Technical Specification Group Services and System Aspects
Meeting #18, New Orleans, USA, 9-12 December 2002

TSGS#18(02)0719

Source: **SA WG3**

Title: **1 CR to 33.210 (Rel-5): Adding requirement to provide mandatory support for 3DES encryption in NDS/IP.Remove AES references and dependencies**

Document for: **Approval**

Agenda Item: **7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020719	33.210	003		Rel-5	Adding requirement to provide mandatory support for 3DES encryption in NDS/IP.Remove AES references and dependencies	F	5.1.0	SEC-NDS-IP	S3-020563

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

Tdoc ⌘S3-020563

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **003** ⌘ **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 **X**

Title:	⌘	Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies.
Source:	⌘	SA WG3
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 RFCs for 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, 5.3.4 and 5.4

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

⌘

Other comments: ⌘

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~~ algorithm~~s~~ 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.~~

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

5.4 Profiling of IKE

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following additional requirement on IKE is made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported;
- Only Main Mode shall be used;
- Only Fully Qualified Domain Names (FQDN) shall be used;
- Support of ~~AES~~ 3DES in CBC mode shall be mandatory for confidentiality;
- Support of SHA-1 shall be mandatory for integrity/message authentication.

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

For IKE phase-2 (IPsec SA):

- Perfect Forward Secrecy is optional;
- Only IP addresses or subnet identity types shall be mandatory address types;
- Support of Notifications shall be mandatory.

~~NOTE: When AES MAC is defined for IKE by the IETF it will also be made mandatory for IKE phase-1 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.~~