3GPP TSG SA WG3 Security — S3#35 **S3-040791**
5 - 8 October 2004
Malta

Source: **Ericsson**

Title: **MBMS Comparison of DCF and XML-encryption**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

There are currently two proposals for transport protection during download in MBMS. One is the use of DCF as presented in S3S4J040007 [1] and the other is the use of XML-encryption/signatures as presented in S3S4J040003 [2].

Although there are large similarities between the two proposals (e.g., they both are object protection oriented rather than packet oriented), there are implications of the way the protections are implemented. The following is a comparison of these two approaches.

2 Discrete Content Format

The Discrete Content Format (DCF) approach reuses the format from OMA DRM for confidentiality protection. The key management is different though, no Rights Object is required. It is proposed that the existing MBMS key management is used instead. For integrity protection XML-signatures are used.

Pros:

- Re-use of DRM encryption
- Has DCF MIME type (fits in FLUTE)
- Can sign FDT/Object separately or combined (using XML-signatures)

Cons:

- Re-use of DRM module requires changes to OMA DRM standard that won't be ready within Rel-6 timeframe.
- Binding MBMS and DRM together
- It is unclear if nesting DCF in DCF (if DCF used from download server) is possible.

3 XML-encryption/signatures

The XML approach is to use XML-encryption for confidentiality protection and XML-signatures for integrity protection.

Pros:

- Not binding DRM and MBMS.

- Can sign FDT/Object separately or combined (using XML-signatures)
- Transparent to DRM, i.e., can carry DCF boxes.
- Can use the Application/Octet-stream MIME type (fits FLUTE)

Cons:

- Requires implementation of XML-encryption and XML-signatures.

4 Comparison

Since the two proposals are so similar, it all boils down to the question if DRM will be present in the UE, and if the DRM implementation can be assumed to be MBMS aware or not.

DCF/XML-sign	**XML-encr/XML-sign**
Requires MBMS aware DRM implementation, or DRM standard changes.	Does not require MBMS aware DRM implementation or DRM standard changes.
Re-use of DRM functionality.	Re-use of DRM functionality **if** DRM is implemented in UE.
Has suitable MIME type.	Has suitable MIME type.
Possibly not transparent to DRM.	Transparent to DRM.

5 Conclusion

It seems as if the major difference between the two approaches is that DCF requires modifications to OMA DRM standards (or an MBMS aware implementation) to be able to re-use DRM functionality.

6 References

[1] Nokia, “Using OMA DRMv2 Content Format for MBMS Download Protection”, S3S4J040007
[2] Ericsson, “MBMS Download Protection using XML”, S3S4J040003