3GPP TSG-SA3 Meeting #29
San Francisco, USA, July 15-19, 2003

Tdoc ⌘S3-030398

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **-** ⌘**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 **X**

Title:	⌘	Clarification to Annex B.2 Trust Relation Editor's Note
Source:	⌘	AT&T Wireless Services
Work item code:	⌘	WLAN
Date:	⌘	08/07/2003
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:	⌘	Editor's Note in Annex B.2 is misleading and inaccurate.
Summary of change:	⌘	Accurately reflect the true intent of the trust relationships as stated in TR 22.934 v6.1.0.
Consequences if not approved:	⌘	Without the clarification security work on trust relationships could result in inaccurate outcome.

Clauses affected:	⌘	Annex B.2

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

Other comments: ⌘

Discussion

According to TR 22.934 v6.1.0, section 5.2.3 states the following:

==========

5.2.3 Internetworking trust

3GPP systems interworking with WLANs should consider the possibility of security weaknesses within the WLAN. The level of trust for physical communications and signalling in the network may be affected by the security of the servers, their operating software and the procedures used in the interworked WLAN. The level of trust of communication between the WLAN and the 3GPP system may be considered to have three levels -

1) The WLAN may be completely untrusted by the UE and the 3GPP system.

2) The WLAN contains elements that may be trusted by the UE and the 3GPP system. For example, the WLAN may include trusted servers that look after aspects of security and authentication interworking with the 3GPP systems (e.g. 802.1x, 802.11i). However, other elements of the network may be untrusted.

3) All of the elements of the WLAN may be fully trusted by the UE and the 3GPP system.

Mutual authentication between the UE and the WLAN/3GPP System should be used to assure the needed level of trust by both entities for interworking and access to services. In the case of an untrusted interworked network, this may limit the charging possibilities as, for example, some messages may be spurious. For a network with trusted servers and authenticated messages, the charging records may be considered trusted.

==========

Given the above, the editor's note in Annex B.2 Trust Relations in TS 33.234 is not accurate, and needs to be modified to correctly reflect the actual intent.

Proposal

B.2 Trust relations

To design or evaluate a security solution, the trust relations between the participants must be identified. In a public WLAN access scenario, we have one or more operators and (possibly independent) access providers, and several subscribers.

The subscribers cannot trust each other. Someone else accessing the network from the same WLAN access network as the user, may be trying to perform DoS attacks targeted at the user, or eavesdrop on his traffic, steal his credentials to gain access at a later time etc.

An operator cannot trust any mobile terminal that tries to connect to the network. Before authentication, the mobile station could belong to anyone, with or without a subscription. Even after a mobile station has been authenticated, the device may act maliciously. The user himself may be performing fiendish activities, or someone else may have hijacked his session.

The operators and/or access providers may choose to trust each other. Such trust relations normally rely on (legally binding) roaming agreements. If such an agreement is in place, a user may use another operator's access network, and will be authenticated by the "home operator". Depending on which solution is chosen, the user may have to put trust in other, visited operators, as well as in his home operator.

[Editor's note: ~~It is probable that~~ T~~t~~he cellular operators may~~will~~ provide the WLAN access in the future~~, and that small WLAN-only operators will be few or non-existent. It is, however, not impossible that~~In addition, there also will be

important WLAN-only operators on the market. ~~*These could team up with one or more cellular operators. The trust relations that are induced by access through such an operator are the same as the ones considered in the case of roaming between two cellular operators*~~*. The level of trust of communication between the WLAN and the 3GPP system may be considered to have three levels -*

1) The WLAN may be completely untrusted by the UE and the 3GPP system.

2) The WLAN contains elements that may be trusted by the UE and the 3GPP system. For example, the WLAN may include trusted servers that look after aspects of security and authentication interworking with the 3GPP systems (e.g. 802.1x, 802.11i). However, other elements of the network may be untrusted.

3) All of the elements of the WLAN may be fully trusted by the UE and the 3GPP system.]