

CHANGE REQUEST

⌘ **33.246 CR 006** ⌘ 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:	⌘ Traffic protection combinations		
Source:	⌘ Nokia		
Work item code:	⌘ MBMS	Date:	⌘ 27/09/2004
Category:	⌘ F	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:	⌘ To clarify the allowed combinations of confidentiality and integrity protection
Summary of change:	⌘ The current text in 5.3 specifying the combinations of confidentiality and integrity protection for MBMS are unclear and are also contradictory with the requirements in annex C. The allowed combinations in the protection of the traffic for MBMS service are clarified: <ul style="list-style-type: none"> - no protection - confidentiality protection and integrity protection - confidentiality protection only - integrity protection only
Consequences if not approved:	⌘ The allowed combinations of confidentiality and integrity protections remains unclear.

Clauses affected:	⌘ 5.3						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">N</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	N	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
N	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">N</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	N	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
N	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:	⌘						

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence requires no additional protection). ~~If (~~If this protection is required, it will be either confidentiality and integrity or ~~just~~ confidentiality only or integrity only. The protection is applied end-to-end between the BM-SC and the UEs and will be based on a symmetric key shared between the BM-SC and the UEs that are currently accessing the service. The actual method of protection specified may vary depending on the type of data being transmitted, e.g. media streaming application or file download.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This "double ciphering" is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.