DRM-0180	The Terminal SHALL NOT prompt the User with information about remaining rights before rendering. This applies for all kind of Rights Objects (including Stateful Rights).	
DRM-0190	Automated use of DCFs:	

[5] Image may be protected using OMA DRM v1.0

REQ. ID	REQUIREMENT	REFERENCES
DRM-0190.1	For automated use, media objects (e.g. ring tones and operator logos) SHALL be installed only if at least one valid corresponding Rights Object without a stateful constraint exists or at least one valid Rights Object with an <interval> constraint exists. Even though these media objects without such Rights Object cannot be installed for automated use, they can be rendered by corresponding applications as initiated by the Terminal or User.	
DRM-0190.2	For media objects with corresponding <interval> constraints, if these are to be installed for automated use (e.g. as a ring tone or screensaver) the start of the interval period SHALL be established at the first usage of the Rights Object, i.e. at the first rendering (either user-initiated or automated), not at reception of the DCF nor at installation for automated use.	
DRM-0190.3	Where Protected Content has been installed for automated use and Rights have expired, the Terminal SHALL automatically replace this media object with the default content (e.g. content provided by manufacturer ex-factory). It is assumed that the Terminal shall always provide a default content. The Terminal SHOULD provide the User with a notification and with the option to navigate to the Rights Issuer URL. This notification SHOULD NOT be presented to the user only during an incoming call. See also DRM-0200.1.	DRM-0200.1
DRM-0200	The option to navigate to the Rights Issuer URL, if present in a DCF, SHALL be enabled by all native applications that support DCF.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0200.1	If there are no remaining rights, the Terminal SHALL provide a notification to the User at an attempt to render the DCF and with the option to navigate to the Rights Issuer URL[6]. For a recommended prompt, see section 3.1.12, requirement DRM-0700.	DRM-0700
DRM-0200.2	If there are remaining rights, the User SHALL have the option to navigate to the Rights Issuer URL.	
DRM-0210	When a Rendering Software executes a playlist, only DCFs with valid Rights Objects SHALL be rendered.[7] A DCF with no rights or no remaining rights but part of the playlist, SHALL be skipped. In this case, a notification to the User and an option to navigate to the Rights Issuer URL SHALL NOT be provided prior, during and after the rendering of the playlist.	

[6] In line with OMA DRM specifications, behaviour may be different in case of DCFs with Silent headers or protocols implicitly triggered by a client receiving a ROAP Trigger from an RI (OMA DRM v2.0, Section 5.1.8).

[7] Assumption: Preview Content will not be renderd as part of playlist. Handling of these is proposed as future work, see section 5.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0210.1	When a Rendering Software executes a playlist, and this playlist includes a DCF for which there exists no valid Rights Object but where this DCF contains a Silent URL, the Terminal SHOULD attempt to acquire the Rights Object for this DCF by using the Silent URL. This request SHALL be executed ahead of time before rendering said track commences. If however, the Rights Object is not delivered in time of rendering, the Rendering Software SHALL skip this DCF and in parallel continue the RO retrieval process with no further User interaction. If the request to the Silent URL fails, the Terminal SHALL NOT notify the User. See also requirements DRM-0430 and DRM-0440.	DRM-0430 DRM-0440
DRM-0220	The User SHALL be able to enquire on the status of the rights e.g. by pressing a 'Property' option menu for the content item. This status enquiry SHALL NOT modify the rights' state for Stateful Rights.	
DRM-0230	If the rendering of a DCF with Stateful Rights is interrupted, either automatically or manually initiated (e.g. by a received call or message), a restart at the pause point and the pause time SHALL NOT consume an additional right.	
DRM-0240	Stateful Rights SHALL only be decremented when a User has requested to render the content (e.g. not for generating thumbnails in a playlist).	
DRM-0250	The Terminal SHALL read the metadata items present in the DCF File (User-Data Box) as described in OMA DRM V2.0 [1] and OMA DRM V2.1 [2].	

REQ. ID	REQUIREMENT	REFERENCES

DRM-0250.1	Such metadata SHALL be made available to a rendering application for display and/or other purposes, e.g.:
	• The Artist/Interpreter (Performer box)
	• The Track Name (Title box)
	• The Album's Name (Album box)
	• The Album Cover picture (e.g. second part of the multipart DCF)
	• Caption or description for the media (DSCP)
	• As part of the progress indication:
	  ○ The Track Length (Calculated from the audio track) and
	  ○ The elapsed time (Calculated from the audio track).
	
	The visibility of which metadata appears in which screen will depend on the specifics of each rendering application's user interface design.	

