

**Source:** SA WG3 (Security)

**Title:** CR to 33.107: Adding an encryption parameter to IRI across X2 interface (Rel-6)

**Document for:** Approval

**Agenda Item:** 7.3.3

---

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-040402	33.107	041	-	Rel-6	Adding an encryption parameter to IRI across X2 interface	F	6.1.0	S3-030310	SEC1-LI

CR-Form-v7

## CHANGE REQUEST

⌘ **33.107 CR 041** ⌘ rev **-** ⌘ Current version: **6.1.0** ⌘

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

<b>Title:</b>	⌘ Adding an encryption parameter to IRI across X2 interface		
<b>Source:</b>	⌘ SA WG3 (LI Group)		
<b>Work item code:</b>	⌘ SEC1-LI	<b>Date:</b>	⌘ 01-04-2004
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)	<b>2</b> (GSM Phase 2)	
	<b>A</b> (corresponds to a correction in an earlier release)	<b>R96</b> (Release 1996)	
	<b>B</b> (addition of feature),	<b>R97</b> (Release 1997)	
	<b>C</b> (functional modification of feature)	<b>R98</b> (Release 1998)	
	<b>D</b> (editorial modification)	<b>R99</b> (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .	<b>Rel-4</b> (Release 4)	
		<b>Rel-5</b> (Release 5)	
		<b>Rel-6</b> (Release 6)	

<b>Reason for change:</b>	⌘ 3GPP TS 33.106 requires that “when network encryption is introduced, it shall be a national option as to whether the network provides the CC to the agency decrypted, <b>or encrypted with a key</b> available to the agency. User provided end to end, encryption, encoding or compression cannot be removed by the network” (33.106v6.0.0; subclause “General principles”, 5.1.2).  Currently this requirement however is not supported by 33.107. CR offers adding a generic statement to the spec, which would align it with 33.106.
<b>Summary of change:</b>	⌘ CR proposes to add a new parameter to X2 interface. That aligns 33.107 with 33.106.
<b>Consequences if not approved:</b>	⌘ Impossible to meet the optional encryption key delivery requirement defined by 33.106.

<b>Clauses affected:</b>	⌘ 7.3.1										
<b>Other specs affected:</b>	<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;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	⌘	X	⌘	X	⌘	X	Other core specifications	⌘
Y	N										
⌘	X										
⌘	X										
⌘	X										
		Test specifications									
		O&M Specifications									
<b>Other comments:</b>	⌘										

### 7.3.1 X2-interface

The following information needs to be transferred from the 3G GSN or the HLR to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (MSISDN, IMSI, IMEI);
- events and associated parameters as defined in section 7.3.2 and 7.4 may be provided;
- the target location (if available) or the IAs in case of location dependent interception;
- Correlation number;
- Quality of Service (QoS) identifier;
- Encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The IRI should be sent to DF2 using a reliable transport mechanism.