CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: 0.3.0 ⌘

*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 ☒

Title:	⌘	Addition of a Clause on backward compatibility to NDS/IP
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	07/07/2003
Category:	⌘	
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:	⌘	Addition of a new clause that describes how 1) NDS/IP and NDS/AF features interwork 2) How the migration can be done from PSK authentication method towards RSA signatures authentication method
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	New Clause

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

Other comments:	⌘	

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 authentication framework whereby IKE phase 1 negotiation is 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.

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 some 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.