3GPP TSG SA WG3 Security — S3#36 **S3-040901**

23 - 26 November 2004

Shenzhen, China

Title:	**An Update to Using OMA DRM V2.0 DCF for MBMS Download Protection**
Source:	**Nokia**
Document for:	**Discussion/Decision**
Agenda Item:	**MBMS**
Work Item:	

1. Introduction

In this discussion paper, we provide an update to the initial proposal of using OMA DRM V2.0 DCF for MBMS download protection [1]. In particular, we provide more details in two aspects: how integrity protection can be achieved using DCF, and how the FLUTE File Description Table (FDT) can be protected, if needed.

A comparison study between using DCF and XML for MBMS download protection in terms of overhead required, as well as performance is given in an accompanying discussion paper [3].

Figure 1 shows the OMA DRM V2.0 DCF structure [2].

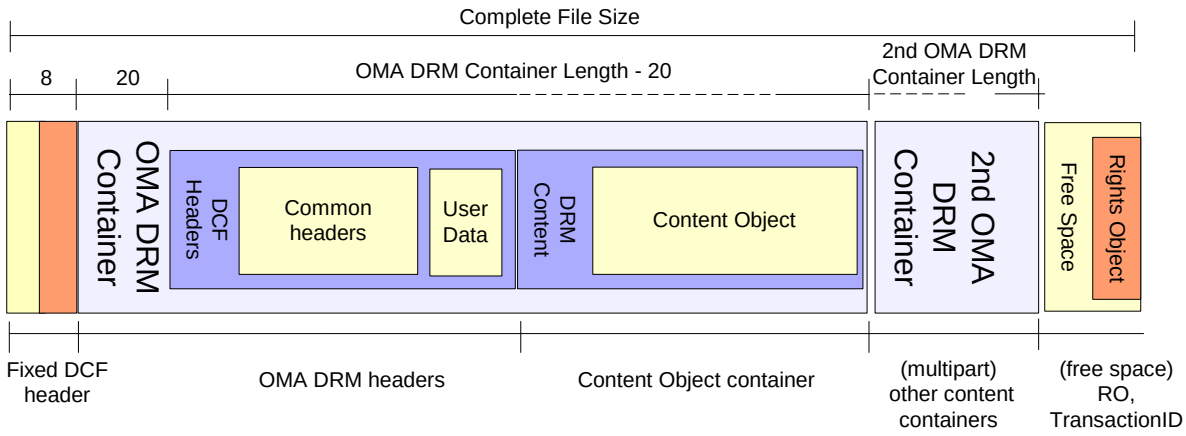

Figure 1 OMA DRM V2.0 DCF Structure.

2. Proposed Integrity Mechanism for MBMS DCF

In OMA DRM V2.0, a DCF hash is included in the Rights Object (RO), which is protected by a Right Encryption Key (REK). In MBMS, we are not using RO. To include a “signature” in the MBMS DCF (e.g. using HMAC-SHA1), we define the following extended box:

```
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 length of the signature is determined by the particular ciphersuite used and is not explicitly specified in the box. (In fact the Fullbox has a size field to indicate the size of the whole box.) The text for the hash calculation is according to Section 5.3 of OMA-DRM-DCF-v2 [2].

Note that this signature is based on shared-key mechanism. The key used in computing the HMAC is derived from MTK, which is indicated by the Key_id in the RightsIssuerURL field of the corresponding Common Headers Box.

The MBMSSignature Box can be added in the Free Space Box (see figure above). Conforming parser can verify the signature. Non-conforming parser will ignore the box.

3. Proposed FDT Protection

The FDT (File Description Table) is part of the FLUTE protocol and contains information about the files that are being transferred using FLUTE. The FDT itself is an XML document. Example of an FDT is the following:

```
<?xml version="1.0" ?>
<FDT-Instance Expires="3285666382">
          <File TOI="1"
          Content-Location="www.example.com/a_file"
          Content-Length="679936"
          Content-MD5="Tt0dxyJfU9mX9YubHsoYUA==" />
</FDT-Instance>
```

If FDT protection (encryption and/or integrity protection) is desired, it may be wrapped in another DCF, as shown in Figure 2.

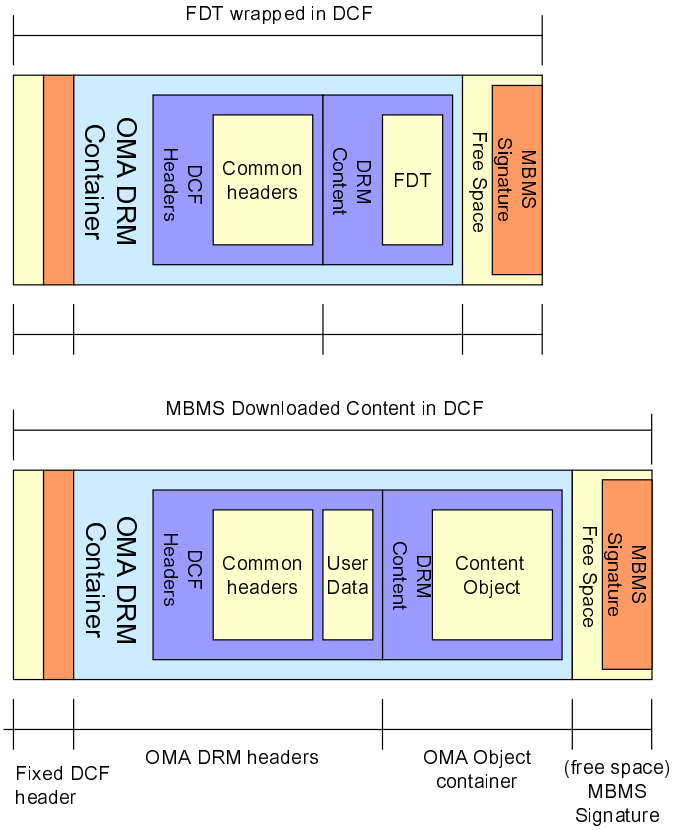

Figure 2 Proposed FDT protection using DCF.

4. Conclusions

In this discussion paper, we have provided an update to the proposal of using OMA DRM V2.0 DCF for MBMS downloaded content protection. Two issues are addressed. Firstly, a signature is defined to provide integrity protection for MBMS downloaded content using DCF based on symmetric key. Secondly, it is proposed that if FDT protection is desired, it may be protected using DCF as well. With this update, we provide a complete solution for MBMS download protection with DCF.

5. References

[1] S3-040781 Extensions to OMA DRM V2.0 DCF for MBMS Download Protection, S3#35, Oct 2004, Nokia.

[2] DRM Content Format, OMA-DRM-DCF-v2_0-20040715-C, www.openmobilealliance.org.

[3] S3-040xxx Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection, S3#36, Nokia.