3GPP TSG-SA WG3 Meeting #37 **S3-050125**
Sophia Antipolis, France, 21–25 February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **054** ⌘ **rev** **1** ⌘ 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 ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	MBMS download protection details
Source:	⌘	SA WG3
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 in response to suggestion from OMA where a specific version of their specification is cited (V2.0)
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 Addition of note in 6.6.3.2 to clarify specific version of OMA specification to be used
Consequences if not approved:	⌘	Incomplete specification

Clauses affected:	⌘	6.6.3, 6.6.3.2

Other specs affected:	Y	N			
⌘	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

NOTE: If the OMA DRM V2.0 DCF [15] specification is upgraded, these upgrades do not apply for the present document.

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 ~~MBMS~~OMADRMSignature 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).