DRM-0250.2	The Terminal SHALL offer an option menu to display the complete list of metadata contained in a DCF's User Data Box.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0265	The Terminal SHALL permit the editing of metadata as defined in OMA DRM v2.1 [2] for the following areas: • The Track Name (Title box*) • The Artist/Interpreter (Performer box*) • The Album's Name (Album box*) • The Album Cover picture (e.g. second part of the multipart DCF) (* as specified in 3GPP TS26.244 [9] Tables 8.1, 8.4, 8.11) Assumption: The following Meta Data is not editable: Description Box (Table 8.2), Copyright box (Table 8.3), The Rating Box (Table 8.7), The Classification Box (Table 8.8), The keyword box (Table 8.9), The keyword Struc (Table 8.9.1), The Location Information box (Table 8.10), The Recording Year Box (Table 8.12), ID3v2 box (Table 8.13).	
DRM-0271	In case of an invalid DCF (e.g. corrupt file, wrong syntax) and –unless DRM-0271.1 is supported-, the Terminal SHALL provide a user notification, informing the User and providing the option to delete the DCF. The default SHOULD be to not delete the content. For a recommended prompt, see section 3.1.12, requirement DRM-0710.	DRM-0271.1 DRM-0710
DRM-0271.1	If a valid RO for the invalid DCF is existing on the Terminal, the Terminal MAY provide the User with the option to navigate to the ContentURL for re-download. The Terminal SHALL NOT use the URL if the syntax does not conform to the uniform resource identifier specification in RFC 2068 [10].	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0285	When the User or an Application tries to render the content, but rights have expired or are missing or not contained in the DCF File, and the use of the SilentURL and Rights Issuer URL contained in the DCF fails, the Terminal SHALL behave as follows:	
DRM-0285.1	The Terminal SHALL NOT use the URL if the syntax does not conform to the uniform resource identifier specification in RFC 2068. The Terminal SHALL prompt the User with an appropriate error message, recommending to delete the file. For a recommended prompt, see section 3.1.12, requirement DRM-0720.	DRM-0720

REQ. ID	REQUIREMENT	REFERENCES
DRM-0285.2	The Terminal SHALL NOT make further requests to the URL, if the SilentURL and Rights Issuer URL are a HTTP URL and the request fails with one of the following status codes[8]: • 400 bad request • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 410 Gone • 411 Length Required • 412 Precondition Failed • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Requested Range Not Satisfiable • 417 Expectation Failed The Terminal SHALL prompt the User with an appropriate error message, recommending to delete the file. For a recommended prompt, see section 3.1.12, requirement DRM-0720.	DRM-0720

[8] Note: Compliance of this requirement requires that the http error code is returned to the DRM agent. If the DRM agent does not make the http request itself, it must receive the http error code from the entity that makes the http request.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0285.3	The Terminal SHALL retry the request at next attempt of rendering, if the request fails with status code, including: • No battery • No (or loss) cellular network • Domain name can not be resolved, • 401 Unauthorized • 402 Payment required • 403 Forbidden • 407 Proxy Authentication Required • 408 Request Timeout, Network Error The Terminal SHALL prompt the User with an appropriate error message. For a recommended prompt, see section 3.1.12, requirement DRM-0725.	DRM-0725
DRM-0285.4	The Terminal SHALL pursue the request if the request fails with status code, including: • redirection 3xx	

3.1.4 STORAGE AND BACKUP OF PROTECTED CONTENT

REQ. ID	REQUIREMENT	REFERENCES
DRM-0290	The Terminal SHALL ensure that storage of protected content, either downloaded or received from another party, SHALL be the same as with unprotected content:	
DRM-0290.1	Users SHALL be able to store protected content on the Terminal or on removable memory where it exists.	
DRM-0290.2	Users SHALL be able to restore protected content from removable memory onto their Terminal.	
DRM-0290.3	Users SHALL be able to move protected content from one folder to another or from phone to removable memory.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0305	After restoring a DCF from removable memory to the Terminal, the DCF file and the RO SHALL be stored in the same way as if they were transferred to the Terminal via any other means. For instance, the RO could be extracted from the DCF and stored in a RO repository.	
DRM-0310	As a minimum, the Terminal SHALL be able to store 1000 Rights Objects.	
DRM-0310.1	As a minimum, each replay cache SHALL be able to store 100 entries.	

3.1.5 HANDLING OF RIGHTS OBJECTS

REQ. ID	REQUIREMENT	REFERENCES
DRM-0320	Rights Objects and Rights Objects repository SHALL not be visible to the User via the file system of the Terminal.	
DRM-0330	If the User chooses to delete a DCF on the Terminal or moves this to external memory, the associated Rights Objects (if still valid) SHALL NOT be deleted. The Terminal SHALL NOT present the User with a prompt.	
DRM-0340	In cases where the Rights Objects expired or are corrupt, these SHALL automatically be deleted without User interaction. The Terminal SHOULD delete these Rights Objects at earliest possible time, e.g. when a RO is found to be corrupt or expired. At the minimum, the Terminal SHALL check for corrupt or expired ROs when it is short of storage space for ROs.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0350	The Terminal SHALL support WAP Push reception of ROAP Triggers as specified below in DRM-0350.1 and DRM-0350.2: This reception and processing SHALL be entirely silent. See also requirements DRM-0100 and DRM-0460.1.	DRM-0100 DRM-0350.1 DRM-0350.2 DRM-0460.1
DRM-0350.1	XML WAP Push as defined in OMA DRM v2.0, section 11.4 [1].	
DRM-0350.2	Binary XML WAP Push (WBXML) as defined in OMA DRM v2.1, sections 14.4 and 16 [2].	

