**3GPP TSG SA WG3 Security — S3#37** **S3-050059**

**21 - 25 February 2005**

**Nice, France**

| | |
|---|---|
| **Title:** | **Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages** |
| **Source:** | **Nokia** |
| **Document for:** | **Discussion and decision** |
| **Agenda Item:** | |
| **Work Item:** | **WLAN-IW** |

# 1 Introduction

SA3 has previously discussed how to keep track of simultaneous WLAN Direct IP Access sessions, so that the number of simultaneous sessions per user can be limited by the home operator. Such control might be useful for example in detecting various fraud cases and in preventing subscribers from sharing their subscription with others.

The 3GPP AAA server also needs to detect when a WLAN Direct IP Access session is established, so that the subscriber information in the HSS can be updated by registering the user with the HSS.

It has been noted that one of the challenges in controlling simultaneous WLAN Direct IP Access sessions is the fact that there is no one-to-one correspondence between EAP authentication exchanges and Direct IP Access sessions. Due to IEEE 802.11 pre-authentication and Pairwise Master Key (PMK) caching, EAP exchanges may be performed without creating Direct IP Access sessions, and Direct IP Access sessions may also be created without an immediately preceding EAP exchange. Hence, the 3GPP AAA server cannot easily use EAP authentication exchanges to detect when a Direct IP Access session is established.

# 2 Discussion

The WLAN AN is expected to report accounting information (charging signalling per WLAN user) to the 3GPP AAA server over the Wa and Wd reference points. Both Diameter, which is the 3GPP AAA protocol, and RADIUS, which is the most commonly used legacy AAA protocol, support accounting.

Diameter accounting is specified in RFC 3588 [1]. As the first accounting message for a given session of a measurable length, such as a WLAN Direct IP Access session, a Diameter client sends an Accounting-Request message with the Accounting-Record-Type AVP set to the value START_RECORD. The last accounting message with include the Accounting-Record-Type AVP set to the value STOP_RECORD.

According to RFC 2866[2], a RADIUS client that is configured to use RADIUS accounting will generate an Accounting Start packet at the start of service delivery. At the end of service delivery, the RADIUS client will generate an Accounting Stop packet.

Since the Diameter or RADIUS accounting start and stop messages denote the start and end of the session, the 3GPP AAA server can use these packets to detect when a WLAN Direct IP Access session starts and when it ends. When the 3GPP AAA server receives an accounting start

message over the Wa or Wd reference point, the 3GPP AAA server can deduce that a new WLAN Direct IP Access session starts. The 3GPP AAA server can verify that a corresponding EAP authentication has been recently performed. When an accounting stop message is received, the 3GPP AAA server should record that the WLAN Direct IP Access session has ended.

Currently, both 23.234 and 33.234 consider the EAP authentication exchange as a potential indication of a new WLAN Direct IP Access session. In 23.234 section 7.2 "WLAN Access Authentication and Authorization", the 3GPP AAA server registers, as part of the EAP authentication procedure, the WLAN Direct IP Access session with the HSS if the WLAN user is not yet registered. In 33.234 section 6.1.1.1, step 25, the AAA server checks whether an EAP authentication exchange relates to a new session.

Simultaneous WLAN Direct IP Access sessions are also discussed in Section 5.7 of 33.234.

# 3 Conclusions

We propose that the 3GPP AAA server should use the Diameter/RADIUS accounting start message instead of a successful EAP authentication exchange to detect when a WLAN Direct IP Access session has been created. If this principle is agreed, then several places in TS 23.234 and 33.234 need to be updated.

# 4 References


1. RFC 3588 “Diameter base protocol”, P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, September 2003.
2. RFC 2866 "RADIUS Accounting", C. Rigney, June 2000

**3GPP TSG SA WG3 Security — S3#37** *Tdoc ⌘att_S3-050059*
**Sophia Antipolis, France 21 - 25 February 2005**

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.234** **CR** **061** ⌘**rev** **-** ⌘ Current version: **6.3.0** ⌘

*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 **X** Core Network **X**

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages |
| ***Source:*** | ⌘ | NOKIA |
| ***Work item code:*** | ⌘ | WLAN |
| ***Date:*** | ⌘ | 5/02/2005 |
| ***Category:*** | ⌘ | **F** |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. |
| ***Release:*** | ⌘ | Rel-6 |
| | | *Use one of the following releases:*<br>*Ph2* *(GSM Phase 2)*<br>*R96* *(Release 1996)*<br>*R97* *(Release 1997)*<br>*R98* *(Release 1998)*<br>*R99* *(Release 1999)*<br>*Rel-4* *(Release 4)*<br>*Rel-5* *(Release 5)*<br>*Rel-6* *(Release 6)*<br>*Rel-7* *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | In WLAN direct IP access if there is an ongoing WLAN Access session for the subscriber there is no way to distinguish whether a new authentication attempt is valid when it has same MAC addresses as the ongoing WLAN Access session, but with different WLAN radio networks information, because it may be a request of setting up a simultaneous session or a pre-authentication. |
| ***Summary of change:*** | ⌘ | The Diameter/RADIUS accounting start message can be used to detect that a WLAN Direct IP Access session is created. In the case described above if there is an accounting start message sent from WLAN AN after the new authentication procedure completes, this simultaneous session is a fraud one and should be stopped. |
| ***Consequences if not approved:*** | ⌘ | There is still no method to distinguish simultaneous session from pre-authentication in WLAN direct IP access if the new authentication attempt has same MAC addresses as the ongoing WLAN Access session, but with different WLAN radio networks information, so that there may exist a fraud simultaneous session if the new authentication attempt isn't a pre-authentication. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.7, 6.1.1, 6.1.2, a new added section 6.1.6 |
| ***Other specs affected:*** | ⌘ | Y / N<br>☐ / **X** Other core specifications<br>☐ / **X** Test specifications<br>☐ / **X** O&M Specifications |
| | ⌘ | |
| ***Other comments:*** | ⌘ | |

