

3GPP TSG-SA3 Meeting #33
 Beijing, China, 10-14 May 2004

Tdoc # S3-040352

CR-Form-v7	CHANGE REQUEST
⌘ 33.234 CR CRNum ⌘ rev - ⌘ Current version: 6.0.0 ⌘	

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:	⌘ WLAN handover scenario		
Source:	⌘ Nokia		
Work item code:	⌘ WLAN-3G interworking security	Date:	⌘ 02/05/2004
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> 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 <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)

Reason for change:	⌘ If the WLAN-UE connects to multiple AAA server, there is no need to keep the previous connection for a genuie UE. The release mechanism can also mitigate any malicious mis-use of the crednital to minimum.
Summary of change:	⌘ The change is added how to handle muliple registrations of the WLAN-UE based on local policy defined for AAA server and HSS.
Consequences if not approved:	⌘ The malicious usage of radio service will not be prevented.

Clauses affected:	⌘ 6.1.1.1										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	X						⌘ 24.234	
Y	N										
X											
Other comments:	⌘										

6.1.1 USIM-based WLAN Access Authentication

USIM based authentication is a proven solution that satisfies the authentication requirements from section 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in section 6.1.1.1.

Editor's note: also see section 4.2.4 on WLAN-UE Functional Split.

6.1.1.1 EAP/AKA Procedure

The EAP-AKA authentication mechanism is specified in ref. [4]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.

