CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.310** **CR** ⌘**rev** **-** ⌘ Current version: **0.5.0** ⌘

*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:	⌘	Clarification on the use of PSK as a fallback mechanism
Source:	⌘	Nokia, Siemens, SSH, Vodafone
Work item code:	⌘	***Date:*** ⌘ 29/09/2003
Category:	⌘	***Release:*** ⌘ 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:	⌘	Lack of specification on the use of PSK as a fallback mechanism could lead to insecure implementation.
Summary of change:	⌘	Addition of specifications on the use of PSK as a fallback mechanism.
Consequences if not approved:	⌘	Possibility of insecure implementation.

Clauses affected:	⌘				
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘
				Test specifications	
				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.

8 Evolution path

[Editor's note: This chapter describes the evolution path from using NDS/IP towards optional PKI structure.]

8.1 Backward compatibility

NDS/IP describes an authentication framework whereby IKE phase 1 negotiation is based on pre-shared secrets authentication method. NDS/AF describes an optional authentication framework which enables NDS/IP SEGs to perform IKE phase 1 negotiation based on RSA Signatures authentication method. An NDS/AF compliant SEG shall also contain NDS/IP functionality. However an NDS/IP compliant SEG need not contain NDS/AF functionality.

Device specific management has to be used to reconfigure a SEG such that NDS/AF functionality will be used at the IKE initiator side for IKE phase 1 negotiation. The transition towards NDS/AF based authentication may be done on a SEG by SEG basis. Before the first NDS/AF SEG is taken into use it shall be assured that all needed NDS/AF functionality like CR, CRL's is available and working. The setting up of a NDS/AF based IPsec tunnel can be tested in parallel to the existing traffic.

A smooth migration may be done in the following way. An NDS/AF SEG shall provide several algorithm proposal's during IKE phase-1 negotiation, some based on RSA signature authentication method, others based on PSK authentication method. The responding IKE peer will select PSK authentication method if it does not support RSA signature authentication method but may select RSA signature authentication method if complies with NDS/AF. The IKE-responder policy shall be configured such that the RSA signature authentication method shall take precedence over PSK authentication method in order to ensure that it is used as soon as the IKE-initiator proposes RSA signature authentication method.

If the SEGs of both operators support NDS/AF based authentication then both SEG settings may be changed. The pre-shared secrets may then be removed from the SEGs and the IKE initiator shall only use RSA signature authentication method. However this removal of PSK is not essential as it may be used as a fallback mechanism. ~~Only~~ S~~s~~ome care has to be taken that the policy between SEGs of different operators be coordinated otherwise this may result in failed tunnel set up. This would be the case if the initiating IKE peer only uses RSA signature authentication method and the responding IKE peer only accept PSK authentication method. Furthermore, if the PSK is kept as a fallback mechanism after the RSA signature authentication method is introduced then fallback to PSK should only be allowed if the operator makes a policy change in the SEGs to allow PSK to be used. The operator may temporarily allow fallback to PSK if, for example, the SEGs are unable to verify the necessary certificates because of problems with the PKI. If PSK is kept as a fallback then it may be necessary to renew the PSK periodically for security reasons, or if PSK compromise is suspected.