3GPP TSG-SA3 Meeting #33
10-14 May 2004 - Beijing, China

S3-040285

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Allow use of IKEv1 and IKEv2 with subscriber certificates
Source:	⌘	Nortel Networks
Work item code:	⌘	WLAN
Date:	⌘	03/05/2004
Category:	⌘	**C**
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:	⌘	To allow the use of IKEv1 and IKEv2 with subscriber certificates as alternative mechanisms during the establishment of IPSec ESP tunnel
Summary of change:	⌘	A note is added to section 6.1.5, stating that when subscriber certificates are available, the alternative mechanisms in Annex E is used and the existing editor's note is deleted. The status of Annex E is changed from informative to normative, allowing the use of either IKEv1 with subscriber certificates or IKEv2 with subscriber certificates, but not both.
Consequences if not approved:	⌘	Specification will not allow the use of IKEv1 (and IKEv2) protocols with subscriber certificates, even though the operator may have subscriber certificates infrastructure available in their network. Support for IKEv2 in commercial products uncertain.

Clauses affected:	⌘	6.1.5, Annex E

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

Other comments: ⌘

********** FIRST SET OF CHANGES TO SECTION 6.1.5 **********

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- The WLAN UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.
- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a SIM and no USIM.
- A profile for IKEv2 is defined in section 6.5.

NOTE: When a HPLMN's WLAN subscribers for scenario 3 have subscriber certificates available, the alternatives presented in Annex E is used.

~~Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.~~

********** END OF CHANGES TO SECTION 6.1.5 **********

********** SECOND SET OF CHANGES TO ANNEX E **********

Annex E: (~~informative~~Normative): Alternative Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

When a HPLMN's WLAN subscriber for scenario 3 have subscriber certificates available, one of the alternatives presented here shall be used.

~~Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.~~

E.1 IKE with subscriber certificates

- The UE and the PDG use IKE, as specified in [rfc2409], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in [rfc2409], is used in order to authenticate the PDG and the UE.
- A profile for IKE is defined in section 6.5.

E.2 IKEv2 with subscriber certificates

- The UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used in order to authenticate the PDG and the UE.
- A profile for IKEv2 is defined in section 6.5.

********** END OF CHANGES TO ANNEX E **********

********** END OF CHANGES **********