3.1.6 PROGRESSIVE DOWNLOAD

REQ. ID	REQUIREMENT	REFERENCES
DRM-0360	The Terminal SHALL support progressive download of OMA DRM v2 [1] Protected Content for audio and video.	
DRM-0360.1	If protected content with a Stateful Rights Object is progressively downloaded, the rendering during download SHALL consume one usage right.	
DRM-0365	When a progressively downloaded DCF contains the DCFHash extension, the Terminal (upon completion of the progressive download) SHOULD follow the same behaviour with regards to the hash validation as for a normal download.	
DRM-0370	The Terminal SHALL progressively download a DCF (i.e. begin rendering the content before the DCF download is complete and as soon as it is possible) if and only if the Download Descriptor contains a progressiveDownloadFlag element with the value “true”. This is applicable to:	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0370.1	• OMA Download v2.0 [8]	
DRM-0370.2	• OMA Download v1.0 [5] In this case, a “progressiveDownloadFlag” (defined like the flag introduced in OMA Download v2.0) will be added in the descriptor when the Service Provider allows rendering during download. If a progressive download is not possible, but the Download Descriptor contains a progressiveDownloadFlag element with the value “true”, then the Terminal SHALL download the DCF file in the same way as a normal download. There SHALL be no error message for this case to the User.	
DRM-0380	Where a progressive download has been initiated, the Terminal SHALL provide the User with an option to cancel immediate rendering at any time during the download. This behaviour MAY be configurable through an option menu.	
DRM-0380.1	When a User cancels rendering during download, the Terminal SHALL continue the downloading of the DCF in the background.	
DRM-0380.2	When a User cancels rendering during download, the Terminal SHOULD follow the same behaviour as for a normal download. See requirement DRM-0080.	DRM-0080

3.1.7 SUBSCRIPTION

REQ. ID	REQUIREMENT	REFERENCES
DRM-0390	The Terminal SHALL support parent/child RO mechanism as specified in section 9.5. of OMA DRM v2 [1].	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0400	The Terminal SHALL support the Download of a RO Response containing at least two protected Right Objects. Note: There could be more than two ROs included in the RO response; the order of inclusion could be either the parent Rights Object and then the child RO or vice versa.	
DRM-0410	The Terminal SHALL always embed a child Rights Object in the DCF (provided it is a Domain Rights Object).	
DRM-0420	The Terminal SHALL NEVER embed the Parent Rights Object in the DCF.	
DRM-0430	The Terminal SHALL support silent headers as defined in OMA DRM Content Format v2.0, section 5.2.2.1 [11].	
DRM-0430.1	The Terminal SHALL support the silent-method “on-demand”.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0430.2	The Terminal SHOULD support the silent-method “in advance” as follows: Upon first reception of a DCF (OTA or via other mechanisms) the Terminal SHOULD inspect the DCF for the presence of a silent header. If the silent-method is “in advance” and the Terminal does not have any valid ROs for this DCF then the Terminal SHOULD attempt to retrieve the RO using the URL from the silent header of the DCF as defined in OMA DRM v2.1 [2]. The Terminal SHOULD maintain a list of DCFs that contain a silent header with the silent-method set to “in advance”. If the Terminal determines that any RO has expired (either as part of a rendering operation or as part of some automatic RO deletion process, see DRM-0340) the Terminal SHOULD check this list to determine whether it has valid ROs for the DCFs on this list. If it does not, the Terminal SHOULD attempt to retrieve the appropriate RO(s) using the URL from the silent header of the DCF as defined in OMA DRM v2.1 [2].	DRM-0340
DRM-0440	Where a DCF includes a Silent URL, a connection to this URL SHALL be automatically triggered by the Terminal whenever a valid Parent Rights Object or Child Rights Object would be missing / expired, in order to allow the User to render the content. Depending on the silent method indicated in the header, the Terminal MAY require the rights in advance, at the earliest opportunity (silent method: “in-advance”) or on demand when the User chooses to play the content (silent method: “on-demand”).	
DRM-0450	The Terminal SHALL support metering as defined in OMA DRM v2.1 [2]	
DRM-0460	When roaming internationally, the requirements DRM-0460.1, DRM-0460.2 and DRM-0460.3 below SHALL apply:	DRM-0460.1 DRM-0460.2 DRM-0460.3

