

## CHANGE REQUEST

⌘ **TS 33.234 CR CRNum** ⌘ rev  ⌘ Current version:  ⌘

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

<b>Title:</b>	⌘ Editorial changes		
<b>Source:</b>	⌘ Vodafone		
<b>Work item code:</b>	⌘ WLAN interworking security	<b>Date:</b>	⌘ 2/2/2004
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ To correct and clarify the specification.		
<b>Summary of change:</b>	⌘ Introduction: refer to "this TS" rather than SA3.  1: Clarification that this TS contains, in general, specifications rather than recommendations.  5.1.6: Clarification to the definition of user identify privacy.		
<b>Consequences if not approved:</b>	⌘		

<b>Clauses affected:</b>	⌘ Introduction, 1, 5.1.6										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘ Other core specifications ⌘ Test specifications ⌘ O&M Specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<b>Other comments:</b>	⌘										

---

## Introduction

WLAN is not a single radio technology, several different technologies fall into the category called WLAN. Existing industry standard is IEEE 802.11b operating at 2,4 GHz ISM band. New entrant for this same band is Bluetooth and technologies such as IEEE 802.11a and ETSI BRAN Hiperlan2 are being developed for the 5GHz band.

Despite the different radio technologies, all these WLAN systems are commonly used for transportation of IP datagrams. The specific WLAN technology used in each wireless IP network is not very visible for the layers above IP.

~~This TS covers TSG-SA-WG3 will study~~ the models and mechanisms under which these technologies can be used to securely interwork with 3GPP networks.

---

## 1 Scope

The present document specifies the security architecture, trust model and security requirements for the interworking of the 3GPP System and WLAN Access Networks.

~~Recommendations~~ Specifications of the appropriate mechanisms for user and network authentication, key management, service authorization, confidentiality and integrity protection of user and signalling data are also provided.

### 5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending any the cleartext permanent subscriber identification information which would compromise the subscriber's identity and location on the radio interface, or allow different communications of the same subscriber on the radio interface to be linked ~~ty (NAI) and make the subscriber's connections unlinkable to eavesdroppers.~~

User identity privacy is based on temporary identities, or pseudonyms. The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementations, but optional for use.

The AAA server generates and delivers the pseudonym to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the pseudonym, it will just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the pseudonym.

To avoid user traceability, the user should not be identified for a long period by means of the same temporary identity. On the other hand, the AAA server should be ready to accept at least two different pseudonyms, in case the WLAN-UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain more than one allowed pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user to send its permanent identity. This represents a breach in the provision of user identity privacy. It is a matter of the operator's security policy whether to allow clients to accept requests from the network to send the cleartext permanent identity. If the client rejects a legitimate request from the AAA server, it will be denied access to the service.

**Editor's note:** The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.