3GPP TSG SA WG3 Security — S3#36
Shenzhen, China, 23–26 November 2004

Tdoc ⌘ S3-041123

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **023** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	OMA DRM DCF for protection of download services
Source:	⌘	Nokia
Work item code:	⌘	MBMS
Date:	⌘	28/10/2004
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:	⌘	It is not specified how to protect the MBMS download services
Summary of change:	⌘	Describes how OMS DRM DCF is used for download protection
Consequences if not approved:	⌘	It will remain unspecified how to protect the MBMS download services.

Clauses affected:	⌘	2, 6.5.4, 6.6.3

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

Other comments: ⌘

****** FIRST CHANGE *******

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246: "MBMS User Services".

[6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] IETF RFC 2617 "HTTP Digest Authentication".

[9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic".

[11] IETF RFC 3711 "Secure Real-time Transport Protocol".

[12] 3GPP TS 43.020: "Security related network functions".

[13] "OMA DRM Content Format", OMA-DRM-DCF-v2_0, www.openmobilealliance.org.

****** NEXT CHANGE *******

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in RFC 3830 [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and start the generation of MTK. The MGV-F provides the MTK to the ME.

The MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of RFC 3830 [9] (MIKEY).

In case of download service, MIKEY key derivation as defined in Section 4.1.3 of MIKEY [9] shall be used to derive MTK authentication and encryption keys from MTK in the ME. These keys shall be provided to the download protection protocol.

****** NEXT CHANGE *******

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. In LS S3-041057 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.

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 [13] shall be used. 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 MBMSSignature as specified below is attached in the FreeSpaceBox of the DCF.

Editor's Note: The 3GPP-MBMS-DCF flag need to be reserved from the OMA Naming Authority (OMNA).

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

```
aligned(8) class MBMSSignature extends Fullbox('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 [13].

The correct MTK for decrypting and verifiying 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 (Network ID || Key Group 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.