DRM Content Format

Candidate Version 1.0 – 13 Nov 2003

Open Mobile Alliance
OMA-Download-DRMCF-v1_0-20031113-C

Contents

Tables

1. Scope

Open Mobile Alliance (OMA) Wireless Application Protocol (WAP) is a result of continuous work to define an industry-wide specification for developing applications that operate over wireless communication networks. The scope for the Open Mobile Alliance is to define a set of specifications to be used by service applications. The wireless market is growing very quickly, and reaching new customers and providing new services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation, and fast/flexible service creation, WAP defines a set of protocols in transport, session and application layers. For additional information on the WAP architecture, refer to "*Wireless Application Protocol Architecture Specification"* [WAPARCH].

The scope of OMA "*Digital Rights Management*" is to enable the controlled consumption of digital media objects by allowing content providers to express usage rights, e.g., the ability to preview DRM content, to prevent downloaded DRM content from being illegally forwarded (copied) to other users, and to enable superdistribution of DRM content. The defined technology is an initial DRM system that can be extended into a more comprehensive and secure DRM system.

The scope for this specification is to define the content format for DRM protected encrypted media objects and associated metadata. The content format is intended to be used in the separate delivery DRM method defined in the OMA "*Digital Rights Management*" specification.

2. References

2.1 Normative References

[CREQ] "Specification of WAP Conformance Requirements". WAP Forum™. WAP-221-CREQ. http://www.openmobilealliance.org/

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. http://www.ietf.org/rfc/rfc2234.txt

[RFC2392] "Content-ID and Message-ID Uniform Resource Locators". E. Levinson. August 1998. http://www.ietf.org/rfc/rfc2392.txt

[RFC2396] "Uniform Resource Identifiers (URI): Generic Syntax". T. Berners-Lee, R. Fielding, L. Masinter. August 1998. http://www.ietf.org/rfc/rfc2396.txt

[RFC2616] "Hypertext Transfer Protocol -- HTTP/1.1". R. Fielding, et al. June 1999. http://www.ietf.org/rfc/rfc2616.txt.

[RFC2630] "Cryptographic Message Syntax". R. Housley. June 1999. http://www.ietf.org/rfc/rfc2630.txt

[WSP] "Wireless Session Protocol". WAP Forum™. WAP-230-WSP. http://www.openmobilealliance.org/

[DRMREL] "DRM Rights Expression Language". Open Mobile Alliance™. OMA-Download-DRMREL-v1_0. http://www.openmobilealliance.org/

2.2 Informative References

[WAPARCH] "WAP Architecture". WAP Forum™. WAP-210-WAPArch. http://www.openmobilealliance.org/

[DRM] "Digital Rights Management". Open Mobile Alliance™. OMA-Download-DRM-v1_0. http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 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].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Asset	Content governed by rights. See DRM content.
Composite object	A media object that contains one or more media objects by means of inclusion e.g. DRM messages, zip file.
Content	A media object
Consuming device	A mobile device consuming DRM content.
DRM agent	A user agent in the device that enforces the rights and controls the consumption of DRM content on the device.
DRM content	Content that is consumed according to a set of rights. DRM content may be in encrypted DRM Content Format or in plaintext delivered inside a DRM message
DRM message	A message containing a media object and an optional rights object. Media objects received inside a DRM message must not leave the device. The optional rights object defines additional consumption rules for the media object.
Media object	A digital resource e.g. a ringing tone, a screen saver, a Java game or a composite object.
Media type	A MIME media type.
Rights	Permissions and constraints defining under which circumstances access is granted to DRM content.
Rights issuer	An entity who issues rights objects.
Rights object	An instance of rights
Separate delivery	Delivery of the rights object and content via separate transports.
Superdistribution	A mechanism that (1) allows the end user to redistribute the encrypted DRM content to other end users through potentially insecure channels and (2) enables the receipients to obtain initial rights for the superdistributed DRM content.

3.3 Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CEK	Content Encryption Key
DRM	Digital Rights Management
HTTP	Hypertext Transfer Protocol
MIME	Multipurpose Internet Mail Extensions
OMA	Open Mobile Alliance
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
WAP	Wireless Application Protocol
WSP	Wireless Session Protocol

4. Introduction

OMA Digital Rights Management [DRM] defines a separate delivery DRM method in which the media object is encrypted and the rights containing the encryption key are delivered to the device via WAP push.

This specification defines the DRM content format for the encrypted media object. In addition to encrypting the media object the DRM content format supports metadata such as

- Original content type of the media object
- Unique identifier for this DRM protected media object to associate it with rights
- Information about the encryption details
- Information about the rights issuing service for this DRM protected media object

The metadata can be easily extended by using a mechanism similar to HTTP and MIME headers.

