3GPP TSG-SA3 Meeting #28
Berlin, Germany, 5th-9th May, 2003

Tdoc ⌘S3-030252

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR CRNum** ⌘**rev** **-** ⌘ Current version: **0.4.0** ⌘

*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:	⌘	Editorial changes to 33.234
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	20/02/2003
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:	⌘	Clean up the text
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	

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

Other comments:	⌘	

.

*** BEGIN SET OF CHANGES ***

1 Scope

The present document ~~studies~~specifies the security architecture, trust model and security requirements for the interworking of the 3GPP System and WLAN Access Networks.

Recommendations of the appropriate mechanisms for user and network authentication, key management, service authorization, confidentiality and integrity protection of user and signalling data are also provided.

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 TR 21.905: "Vocabulary for 3GPP Specifications"~~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)", ~~September~~November 2001

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

[19] IEEE P802.1X/D11, ~~March~~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".

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.1 Security architecture and Roles

~~*[Editor’s note: This architecture is copied from SA2's TS 23.xxx v0.1.0 for the first draft of this TS, and shall be updated in later versions according to the work done in SA3]*~~

4.1.2 Network elements

The list below describes the access control related functionality in the network elements of the 3GPP-WLAN interworking reference model:

- The **WLAN-UE,** equipped with a UICC (or SIM card), for accessing the WLAN interworking service).
  - May be capable of WLAN access only
  - May be capable of both WLAN and 3GPP System access.
  - May be capable of simultaneous access to both WLAN and 3GPP systems

  [Editors note: definition of simultaneous access still TBA with SA1- LS in S3 030169]

  - May be a laptop computer or PDA with a WLAN card, UICC (or SIM card) card reader, and suitable software applications,
  - The UICC (or SIM card) may reside in the UE and accessed by the WLAN-UE through Bluetooth, IR or serial cable interface.

[Editors Note: All these alternatives must be carefully studied from a security perspective.]

- The **AAA proxy** represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.

The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA server or any other physical network node.

- The **3GPP AAA server** is located within the 3GPP network. The 3GPP AAA server :
  - Retrieves authentication information ~~and subscriber profile (including subscriber's authorisation information)~~ from the HLR/HSS of the 3GPP subscriber's home 3GPP network;
  - Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies.
  - Communicates authorisation information to the WLAN potentially via AAA proxies.
  - ~~Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorised 3GPP subscriber.~~

~~– May act also as a AAA proxy (see above).~~

4.2 Security Requirements

4.2.1 General

- The authentication scheme shall be based on a challenge response protocol.
- All long-term security credentials used for subscriber and network authentication shall be stored on UICC or SIM card.
- Long term security credentials, which are stored on the UICC or SIM card, shall not leave the UICC or SIM card.
- Mutual Authentication shall be supported.

~~– The selected Authentication solution should also allow for Authorisation.~~

4.2.2 Signalling and user data protection

- As a guideline, ~~T~~the subscriber should have at least the same security level for WLAN access as for ~~his current~~ a normal cellular access subscription.

~~– 3GPP systems should not compromise the security offered by the interworking WLAN subsystems.~~

- 3GPP systems should support authentication methods that support protected success/failure indications. Editors note: FFS if this is possible.
- The selected WLAN (re-) authentication mechanisms for 3GPP interworking shall provide at least the same level of security as [33.102] for USIM based access.
- The selected WLAN (re-authentication mechanism for 3GPP interworking shall provide at least the same level of security as [43.020} for SIM based access.
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.

~~– 3GPP systems should provide the required keying material with sufficient length and the acceptable levels of entropy as required by the WLAN subsystem~~

[Editors note: LS (S3-030166) sent to IEEE 802.11-task group i on their requirements over key length and entropy of keying material]

- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks.

- Protection should be provided for WLAN authentication data and keying material on the Wr interface

- The WLAN technology specific connection between the WLAN-UE and WLAN AN shall be able to utilise the generated session keying material for protecting the integrity of an authenticated connection.

[Editor's note: Threats on Wr interface are not clear yet so protection on this interface is FFS]

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.2.4 WLAN-UE Functional Split

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. If this is the case, then the following requirements shall be satisfied:

- Any local interface shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

- The endpoints of a local interface should be authenticated and authorised. The ~~authorisation~~ authentication may be implicit in the security set-up.

- The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

[Editor's note: LS (S3-030145) sent to SA1 - SA3 would like to thank SA1 for the LS and attached documents on the proposal "Having a Single USIM to Authenticate Multiple Devices Simultaneously using local Wireless Link" (Tdoc S3-030006, S1-022388). It was noted at the meeting that there was interest in studying the security issues related to this proposal and also UE functionality split scenarios. It was also noted at the meeting that the TR 22.944 v5.1.0 doesn't address the User Equipment Functionality Split (UEFS) issues for Release 6, but only for Release 5. However there was concern among some members on enhancing the USIM as part of this proposal. SA3 wishes to inform SA1 that a decision on the feasibility of this proposal needs further evaluation.]

4.2.5 Link layer security requirements

[Editors note: This section is FFS, LS (S3-030167) sent to SA2 group. On 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wr interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network]

Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.

In order to set the bar for allowed WLAN protocols, 3GPP should define requirements on link layer security. The existing and work-in-progress WLAN standards can then be evaluated based on these requirements.

Areas in which requirements should be defined are:

4.2.5.1 Confidentiality and integrity protection of user data

- Can user data be sent in the clear or is some kind of protection required?
- Is it enough to integrity protect user data or should it be encrypted as well?
- How strong must the WLAN security protocols be? Compare e.g. WEP, TKIP and CCMP in the case of 802.11 WLAN.

4.2.5.2 Protection of signaling

- What implications on 3GPP-WLAN security does it have if the WLAN control signaling is unprotected? (Currently 802.11 management frames are not protected by 802.11i).

4.2.5.2 Key distribution, key freshness validation and key ageing

- Can encryption keys generated during EAP authentication be used directly as encryption keys for the link layer or must there be a handshake between UE and AP to e.g. ensure freshness? (Like the 4-way handshake of 802.11i).
- What are the security implications of not having a UE-AP key handshake?

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.4 User Identity Privacy

User identity privacy (Anon~~i~~ymity) is used to avoid sending the cleartext permanent subscriber identity (NAI) and make the subscriber's connections unlinkable to eavesdroppers.

User identity privacy is based on temporary identities, or pseudonyms. The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementations, but optional for use.

The AAA server generates and delivers the pseudonym to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the pseudonym, it will just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the pseudonym.

To avoid user traceability, the user should not be identified for a long period by means of the same temporary identity. On the other hand, the AAA server should be ready to accept at least two different pseudonyms, in case the WLAN-UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain more than one allowed pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user to send its permanent identity. This represents a breach in the provision of user identity privacy. It is a matter of the operator's security policy whether to allow clients to accept requests from the network to send the cleartext permanent identity. If the client rejects a legitimate request from the AAA server, it will be denied access to the service.

[Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.]

*** END SET OF CHANGES ***