TSGS#27(05) 0265

Source: **SA3**

Title: **CRs to 33.234 on Wireless Local Area Network (WLAN) interworking security (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050265	33.234	064	2	Rel-6	F	Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	6.4.0	6.5.0	S3-050314
SP-28	SP-050265	33.234	065	1	Rel-6	F	Terminate WLAN session by AAA server	6.4.0	6.5.0	S3-050312
SP-28	SP-050265	33.234	066	-	Rel-6	F	Correction to the definition of the Wn Reference Point	6.4.0	6.5.0	S3-050266

3GPP TSG SA WG3 Security — S3#38
Geneva, Switzerland 26 - 29 April 2005

Draft Tdoc S3-050314

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **064** ⌘ **rev** **2** ⌘ Current version: **6.4.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access
Source:	⌘	SA3 (NOKIA, T-mobile, Ericsson)
Work item code:	⌘	WLAN
Date:	⌘	28/04/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	There are no security holes in using multiple IPSec SAs per IKE_SA, so release-6 specifications should not carry text that suggests that it does. Considering rekeying to avoid session interruption, at some point in time, two IPsec SAs need to coexist if there is only one IPsec SA per IKE SA.
Summary of change:	⌘	Allow operator to configure the maximum value for the number of IPsec SAs per IKE SA. Also have re-keying in consideration.
Consequences if not approved:	⌘	It's impossible to deal with re-keying and cause session interruption.

Clauses affected:	⌘	5.7

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

⌘

Other comments:	⌘	The mechanisms may need to be re-visited in Rel-7 if support for QoS is introduced.

*** BEGIN OF CHANGE ***

5.7 Simultaneous access control

The home network operator needs to be aware of how the user is accessing the WLAN network. If the user is making the SIM or UICC card available for several devices that have WLAN access capabilities, the home network operator may decide, at any time, to allow or bar t he access of two or more network devices simultaneously.

WLAN direct IP access

The control of simultaneous sessions in WLAN direct IP access can be performed, under some circumstances, using the MAC address of the user's device.

After a number of successful authentications, if a subsequent authentication attempt is being performed by another device, the MAC address will be different and the AAA server will be able to detect it. However, this mechanism has some limitations. One of them is that if the two devices are accessing two different WLAN access points (assuming that a WLAN access point has a independent control of MAC address space), the MAC address of one of them can be spoofed and made equal to the other one. This is a fraud situation the home network should avoid. However, it may happen that the user is accessing other WLAN access point and a pre-authentication is performed in this new access point. In this case there is no fraud attempt. Then, in this situation (same MAC addresses, different WLAN radio networks) the AAA server should check if there is a AAA accounting start message sent from WLAN AN after the authentication procedure completes. If there is such accounting start message and the number of simultaneous sessions for the subscriber has already been reached, it is considered to be a fraud attempt and the AAA server should send a message to WLAN AN to stop this simultaneous session.

WLAN 3GPP IP access

The control of simultaneous sessions in WLAN 3GPP IP access has to be performed in a different way than in WLAN direct IP access as in this case the MAC addresses cannot be trusted by the home network and may not be available.

The user gets connected to the 3GPP network using the W-APNs. When a W-APN is activated by the user, an IKEv2 exchange will be initiated and, if successful, an IKE SA and an IPsec SA will be established.

The IKEv2 procedure is authenticated using EAP SIM or EAP AKA, so the AAA server has to be contacted in order to perform this authentication. Then the AAA server will be aware of the fact that a new W-APN is going to be activated.

The mechanism to control simultaneous sessions is to limit the number of W-APNs to be activated by the user and control the number of IKEv2 security associations per W-APN. The home operator shall configure, by subscription, the Maximum Number of IKE SAs per W-APN. With this mechanism, it is ensured that only as many devices as defined by the Maximum Number make use of the same subscription to access the 3GPP network, because each device will have to activate a W-APN (and use a different IKE SA and IPsec SA).

According to the IKEv2 protocol, ~~Since~~ one IKE SA allows to establish multiple IPsec SAs. ~~Sas,~~ Operators shall be able to configure the maximum value for the number of IPsec SAs per IKE SA at PDG. ~~and~~

~~the establishment of a new IPsec SA (under the same IKE SA) does not imply to contact the AAA server, the PDG shall reject more than one IPsec SA per IKE SA. This measure forces the WLAN UE to setup a new IKE SA if the WLAN UE wants to setup a new IPsec SA, hence making the AAA server aware of this establishment attempt and enforcing the authorization mechanism specified previously.~~ To avoid session interruptions when the first IPsec SA reaches the end of its lifetime, re-keying is needed. Implementations shall correctly handle this re-keying, even though this may temporarily raise the number of IPsec SAs to 2 if there is only one IPsec SA per IKE SA.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#38
Geneva, Switzerland 26 - 29 April 2005

Tdoc S3-050312

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **065** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Terminate WLAN session by AAA server
Source:	⌘	SA3 (NOKIA)
Work item code:	⌘	WLAN
Date:	⌘	14/04/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	To support the control of simultaneous WLAN direct IP access session numbers, AAA server needs to be able to send termination message to WLAN AN. SA2 has agreed the immediate purging of a user from the WLAN AN shall be supported by all WLAN ANs, and will provide the necessary changes in TS23.234 clause 6.3.1.2 making this function mandatory.
Summary of change:	⌘	Add a NOTE about this in section 6.1.6.
Consequences if not approved:	⌘	Will be inconsistent with other 3GPP specifications.

Clauses affected:	⌘	6.1.6

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

Other comments: ⌘

*** BEGIN OF CHANGE ***

6.1.6 WLAN Direct IP Session Start

This section describes how to use AAA accounting start message to detect a fraud simultaneous session in WLAN Direct IP Access.

