3GPP TSG SA WG3 Security — S3#32 **S3-040085**
9 - 13 February 2003, Edinburgh, UK

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.3.0** ⌘

*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:	⌘	Addition of AES transform
Source:	⌘	Nokia and Telenor
Work item code:	⌘	SEC1-NDS-IP
Date:	⌘	02/02/2004
Category:	⌘	**B**
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:

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:	⌘	Support for the AES encryption was originally intended for Release 5, but due to delays in the IETF process the RFC was not ready in time for Release 5. Now when the transform is available it is desirable to permit it to be used by NDS/IP compliant IPsec solutions.
Summary of change:	⌘	The change introduces support for AES-CBC mode encryption.
Consequences if not approved:	⌘	NDS/IP will not be able to offer the confidentiality protection by means of the AES based transform.

Clauses affected:	⌘	2, 5.3.3, 5.4			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	The proposed changes will update NDS/IP to reflect the current state of IPsec.			

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.

*************** First change ***************

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.133: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements".

[2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[4] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[7] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[8] 3GPP TS 33.103: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines".

[9] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".

[10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".

[11] RFC-2393: "IP Payload Compression Protocol (IPComp)".

[12] RFC-2401: "Security Architecture for the Internet Protocol".

[13] RFC-2402: "IP Authentication Header".

[14] RFC-2403: "The Use of HMAC-MD5-96 within ESP and AH".

[15] RFC-2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

[16] RFC-2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".

[17] RFC-2406: "IP Encapsulating Security Payload".

[18] RFC-2407: "The Internet IP Security Domain of Interpretation for ISAKMP".

[19] RFC-2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

[20] RFC-2409: "The Internet Key Exchange (IKE)".

[21] RFC-2410: "The NULL Encryption Algorithm and Its Use With IPsec".

[22] RFC-2411: "IP Security Document Roadmap".

[23] RFC-2412: "The OAKLEY Key Determination Protocol".

[24] RFC-2451: "The ESP CBC-Mode Cipher Algorithms".

[25] RFC-2521: "ICMP Security Failures Messages".

[26] RFC-3554: "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec".

[27] RFC-1750: “Randomness Recommendations for Security".

[28] 3GPP TS 25.412: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signalling transport".

[29] RFC-3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec"

********** **Second change** **********

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.

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 transform.

Support for the AES-CBC cipher algorithm [29] is mandatory. It is noted that the AES-CBC key length for use with this specification shall be 128 bits.

*************** Third 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;
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;
- Support of 3DES in CBC mode shall be mandatory for confidentiality;
- Support of AES in CBC mode [29] 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.

The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires. The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data being transmitted within the old SA.

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.

Key Length and support of AES transform:

Since the AES-CBC allows variable key lengths, the Key Length attribute must be specified in both a Phase 1 exchange [20] and a Phase 2 exchange [18]. It is noted that the key length for use with this specification shall be 128 bits.