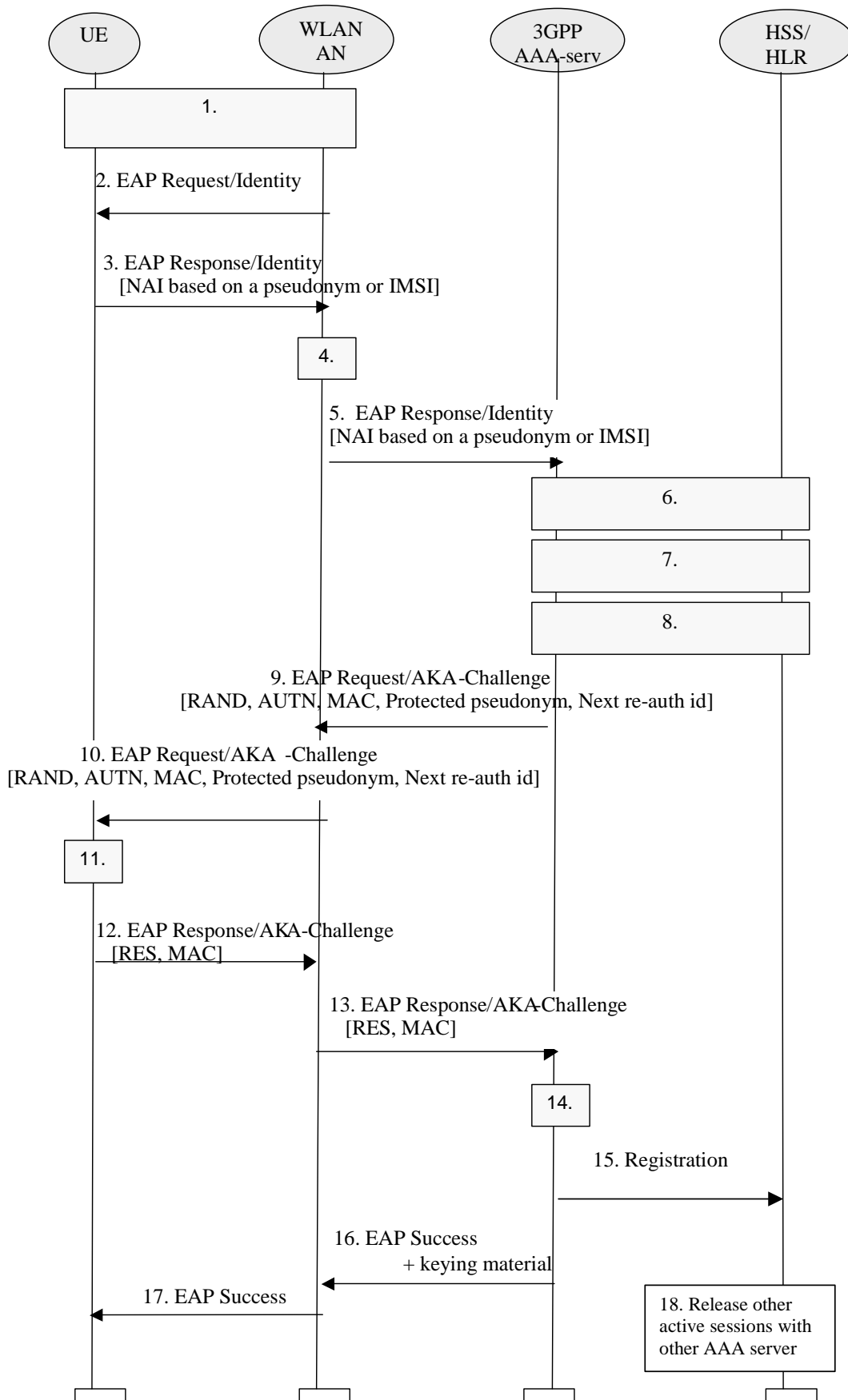


Figure 4: Authentication based on EAP AKA scheme

1. A connection is established between the WLAN-UE and the WLAN-AN, using a Wireless LAN technology specific procedure (out of scope for this specification).
2. The WLAN-AN sends an EAP Request/Identity to the WLAN-UE.

EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The WLAN-UE sends an EAP Response/Identity message. The WLAN-UE sends its identity complying with Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to the WLAN-UE in previous authentication or, in the case of first authentication, the IMSI.

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in EAP/AKA [4].

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).

NOTE 2: Diameter referral can also be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity. [The identifier of the WLAN radio network and the MAC address of the WLAN-UE shall also be received by the 3GPP AAA server in the same message.](#)

6. 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-AKA, based on the received identity. The 3GPP AAA Server then checks that it has an unused authentication vector available for that subscriber. If not, a set of new authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

NOTE 3: It could also be the case that the 3GPP AAA Server first obtains an unused authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a UMTS authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-AKA.

7. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)

8. New keying material is derived from IK and CK., cf. [4]. This keying material is required by EAP-AKA, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.

A new pseudonym may be chosen and protected (i.e. encrypted and integrity protected) using EAP-AKA generated keying material.

9. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated): protected pseudonym and/or re-authentication id to WLAN-AN in EAP Request/AKA-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

10. The WLAN-AN sends the EAP Request/AKA-Challenge message to the WLAN-UE.

11. The WLAN-UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes RES, IK and CK.

The WLAN UE derives required additional new keying material from the new computed IK and CK from the USIM, checks the received MAC with the new derived keying material.

If a protected pseudonym was received, then the WLAN-UE stores the pseudonym for future authentications.

12. The WLAN UE calculates a new MAC value covering the EAP message with the new keying material. WLAN-UE sends EAP Response/AKA-Challenge containing calculated RES and the new calculated MAC value to WLAN-AN.

13. WLAN-AN sends the EAP Response/AKA-Challenge packet to 3GPP AAA Server

14. ~~14.~~—3GPP AAA Server checks the received MAC and compares XRES to the received RES. [If successful, the AAA server shall compare the MAC address and the WLAN radio network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for the old sessions \(skip step 15\).](#)

15. [Otherwise, the AAA server considers the authentication exchange is related to a new scenario-2 session. In this case the AAA server shall register the to the HSS for decision. The AAA server shall also inform the WLAN-UE's MAC address as well as the identifier of the WLAN radio network used.](#)

In case a pre-Rel 6 HSS is used, the AAA server shall instead, to handle the decision locally. The AAA shall create a new session and records in local database the terminal's MAC address and the WLAN radio network identification, received over the Wa or Wd reference point, with the session information. [If the AAA server identifies that the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything about the old sessions. Otherwise, if the comparison in step 2 indicates that the MAC address or the radio network information is different than in any ongoing session, then the authentication exchange is related to a scenario-2 session that was previously unknown to the 3GPP AAA server. Since a pre-release 6 HLR/HSS is being used, the 3GPP AAA needs to make the decision about closing an old session itself. If simultaneous sessions are not allowed, or if the number of allowed sessions has been exceeded, then the 3GPP AAA server closes an old scenario-2 session.](#)

16. ~~15.~~—If all checks in step 14 are successful, then 3GPP AAA Server sends the EAP Success message to WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection then the 3GPP AAA Server includes this keying material in the underlying AAA protocol message (i.e. not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

~~16.~~17. WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the WLAN-UE and the WLAN-AN share keying material derived during that exchange.

