3GPP TSG SA WG3 Security — S3#36 **S3-040900**
23 - 26 November 2004
Shenzhen, China

Source: **Ericsson**

Title: **Comparison of DCF and XML encryption for MBMS Download**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

In the past discussion, two different proposals have been made for MBMS download protection: OMA DRM DCF S3-040781 [4] and XML encryption S3-040809 [8]. In order to come to a consensus, several aspects of the proposals have already been compared. Specifically, functional (S3-040791 [1]) and complexity and overhead (S3-040899 [3]) comparisons have been presented. In order to arrive at a final assessment, some more aspects of functionality/suitability and specification maturity of the proposals should also be compared. This is done in the present document.

2 Comparison

The following table summarizes the comparison with respect to several aspects deemed important for a fair evaluation of the merits of both proposals.

Aspect	OMA DRM 2.0 DCF proposal [4]	XML-encryption proposal
Required specification changes	▪ The proposal proposes to introduce a new flag with a “value assigned by OMA” that enables a DRM agent to distinguish between DCFs used for DRM and for MBMS download, respectively. This flag and its meaning (use of the MTK) needs to be specified in the DCF specification. It is not possible to define this flag outside the DCF specification. Because of consistency - the existing possible values of all flags are defined in the DCF specification [2], (for example sections 5.2.1.2, 5.2.1.3, 7.1.4 Table 15, Appendix A Table 17/18), and the OMA naming authority (OMNA) does not administer any values or fields used in the DCF specifications as can be seen on the OMNA page (found in [9]). ▪ It is proposed that the RightsIssuerURL is used to carry MBMS Key_ID information. Thus, a new URI scheme for the RightsIssuerURL has	▪ No XML specification changes required

	to be defined for MBMS. (Note: this is technically possible but also somehow changes the semantics of this URL, which is so far a URL to a server, and now an identifier/URI). ▪ Explanatory text should be added to the DRM [5] and ARCH (architecture) specifications [6], to explain that the OMA DRM DCF is used outside its usage area expressed in the specification, namely DRM protection. ▪ One basic assumption in the DRM 2.0 specification is that the content in a DCF may be accessed *only* according to permissions contained in Rights Objects. (Rights Expression Language specification [7] section 5.4 specifies that “*The DRM Agent MUST NOT grant alternative, not explicitly specified rights to access Content […]*.”). It is unspecified in the “DCF proposal” what permissions exist to access MBMS content in a DCF. Therefore it is not clear how the DRM agent should behave when, instead of DRM RO, it receives MBMS key where no permissions for a DCF are specified. If permissions are not specified in case of MBMS content, it is not clear how the DRM agent can handle DRM content and MBMS content differently. The behavior of DRM agent in case of MBMS content requires a clarification in the DRM specification. ▪ The control of DRM specification changes is not in 3GPP. The timetable for standardization efforts needed in OMA is unclear.	
Implementation re-use	▪ We consider it as a disadvantage that this proposal binds MBMS and OMA DRM 2.0 together. We foresee that there will be demand for MBMS services and devices that require service protection, but not OMA DRM 2.0 o In this case, instead of using an OMA DRM agent, a smaller “MBMS DCF agent” could be used, as mentioned in the discussion. However, this would be new implementation effort without implementation re-use (except for the decryption primitives etc.). ▪ Existing OMA DRM 2.0 agents cannot be used without modifications. They need to be modified, since they currently do not use the MTK as a content key, and since they assume the content key to be contained in an OMA	▪ XML encryption is used as a primitive in OMA DRM 2.0 (in the ROAP protocol). Thus, it can be re-used, if the mentioned functionality is already implemented. Otherwise, the implementation complexity if comparable to the one for the DCF.

	DRM Rights Object, and since they only grant access to content in a DCF according to permissions granted in a Rights Object. Thus, only limited re-use of OMA DRM implementations is possible.	
Open problems	▪ According to [4] it is not clear how the DCF proposal will integrity protect the File Delivery Table (FDT) if XML signatures are not used for integrity protection.	▪ No open problems known. o A DCF can be protected with XML encryption. o Integrity protection can be applied
Stability of the specifications	▪ ISO MPEG has recently sent an LS to OMA (MPEG document number N6843) which outlines incompatibilities between the ISO file format and the OMA DRM DCF, and requests changes in the DCF specification (either functional changes, or removal of reference to the ISO file format).	▪ Specification is considered stable
Privacy	▪ The FDT (File Delivery Table) used in FLUTE may include information that is privacy sensitive, e.g. names of protected files. There maybe privacy issues if the FDT is not encrypted, but send as clear text in multicast. In DCF the encryption of FDT is not possible while in XML encryption it is possible do that if needed.	▪ XML encryption enables the encryption of FDT if needed.

5 Conclusion

We conclude that XML encryption is favorable with respect to the aspects discussed in the present contribution. It is proposed that XML encryption is adopted as encryption method for MBMS download.

6 References

[1] Ericsson, “MBMS Comparison of DCF and XML-encryption”, S3-040791, 3GPP
[2] OMA DRM 2.0 Content Format, OMA-DRM-DCF-V2_0-20040715-C
[3] Ericsson, “MBMS Performance Comparison of DCF and XML-encryption”, S3-040899, 3GPP
[4] Nokia, “Extensions to OMA DRM V2.0 DCF for MBMS Download Protection”, S3-040781, 3GPP
[5] OMA DRM 2.0, OMA-DRM-DRM-V2_0-20040716-C
[6] OMA DRM 2.0 Architecture, OMA-DRM-ARCH-V2_0-20040715-C
[7] OMA DRM 2.0 Rights Expression Language, OMA-DRM-REL-V2_0-20040716-C
[8] Ericsson, “Updated: MBMS Download Protection using XML”, S3-040809, 3GPP
[9] OMNA page for a list of administered numbers, http://www.openmobilealliance.org/tech/omna/index.htm