3GPP TSG-SA3 Meeting #25
Munich, Germany, October 8-11, 2002

Tdoc ⌘S3-020552

CR-Form-v7

CHANGE REQUEST

⌘	**33.210**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**5.1.0** ⌘

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 ☒

Title:	⌘	Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies.		
Source:	⌘	Telenor		
Work item code:	⌘	SEC-NDS-IP	***Date:*** ⌘	08/10/2002
Category:	⌘	**F**	***Release:*** ⌘	Rel-5

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:

2	*(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)*

Reason for change:	⌘	The only mandated encryption transform in NDS/IP is the AES transform. For integrity protection one has the choice of SHA-1 or AES in XCBC-MAC mode. The IETF has not completed the AES transforms for encryption and integrity protection. Technical uncertainties with AES means that the IETF may delay the RFCs for a prolonged period.
Summary of change:	⌘	The change mandates support of the 3DES encryption transform and removes the requirements to support AES.
Consequences if not approved:	⌘	Due to the lack of a mandatory to support encryption transform one may have interoperability problems.

Clauses affected:	⌘	5.3.3 and 5.3.4				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.3.3 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The transforms that compliant IPsec implementations are required to support are the ESP_NULL and the ESP_DES transforms. However, the Data Encryption Standard (DES) transform is no longer considered to be sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [18] to the effect that the ESP_DES transform is likely to be deprecated as a mandatory transform in the near future. ~~A new Advanced Encryption Standard (AES) is being standardized to replace the aging DES.~~

It is therefore explicitly noted that for use in NDS/IP, the ESP_DES transform shall not be used and instead it shall be mandatory to support the ESP_3DES~~AES~~ transform.

~~Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.~~

5.3.4 Support of ESP authentication transforms

The transforms that compliant IPsec implementation is required to support are the ESP_NULL, the ESP_HMAC_MD5 and the ESP_HMAC_SHA-1 transforms. For NDS/IP traffic ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the ESP_NULL authentication algorithm is explicitly not allowed for use. ESP shall support ESP_HMAC_SHA-1 ~~and AES MAC~~ algorithms in NDS/IP.

~~Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.~~