3GPP TSG SA WG3 Security — S3#29 *Tdoc ⌘S3-030383*
San Francisco, USA 15 - 18 July 2003

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.234 CR CRNum** ⌘**rev -** ⌘ Current version: **0.5.0** ⌘

*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:	⌘	Support for interleaving authentication
Source:	⌘	Siemens
Work item code:	⌘	WLAN
Date:	⌘	07/07/2003
Category:	⌘	
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:	⌘	In order to avoid more frequent authentication failures due to Sequence number synchronisation problems the AuC shall be made aware of that the authentication request came from WLAN.
Summary of change:	⌘	Inclusion of informative Annex similar as for IMS (TS 33.203 informative annex G)
Consequences if not approved:	⌘	Increase in the rate of authentication failures due to synchronisation failures if simultaneous access to the WLAN and 3GPP systems is permitted

Clauses affected:	⌘	2, New Annex D

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

Other comments:	⌘	The requirement that the HSS/HLR must be able to determine whether the node requesting authentication vectors is in the CS, PS, IMS and WLAN domains needs to be made known to SA2 for possibe CR to 23.234 and to CN4 to enhance MAP.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 22.934: " Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking;".

[2] 3GPP TR 23.934: "3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] RFC 2284, March 1998, "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-06, November 2002, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-07, November 2002, "EAP SIM Authentication".

[6] IEEE Std 802.11i/D2.0, March 2002, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[7] RFC 2716, October 1999, "PPP EAP TLS Authentication Protocol".

[8] SHAMAN /SHA/DOC/TNO/WP1/D02/v050, 22-June-01, "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4v1.3.1B "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1 "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234 "3GPP system to Wireless Local Area Network (WLAN) Interworking System Description".

[14] RFC 2486, January 1999, "The Network Access Identifier".

[15] RFC 2865, June 2000, "Remote Authentication Dial In User Service (RADIUS)".

[16] RFC 1421, February 1993, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[17] Federal Information Processing Standard (FIPS) draft standard, "Advanced Encryption Standard (AES)", November 2001.

[18] 3GPP TS 23.003: "Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001, "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

Annex D (informative): Management of sequence numbers

The example sequence number management schemes in [21] Informative Annex C can be used to ensure that the authentication failure rate due to synchronization failures to kept sufficiently low when the same sequence number mechanism and data is used for authentication in the PS/CS domains, in IMS and WLAN. This can be done by enhancing the method for the allocation of index values in the AuC so that authentication vectors distributed to different service domains shall always have different index values (i.e. separate ranges of index values are reserved for PS, CS ,IMS operation and WLAN access). The AuC is required to obtain information about which type of service node has requested the authentication vectors. Reallocation of array elements to the IMS domain can be done in the AuC with no changes required to already deployed USIMs.

As the possibility for out of order use of authentication vectors within the WLAN service domain may be quite low, the number of existing array elements that need to be reallocated to the WLAN domain could be quite small. This means that the ability to support out of order authentication vectors within the PS, CS and IMS domains would not be significantly affected.

Sequence number management is operator specific and for some proprietary schemes over the air updating of the UICC may be needed.