REQ. ID	REQUIREMENT	REFERENCES
DRM-0460.1	Unless specified differently by the user (see DRM-0460.3), the Silent URL SHALL NOT be triggered silently. The Terminal SHALL present the User with a message. For recommended prompt, see section 3.1.12, requirement DRM-0740.	DRM-0460.3 DRM-0740
DRM-0460.2	The reception of a WAP Push ROAP Trigger (whether XML or WBXML) SHALL be discarded, unless specified differently by the user (see requirement DRM-0460.3).	DRM-0460.3
DRM-0460.3	The Terminal MAY provide means to the User to enable customisation of the settings in DRM-0460.1 and DRM-0460.2	DRM-0460.1 DRM-0460.2

3.1.8 CONTENT SEPARATION

REQ. ID	REQUIREMENT	REFERENCES
DRM-0470	To ensure, that the Terminal can differentiate between different content types (e.g. ring tone versus full track music) and respectively their usage by different applications, the terminal SHALL support content differentiation as defined in OMA-DRM-REL-V2.1 [2] and enforce OMNA / DRMS system registrations.	

3.1.9 CONTENT SHARING

3.1.9.1 Superdistribution

REQ. ID	REQUIREMENT	REFERENCES
DRM-0480	The Terminal SHALL support the reception of DCF files from other Users via the following means where supported by the Terminal:	
DRM-0480.1	Via Email	
DRM-0480.2	Via wireless connections such as Bluetooth®, IrDA®	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0480.3	Via wired connections such as USB or cable	
DRM-0480.4	Via removable storage media	
DRM-0490	The Terminal SHOULD support the reception of DCF files from other Users via any means not listed in DRM-0480 and related sub-requirements where supported by the Terminal and where the means also allow the reception of unprotected content.	DRM-0480
DRM-0500	The Terminal SHALL support the following file extension as defined in OMA DRM V2.1 • o4a for audio • o4v for video • odf	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0500.1	When downloading a DCF that has a known OMA DRM file extension (.o4a, .o4v or .odf), the Terminal SHALL store the file with that file extension. If when downloading a DCF there is no file extension specified or the DCF has a file extension which is not recognised (i.e. not one of the known OMA DRM file extensions), then the DCF SHALL be stored as follows: - If the default media type of the Content Object(s) in the DCF is audio then the DCF file extension SHALL be ".o4a" - If the default media type of the Content Object(s) in the DCF is video then the DCF file extension SHALL be ".o4v" - For all other media types the DCF file extension MUST be ".odf". (Note: The download method itself may specify the filename by a number of means depending on other Terminal specifications that are not in scope of this document e.g. downloaded filename, from DLOTA 'name' parameter, use of RFC2183 [12] Content-Disposition method, etc).	
DRM-0500.2	When receiving a DCF via superdistribution, the Terminal MAY rely on file extensions .o4a and .o4v to determine the type. Note: For files with extension .odf, the DCF file header will need to be inspected to determine file type(s) (e.g. ContentType field in 'odhe' headers).	
DRM-0510	Unless a DCF is marked Forward Locked (according to OMA DRM v1.0, section 5.5 [6]), the Terminal SHALL support distribution of protected content via the following means where supported by the Terminal:	
DRM-0510.1	Via Email	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0510.2	Via wireless connections such as Bluetooth®, IrDA®)	
DRM-0510.3	Via wired connections such as USB or serial port	
DRM-0510.4	Via removable storage media	
DRM-0515	The Terminal SHOULD support the distribution of DCF files to other Users via any means not listed in requirement DRM-0510 where supported by the Terminal and where the means also allow the forwarding of unprotected content and the DCF is not marked as Forward Locked (according to OMA DRM v1.0, section 5.5 [6]).	DRM-0510
DRM-0520	The Terminal SHALL provide the ability for the User to be able to choose whether to forward the DCF or to forward the ContentURL only.	
DRM-0530	When Users choose to forward the ContentURL, the Terminal SHALL provide the User with the ability to forward it via the following means where supported by the Terminal:	
DRM-0530.1	SMS	
DRM-0530.2	Messaging Services, including but not limited to MMS, Email	
DRM-0530.3	The Terminal SHALL provide the User with the ability to add text to the message containing the ContentURL or the DCF they want send via SMS, MMS or e-mail.	
DRM-0540	The Terminal SHALL support the ‘transaction tracking’ mechanism as defined in OMA DRM v2 section 12.3 [1].	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0540.1	The Terminal SHALL ensure the consent of the User for transaction tracking related operations performed by the Terminal to ensure the privacy issues of the User.	
DRM0540.2	The Terminal SHALL provide the User with the option to provide his consent for transaction tracking per Rights Issuer or once for all further requests.	
DRM-0540.3	The Terminal SHALL provide the ability for the User to be able to revoke at any time the consent for transaction tracking he has given. The Terminal SHALL provide the User with the option to revoke on a per Rights Issuer basis or to revoke all consent at the same time.	