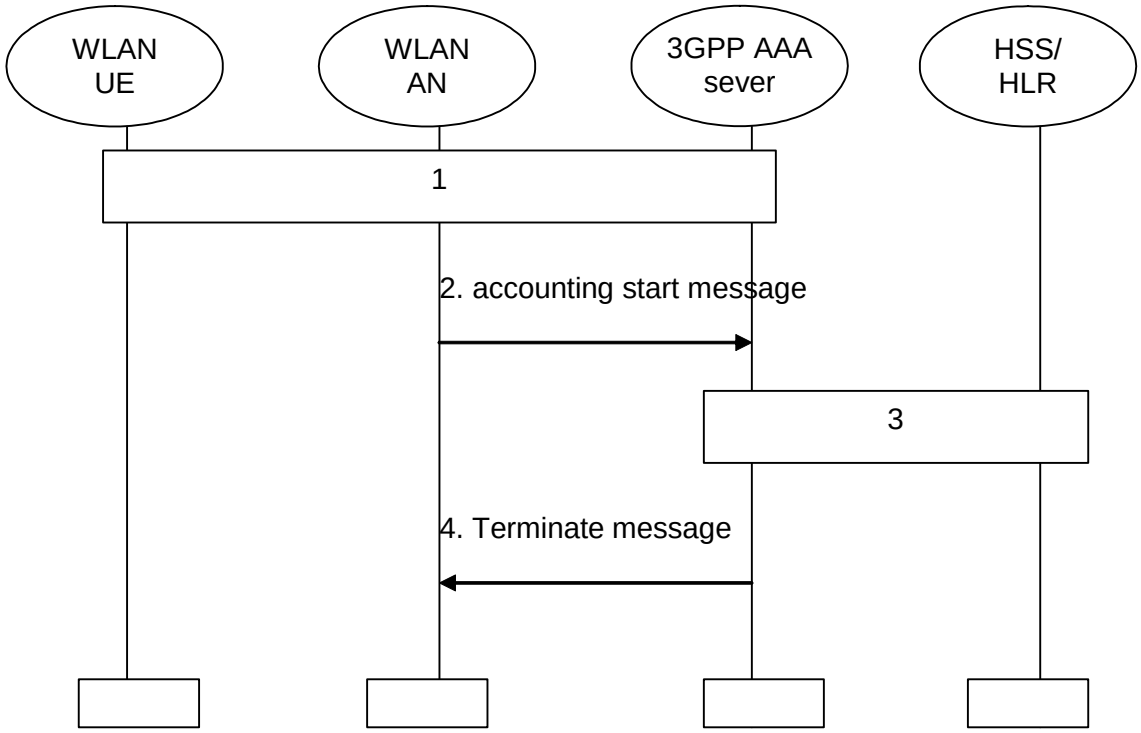

Figure 7C: detecting and stopping WLAN session

1. EAP/AKA or EAP/SIM procedure completes.

~~1~~2. 3GPP AAA server receives an accounting start message from WLAN AN.

~~2~~3. 3GPP AAA server verifies that a corresponding authentication procedure has been completed. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN access 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 old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or with different radio network information that is received than in any ongoing session, the 3GPP AAA server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. If the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one, the new session is considered to be a fraudulent one.

~~3~~4. If in step 3 the new session is considered to be a fraudulent one, 3GPP AAA server terminates the new session.

NOTE: To control the number of simultaneous WLAN direct IP access sessions and the immediate purging of a user from the WLAN AN, both the AAA server and the WLAN AN need to support Diameter/RADIUS extension, see subclause 5.5.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#38
Geneva, Switzerland 26 - 29 April 2005

Tdoc S3-050266

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **066** ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Correction to the definition of the Wn Reference Point
Source:	⌘	SA3 (NOKIA)
Work item code:	⌘	WLAN
Date:	⌘	14/04/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Analysis by CT4 on the text in TS 29.234 related to Wn has led to the conclusion that it should be clarified that the specific method to implement this Reference Point is out of scope of 3GPP. CT4 have agreed a CR to 29.234 removing the description of the Wn reference point from Stage 3. The change proposed in this CR brings 33.234 in line with CT4's analysis and the changes made to 29.234.
Summary of change:	⌘	Text added in 4.1.5 to clarify that it is out of scope of 3GPP to specify the method to implement Wn.
Consequences if not approved:	⌘	Stage 2 specifications will be inconsistent with Stage 3 regarding the Wn Reference Point.

Clauses affected:	⌘	4.1.5

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

Other comments:	⌘	

*** BEGIN OF CHANGE ***

4.1.5 Reference points description

Wa
The reference point Wa connects the WLAN Access Network to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The main purpose of the protocols implementing this interfaces is to transport authentication and keying information (WLAN UE - 3GPP network), and authorization information (WLAN AN – 3GPP network). The reference point has to accommodate also legacy WLAN Access Networks and thus should be Diameter [23], [24] or RADIUS [15], [26] based.

Wx
This reference point is located between 3GPP AAA Server and HSS. The main purpose of the protocols implementing this interface is communication between WLAN AAA infrastructure and HSS, and more specifically the retrieval of authentication vectors, e.g. for USIM authentication, and retrieval of WLAN access-related subscriber information from HSS. The protocol is either MAP or Diameter based.

D'/Gr'
This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The main purpose of the protocol implementing this interface is communication between WLAN AAA infrastructure and HLR, and more specifically the retrieval of authentication vectors, e.g. for USIM authentication, from HLR. The protocol is MAP-based.

Wn
This reference point is located between the WLAN Access Network and the WAG. This interface is to force traffic on a WLAN UE initiated tunnel to travel via the WAG. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN and is out of the scope of this Release of 3GPP specifications.

*** END OF CHANGE ***