3GPP TSG SA WG3 Security — S3#37 **S3-050108**
21 - 25 February 2005
Sophia Antipolis, France

3GPP TSG-CN1 Meeting #37 Tdoc N1-050376
Sydney, Australia, 14-18 February 2005

Title: **Alignment of specifications between CN1 and SA3 with respect to fallback to full authentication**

Response to:

Release: Rel-6

Work Item: WLAN-IW

Source: CN1

To: SA3

Cc:

Contact Person:
Name: Paul Sitch
E-mail Address: paul.sitch@nokia.com

Attachments: N1-050354

---

1. Overall Description:

CN1 would like to draw SA3 attention to the following issue:

SA3 recently introduced the requirement that the 3GPP AAA server shall always send a pseudonym every time a re-authentication identity is sent to the WLAN UE, in order that fallback to full authentication is always possible. On attempting to align the CN1 specification with this new requirement, it was noted that the EAP-SIM and EAP-AKA specifications, to which our specifications shall comply, state that a pseudonym can be sent only during full authentication, and not during re-authentication. CN1 therefore agreed the text as indicated in the attached CR.

2. Actions:

CN1 kindly ask SA3 to consider the attached CR that was agreed in CN1#37 and align the SA3 specification, if appropriate.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37
Sydney, Australia, 14-18 February 2005

Tdoc N1-050354
Revision of N1-050327

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **20** ⌘ **rev** **2** ⌘ Current version: **6.1.1** ⌘

*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:	⌘	Fallback to full authentication
Source:	⌘	Ericsson, Nokia
Work item code:	⌘	WLAN
Date:	⌘	15/02/2005
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:	⌘	At SA3#36 the agreed CR in S3-041110 introduced a new requirement into TS 33.234, which is now implemented in the latest version of the specification (i.e. v6.3.0). The requirement mandates the 3GPP AAA server to send a pseudonym every time a re-authentication identity is sent to the WLAN UE. Therefore, fallback to full authentication is always possible.
Summary of change:	⌘	The stage 2 requirement is introduced into TS 24.234.
Consequences if not approved:	⌘	Misalignment with stage 2 (i.e. TS 33.234) remains. Therefore, mandatory requirements will not be included in the appropriate stage 3 specification (i.e. TS 24.234). This may lead to different 3GPP AAA server implementations.

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

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.1.1.3.5 Re-authentication

The 3GPP AAA server shall support re-authentication as specified in the 3GPP TS 33.234 [5].

Re-authentication should be enabled in the 3GPP AAA server. If re-authentication is enabled, the re-authentication may be full or fast, as follows:

- Full re-authentication means that a new full authentication procedure shall take place as the initial authentication procedure, where all keys are generated afresh in both the (U)SIM and network. Full re-authentication requires that the WLAN UE sends pseudonym or permanent IMSI-based identity.

- Fast re-authentication means that a new authentication procedure takes place in which Master Key and Transient EAP Keys are not generated in both the (U)SIM and network, but reused from the previous authentication process to generate the remaining keys necessary for this procedure. Fast re-authentication requires that the WLAN UE sends re-authentication identity.

The decision of using fast re-authentication is taken in the 3GPP AAA server depending on operator's policies. Operator's policies regarding fast re-authentication may contain for example, a timer to control start of fast re-authentication, a counter to control the maximum number of allowed fast re-authentications before a full EAP authentication shall be initiated towards the WLAN UE or a restriction on whether fast re-authentication is allowed to visiting subscribers.

The 3GPP AAA server indicates to the WLAN UE the decision of using fast re-authentication by means of sending the re-authentication identity in the EAP authentication procedure (i.e. in EAP-Request/AKA/-Challenge or EAP-Request/AKA/-re-authentication or EAP-Request/SIM/Challenge or EAP-Request/SIM/re-authentication messages). On each fast re-authentication procedure the 3GPP AAA server has the ultimate point of decision of whether to continue with the ongoing fast re-authentication procedure or to defer to a full re-authentication. Therefore, whenever the 3GPP AAA server sends a re-authentication identity to the WLAN UE, the 3GPP AAA server shall also include a pseudonym when allowed by the draft-haverinen-pppext-eap-sim [10] and draft-arkko-pppext-eap-aka [9]. In this way, the WLAN UE retains a pseudonym if the 3GPP AAA server defers to full authentication.

NOTE 1: In the current version of the draft-haverinen-pppext-eap-sim [10] and draft-arkko-pppext-eap-aka [9] the pseudonym (i.e. AT_NEXT_PSEUDONYM attribute) can only be sent during a full re-authentication procedure (i.e. in EAP-Request/SIM/Challenge or EAP-Request/AKA/Challenge).

NOTE 2: The use of fast re-authentication implies to save power consumption in the WLAN UE and processing time in both the WLAN UE and the 3GPP AAA server. However, when the fast re-authentication is used through a low trusted I-WLAN, it is strongly recommended to refresh the keys using full re-authentication. The use of fast re-authentication should be left for situations in which the user is accessing a high trusted I-WLAN.

The full and fast re-authentication signalling flows are described in 3GPP TS 33.234 [5].