3GPP TSG SA WG3 Security — S3#31 **Tdoc ⌘S3-030734**
Munich, Germany 18 - 21 November 2003

CR-Form-v7

CHANGE REQUEST

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

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:	⌘	Re-authentication identities generation		
Source:	⌘	Ericsson		
Work item code:	⌘	WLAN	***Date:*** ⌘	23/10/2003
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:	⌘	Ericsson submitted in SA3#30 meeting a CR to introduce in TS 33.234 the re-authentication procedure, which was approved. Nevertheless, to have the complete solution it was missing how the re-authentication identities are generated. The present CR covers it.
Summary of change:	⌘	Chapter 6.4.1 is modified so that the current method for pseudonym generation is also used for re-authentication identity generation. The term “pseudonym” is replaced by “temporary identity”, which is more generic and includes the re-authentication identities as well.
Consequences if not approved:	⌘	Re-authentication process not complete.

Clauses affected:	⌘	6.4 Temporary identity management.				
		Y	**N**			
Other specs affected:	⌘			Other core specifications	⌘	
				Test specifications		
				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.

*** BEGIN SET OF CHANGES ***

6.4.1 ~~Pseudonym~~Temporary Identity Generation

Temporary Identities (Pseudonyms or re-authentication identities) are generated as some form of encrypted IMSI. Advanced Encryption Standard (AES) (see ref. [17]) 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 ref. [18], 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)

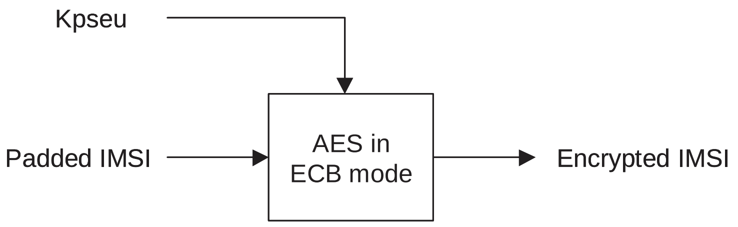
   Compressed IMSI = 0xF2 0x14 0x07 0x01 0x23 0x45 0x67 0x89

   Observe that, at reception of a temporary identity~~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 temporary identity~~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 temporary identity~~pseudonym~~.
- *Key Indicator*, so that the AAA server that receives the temporary identity~~pseudonym~~ can locate the appropriate key to de-encrypt the Encrypted IMSI. (See section 6.4.2.)
- *~~Pseudonym~~ Temporary identity Tag*, used to mark the identity as temporary (~~a~~ pseudonym or re-authentication identity). The tag should be different for pseudonyms and re-authentication identities, generated for EAP-SIM and for EAP-AKA

6 bits	4 bits	128 bits (16 octets)
Tag	Key Indicator	Encrypted IMSI
138 bits		

The ~~Pseudonym~~ Temporary Identity 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~~which does not recognize, then the permanent user identity ~~must be requested from the WLAN client~~(if the process was full authentication) or a full authentication identity (if the process was re-authentication) shall 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~~ Temporary Identity Tag must be different for EAP-SIM (pseudonyms or re-authentication identities) and for EAP-AKA (pseudonyms or re-authentication identities), so that the AAA can determine which procedure to follow.

The last step in the generation of the ~~pseudonym~~ temporary identities 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~~ temporary identity is 23 characters, and no padding is necessary. Observe that the length of the ~~Pseudonym~~ Temporary Identity 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~~ temporary identity, for EAP-SIM or ~~a pseudonym~~ temporary identity for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

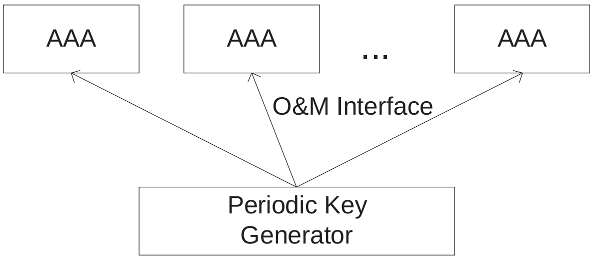
6.4.2 Key Management

A 128-bit encryption key shall be used for the generation of temporary identities~~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 temporary identities~~pseudonyms~~, but the AAA servers must keep a number of suspended (old) keys for the interpretation of received temporary identities~~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 temporary identity~~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 temporary identity ~~pseudonym~~ (see Key Indicator field in section 6.4.1), so that when a WLAN AAA receives the temporary identity~~pseudonym~~, it can use the corresponding key for obtaining the Padded IMSI (and thence the Username).

If a temporary identity~~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 temporary identity~~pseudonym~~ could eventually be removed from all the WLAN AAA servers. If the user initiates an authentication attempt after that time using that old temporary identity~~pseudonym~~, the receiving AAA server will not be able to recognise the temporary identity~~pseudonym~~ as a valid one, and it will request the permanent user identity from the WLAN client (if the process was re-authentication, the AAA server will request first a pseudonym, and if it is not recognized, the permanent user identity). Hence, 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.

*** END SET OF CHANGES ***