3GPP TSG SA WG3 Security — S3#29 **Tdoc ⌘S3-030334**
San Francisco, USA 15 - 18 July 2003

CR-Form-v7

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:	⌘	BT Group		
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: ⌘ 3GPP to WLAN interworking will result in an increased number of:

- Operators issuing UICC and USIM applications
- Operators hosting AuC applications e.g. “thick MVNO”
- Changes of ownership of networks and their subscribers
- Suppliers of both USIM applications and AuC applications when WLAN access is added to 3GPP networks

Hence WLAN and 3G operators will require the ability to move subscribers from the AUC of one vendor to that supplied by another one implementing a sequence number management scheme, with minimal disruption e.g. re-issuing UICC’s or co-ordinating software upgrades.

There will also be an increase in subscribers moving between nodes, which do not exchange authentication data and utilise unused quintets when the UE returns into the location of previously node. This interleaving authentication may cause an increase in the rate of authentication failures due to synchronisation failures. This is especially true if simultaneous access to the WLAN and 3GPP systems is permitted

These changes place a number of additional requirements on the design of sequence number management scheme. A scheme meeting these additional requirements is already defined in Annex C.3.2 of 3GPP TS33.102 V5.1.0 and shall be included in the main body of TS 33.234

Summary of change: ⌘

1. Additional requirements added to support simultaneous access to the WLAN and 3GPP systems

		2. Annex C.3.2 of 3GPP TS33.102 V5.1.0 included in the main body of TS 33.234
Consequences if not approved:	⌘	Inability to move subscribers from the AUC of one vendor to that supplied by another one implementing a sequence number management scheme, without re-issuing UICC's or co-ordinating software upgrades. Increase in the rate of authentication failures due to synchronisation failures if simultaneous access to the WLAN and 3GPP systems is permitted

Clauses affected:	⌘	4.2 Security Requirements 6.1.1 USIM-based Authentication				
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	TS 23.234
				Test specifications		
				O&M Specifications		
Other comments:	⌘	The requirement that the HSS 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				

4.2 Security Requirements

4.2.6 Requirements to support 3GPP/WLAN simultaneous access

1. To keep the failure rate to a sufficiently low level the sequence number management part of the authentication mechanism shall support interleaving authentication.

2. The sequence number must be constructed from two concatenated parts, SQN =SEQ||IND where IND is the index to an array of size a.

3. The HSS must be able to determine whether the node requesting authentication vectors is in the CS, PS, IMS and WLAN domains.

4. Authentication vectors distributed to different service domains shall have different values (i.e. separate ranges of index values IND are reserved for CS PS, IMS and WLAN operation).

5. Authentication vectors distributed within the same batch shall have the same index value IND. To prevent duplicate values of SQN_{he} being sent in different authentication vectors to the USIM, different SEQ values must be used in a batch.

6. If the new request comes from the same serving node as the previous request, then the index value IND used for the new request shall be the same as was used for the previous request. To prevent duplicate values of SQN_{he} being sent in different authentication vectors to the USIM, different SEQ values must then be used.

7. A scheme shall be selected which minimises the number of parameters that, if missconfigured will weaken the security, even if this is at the expense of some additional security functionally. User anonymity with a clock-based scheme can only be achieved with careful choice of clock and frequency of generating new batches. A counter-based scheme on the other hand will always require the additional anonymity function, giving a known level of protection independent of system configuration and end user behaviour.

8. The scheme shall be selected which minimises the number of administration steps when moving users from one AuC to another. A clock based scheme, while not requiring any real time synchronisation, does require a number additional steps, when moving users from one from AuC1 to AuC2 as compared to what would be necessary for a purely counter based scheme.

6.1.1.2 Management of sequence numbers

Generation of sequence numbers in the HE/AuC

The HE/AuC shall maintain a counter for each user, $SQN_{HE} = SEQ_{HE} \,||\, IND_{HE}$. To generate a fresh sequence number, SEQ_{HE} is incremented by 1, and the new counter value is used to generate the next authentication vector. Each time an authentication vector is generated, the AuC shall retrieve IND_{HE} from storage and allocate a new index value *IND* for that vector according to suitable rules and include it in the appropriate part of *SQN*. The index value may range from 0 to *a* -1 where *a* is the size of the array.

Handling of sequence numbers in the USIM

The USIM keeps track of an array of sequence number values it has accepted. Let $SQN_{MS} = SEQ_{MS} \,||\, IND_{MS}$ denote the highest sequence number in the array. The USIM shall maintain an array of *a* previously accepted sequence number components: SEQ_{MS} (0), SEQ_{MS} (1),… SEQ_{MS} (*a*-1). The initial sequence number value in each array element shall be zero.

To verify that the received sequence number *SQN* is fresh, the USIM shall compare the received *SQN* with the sequence number in the array element indexed using the index value *IND* contained in *SQN*, i.e. with the array entry SEQ_{MS} (i) where i = *IND* is the index value.

(a) If *SEQ* > SEQ_{MS} (i) the USIM shall consider the sequence number to be guaranteed fresh and subsequently shall set SEQ_{MS} (i) to *SEQ*.

(b) If *SEQ* ≤ SEQ_{MS} (i) the USIM shall generate a synchronisation failure message using the highest previously accepted sequence number anywhere in the array, i.e. SQN_{MS}.

The USIM shall also be able to put a limit *L* on the difference between SEQ_{MS} and a received sequence number component *SEQ*. If such a limit *L* is applied then, before verifying the above conditions (a) and (b), the sequence number shall only be accepted by the USIM if $SEQ_{MS} - SEQ < L$. If *SQN* can not be accepted then the USIM shall generate a synchronisation failure message using SQN_{MS}.

Sequence number management Profile (C.3.2 in TS33.102)

Generation of sequence numbers:

This follows the scheme for the generation of sequence numbers specified in Annex C.1.1.2 of TS 33.102. The following parameter values are suggested for reference:

Length of IND in bits = 5.

Start conditions: $SQN_{HE} = 0$ for all users.

Verification of sequence numbers in the USIM:

Length of the array: a = 32

Protection against wrap around: Choose $\Delta = 2^{28}$.
Choosing $\Delta = 2^{28}$ means that an attack to force the counter in the USIM to wrap around would require at least $SEQmax/\Delta = 2^{15} > 32.000$ successful authentications (cf. note 6 of C.2.3 of TS 33.102). Note 7 of Annex C.2.3 of TS 33.102 does not apply.

Age limit for sequence numbers:
There is no clock here. So, the “age” limit would be interpreted as the maximum allowed difference between SQN_{MS} (see section 6.3) and the sequence number received. The use of such a limit is optional. The choice of a value for the parameter L affects only the USIM. It has no impact on the choice of other parameters and it entirely up to the operator, depending on his security policy. Therefore no particular value is suggested here.

User anonymity: the value of SQN may allow to trace the user over longer periods. If this is a concern then SQN has to be concealed by an anonymity key as specified in section 6.3 of TS 33.102.