3GPP TSG SA WG3 Security — S3#36 **S3-040899**
23-26 November 2004
Shenzhen, China

Source: **Ericsson**

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

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

In S3-040791 [1] there was a functional comparison of the two proposals for download protection in MBMS. This document will focus on performance and overhead in terms of bytes transported over the air. Since the only specified integrity protection method for both proposals is XML-signatures, the overhead of the signatures will be left out.

2 DRM Content Format

The DRM Content Format (DCF) is specified in [2].

2.1 Encryption

DCF uses 128-bit AES [3] as block-cipher, and runs it in either CBC or CTR mode [4]. When CTR mode is used there is no need for padding, since it is in essence a stream-cipher; the Initialization Vector (IV) of 128 bits is required to be sent along with the data though. When CBC mode is used, the last block may need padding to the next 128-bit boundary. The padding adds 0 to 120 bits of overhead, in addition to the 128 bits added by the IV.

2.2 Encoding, Wrapping and Signaling

In S3-040781 [5] it is estimated that the overhead in terms of byte sent per downloaded content is 110 + Content ID length + Content Type length + Key ID length. Since the content type and key ID are probably less than 20 bytes each and the content ID will be a URI, it is probably fair to say that this sum is less than 200 bytes.

3 XML-encryption

XML-encryption is specified in [6].

3.1 Encryption

XML-encryption can also use 128-bit AES [3] as block-cipher, and run it in either CBC mode. Also here a 128-bit IV is sent along with the encrypted data. And similarly to DCF there is a 0 to 120 bit overhead added by the padding.

3.2 Encoding/Wrapping

XML-encryption does not require any special encoding of the actual encrypted object when the object is external to the XML file. The preferred way of using XML-encryption in MBMS is to use an external encrypted object and reference this using a CipherReference element in the FDT or in a separately downloaded XML file.

3.3 Signalling of Keys and Parameters

To specify which algorithms and keys are to be used with XML-encryption, the following snippet would be added to the FDT. It could be sent as a separate XML file, but this is less convenient (in the end this is up to SA4 to decide). The snippet contains ~8 lines of less than 30 characters each. This gives less than 8 * 30 * 0.33 = 79 bytes overhead when the Base64 encoding is taken into account. Allowing a longer URI for the cipher reference, we adjust this overhead to approximately 150 bytes.

```
<EncryptedData
xmlns="http://www.w3.org/2001/04/xmlenc#">

        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:KeyName>MSK_ID || MTK_ID</ds:KeyName>
        </ds:KeyInfo>

        <EncryptionMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>

        <CipherReference URI="http://www.example.com/a_file"></CipherReference>
</EncryptedData>
```

4 Comparison

The following table summarizes the comparison of overhead in terms of bytes over the air and algorithms used.

	DCF	**XML-encr**
Bulk Encryption	128-bit AES (CBC, CTR) Overhead: 0-15 bytes padding 16 bytes for IV	128-bit AES (CBC) Overhead: 0-15 bytes padding 16 bytes for IV
Encoding, wrapping and Signaling	The wrapping of the content and the signaling sums to less than 200 bytes.	No additional encoding or wrapping of data. The parameters in the FDT add approx. 150 bytes.

Hence there is little difference between the two proposals when it comes to processing and additional bytes sent over the air.

5 Conclusion

The estimates for the overhead induced by signaling are very rough, but shows that both solutions have very similar properties. In both cases the overhead is negligible (less than a few hundred bytes), when compared to the actual content to be downloaded (which easily can be 1 MB or more).

So, from a processing and overhead point of view none of the proposals has a significant advantage over the other. Hence the choice must be based on other facts.

6 References

[1] Ericsson, “MBMS Comparison of DCF and XML-encryption”, S3-040791, 3GPP
[2] OMA, “DRM Content Format”, Candidate Version 2.0, 15 July 2004
[3] NIST, Advanced Encryption Standard, FIPS 197
[4] Menezes et. al., “Handbook of Applied Cryptography”, CRC Press 1997
[5] Nokia, “Extensions to OMA DRM V2.0 DCF for MBMS Download Protection”, S3-040781, 3GPP
[6] W3C, “XML-encryption”, W3C, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, “XML Encryption Syntax and Processing”