3.1.9.2 Domain Sharing

REQ. ID	REQUIREMENT	REFERENCES
DRM-0550	An OMA DRM v2 [1] enabled Terminal SHALL be capable of joining Domains established by a RI with which that Terminal has previously established a RI Context.	
DRM-0560	The Terminal supporting the Domain feature SHALL conform to the protocols and operations identified within the OMA DRM v2 specification [1] for joining and leaving a Domain as well as for acquiring Domain Rights Objects.	
DRM-0590	The Terminal SHALL be capable of belonging to multiple Domains simultaneously provided by the same RI (i.e. multiple Domains based on the same RI Context). The Terminal must be capable of belonging to at least 6 Domains at any time distributed among the established RI Contexts supported. The maximum number of Domains any Terminal MAY support based on a single RI Context will be decided by the RI involved.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0600	The Terminal SHALL be capable of supporting the storage and use of multiple Domain Keys for the different generations of the same Domain for every Domain in which the Terminal is a member. Note: The Terminal is capable to support up to 999 generations of a Domain as defined in OMA DRM v2 [1], however the individual Rights Issuer is able to limit this number.	
DRM-0610	The Terminal SHALL support receiving and installing the Domain Rights Objects using any of several mechanisms including in a ROAP-RO Response message or as a separate object or inside a DCF.	
DRM-0620	The Terminal SHALL insert all the Domain Rights Objects in the DCF as soon as possible and before the DCF leaves the Terminal. The Terminal MAY take this action immediately after download or after first rendering, however this SHOULD not impact the performance of the Terminal.	
DRM-0625	In case where one or more Rights Object are already present in the DCF, then the Rights Object to insert must be inserted at the first position in the list of Rights Objects. [9]	
DRM-0630	The Terminal SHALL check all Domain ROs embedded within a DCF when attempting to render that DCF:	
DRM-0630.0	The Terminal SHALL always attempt to install all received Domain Rights Object within a DCF.	

[9] First position is the first slot closest to the head of the Mutable DRM Information box.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0630.2	If the Terminal discovers that all inserted Rights Objects fail (i.e. Terminal cannot join the domain), the Terminal SHALL use the RI URL of the first Domain Rights Object in the list to connect to that RI[10].	
DRM-0640	When a Terminal receives content bound to a Domain, which the Terminal does not belong to, it SHALL conform as defined in section 8.6.2.1 of OMA DRM v2 [1]. In this case, the Terminal SHALL send an HTTP GET to the URL specified in the RI URL attribute of the roap:ROPayload.	

3.1.10 TRUST MODEL

OMA DRM v2 [1] provides a solution which is only as strong as the quality of the implementation. A Trust Model is fundamentally a set of processes, implementations and legal agreements that provide Content Providers with assurance that their content can be safely distributed to consumers.

In OMA DRM v2 [1], a Public Key Infrastructure (PKI) is used to provide the security model. However, the implementation of the PKI is not defined, but is required to enable a complete solution. A generic Trust Model for OMA DRM v2 [1] must, therefore, provide:

- A Public Key Infrastructure (PKI) with a trusted root, a security framework to which all parties agree
- the provision of the Certificate Authority (CA) root certificate to Terminals and servers
- the provision of individual certificates and private keys for Terminals
- the provision of individual certificates and private keys for Rights Issuers
- a legal framework including obligations and limitations on liabilities
- robustness rules for server and Terminal implementations

[10] Assumption: The Terminal shall follow the behaviour as stated in DRM-0200.1, unless there is a Silent URL in the DCF. In this case, the user shall not be prompted, unless roaming (see DRM0460.1).

- compliance rules

The end goal is to ensure that end Users may only use the content that they obtain in the manner in which the content provider and distributors allow and that badly implemented Terminals or Rights Issuers are removed from the trusted DRM system.

Service Providers (RI) may choose to set up their own Trust Model or use an existing one. If an operator uses their own trust model, interoperability may be difficult with other operators using a different trust model as the PKI will be different. Solutions such as cross certification of root CAs may be possible, but is dependent upon agreements between the trust model providers and the legal provisions for each.

Depending on the trust model selected, Terminals must meet the Terminal robustness requirements, secure clock requirements and other DRM-related security issues specified by that trust model.

To date, the only known industry wide Trust Model existing is CMLA.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0650	The Terminal SHALL meet all further requirements as specified by the trust model chosen by the operator.	
DRM-0660	Where operators have selected CMLA as the trust model, the following SHALL apply:	
DRM-0660.1	The Terminal SHALL meet all requirements on CMLA compliant Terminals as outlined in the "CMLA Client Adopter Agreement" [13].	
DRM-0660.2	A CMLA production Terminal key pair with the corresponding certificate and the CMLA Production CA root certificate SHALL be installed on the Terminal.	

