3GPP TSG SA WG3 Security — SA3#35 **S3-040771**

October 5-8, 2004, St Paul's Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **036** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Deletion of inconclusive text on A5/2 countermeasures
Source:	⌘	Siemens
Work item code:	⌘	WLAN
Date:	⌘	28/09/2004
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:	⌘	There is text in Annex C.3.5 which mentions ongoing discussions, without coming to conclusions. Such text is inappropriate in a complete specification.
Summary of change:	⌘	Deletion of inappropriate text.
Consequences if not approved:	⌘	Inappropriate text in specification.

Clauses affected:	⌘	C.3.5

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

Other comments:	⌘	-

C.3.5 Implications of the A5/2 Attack for 3GPP WLAN Access

This annex provides an analysis of the implications of the A5/2 attack on 3GPP WLAN access, and provides recommendations on how to mitigate the impacts of the attack to 3GPP WLAN access

Barkan et.al. [28] presented a real-time attack on A5/2 algorithm in [Bar03]. The attack breaks the A5/2 algorithm. In the man-in-the-middle version of the attack, the terminal is forced to use A5/2, while the attacker can use A5/1 against the network. The keys that are used for A5/2 algorithm can be used also with A5/1 cipher. Unfortunately, the vulnerability spreads also to A5/3 and GEA algorithms. The main reasons to the A5/2 flaws are: weak cipher, no bidding down protection and usage of same keys for different algorithms. The attack affects SIM usage. This analysis reflects the impacts from WLAN access point of view. The implications can be analyzed as follows:

Table C.1

Scenario:	Implication:
1. SIM shared between WLAN device and GSM device	1 A5/2 should not be allowed in the terminal, OR 2 Some key separation countermeasures should be used in the terminal, OR 3 A5/2 vulnerability may reveal Kc and this may allow WLAN terminal impersonation towards 3G network

Based on the analysis, it may make sense to avoid the use of the A5/2 algorithm in the terminal and/or provide some countermeasures against the attack. If A5/2 is used and there is an attack against it, Kc may be revealed. This implies that the A5/2 vulnerability can spread from the GSM network to the WLAN network. This, in turn, implies that the revealed Kc may be used to impersonate a terminal in the WLAN-3G network towards the network. Similarly an attack using A5/2 can destroy the confidentiality of the WLAN radio access, as the Kc:s used can be retrieved via A5/2 attacks.

It should be noted that the threats applies to EAP-SIM, as specified in 33.234. EAP-SIM can be attacked whenever a few valid GSM triplets have been retrieved.

~~It should also be noted that in order to alleviate the security problem with the A5/2 attack new terminals are required cf. the discussion on the Special RAND or that a USIM is used instead of a SIM. The exact terminal and network requirements on how to alleviate the A5/2 issues are currently studied in 3GPP and it is proposed that those requirements shall also apply to WLAN and 3G interworking for consistency reasons. So, for example, if the special RAND mechanism is adopted then special RANDs should be sent to WLAN AAA servers to prohibit the use of all A5 and GEA algorithms. When the GSM device implements the special RAND mechanism, this will protect against a man-in-the-middle exploiting a weakness in any GSM algorithm in order to masquerade as a WLAN client or eavesdrop the WLAN communications.~~