3GPP TSG-SA WG3 Meeting #26
Oxford, UK, 19-22 November 2002

Tdoc ⌘S3-020653

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.2.0** ⌘

*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:	⌘	Pseudonym generation and management in 3G-WLAN
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	14/11/2002
Category:	⌘	**B**
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:	⌘	Introducing a scheme for pseudonym generation and management
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 4.2, 5.1.4 (new), 6.4 (new)

		Y	N		
Other specs affected:	⌘		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.

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-04, June 2002, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-05, June 2002, "EAP SIM Authentication".

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

[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"

[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"

Next modified section

4.2 Security Requirements

[Editor's note: These requirements are copied from TS 23.xxx v0.1.0 for the first version of this TR, and shall be reviewed and updated according to the input from the preceding sections]

- Legacy WLAN terminals should be supported.
- Minimal impact on the user equipment, i.e. client software.
- The need for operators to administer and maintain end user SW should be minimized
- Existing UICC cards should be supported.
- Changes in the HSS/HLR/AuC should be minimized.
- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.
- The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription (i.e. GSM or UMTS)
- Mutual Authentication shall be supported for GSM and UMTS subscribers
- The selected Authentication solution should also allow for Authorisation
- Methods for key distribution to the WLAN access NW shall be supported
- For UMTS subscribers, the selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as 3GPP System authentication procedure. For GSM subscribers, the selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as the GSM system authentication procedure
- Subsequent WLAN re-authentication shall not compromise the requirement for 3GPP/GSM System equivalent security
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks. In other words, a man in the middle shall not be able to learn the session key material.
- The WLAN technology specific connection between the WLAN UE and WLAN AN shall be able to utilise the generated keying material for protecting the integrity of an authenticated connection
- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper resistant memory such as the UICC card.

Any secret keys used in WLAN AAA servers for the generation of pseudonyms should be infeasible to recover (even for an attacker that has available a number of matching permanent identities and pseudonyms).

Given a pseudonym (or even a number of correlated pseudonyms), it should be infeasible for an attacker to recover the corresponding permanent identity.

It should be infeasible for an attacker to determine whether or not two pseudonyms correspond to the same permanent identity.

It should be infeasible for an attacker to generate a valid pseudonym (irrespective of the underlying permanent identity).

It should be infeasible for an attacker to generate a valid pseudonym corresponding to a given permanent identity.

Next modified section

5.1.4 User Identity Privacy

User identity privacy (Anonimity) 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 UE as part of the authentication process. The UE shall not interpret the pseudonym, it will just use the received identifier at the next authentication. Pseudonyms are not stored in any node in the network. 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 maintain at least two pseudonyms in case the UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain a number of "active" pseudonyms.

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.

Next modified section

6.4 Temporary identity management

6.4.1 Pseudonym Generation

Pseudonyms are generated as some form of encrypted IMSI. Advanced Encryption Standard (AES) in Electronic Codebook (ECB) mode of operation with 128-bit keys is used for this purpose.

In order to encrypt with AES in ECB mode, it is necessary that the length of the clear text is a multiple of 16 octets. This clear text is formed as follows:

1. A *Compressed IMSI* is created utilising 4 bits to represent each digit of the IMSI. According to [TS23.003], the length of the IMSI is not more than 15 digits (numerical characters, 0 through 9). The length of the *Compressed IMSI* shall be 64 bits (8 octets), and the most significant bits will be padded by setting all the bits to 1.

   E.g.: IMSI = 214070123456789 (MCC = 214 ; MNC = 07 ; MSIN = 0123456789)

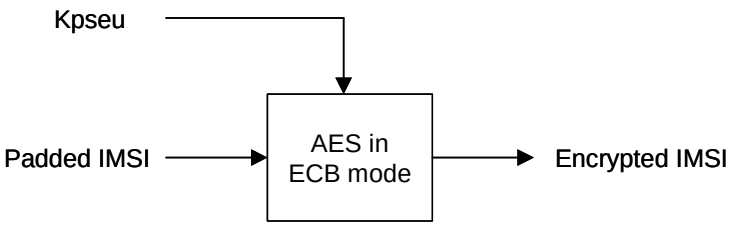
   Compressed IMSI = 0xF2 0x14 0x07 0x01 0x23 0x45 0x67 0x89

   Observe that, at reception of a pseudonym, it is easy to remove the padding of the *Compressed IMSI* as none of the IMSI digits will be represented with 4 bits set to 1. Moreover, a sanity check should be done at reception of a pseudonym, by checking that the padding, the MCC and the MNC are correct, and that all characters are digits.

2. A *Padded IMSI* is created by concatenating an 8-octet random number to the *Compressed IMSI*.

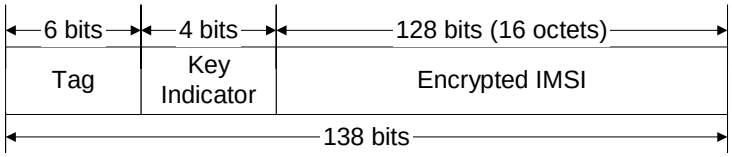
A 128-bit secret key, Kpseu, is used for the encryption. The same secret key must be configured at all the WLAN AAA servers in the operator network so that any WLAN AAA server can obtain the permanent identity from a pseudonym generated at any other WLAN AAA server (see section 6.4.2).

The figure below summarises how the *Encrypted IMSI* is obtained.



Once the *Encrypted IMSI* has been generated, the following fields are concatenated:

- *Encrypted IMSI*, so that a AAA server can later obtain the IMSI from the pseudonym.
- *Key Indicator*, so that the AAA server that receives the pseudonym can locate the appropriate key to de-encrypt the Encrypted IMSI. (See section 6.4.2.)
- *Pseudonym Tag*, used to mark the identity as a pseudonym. The tag should be different for pseudonyms generated for EAP-SIM and for EAP-AKA.



