CR-Form-v7

CHANGE REQUEST

| ⌘ | **33.220** 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 **X**   Radio Access Network ☐   Core Network ☐

Title: ⌘	Generic Ua interface requirements	
Source: ⌘	Nokia	
Work item code:⌘	GBA-SSC	***Date:*** ⌘ 07/05/2004
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: ⌘	Ua interface requirements that are generic to all protocols implementing the interface are not listed clearly in the specification.	
Summary of change:⌘	This CR adds a new subclause on generic Ua interface requirements. Currently the specification does not have one place where the generic requirements are listed.	
Consequences if not approved: ⌘	Generic Ua interface requirements are not listed in a subclause of their own.	

Clauses affected: ⌘	4.3.8 (new)	

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

Other comments: ⌘		

4.3.8   Requirements on Ua interface

The generic requirements for Ua interface are:

- The UE and the NAF shall be able to mutually authenticate each other using the GBA-based shared secret;

- The UE shall be able to send the hostname of the NAF (i.e., FQDN of the NAF) to the NAF when the GBA-based authentication over Ua interface is being intiated;

NOTE: The ability to send the hostname of the NAF is particularly necessary if a NAF can be addressed using different hostnames, and the NAF cannot otherwise discover what is the hostname that the UE used to contact the NAF. The hostname is needed by the BSF during key derivation.

- The UE shall be able to indicate the capability of supporting GBA-based authentication to the NAF;

- The NAF shall be able to indicate to the UE that GBA-based shared secret should be used;

- The NAF shall be able to indicate to the UE that the current shared secret has expired and the UE should use newer shared secret with the NAF;

NOTE: If the UE has a newer shared secret than the one it is currently using, the UE should first offer to use the newest shared secret in the UE. If the NAF does not accept the latest shared secret or the UE does not have newer shared secret, the UE shall establish new shared secret with the BSF.

- The UE and the NAF may use the GBA-based shared secret for confidentiality and integrity protection.