3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘S3-040810

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**017**	⌘**rev**	**-**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	XML protection for download services		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	28/09/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

Use <u>one</u> of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use <u>one</u> of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	It is not specified how to protect the MBMS download services
Summary of change:	⌘	XML encryption and signatures are proposed
Consequences if not approved:	⌘	It will remain unspecified how to protect the MBMS download services.

Clauses affected:	⌘	2, 6.5.4, 6.6.3				
		Y	**N**			
Other specs Affected:	⌘	**Y**		Other core specifications	⌘	26.346
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

****** NEXT CHANGE *******

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246: "MBMS User Services".

[6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] IETF RFC 2617 "HTTP Digest Authentication".

[9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic".

[11] IETF RFC 3711 "Secure Real-time Transport Protocol".

[12] 3GPP TS 43.020: "Security related network functions".

[13] IETF RFC 3275: “XML-Signature Syntax and Processing”.

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

****** NEXT CHANGE *******

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and start the generation of MTK. The MGV-F provides the MTK to the ME.

The MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

~~NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of MIKEY [9].~~

In case of download service, MIKEY key derivation as defined in section 4.1.3 of MIKEY [9] shall be used to derive MTK authentication and encryption keys from MTK in the ME. These keys shall be provided to download protection protocol.

****** NEXT CHANGE *******

6.6.3 Protection of download data ~~content~~

6.6.3.1 General

Data that belongs to a download MBMS User Service is decrypted as soon as possible by the UE, if the MSK needed to provide the relevant MTK is already available on the UE.

6.6.3.2 Usage of XML encryption and signatures

When it is required to protect MBMS download data XML Encryption and Signatures as defined in [13, 14] shall be used.

NOTE: The usage of signatures in this context refers to using message authentication codes with shared secrets.

The MTK encryption and integrity keys shall be derived by MIKEY as described in subclause 6.5.4.

The following methods shall be supported as defined by W3C (World Wide Web Consortium):

- SignatureMethod: Algorithm = http://www.w3.org/2000/09/xmldsig#hmac-sha1
- DigestMethod Algorithm = http://www.w3.org/2000/09/xmldsig#sha1
- EncryptionMethod Algorithm = http://www.w3.org/2001/04/xmlenc#aes128-cbc

The correct MTK to use to decrypt and verify the integrity of the data is indicated using KeyInfo element as defined in [14] as a concatenation (Network ID || Key Group ID || MSK ID || MTK ID).