The DRM Content Format is closely related to the Rights Expression Language specification [DRMREL] that defines the syntax and semantics for the rights objects.

5. DRM Content Format

This section defines the content format for protected DRM content.

5.1 Media type

The MIME type for objects conforming to the format defined in this section MUST be

```
application/vnd.oma.drm.content
```

5.2 Application/vnd.oma.drm.content

The structure of DRM protected content MUST be according to the table below.

Table 1. DRM content fields

Field name	Type	Purpose
Version	Uint8	Version number
ContentTypeLen	Uint8	Length of the ContentType field
ContentURILen	Uint8	Length of the ContentURI field
ContentType	ContentTypeLen octets	The MIME media type of the plaintext data.
ContentURI	ContentURILen octets	The unique identifier of this content object.
HeadersLen	Uintvar	Length of the Headers field
DataLen	Uintvar	Length of the Data field
Headers	HeadersLen octets	Headers define additional meta data about this content object.
Data	DataLen octets	The encrypted data

Uint8, uintvar and octet are as defined in Wireless Session Protocol [WSP].

DataLen includes the size of the encrypted data plus the initialization vector described in section 5.2.4.1.

5.2.1 Version

The *Version* field defines which version of DRM Content Format specification was used by the author of the content object. The value for the *Version* field MUST be 1 for objects conforming to this specification.

5.2.2 ContentURI

The *ContentURI* field MUST contain a unique identifier for this DRM protected content object. The value MUST be a URI according to [RFC2396]. It is the responsibility of the content author to guarantee the uniqueness of the *ContentURI.* URI schemes like “cid:local-part@domain” as defined in [RFC2392] MAY be used.

If the content object is referenced from a DRM rights object, the value of the *ContentURI* field MUST match the value of the referencing element of the rights object as defined in [DRMREL].

5.2.3 ContentType

The *ContentType* field MUST define the original MIME media type of the DRM protected content i.e. what content type the result of a successful decryption of the *Data* field represent.

5.2.4 Headers

The *Headers* field MAY contain headers defining additional meta data about the content. The headers are represented by name value pairs similar to HTTP headers [RFC2616]. Each header is defined using augmented Backus-Naur Form (BNF) [RFC2234].

Headers are encoded using textual encoding.

5.2.4.1 Encryption-Method header

The *EncryptionMethod* header defines how the encrypted content can be decrypted. The Augmented BNF grammar for the Encryption-Method header is defined below:

```
Encryption-Method := “Encryption-Method” “:” algorithm-id [“;” parameter ]
algorithm-id := token
parameter :=    padding-scheme [“;” plaintext-length]
```

Values for the *algorithm-id* field are defined in the table below.

Table 2. Algorithm-id values

Algorithm-id	Semantics
“AES128CBC”	AES symmetric encryption as defined by NIST. 128 bit keys. Cipher block chaining mode (CBC). 128 bit initialization vector prefixing the ciphertext. Padding according to RFC 2630, unless overridden by the *Padding-scheme* parameter.

5.2.4.1.1 Encryption-method parameters

All of the *Encryption-method* parameters are optional.

padding-scheme

The *padding-scheme* parameter defines how the last block of ciphertext is padded.

```
padding-scheme := “padding” “=” padding-scheme-id
padding-scheme-id := token
```

Values of the padding-scheme-id field are defined in the table below:

Table 3. Padding-scheme-id values

Padding-scheme-id	Semantics
“RFC2630”	Padding according to RFC 2630.

plaintext-length

The *plaintext-length* parameter defines the length of the original plaintext. Some simple padding schemes may require that the plaintext length is explicitely defined. The device MUST support the plaintext-length parameter.

```
plaintext-length := “plaintextlen” “=” 1*DIGIT
```

If the plaintext length determined during decryption contradicts the plaintext-length signalled using the plaintext-length parameter, the plaintext length as determined during decryption precedes.

5.2.4.2 Rights-Issuer header

The *Rights-Issuer* header defines the Rights Issuer URLs. The Rights-Issuer URLs MAY be used by the consuming device to obtain rights for this DRM protected content object. The mechanism is defined in OMA DRM specification [DRM].

```
Rights-Issuer := “Rights-Issuer” “:” issuer-url CRLF
issuer-url := URI-reference
```

The value of the issuer-url MUST be a URL according to [RFC2396] , and MUST be an absolute identifier.

