3GPP TSG SA WG3 Security — S3#29
San Francisco, USA 15 - 18 July 2003

Tdoc ⌘S3-030364

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **0.5.0** ⌘

*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:	⌘	Clarification on pseudonyms
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	16/06/2003
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:	⌘	Wrongly deleted requirement in TS 33.234 v0.4.0
Summary of change:	⌘	Re-inserted sentence in chapter 4.2.3
Consequences if not approved:	⌘	An attacker could associate two or more pseudonyms to the same subscriber and, even without getting his/her real identity, track subscriber signalling and behaviour. The pseudonym generation method already covers this, but the requirement is not explicitly written. There has to exist no correlation between two or more pseudonyms of the same user.
Clauses affected:	⌘	4.2.3 User identity privacy

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

4.2.3 User identity privacy

- Any secret keys used in 3G AAA servers for the generation of pseudonyms should be infeasible for an attacker to recover.
- It shall be infeasible for an attacker to recover the corresponding permanent identity, given any pseudonym(s).
- It should be infeasible for an attacker to determine whether or not two pseudonyms correspond to the same permanent identity.
- It shall be infeasible for an attacker to generate a valid pseudonym.