3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040556

CR-Form-v7

CHANGE REQUEST

⌘ **33.141** **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:	⌘	PSK TLS and SSC support
Source:	⌘	Nokia, Nortel
Work item code:	⌘	Presence security
Date:	⌘	29/06/2004
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:	⌘	To conform with TS 33.222, the AP/Presence server may also authenticate the UE using PSK TLS or subscriber certificates.
Summary of change:	⌘	AP/Presence server may also authenticate the UE using PSK TLS or subscriber certificates.
Consequences if not approved:	⌘	The TS is not inline with TS 33.222.

Clauses affected:	⌘	6.1.1

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

Other comments:	⌘	

6.1.1 Authentication of the Subscriber

~~From a TLS point of view the UE shall be considered as un-authenticated, cf. RFC 2246 [6].~~

The authentication of the UE may take place in either the Authentication Proxy or the Presence server. However the AP or the Presence server may, depending on given the policy of the operator conclude that the AP/Presence Server shall not authenticate the UE using GBA i.e. the UE is considered as authenticated already or the UE is authenticated by other means, cf. initiation of bootstrapping in TS 33.220 [11], section 4.5.1.

Otherwise if the AP/Presence Server concludes that the authentication shall take place in the AP/Presence Server then the UE may be authenticated as specified in TS 33.220 [11] (where the Ua interface is between the UE and the AP/Presence Server).

The AP/Presence Server may also authenticate the UE using PSK TLS or subscriber certificates as specified in TS 33.222 [19], if the AP/Presence Server supports such capability.

It shall be possible for the AP/Presence Server at any time to request a re-authentication of an active UE, cf. TS33.220 [11], section 4.5.3.