3GPP TSG SA WG3 Security — S3#34
Acapulco, Mexico, 6-9 Jul 2004

Tdoc ⌘S3-040486

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Conditional support of NAT
Source:	⌘	Nokia
Work item code:	⌘	WLAN
Date:	⌘	27/06/2004
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:

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:	⌘	NAT support is an optional feature in IKEv2 and NAT is not required in all transport IP layer scenarios.
Summary of change:	⌘	NAT support is made to conditional i.e. NAT support is required only in IP network scenarios, which uses private IP addresses.
Consequences if not approved:	⌘	NAT support must be implemented in all implementations even if it is not required.

Clauses affected:	⌘	6.5 and 6.6

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

*** BEGIN SET OF CHANGES ***

6.5 Profile of IKEv2

IKEv2, as specified in ref. [29], contains a number of options, where some are not needed for the purposes of this specification and others are required. IKEv2 is therefore profiled in this section. When IKEv2 is used in the context of this specification the profile specified in this section shall be supported.

Access to services offered by the HPLMN (scenario 3) follows a VPN-like approach. In ref. [31] it can be found a set of recommendations of IKEv2 profiles, suitable for VPN-like solutions. On the other hand, ref. [33] sets rules and recommendations for individual algorithms support. Following recommendation from both papers, the below two profiles shall be supported by the PDG and the WLAN-UE:

First cryptographic suite:

- Confidentiality: 3DES in CBC mode;
- Pseudo-random function: HMAC-SHA1;
- Integrity: HMAC-SHA1-96;
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33].

Second cryptographic suite:

- Confidentiality: AES with fixed key length in CBC mode. The key length is set to 128 bits;
- Pseudo-random function: AES-XCBC-PRF-128;
- Integrity: AES-XCBC-MAC-96.
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33]

~~For NAT traversal, t~~The NAT support of IKEv2 shall be supported as specified in section 2.23 of [29] if transport IP layer supports NAT.

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) 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, t~~The UDP encapsulation for ESP tunnel mode specified in [32] shall be supported if transport IP layer supports NAT.

Editor's note: An example of a profile of IPSec ESP, which may be useful to study when writing this section, can be found in TS 33.210, section 5.3. Future editions of this specification will define additional profiles.

*** END SET OF CHANGES ***