The *Pseudonym Tag* is necessary so that when a WLAN AAA receives a user identity it can determine whether to process it as a permanent or a temporary user identity. Moreover, according to EAP-SIM/AKA specifications, when the Authenticator node (i.e. the AAA server) receives a temporary user identity from which a permanent user identity cannot be successfully obtained, then the permanent user identity must be requested from the WLAN client. As the procedure to request the permanent user identity is different in EAP-SIM and EAP-AKA, the *Pseudonym Tag* must be different for EAP-SIM pseudonyms and for EAP-AKA pseudonyms, so that the AAA can determine which procedure to follow.

The last step in the generation of the pseudonym consists on converting the concatenation above to a printable string using the BASE64 method described in section 4.3.2.4 of ref. [16]. With this mechanism, each 6-bit group is used as an index into an array of 64 printable characters. As the length of the concatenation is 138 bits, the length of the resulting pseudonym is 23 characters, and no padding is necessary. Observe that the length of the *Pseudonym Tag* has been chosen to be 6 bits, so that it directly translates into one printable character after applying the transformation. Therefore, at reception of a user identity, the AAA server can recognise that it is a pseudonym for EAP-SIM or a pseudonym for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

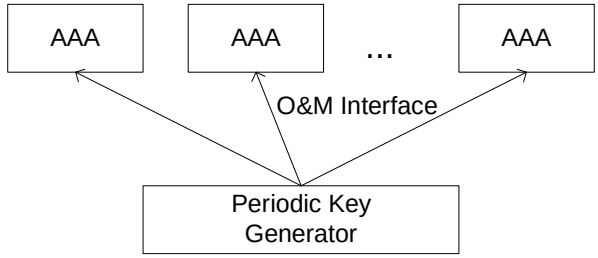
6.4.2 Key Management

A 128-bit encryption key shall be used for the generation of pseudonyms for a given period of time determined by the operator. Once that time has expired, a new key shall be configured at all the WLAN AAA servers. The old key shall not be used any longer for the generation of pseudonyms, but the AAA servers must keep a number of suspended (old) keys for the interpretation of received pseudonyms that were generated with those old keys. The number of suspended keys kept in the AAA servers (up to 16) should be set by the operator, but it must be at least one, in order to avoid that a just-generated pseudonym becomes invalid immediately due to the expiration of the key.

Each key must have associated a Key Indicator value. This value is included in the pseudonym (see *Key Indicator* field in section 6.4.1), so that when a WLAN AAA receives the pseudonym, it can use the corresponding key for obtaining the *Padded IMSI* (and thence the Username).

Observe that, if a pseudonym is sent to a WLAN client but then the user does not initiate new authentication attempts for a long period of time, the key used for the generation of that pseudonym will eventually be removed from all the WLAN AAA servers. If the user initiates an authentication attempt after that time, using that old pseudonym, the receiving AAA server will not be able to recognise the pseudonym as a valid one, and it will request the permanent user identity from the WLAN client. Thence, in order to achieve that permanent user identities are used as little as possible, it is recommended that the encryption key is not renewed very often.

The configuration of the keys could be done via O&M, as shown in the figure below.



Handling of these secret keys, including generation, distribution and storage, should be done in a secure way (out of the scope of this proposal).

6.4.3 Impact on Permanent User Identities

User identities (permanent or temporary) are sent with the form of a NAI, according to the EAP-SIM/AKA specifications, and the maximum length of a NAI that we can expect to be handled correctly by standard equipment is 72 octets (see ref. [14]). Moreover, this NAI will be transported inside the User-Name attribute of a RADIUS Access-Request, with standard length up to 63 octets (see ref. [15]). Therefore, it can be assumed that the maximum length of a WLAN user identity should be 63 octets (i.e. 63 characters).

Since the length of the pseudonym proposed in section 6.4.1 is 23 characters, the length of the realm part of any WLAN permanent user identity must always be 40 characters or less. This applies regardless of whether the length of the username part of the permanent user identity is less than 23 characters. (Note that a WLAN temporary user identity is formed as a NAI with the pseudonym as the username part and the same realm part as the permanent user identity.)

Moreover, the WLAN permanent user identities should not begin with the character resulting of the printable encoding transformation (see section 6.4.1) of the *Pseudonym Tag* used for EAP-SIM and EAP-AKA pseudonyms. This is needed so that at reception of a WLAN user identity, the AAA server can determine whether it is a permanent or a temporary user identity.

6.4.4 Acknowledged Limitations

This mechanism does not prevent forging of pseudonyms generated with keys that are no longer maintained in the AAA servers. That is, an attacker may form a pseudonym by concatenating the desired *Pseudonym Tag* and 132 bits of random information, and then applying the printable encoding transformation (see section 6.4.1). At reception of such pseudonym in a AAA server, the following cases are possible:

· The *Key Indicator* may not correspond to any key (active or suspended) maintained at the AAA server.

· If the *Key Indicator* corresponds to any of the keys maintained at the AAA server, then that key is used for the de-encryption of the *Encrypted IMSI*, but the sanity check over the padding, the MCC and the MNC would show that the IMSI is not correct.

In any case, the AAA server must interpret that the received pseudonym was generated with a key that is no longer available, and therefore it must request the permanent user identity to the WLAN client.

This could be exploited to perform DoS attacks by initiating a large amount of authentication attempts presenting different forged temporary identities. Nonetheless, the consequences of this attack should not be worse than the already possible attack of initiating a large amount of authentication attempts presenting different forged permanent identities.