5.2.4.3 Content-Name header

The *Content-Name* header contains a descriptive name for this DRM protected content object. The name is only informative and the device MAY use it e.g. to derive a filename when the DRM protected object is received and stored into a local repository. Other names may be transmitted outside this object (e.g. Content-Disposition header in HTTP) and they may override the name specified in this element.

```
Content-Name := “Content-Name” “:” *TEXT CRLF
```

5.2.4.4 Content-Description header

The *Content-Description* header contains a description of the DRM protected content object. This text is informative and the device MAY display it to the user prior to using the Rights-Issuer-URL field.

```
Content-Description := “Content-Description” “:” *TEXT CRLF
```

5.2.4.5 Content-Vendor header

The *Content-Vendor* header contains a textual string representing the name of the organisation that provided the media object. This text is informative and the device MAY display it to the user prior to using the Rights-Issuer URL field.

```
Content-Vendor := “Content-Vendor” “:” *TEXT CRLF
```

5.2.4.6 Icon-URI header

The *Icon-URI* header contains a URI where an appropriate icon for this content may be retrievable from. The device MAY use this header to request the object at this URI, and if an appropriate content is returned, use this as an icon associated with the content to the user.

The value of the Icon-URI MUST be a URI according to [RFC2396].

```
Icon-URI := “Icon-URI” “:”  URI-reference CRLF
```

5.2.4.7 Unsupported headers

Content author MAY insert additional headers to the *Headers* field. Additional headers MUST follow the generic syntax defined below.

```
Other-Header := Header-name “:” Header-value CRLF
Header-name := token
```

```
Header-value := *TEXT
```

Consuming devices MUST ignore headers that they do not recognize.

Appendix A Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
OMA-Download-DRMCF-v1_0-20020913-C	13 Sept 2002	n/a	Initial candidate specification
OMA-Download-DRMCF-v1_0-20030327-C	27 Mar 2003	5.2.4.1, Appendix C	Modifications to Encryption-Method header
OMA-Download-DRMCF-v1_0-20030619-C	19 June 2003	5.2.4.2	Restrict Rights-Issuer URL to absolute identifier
OMA-Download-DRMCF-v1_0-20030801-C	01 Aug 2003	5.2.4.1, Appendix B	Removed NULL padding (OMA-MAG-DLDRM-2003-0137)
		5.2.4	Replaced the use of “token” in the headers with “URI-reference” or “*TEXT” as appropriate and terminate headers with CRLF (OMA-MAG-DLDRM-2003-0141)
OMA-Download-DRMCF-v1_0-20031113-C	13 Nov 2003	5.2, Appendix C	Clarify informative example in DCF specification to show “Datalen” header reflects the combination of the original data size plus the 128 bit initialization vector. [OMA-MAG-DLDRM-2003-0256]

Appendix B Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [CREQ].

B.1 Terminal Features

General terminal features

Item	Function	Reference	Status	Requirement
DRMCFT-GEN-1	AES128CBC encryption algorithm	5.2.4.1	M	
DRMCFT-GEN-2	RFC 2630 padding scheme	5.2.4.1.1	M	
~~DRMCFT-GEN-3~~	~~NULL padding scheme~~	~~5.2.4.1.1~~	~~M~~	
DRMCFT-GEN-4	Plaintext-length	5.2.4.1.1	M	
DRMCFT-GEN-5	Rights-Issuer header	5.2.4.2	M	
DRMCFT-GEN-6	Content-Name header	5.2.4.3	O	
DRMCFT-GEN-7	Content-Description header	5.2.4.4	O	
DRMCFT-GEN-8	Content-Vendor header	5.2.4.5	O	
DRMCFT-GEN-9	Icon-URI header	5.2.4.6	O	
DRMCFT-GEN-10	Ignore unsupported headers	5.2.4.7	M	

Appendix C Examples (Informative)

Example 1 – encrypted jpeg image

Application/vnd.oma.drm.content	Field name	Purpose
01	Version	Version number
0A	ContentTypeLen	Length of the ContentType field
17	ContentURILen	Length of the ContentURI field
image/jpeg	ContentType	The MIME media type of the plaintext data.
cid:image239872@foo.bar	ContentURI	The unique identifier of this content object.
72	HeadersLen	Length of the Headers field (= decimal 114 as Uintvar)
74	DataLen	Length of the Data field (= decimal 116[1] as Uintvar)
Encryption-Method: AES128CBC;padding=RFC2630;plaintextlen=100 Content-Name: “Kilimanjaro Uhuru Peak” Rights-Issuer: http://foo.bar/pics/image239872	Headers	Headers define additional meta data about this content object.
03, 01, 6A, …	Data	The encrypted data. 100 bytes of encrypted jpeg image.

[1] Length of the data field includes the size of the encrypted data (100 bytes) plus the 16 byte initialization vector as described in section 5.2.4.1.