3.1.11 SECURE IMPLEMENTATION

REQ. ID	REQUIREMENT	REFERENCES
DRM-0670	The Terminal SHALL ensure that the User or any third party (e.g. malware) is not able to manipulate the permissions and rights associated with the DRM protected content.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0680	The Terminal SHALL ensure that the User or any third party (e.g. malware) is not able to roll back or manipulate the DRM Time used by the DRM system in order to change usage rights.	
DRM-0685	The Terminal SHALL support the DRM security requirements as defined in OMTP Trusted Environment TR0, Chapter 10 [14].	

3.1.12 PROMPTING RECOMMENDATIONS

With usability being one of the key success factors for adoption of DRM enabled services, it is important to ensure that the Terminal implementations respect usability principles as outlined in section 2.2.3.

The following list of terminologies and recommendations are intended to provide *guidance* to manufacturers when implementing user notifications as required in chapter 2.

The recommendations are based on findings from the GSMA DRM Usability conducted in the UK, Germany, Netherlands and the US in 2006 [15], with further inputs from operator and OMTP UE experts.

It is the expectation that implementations closely follow the OMTP recommendations (to ensure similar user experiences across Terminals) unless operators specifically request different implementations.

Overview of recommended terminology:

Functionality	Terminology
Rights Object	Licence
Acquiring Rights Object	Processing
Rights Object delivered	Complete
No valid Rights Object	Locked
Valid Rights Object	Unlocked
Attempt to render content without valid Rights Object	[Content name] is locked. Would you like to unlock it now?
Domain	Device Network

Join Domain	Connect to Device Network
Leave Domain	Remove from Device Network

The table lists the recommended wordings for a prompt where such has been required in the previous sections.

REQ. ID	RECOMMENDATION	REFERENCES
DRM-0690	Relevant Requirement: DRM-0120 "Download of <FILE ABC> complete. Open File? YES / NO". If "YES" is selected, the appropriate player SHALL be launched such that the content is rendered. If "NO" is selected, the User SHALL be returned to the browsing session or the application that initiated the download.	DRM-0120
DRM-0700	Relevant Requirement: DRM-0200.1 "<FILE ABC> is locked. Do you want to unlock it? YES / NO". The default SHOULD be "YES". In the case of "YES", the DRM agent SHALL launch the browser.	DRM-0200.1
DRM-0710	Relevant Requirement: DRM-0271 "Unable to open <File ABC>. Delete File? YES / NO" The default SHOULD be "NO".	DRM-0271
DRM-0720	Relevant Requirements: DRM-0285.1 & DRM-0285.2 “<FILE ABC> cannot be unlocked. Delete? YES/NO”. The default SHOULD be "YES".	DRM-0285.1 DRM-0285.1 .2
DRM-0725	Relevant Requirement: DRM-0285.3 “<FILE ABC> cannot be unlocked now. Please try again later.	DRM-0285.3

REQ. ID	RECOMMENDATION	REFERENCES
DRM-0730	Relevant Requirement: DRM-0150 “Processing…”	DRM-0150
DRM-0740	Relevant Requirement: DRM-0460.1 "<FILE ABC> is locked. Do you want to unlock it? YES / NO. Additional data charges may apply.” Default SHOULD be "YES". In case of "YES", the DRM agent SHALL launch the browser.	DRM-0460.1

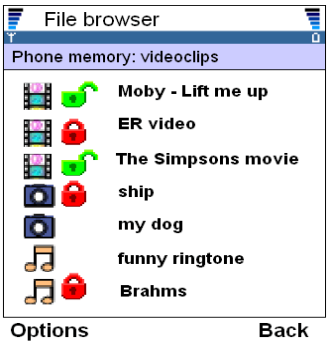
3.1.13 DRM ICON REQUIREMENTS

In order to ensure a similar user experience on different domain Terminals, the following requirements are defined with the intention to harmonize the use of a DRM icon across Terminals and across operators.

The requirements are based on findings from the GSMA DRM Usability Study [15] which clearly indicates the DRM padlock as most suitable icon.

It is the expectation that implementations closely follow the OMTP requirements (to ensure similar user experiences across Terminals) unless operators specifically request for different implementations.

REQ. ID	REQUIREMENT	REFERENCES
DRM-0750	The Terminal SHALL present the status of the DCF to the User by means of the relevant icon (called DRM icon).	
DRM-0750.1	The Terminal SHALL NOT present a DRM icon for a content item that is not protected or is marked Forward Lock (according to OMA DRM v1.0, section 5.5 [6]).	
DRM-0750.2	The Terminal SHALL present a “green open padlock” icon where a content item has valid rights.	
DRM-0750.3	The Terminal SHALL present a "red closed padlock" icon where a content item cannot be rendered either because no rights are existing - or these have expired, or the Terminal is not member of the domain the content is bound to.	

