3GPP TSG-SA WG3 Meeting #37 **S3-050104**
Sophia Antipolis, France, 21–25 February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **054** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	MBMS download protection details
Source:	⌘	Nokia
Work item code:	⌘	MBMS
Date:	⌘	18/02/2005
Category:	⌘	**C**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	Align with the proposal from OMA BAC DLDRM
Summary of change:	⌘	The name of MBMSSignature Box is changed because of the generic nature of this feature. The definition of the special value 1 of the flags field in the CommonHeaders box is unnecessary as the structure of the value of the RightsIssuerURL field is enough information to prevent misunderstanding of a MBMS DCF in a general OMA DRM context, or vice versa. Deletion of the editor's note in 6.6.3
Consequences if not approved:	⌘	MBMS download protection is not conforming OMA DRM v2.0

Clauses affected:	⌘	6.6.3, 6.6.3.2

		Y	N			
Other specs affected:	⌘	Y		Other core specifications	⌘	26.346
			N	Test specifications		
			N	O&M Specifications		

Other comments:	⌘	

6.6.3 Protection of download content

~~Editor's Note: The details of MBMS download protection are subject to the response from OMA BAC DLDRM. SA3 has asked OMA BAC DLDRM whether it is possible to include the extensions and deviations needed for using the DCF format for MBMS download protection to OMA DRM v2.0 DCF specification. If the answer is positive, some material in this section will be removed and the OMA specification referenced instead.~~

6.6.3.1 General

Data that belongs to a download MBMS User Service is decrypted as soon as possible by the UE, if the MSK needed to provide the relevant MTK is already available on the UE.

6.6.3.2 Usage of OMA DRM DCF

When it is required to protect MBMS download content, OMA DRM V2.0 DCF as defined in reference [15] shall be used. . In particular, minor version 0x00000003 of OMA DRM V2.0 DCF specifies how DCF is used to protect MBMS download content. MBMS download contents are therefore indicated by minor version 0x00000003 in a DCF. ~~MBMS download contents are indicated by the 3GPP-MBMS-DCF flag in the Common Headers Box of a DCF.~~ OMA DRM Rights Objects are not utilized. Instead, encryption and authentication keys are generated from MTK. For integrity protection, an OMADRM~~MBMS~~Signature as specified below is attached -inside the optional Mutable DRM information box ('mdri').~~in the FreeSpaceBox~~ of the DCF.

The MBMSSignature Box is an extension to OMA DRM V2.0 DCF for use by MBMS, and is defined as follows:

```
aligned(8) class OMADRM~~MBMS~~Signature extends Fullbox('odfs~~sign~~', version, flags)
{
   Unsigned int(8) SignatureMethod;   // Signature Method
   Char            Signature[];       // Actual Signature
}

SignatureMethod Field:
NULL   0x00
HMAC-SHA1 0x01
```

The range of data for the HMAC calculation shall be according to section 5.3 of reference [15].

The correct MTK for decrypting and verifying the integrity of the download content is indicated by the key_id in the RightsIssuerURL field as follows:

mbms-key://<key_id>

where key_id is defined as the base64 encoded concatenation (Key Domain ID || MSK_ID || MTK ID).

In case the FDT of the FLUTE protocol needs to be protected, the FDT may also be wrapped in a different DCF. Confidentiality and/or integrity protection of FDT can be provided this way.

Editors' note: The optionality of FDT protection is still under study (i.e. whether it should be mandated).

LIAISON STATEMENT

Title:	Answer to LS on Adapting OMA DRM v2.0 DCF for MBMS download protection ☒ Public ☐ Confidential LS[1]
Date:	17 feb 2005
To:	3GPP SA3 contact: Tiina Koskinen, tiina.s.koskinen@nokia.com
Response to:	LS on Adapting OMA DRM v2.0 DCF for MBMS download protection (S3-041129)
Source:	BAC Download Digital Rights Management SWG of the Open Mobile Alliance
Send Replies to:	BAC Download Digital Rights Management SWG of Open Mobile Alliance OMA-LIAISON@mail.openmobilealliance.org
Contact(s):	Frank Hartung, Ericsson Research, frank.hartung@ericsson.com Oliver Bremer, Nokia, oliver.bremer@nokia.com Robert Lukassen, Philips, robert.lukassen@philips.com
Attachments:	<list of attachments> or n/a

1 Overview

This Liaison Statement is in answer to the S3-041129 Liaison Statement from 3GPP TSG WG3 Security – S3#36 in which extensions and deviations to OMA DRM v2.0 DCF for MBMS download protection have been proposed to OMA BAC DLDRM.

The proposals and extensions have been reviewed by the OMA BAC DLDRM sub working group.

2 Proposal

With the understanding that 3GPP MBMS DCF content files are used in a transient manner, and will not be exported from receiving devices in their received format, OMA BAC DLDRM does not have objections to the proposed extensions and adaptations as specified by the S3-041129 Liaison Statement.

Specifically:

- OMA BAC DLDRM proposes to define the required new semantics of the extensions and adaptations in the scope of a new minor version of the DCF structure specification. The value of this new minor version will be 0x00000003.
- OMA BAC DLDRM does not see any problem in adding the MBMSSignature Box in the Free Space Box of the OMA DRM v2.0 DCF structure.

  However, because of the generic nature of this feature, OMA BAC DLDRM proposes to change the name:

```
aligned(8) class OMADRMSignature extends FullBox('odfs', version, flags)
{
```

[1] If the "Confidential LS" box is selected, this liaison statement is intended to be Confidential per agreement by OMA and the addressed organization. Neither side should make this communication available to non-members.

```
unsigned int(0)   SignatureMethod;  // Signature Method
char              Signature[];      // Actual Signature
}
SignatureMethod field:
NULL        0x00
HMAC-SHA1   0x01
```

This box will be optional, and will appear inside the optional Mutable DRM information box ('mdri').

- OMA BAC DLDRM does not regard global uniqueness of ContentID as critical for DCF files used in the MBMS transport layer. However, if the ContentID is to propagate above the MBMS transport layer, OMA BAC DLDRM does recommend 3GPP SA3 to reconsider and define a method to ensure globally unique ContentIDs.
- OMA BAC DLDRM will define the 'mbms-key://<key_id>' mechanism as the URL scheme to use to interpret the value of the RightsIssuerURL field in case the DCF is used in the MBMS context.
- OMA BAC DLDRM feels that the new minor version number along with the structure of the value of the RightsIssuerURL field should be enough information to prevent misunderstanding of a MBMS DCF in a general OMA DRM context, or vice versa. Hence the definition of the special value 1 of the flags field in the CommonHeaders box is unnecessary.

3 Requested Action(s)

OMA BAC DLDRM requests 3GPP SA3 to review this answer and in particular see whether the changes proposed by this liaison statement are acceptable to 3GPP SA3. This refers in particular to the proposed name of the signature box and its positioning in the Mutable DRM information box, and the proposed use of the minor version number 0x00000003 instead of using the 'flags=1' indicator.

The extensions and adaptations as presented by this document will be incorporated into the specifications that are now work-in-progress. As soon as the references to the final specifications containing these extensions and adaptations are known, OMA BAC DLDRM will make these references known to 3GPP SA3. According to the current work schedule, this may be expected in August 2005.

4 Conclusion

Open Mobile Alliance, through its active sub-working group BAC-DLDRM, wishes to express its gratitude to 3GPP for considering this liaison statement.