TSGS#24(04)0463

Source: SA WG3 (Security)

Title: CR to 33.234: Support of EAP SIM and AKA in AAA server and WLAN UE (Rel-6)

Document for: Approval

Agenda Item: 7.3.3

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-040463	33.234	004	1	Rel-6	Support of EAP SIM and AKA in AAA server and WLAN UE	F	6.0.0	S3-040420 (revised at TSG SA#24)	WLAN

3GPP TSG SA WG3 Security — S3#33
Beijing, China 10 - 14 May 2004

Tdoc ⌘S3-040420-rev
(revised at TSG SA#24)

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **004** ⌘ **rev** **1** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Support of EAP SIM and AKA in AAA server and WLAN UE
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	13/06/2004
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:

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:	⌘	It was received in SA3#32 meeting an LS from CN1 in which it was questioned if EAP SIM and EAP AKA methods should be supported by the WLAN UE and the AAA server. SA3 answered that both methods must be supported by the WLAN UE and AAA server (see S3-040195). However, it was considered that pre-R6 WLAN UEs may support only one method and WLAN access has to be granted for these WLAN UEs instead of reporting an error when they request an EAP method which does not correspond to the (U)SIM card they are hosting.
Summary of change:	⌘	The present CR clarifies in TS 33.234 the requirement to support EAP SIM and AKA by the WLAN UE and AAA server for R6+, and sets policies as operator-specific for EAP method selection for pre-R6 WLAN UEs.
Consequences if not approved:	⌘	Multitude of situations may occur if it is not specified what WLAN UEs must support. There has to be an standardized behaviour of the AAA server and WLAN UE when negotiating the EAP method.

Clauses affected:	⌘	6.1, add a new annex F.

Other specs affected: ⌘

Y	N		
X		Other core specifications	⌘ 24.234
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘

*** BEGIN SET OF CHANGES ***

6.1 Authentication and key agreement

The WLAN UE and AAA server shall support both EAP AKA and EAP SIM methods. ~~The~~ A WLAN UE ~~will insert~~ with either a USIM or a SIM ~~card~~inserted~~, and will~~ shall request the authentication method corresponding to the type of smart card it holds (i.e. the user's subscription type). The procedure to select the method is:

1) The WLAN UE shall send an identity (whatever it is: permanent, pseudonym, etc.~~.~~) to the AAA server. ~~If this identity is an IMSI, it shall contain an indication of the EAP method to be used.~~ In the first authentication, the identity ~~will~~ shall be an IMSI and the message containing the identity ~~it will~~ shall also contain an indication of the authentication method to be used. In ~~the rest of~~ subsequent authentications, ~~it will~~ the identity shall be a temporary identity ~~in~~ for which the AAA server has already an indication of the associated authentication method.~~, and that~~The associated authentication method indication ~~must~~ shall not be modified by the WLAN UE.

2) If the AAA server recognizes the EAP method but not the user identity (for example an obsolete pseudonym), it shall request a new identity using the EAP method indicated by the WLAN UE.

3) If the AAA server recognizes the user identity (and hence the EAP method), it shall fetch AVs from HSS. If they don't match the EAP method received (e.g. the EAP method received is EAP AKA and triplets are received from HSS), the user's subscription shall prevail (in the previous example EAP SIM shall be used).

4) If the user identity is not recognized, the AAA server shall decide which method to use (there may exist a default method ONLY in this situation). If this default method does not match user's subscription (e.g. EAP AKA for a SIM user), the WLAN UE shall respond a NACK to the AAA server and then the AAA shall try with the other EAP method until a recognised identity is received.

[Editor's note: This section shall describe in detail how the authentication is performed and how the keys are derived and delivered to the different nodes.]

[Editor's note: The content of this section is directly copied from TS 23.xxx v0.1.0 and shall be reviewed by SA3]

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

Annex F (informative): Handling of the incompatibilities between the WLAN UE and the UICC or SIM card inserted

~~For~~ If a WLAN UE~~s which~~ does not conform to Release 6 specifications, it may ~~happen that a WLAN UE does~~ not support both authentication methods. In ~~that~~ this case, ~~it is up to~~ the home network operator needs to decide either to reject the authentication, or to proceed to authenticate the UE~~m~~ using a suitable EAP method. For instance, when a USIM is inserted in a ~~r~~Release 6 non-compliant WLAN UE which does not support~~s~~ a ~~non~~ compatible method with the USIM (~~i~~e.g. WLAN UE supporting EAP SIM). ~~Such WLAN UE is not compliant with this standard. However, a~~An operator may decide to convert the authentication vectors in order to adapt them to the EAP SIM authentication. This authentication vector conversion is defined in ref. [21].

As specified in ref. [21], it is not possible to have UMTS authentication using a SIM, as some parameters cannot be created from triplets (e.g. sequence number). Similarly, ~~in case that~~ if the WLAN UE only supports EAP AKA and the smart card is a SIM, it is not possible to perform an EAP AKA authentication.

~~For~~ If a AAA server ~~which~~ does not conform to Release 6 specifications, it may not be able to support EAP-AKA for USIM subscribers. It is recommended that operators ~~can~~ avoid this by upgrading AAA servers when ~~USIM cards~~ UICCs are issued. In this case, the default policy of the ME should be to not accept~~ing~~ EAP-SIM, but the ME can support an alternative policy that accepts EAP-SIM, if enabled.

*** END SET OF CHANGES ***