3GPP TSG SA WG3 Meeting S3#36
Shenzhenn, China, 23 - 26 November 2004

Tdoc ⌘S3-040957

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**046**	⌘**rev**	**-**	⌘	Current version:	**6.2.1** ⌘

*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:	⌘	Clarification on storage of Temporary Identities in UICC	
Source:	⌘	Samsung and Ericsson	
Work item code:	⌘	WLAN	***Date:*** ⌘ 09/11/2004
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:

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:	⌘	This CR introduces a change in the text proposed in CR S3-040875, to add clarification on the storage and use of temporary identities (pseudonym and re-authentication) in UICC.
Summary of change:	⌘	To add clarification on the storage and use of temporary identities as the temporary identities shall be used for only one EAP authentication procedure and maked as deleted after the EAP procedure.
Consequences if not approved:	⌘	Clarity on use of temporary identities is not well defined and also the temporary identities should not be used for more than one EAP authentication procedure.

Clauses affected:	⌘	6.1.3				
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	TS 24.234
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘	This CR can be approved only if CR S3-040875 has been approved.				

*** BEGIN SET OF CHANGES ***

6.1.3 EAP support in UICC

6.1.3.1 EAP-AKA procedure

It shall be possible as an implementation option to have the termination of EAP in the UICC. For this purpose, all steps of the EAP-AKA authentication mechanism described in 6.1.1.1 apply with the exception of step 15 that shall be replaced with the following:

> The WLAN-UE runs EAP authentication method (see TS 102.310 [yy]) on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the USIM rejects the authentication (not shown in this example). If the sequence number is out of synch, USIM initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes the Master Session Key and Extended Master Session Key and checks the received MAC with the new derived keying material.

If temporary identities (~~a~~ pseudonym and/or re-authentication identities) ~~w~~are received, then the ~~WLAN-UE~~ UICC stores the temporary identites for the next full or fast ~~future~~ authentication~~authentications~~ procedure and mark it as deleted after the authentication procedure.

6.1.3.2 EAP-SIM procedure

It shall be possible as an implementation option to have the termination of EAP in the UICC. To handle EAP-SIM the USIM uses GSM AKA by applying conversion functions c2 and c3 (as defined in 33.102 [21]). For this purpose, all steps of the EAP-SIM authentication mechanism described in 6.1.2.1 apply with the exception of step 14 that shall be replaced with the following:

> The WLAN-UE runs EAP authentication method (see TS 102.310 [yy]) on the USIM. The WLAN-UE continues the authentication exchange only if the MAC is correct.

If temporary identites ~~a~~(pseudonym and/or re-authentication identities) are received, then the UICC stores the temporary identites for the next full or fast ~~future~~ authentication~~s~~ procedure and mark it as deleted after the authentication procedure.

*** END SET OF CHANGES ***