18. [If the same subscriber but different MAC address or the radio network information is received than in any ongoing session, then the registration is related to a new scenario-2 session. The HSS shall close an old scenario-2 session by indicating the 3GPP AAA server of the old session to terminate the session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.](#)

10 - 14 May 2004

Beijing, China

Title: Limiting simultaneous WLAN scenario-2 connections

Source: Nokia

Document for: Discussion and approval

Agenda Item: WLAN

1 Introduction

This submission proposes a mechanism to limit the number of simultaneous scenario-2 sessions per subscriber in order to prevent certain fraud scenarios. The proposed mechanism works with IEEE 802.11i pre-authentication and it can also be adapted to allow some limited number of simultaneous scenario-2 sessions.

2 Discussion

2.1 Motivation

If a single subscriber is allowed to establish an unlimited number of WLAN scenario-2 sessions, then certain fraud scenarios can occur. For example, a malicious user might buy a subscription, share the subscription with a large number of users and later refuse to pay the incurred bills. Another example is that a malicious user buys a flat-rate subscription, and then charges for connectivity provided for other users.

It would be advantageous to limit the number of scenario-2 sessions a subscriber can have in order to eliminate these fraud scenarios.

2.2 How many simultaneous sessions are needed?

In general, a single WLAN radio can only have one scenario-2 session at a time, because there is a one-to-one correspondence between a scenario-2 session and a WLAN association. If we assume that only one WLAN radio is available, then the number of simultaneous sessions could be limited to at most one per subscriber at a moment.

It is conceivable that UEs might have several different WLAN radios, so there might be some use for a very small number of simultaneous scenario-2 sessions. Also in the split UE case, it might be desirable to allow two simultaneous connections, one from a phone and another from a laptop.

Hence, the required number of simultaneous scenario-2 sessions per subscriber is either one, or in some cases, some very small number such as two or three.

2.3 New sessions should prevail over old sessions

When simultaneous sessions are to be prevented, it would be better to disconnect the old sessions when a new session is established, rather than to block new session attempts when there is an ongoing session. Blocking new session attempts would be problematic because it may be difficult

to close all WLAN sessions in a timely manner. The valid user might have left the radio coverage of some previous WLAN network without explicitly closing the session, so an old WLAN session might still be dangling. Even though dangling sessions should be automatically closed as soon as possible, there can still be delays of at least a minute. Such dangling sessions should not prevent the valid user from creating new sessions.

Hence the preferred way of limiting the number of simultaneous scenario-2 sessions is to close the old session when a new session is established. Draft TS 23.234 already includes a procedure in the Wa and Wd reference points by which the 3GPP AAA server can disconnect a scenario-2 session, and a procedure in the Wx reference point by which the HSS can tell the 3GPP AAA server to disconnect a scenario-2 session.

2.4 IEEE 802.11i Pre-Authentication and Pairwise Master Key Caching

IEEE 802.11i specifies the concepts of Pairwise Master Key (PMK) caching and pre-authentication. In pre-authentication, the terminal can authenticate with several APs (AP2, AP3, ...) while associated with a single AP (AP1). The AP1 with which the terminal is associated relays authentication information to the other APs (AP2, AP3, ...), in other words, the terminal is not in radio communications with AP2, AP3,

The purpose of pre-authentication is to enable the terminal and other APs to establish Pairwise Master Keys in advance, so that handovers can later be performed quickly. PMK caching refers to the procedure where the terminal maintains copies of PMKs shared with several APs, and is able to quickly handover back to the previously visited APs.

Due to pre-authentication and PMK caching, WLAN authentication exchanges do not have a one-to-one correspondence to WLAN scenario-2 sessions or WLAN associations. When the terminal pre-authenticates with an AP, the AAA server should not close the connection with the original AP. Also when the terminal performs a handover between access points within the same WLAN radio network, the AAA server should not close the old connection, because PMK caching can later be used to return to the same AP quickly.

2.5 Proposed Mechanisms

2.5.1 General

WLAN radio network implementations already prevent having simultaneous sessions with the same MAC address in a single WLAN network. The access points usually use an Inter Access Point Protocol (IAPP) to notify each other when an association with a certain terminal MAC address is established. If some other access point also has an association, it will disassociate because it interprets it as the terminal having moved to a new access point.

