3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050016

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **053** ⌘ **rev** **-** ⌘ Current version: **6.3.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Security visibility and configurability descriptions
Source:	⌘	ZTE Corporation
Work item code:	⌘	WLAN
Date:	⌘	21/01/2005
Category:	⌘	**B**
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	There is no security visibility and configurability description in current specification.
Summary of change:	⌘	Adding contents on security visibility and configurability.
Consequences if not approved:	⌘	Specification is not complete.

Clauses affected:	⌘	5.4

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

⌘

Other comments: ⌘

*** BEGIN OF CHANGES ***

5.4 ~~Void~~Visibility and configurability

5.4.1 Visibility

Security visibility contains what is visible for the subscriber regarding the actual protection the subscriber is provided with. Following security features or related information should be visible to the user:

- USIM-based WLAN access authentication result (success or failure), and the reason if failed.
- UE-initiated tunnelling authentication result (success or failure), and the reason if failed.
- Whether link layer protection is implemented.
- Whether tunnel protection in 3GPP IP access is implemented.
- Whether user permanent identity is sent in clear text during authentications.

5.4.2 Configurability

Security configurability contains what the subscriber shall be able to configure:

- Enable/disable link layer protection, and decide what cipher and security strength to use, i.e. the protection protocol and key length, etc.
- Enable/disable EAP-SIM authentication in WLAN direct IP access authentication and 3GPP IP access authentication, when UE contains a USIM.
- Enable/disable fast re-authentication in WLAN direct IP access.
- Choose which network to access in 3GPP IP access, foreign network or home network.
- Configurations in 3GPP IP access:
  - Configure the certificate trust anchor, i.e. root CA certificate to verify PDG certificate.
  - Choose the method to check the validity of PDG certificates, i.e. CRL or OCSP (see section 6.6A).
  - Configure the OCSP responder certificate to verify OCSP response.
  - Enable/disable tunnel encryption, and choose the cryptographic suite of IPsec ESP (see section 6.6).
  - Enable/disable sending user permanent identity in clear text.

*** END OF CHANGES ***