*** 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 Diameter/RADIUS accounting start message sent from WLAN AN after the authentication procedure completes. If there is such accounting start message, it is a fraud attempt and the AAA server should send a Diameter/RADIUS accounting stop message to WLAN AN to stop the fraud simultaneous sessions.~~will not be able to distinguish between a legal and a fraud situation and shall not reject the authentication process.~~

*** NEXT CHANGE ***

25. ~~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. The exception in this process is when 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. In that case the authentication process continues normally.~~

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP AKA process will be terminated as specified in ref. [4] and an indication shall be sent to HSS/HLR.

## 6.1.2 GSM SIM based WLAN Access authentication

SIM based authentication is useful for GSM subscribers that do not have a UICC with a USIM application. This form of authentication shall be based on EAP-SIM (ref. [5]), as described in section 6.1.2.1. This authentication method satisfies the authentication requirements from section 4.2, without the need for a UICC with a USIM application

*** NEXT CHANGE ***

24. ~~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 whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. The exception in this process is when 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. In that case the authentication process continues normally.~~

NOTE 4: The derivation of the value of N is for further study.

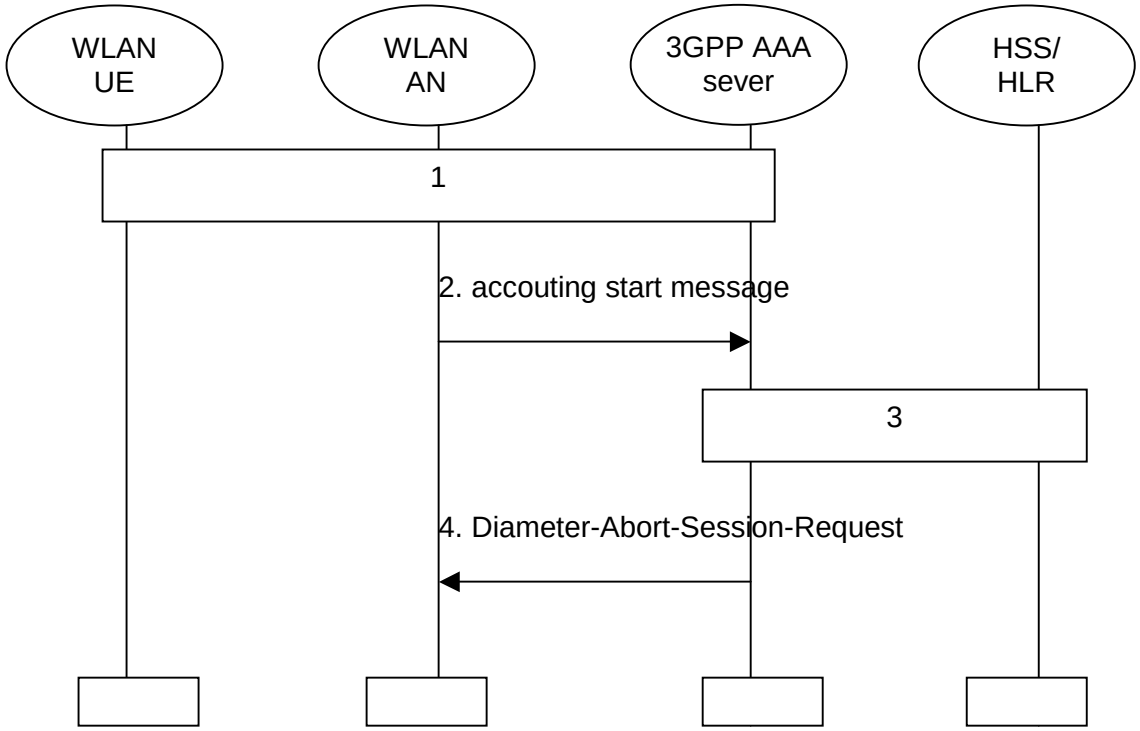
The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP SIM process will be terminated as specified in ref. [5] and an indication shall be sent to HSS/HLR.

### 6.1.3 EAP support in Smart Cards

*** NEXT 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.



1. EAP/AKA or EAP/SIM procedure completes.
2. 3GPP AAA server receives an accounting start message from WLAN AN.
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 a fraud one.
4. If in step 3 the new session is detected to be a fraud one, 3GPP AAA server sends an Diameter-Abort-Session-Request to WLAN AN to stop the fraud session.

*** END OF CHANGE ***