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

Tdoc ⌘S3-040928

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234 CR 039** ⌘**rev** – ⌘ Current version: **6.2.1** ⌘

*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:	⌘	Confidentiality and integrity can't be both NULL in the IPsec tunnel			
Source:	⌘	Nokia			
Work item code:	⌘	WLAN	***Date:***	⌘	11/11/2004
Category:	⌘	**F**	***Release:***	⌘	Rel-6
		Use one 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 one 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:	⌘	In 6.6 it says "It shall be possible to turn off security protection (confidentiality and/or integrity) in the tunnel". This is in conflict with IETF RFC2406. Although both confidentiality and authentication are optional, at least one of these services MUST be selected hence both algorithms MUST NOT be simultaneously NULL.
Summary of change:	⌘	Change to "It shall be possible to turn off security protection (confidentiality or integrity, but not both)".
Consequences if not approved:	⌘	Conflict with IETF specification.

Clauses affected:	⌘	6.6				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

********** START OF CHANGE **********

6.6 Profile of IPSec ESP

IPSec ESP, as specified in RFC 2406 [30], contains a number of options and extensions, where some are not needed for the purposes of this specification and others are required. IPSec ESP is therefore profiled in this section. When IPSec ESP is used in the context of this specification the profile specified in this section shall be supported. Rules and recommendations in ref. [31] and [33] have been followed, as in case of IKEv2.

First cryptographic suite:

- Confidentiality: 3DES in CBC mode;
- Integrity: HMAC-SHA1-96. The key length is 160 bits, according to RFC 2104 [34] and RFC 2404 [35];
- Tunnel mode must be used.

Second cryptographic suite:

- Confidentiality: AES with 128-bit keys in CBC mode. The key length is set to 128 bits;
- Integrity: AES-XCBC-MAC-96;
- Tunnel mode must be used.

It shall be possible to turn off security protection (confidentiality ~~and/~~or integrity, but not both) in the tunnel (for example high trust-between the 3GPP network operator and the WLAN access provider). This means that transform IDs for encryption ENCR_NULL and NONE for integrity shall be allowed to negotiate, as specified in ref. [29]

For NAT traversal, the UDP encapsulation for ESP tunnel mode specified in [32] shall be supported.

********** END OF CHANGE **********