3GPP TSG SA WG3 Security — S3#36 **S3-040909**

23 - 26 November 2004

Shenzhen, China

Title:	**Comments to Ericsson contribution (S3-040900) on Comparison of DCF and XML encryption for MBMS Download**
Source:	**Nokia**
Document for:	**Discussion**
Agenda Item:	**6.20**
Work Item:	**MBMS**

1. Introduction

There have been some confusion and misunderstanding about the proposal of using OMA DRM V2.0 DCF for MBMS download protection (called the “DCF proposal” in the following). This document attempts to provide clarifications regarding the DCF proposal.

The main idea behind the DCF proposal is that we believe a simple format should be chosen for protection of MBMS downloaded contents, so that over-the-air overhead can be minimized, as well as the processing needed in handling these contents. The file format defined by OMA DRM v2.0, namely, DCF, is a good candidate under these considerations. The DCF is in binary format and is probably one of the simplest formats available for encrypted data. Our proposal is simply to re-use the DCF file format for MBMS, without imposing the other requirements and assumptions needed in OMA DRM V2.0. This is explained in more details in the following.

In [1], a comparison of DCF and XML encryption for MBMS download is given. We do not agree with the discussions and we attempt to address them as follows.

2. Comments on the comparison table

The subtitles below refer to the aspects in the table summarizing the comparison of DCF and XML encryption in [1].

2.1. Required specification changes

- 3GPP-MBMS-DCF flag: OMNA as of now has not done any registrations for DCF, simply because there has been no one trying to extend DCF for other use before. It is, however, OMNA’s responsibility for such naming and numbering issues. The flags currently defined in DCF are for use by OMA DRM V2.0 contents.

  Besides, the need of the 3GPP-MBMS-DCF flag is in fact not strictly necessary. It is an optional feature in cases where a device indeed tries to store MBMS contents in its original delivered format in the DCF wrapper. In these cases, the device can quickly distinguish between DRM DCF and MBMS DCF using the 3GPP-MBMS-DCF flag. However, it is more realistic for the device to store the format as is (or in a re-encrypted form preferable by the device) once the content is downloaded and decrypted. In this case, the 3GPP-MBMS-DCF flag is not necessary. The MBMS stack knows that the received content is using MBMS-DCF format, and the MBMS module will be able to handle it appropriately (See Section 2.2 below)

- MBMS-KEY URI: Registration of this URI needs to be done with IANA. We do not see any issue with carrying the MBMS-KEY information using the RightsIssuerURL in DCF, since it is an adapted DCF for MBMS use anyway.
- DCF usage outside of DRM: It is said in [1] that explanatory text should be added to DRM and ARCH specifications to explain OMA DRM DCF usage outside DRM specification. We do not see this as necessary, as only the DCF format is borrowed here for MBMS use.
- Issues with ROs: Again, we stress that we are only borrowing the DCF file format here. The DCF format is not tied to DRM. The assumptions that a DCF may be accessed only according to permissions contained in ROs are true only to DRM downloaded objects. The MBMS module handling the MBMS-DCF does not need to be restricted by this.

In conclusion, we believe that nothing needs to be changed in the existing OMA DRM V2.0 specifications to accommodate the proposed re-use of the DCF format for MBMS purpose. The 3GPP-MBMS-DCF flag, if needed, could be registered at OMNA. The MBMS-KEY URI has to be registered at IANA.

Regarding the XML proposal, XML encryption [5] and signatures [6] require number of complex algorithms (e.g. 3DES, RSA-v1.5, RSA-OAEP and DSAwithSHA1), which are not needed by MBMS download. It is necessary to change specifications so that it is not mandatory support unnecessary algorithms.

2.2. Implementation re-use

It is true that existing OMA DRM V2.0 agents cannot be used without modifications. We never claimed that. The important point is, for future implementations, implementers have an option to re-use some of the building blocks in DRM agent for MBMS purpose. In particular, by incorporating minor changes to the DCF file parser, the same parser can be re-used for parsing MBMS download content for MBMS usage.

Regarding the XML proposal where it is claimed that XML security built into OMA DRM V2.0 (in the ROAP protocol) can be re-used for MBMS, it should be noted that in the DRM case, the DRM agent actually does not have a canonicalization module in order to reduce the complexity of the terminal. The content provider or whoever performing the encryption of the content will be responsible for performing the canonicalization of the XML document to produce a format known by the DRM agent.

In cases where DRM agent does not exist in a device, implementing a simple MBMS-DCF file parser would be easy and the resulting parser will be lightweight. However, implementing XML-encryption and XML-signature involve far more complexity. We do not agree with the claim that implementing XML security is comparable to that of DCF.

2.3. Open problems

How FDT may be protected when using OMA V2.0 DCF for MBMS download protection is addressed in the updated proposal from Nokia [2].

Regarding the XML proposal, it is not shown how encryption and integrity protection are combined. If SignedInfo refers to EncryptedData (i.e. data is not embedded into EncryptedData) and EncryptedData refers to the actual data then MAC covers only the reference and not the actual encrypted data. The encrypted data is not included into the MAC calculation, because RFC3275 specifies:

> "Unless the URI-Reference is a 'same-document' reference as defined in [URI, Section 4.2], the result of dereferencing the URI-Reference MUST be an octet stream. In particular, an XML document identified by URI is not parsed by the signature application unless the URI is a same-document

reference or unless a transform that requires XML parsing is applied. (See Transforms (section 4.3.3.1).)"

2.4. Stability of the specifications

The LS from ISO [3] says that OMA DRM specification claims to be in conformance with ISO 14496 Part 12. However, the latest OMA DRM specification [4] states clearly that it is does not conform ISO's specification:

> " There are two profiles of the DRM Content Format. One is used for Discrete Media (such as still images) and one for Continuous Media (such as music or video). The profiles share some data structures. Both profiles are based on a widely accepted and deployed standard format, the ISO Base Media File format [ISO14496-12], but the Discrete Media profile is meant to be an all-purpose format, not aiming for full compatibility with ISO media files."

It would be fairly easy for OMA to remove all references to ISO specifications if it is really required.

2.5. Privacy

See Section 2.3 above.

---

3. References

[1] Ericsson, “Comparison of DCF and XML encryption for MBMS Download”, S3-040900, 3GPP.

[2] Nokia, “An Update to Using OMA DRM V2.0 DCF for MBMS Download Protection”, S3-040901, 3GPP.

[3] “Liaison Statement to OMA on Base Media File Format”, ISO/IEC/JTC1/SC29/WG11/N6843, Oct 2004.

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

[5] W3C, “XML-encryption”, W3C, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, “XML Encryption Syntax and Processing”.

[6] IETF RFC 3275, "(Extensible Markup Language) XML-Signature Syntax and Processing", http://www.ietf.org/rfc/rfc3275.txt.