REQ. ID	REQUIREMENT	REFERENCES
DRM-0750.4	The Terminal SHALL ensure that the DRM icon is clearly recognisable as padlock, in line with the attached icon. The Vendor proposal is to be approved by the operator. 	
DRM-0750.5	The Terminal SHALL not present another icon where count or time based rights are used.	

4 RECOMMENDATION FOR MID TERM SUPPORT

Note. The following requirement enables the use case outlined in section 2.3 Support of Key Use Cases for mid term implementation and is recommended for the time being as the respective OMA specification [4], formerly known as 'Secure Removable Media' (SRM), is still being worked on:

REQ. ID	REQUIREMENT	REFERENCES
DRM-0760	The Terminal SHOULD support SRM, as defined in OMA-SRM V1.0 [4].	
DRM-0.760.1	If the Terminal supports SRM it SHALL, as a minimum, implement SRM support with respect to the UICC, i.e. this does not prevent the implementation of additional SRM support with respect to other removable media.	

5 FUTURE WORK

As stated in section 2, this document focuses on the **most prominent use cases** to ensure that the relevant set of requirements can be delivered in the **short term**.

However, there are further requirements that are relevant and need to be addressed to ensure support in the **mid term and long term** respectively. These are to be addressed as direct follow-up work. They include but are not limited to the following (order does not reflect the priority):

- Support for content sharing also with unconnected Terminals
- Support for the content types not listed yet but as supported by the Terminal: Programs and/or applications
- Support for protection of content streams and PDCF as a file format.
- Support for receiving and sending protected content via messaging clients (e.g. MMS or Email) and rendering such content as part of the message.
- Support for multipart DCF
- Export to other DRM Mechanisms
- Further Transaction Tracking related requirements as applicable (in order to enhance usability etc.)
- Support of DCFs with Preview URLs (e.g. if such DCFs are included in playlists)
- Support for a DCF that includes more than one GroupID box.

6 DEFINITION OF TERMS

TERM	DESCRIPTION
CONNECTED TERMINAL	A Terminal that is capable of directly connecting to a Rights Issuer using an appropriate protocol over an appropriate wide area transport/network layer interface. (example, HTTP over TCP/IP)
DOMAIN	A set of Devices, which are able to share Domain Rights Objects. Devices in a Domain share a Domain Key. A Domain is defined and managed by an RI
DOMAIN CONTEXT	The Domain Context consists of information necessary for the Device to install Domain Rights Objects, such as Domain Key, Domain Identifier and Expiry Time.
DOMAIN EXPIRY TIME	An absolute time after which the Device is not allowed to install ROs for this Domain. Usage of ROs installed before the expiry time are not affected by the expiry.
DOMAIN IDENTIFIER	A unique string identifier of the Domain Key
DOMAIN KEY	A 128 bit symmetric cipher key
DRM AGENT	The DRM Agent is the application that sits on the consumer's Terminal and performs the decryption of downloaded content, using rights object and DCF.
DRM TIME	A secure, non user-changeable time source. The DRM Time is measured in the UTC time scale.
PORTAL	The portal is considered to be the business interface from the end User to the Rights Issuer for the express purpose of purchasing/ obtaining content and/or usage rights. There are two ways in which the User will enter the RI portal. The first is via a normal browser session where the User chooses a specific piece of content and makes a purchase of the usage rights. The second method is where a customer has received a piece of protected content or a link to that content and connects to a specific URL for the usage rights. The portal may be accessed either from the User Terminal (example: a small screened mobile phone type Terminal) or through a PC or other computer.
PROTECTED CONTENT	Media objects (ring tones, music or video clip etc.) that are consumed according to a set of permissions and rights objects. The term "DCF" is used as synonym for a Protected Content object in line with the OMA DRM specifications.

TERM	DESCRIPTION
RENDERING SOFTWARE	Rendering Software is the software which executes on a Terminal and includes both the rendering aspects and the applicable codec required to convert the file into a format which the Terminal can render.
RIGHTS ISSUER	The Rights Issuer (RI) is the party who is in control of the sell/offer component. It will define the usage permissions and constraints for a particular piece of content (what can be done with the content (example: view, copy, forward), how long can the content be used (example: time based, count based), on which Terminals can content be used (example: mobile, PC). In addition, the RI will define the requirements Terminals must fulfill to qualify for download of protected content (example: supported trust model). The content provider and the Rights Issuer may be the same, however could also be managed by different parties.
RIGHTS OBJECT	A collection of Permissions and other attributes which are linked to Protected Content.
SERVICE PROVIDER	The Service Provider (SP) is the party providing the content download service to the mobile User.
SILENT URL	A DCF file may contain a Silent header that indicates to the Terminal that the Rights Object for this protected content can be silently obtained from the Rights Issuer without user consent. The Silent URL is the URL to request the Rights Object from.
STATEFUL RIGHTS	Stateful Rights are Rights Objects for which the Terminal has to explicitly maintain state information, so that the constraints and permissions expressed in the RO can be enforced correctly. An RO containing any of the following constraints or permissions is considered Stateful Rights :<interval>, <count>, <timed-count>, <datetime>, <accumulated> or <export>.
TERMINAL	A Terminal is the entity (hardware/software or combination thereof) within a user-equipment that implements a DRM Agent. It is used as an alternative term for a cellular telephone, device or handset.
TRUST MODEL	A Trust Model is an industry-agreed set of technical specifications, robustness and compliance rules, enforceable legal obligations and limits of liability.
UNCONNECTED TERMINAL	An “Unconnected Terminal” is a simple Terminal that does not support an IP network connection (e.g. connects only through USB bus)