Hence, it is only necessary to limit the simultaneous sessions in different WLAN radio networks, and with different MAC addresses. The terminal's MAC address is included in the AAA packets even according to current AAA protocols, and there will most likely be need to include some identifier of the WLAN radio network as well, for example to produce detailed and itemized bills about WLAN usage with WLAN network identification information to the end users.

Therefore it is proposed that the Wa and Wd reference points enable communicating the terminal's MAC address and an identifier of the WLAN radio network from the WLAN AN to the 3GPP AAA server. It is also proposed that the Wx reference point should enable communicating the terminal's MAC address and an identifier of the WLAN radio network from the 3GPP AAA server to the HSS (see section below the justification).

2.5.2 Operation with a release-6 HSS

If a release-6 compliant HSS is used, then the decision about whether to close an old session upon the establishment of a new session can be done by the HSS. The HSS is the only element that is aware of all the sessions a subscriber has, since there can be several 3GPP AAA servers. The 3GPP AAA server cannot be aware of the sessions the subscriber might have with other 3GPP AAA servers.

It is proposed that the AAA server operates as follows upon a scenario-2 authentication exchange:

1. After successful authentication, the AAA server checks whether there is an ongoing scenario-2 session for the subscriber. If there is no ongoing session, the AAA server registers this session with the HSS over the Wx reference point (as described in draft TS 23.234). The AAA server includes the terminal's MAC address and the WLAN radio network identification, received over the Wa or Wd reference point, in the registration.
2. If the AAA server detects that there is an ongoing session, the AAA server compares the MAC address and the WLAN radio network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for the old sessions.
3. If the comparison in step 2 indicates that the MAC address or the radio network information is different than in any ongoing sessions, then the authentication exchange is related to a new scenario-2 session or to a scenario-2 session that has been so far managed by a different 3GPP AAA server. Since a release 6 compliant HSS is being used, the 3GPP AAA server registers the new session with the HSS to let the HSS decide whether something needs to be done with the old sessions.

When an AAA server registers a scenario-2 session with the HSS, the HSS should operate as follows:

1. The HSS server compares the MAC address and the WLAN radio network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to close any sessions. (It should be noted that the 3GPP AAA server might change during a session, so not all new registrations necessarily relate to a new scenario-2 session).
2. If the comparison in step 1 indicates that the MAC address or the radio network information is different than in any ongoing session, then the registration is related to a new scenario-2 session. If simultaneous sessions are not allowed, or if the number of allowed sessions has been exceeded, then the HSS can close an old scenario-2 session by indicating the 3GPP AAA server of the old session to terminate the session.

2.5.3 Operation with a pre-release 6 HLR/HSS

If a pre-release 6 HLR/HSS is used, then there is no centralized element that would be aware of all the sessions. In this case, the 3GPP AAA server needs to make the decisions about closing the old sessions itself. As the AAA server cannot be aware of the sessions the subscriber might have with other AAA servers, this mechanism cannot guarantee that simultaneous sessions would always be prevented.

It is proposed that when a pre-release 6 HLR/HSS is used, the 3GPP AAA server operates as follows upon a scenario-2 authentication exchange:

1. After successful authentication, the AAA server checks whether there is an ongoing scenario-2 session for the subscriber. If the subscriber has no ongoing sessions, the AAA server creates a new session and records the terminal's MAC address and the WLAN radio

network identification, received over the Wa or Wd reference point, with the session information.

2. If the 3GPP AAA server detects that the subscriber has an ongoing session after successful scenario-2 authentication, the AAA server compares the MAC address and the WLAN radio network information of the authentication exchange with the same information of the ongoing session(s). If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything about the old sessions.
3. If the comparison in step 2 indicates that the MAC address or the radio network information is different than in any ongoing session, then the authentication exchange is related to a scenario-2 session that was previously unknown to the 3GPP AAA server. Since a pre-release 6 HLR/HSS is being used, the 3GPP AAA needs to make the decision about closing an old session itself. If simultaneous sessions are not allowed, or if the number of allowed sessions has been exceeded, then the 3GPP AAA server closes an old scenario-2 session.

3 Proposal

We propose that SA3 adopt the mechanisms presented in Section 2.5.