TERM	DESCRIPTION
UNLOCK CONTENT	Obtaining the appropriate Rights Object such that the Terminal is able to decrypt the Protected Content File for further usage.
USER	A “User” is the human user of a Terminal. The User does not necessarily own the Terminal.
WHITELIST	A list containing the names of authorised RIs.

7 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
CD	Combined Delivery
DCF	DRM Content Format
DD	Download Descriptor
DRM	Digital Rights Management
DRMS	Digital Rights Management System
FL	Forward Lock
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority Digital Rights Management System
OS	Operating System
PC	Personal Computer
PDCF	Packetised DCF
RI	Rights Issuer
RI URL	Rights Issuer URL
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
URI	Universal Resource Identifier
SD	Separate Delivery
SIM	Subscriber Identity Module
SP	Service Provider
SRM	Secure Removable Media

ABBREVIATION	DESCRIPTION
UAPROF	User Agent Profile
UI	User Interface
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
WAP	Wireless Application Protocol
WBXML	WAP Binary XML
XML	Extensible Markup Language

8 REFERENCED DOCUMENTS

NO.	DOCUMENT	AUTHOR	DATE
1	OMA-DRM v2 OMA Digital Rights Management V2.0 OMA-TS-DRM-DRM-V2_0-20060303-A Version 2.0.	OMA	03 Mar 2006
2	OMA DRM v2.1 http://member.openmobilealliance.org/ftp/Public_documents/DRM/Permanent_documents/	OMA	
3	RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels	IETF	
4	OMA-SRM V1.0. OMA Secure Removable Media Specification OMA-TS-SRM-V1_0-20070320-D[11]	OMA	02 Feb 2007
5	OMA DRM v1.0 Digital Rights Management OMA-Download-DRM-v1_0	OMA	15 June 2004
6	OMA Download v1.0 OMA-Download-OTA-V1_0	OMA	15 June 2004
7	RFC2616 http://rfc.net/rfc2616.html	The Internet Society	June 1999
8	OMA Download v2.0 OMA-Download-OTA-V2_0	OMA	
9	3GPP TS26.244	3GPP	

[11] This reference will be updated with the Candidate Enabler Version number and\or the Approved Enabler Version as soon as they become available.

No.	Document	Author	Date
10	RFC 2068 Hypertext Transfer Protocol - HTTP 1.1 http://www.ietf.org/rfc/rfc2068.txt?number=2068	IETF	January 1997
11	DRM Content Format V2.0 OMA-TS-DRM-DCF-V2_0	OMA	03 March 2006
12	RFC2183 http://www.ietf.org/rfc/rfc2183.txt	IETF	August 1997
13	CMLA Client Adopter Agreement v1.2-070326	CMLA	26 Mar 2007
14	OMTP Trusted Environment TR0 Version 1.1, Release 1 Author: OMTP Hardware Working Group.	OMTP	27 Mar 2006
15	GSMA DRM Usability Recommendations Version 1.0 Document can be made available on request. Please contact GSMA.	GSMA	Sept 2005

APPENDIX 1 - NOTES ON CHANGES FROM V1.3

If the wording of a requirement in v1.3 has been changed, then a new requirement id is assigned in this version, unless otherwise stated in the table below.

Unless otherwise stated in the table below, where the requirement id is unchanged between version 1.3 and this version, then the wording of the recommendation is also unchanged.

REQ. ID	COMMENT
DRM-0040.3	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0040) is unchanged
DRM-0060.1	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0060) is unchanged
DRM-0190.2	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0190) is unchanged
DRM-0190.3	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0190) is unchanged
DRM-0200.1	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0200) is unchanged
DRM-0210.1	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0210) is unchanged
DRM-0480.2	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0480) is unchanged
DRM-0480.3	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0480) is unchanged
DRM-0500.1	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0500) is unchanged
DRM-0510.2	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0510) is unchanged
DRM-0510.3	The wording of this requirement has changed since version 1.3, but the parent requirement (DRM-0510) is unchanged
DRM-0620	The wording of this requirement has changed since version 1.3 but only for clarification reasons. The requirement id has been left unchanged.

End of Document.