3GPP TSG SA WG3 Security — S3#23 **S3-020295**
14 - 17 May 2002, Victoria, Canada

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.102** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **3.b.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: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [X]

Title:	⌘	Clarification of sequence number management
Source:	⌘	Vodafone
Work item code:	⌘	Security
Date:	⌘	16 May 2002
Category:	⌘	**F**
Release:	⌘	R99

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)

Reason for change:	⌘	The starting conditions for clock-based schemes are slightly ambiguous since it could be interpreted that GLC=1 is the starting condition for all USIMs - even those that are added a long time after the AuC has been created. This implies that there may be multiple GLCs per AuC which is not intended. The interoperability guidelines do not properly identify the requirements on the IND length.
Summary of change:	⌘	The starting conditions for clock-based schemes are clarified such that GLC=1 is the starting condition when creating the AuC and SQN_{HE}=0 or DIF=0 is the starting condition when adding a USIM to the AuC. An IND length of 5 bits is proposed in the interoperability guidelines.
Consequences if not approved:	⌘	Misleading specifications could lead to interoperability problems.

Clauses affected:	⌘	C.3.1, C.3.3, C.4
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

C.3 Sequence number management profiles

This section provides examples how values for the parameters defined in sections C.1 and C.2 may be chosen in a coherent way. These examples may serve as references when specifying practical sequence number management schemes. There is one example set of values for each of the three types of sequence number generation schemes:

- partly time-based corresponding to Annex C.1.1.1;
- not time-based corresponding to Annex C.1.1.2;
- entirely time-based corresponding to Annex C.1.1.3.

C.3.1 Profile 1: management of sequence numbers which are partly time-based

Generation of sequence numbers:

This follows the general scheme for the generation of sequence numbers specified in Annex C.1.1.1. The following parameter values are suggested for reference:

Time unit of the clock: 1 second

Length of IND in bits = 5.

Length of SEQ2 in bits = n : 24
This means that GLC will wrap around after $p = 2^n = 2^{24}$ seconds = 194 days. This ensures that most users will have become active at least once during this period.
This implies a length of SEQ1 in bits = 19.

Start ~~condition~~value for GLC when creating the AuCs: ~~Choose SQN_{HE} = 0 for all users and~~ GLC = 1.

Start value for SQN_{HE} when adding a USIM to the AuC: SQN_{HE} = 0.

Arrival rate temporarily higher than clock rate: Choose $D = 2^{16}$.
D may be chosen quite large as long as the conditions in C.1.1.1 (4)(ii) and (iii) are satisfied. Choosing $D = 2^{16} = 65536$ means that the condition in C.1.1.1 (4)(i) is satisfied unless more than 65536 requests for batches arrive within over 18 hours which is practically impossible.

Verification of sequence numbers in the USIM:

This follows the handling of sequence numbers in the USIM specified in Annex C.2.

Length of the array: a = 32.
This satisfies the requirement in section 6.3.2 that the mechanism for the verification of sequence numbers shall ensure that a sequence number can still be accepted if it is among the last x sequence numbers generated.

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). We have $\Delta > p$, as required in note 7 of C.2.3.

Age limit for sequence numbers:
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. To give an example: if the policy stipulates that authentication vectors older than x seconds shall be rejected then L has to be set to x as the time unit of the clock is 1 second.

User anonymity: the value of SQN does not allow to trace the user over longer periods. Therefore, there may be no need to conceal SQN by an anonymity key as specified in section 6.3.

C.3.2 Profile 2: management of sequence numbers which are not time-based

Generation of sequence numbers:

This follows the scheme for the generation of sequence numbers specified in Annex C.1.1.2. 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). Note 7 of Annex C.2.3 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.

C.3.3 Profile 3: management of sequence numbers which are entirely time-based

Generation of sequence numbers:

This follows the scheme for the generation of sequence numbers specified in Annex C.1.1.3. The following parameter values are suggested for reference:

Time unit of the clock: It has to be chosen in such a way that no two requests for a batch of authentication vectors arrive during one time unit. Value = 0.1 seconds

Length of IND in bits = 5.

Start ~~condition~~value for GLC when creating the AuC~~s~~: GLC = 1.

Start value for DIF when adding a USIM to the AuC ~~and, for all users,~~: DIF = 0.

Verification of sequence numbers in the USIM:

This is done according to the handling of sequence numbers in the USIM specified in Annex C.2.

Length of the array: a = 32.
This satisfies the requirement in section 6.3.2 that the mechanism for the verification of sequence numbers shall ensure that a sequence number can still be accepted if it is among the last x sequence numbers generated.

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). Note 7 of C.2.3 does not apply.

Age limit for sequence numbers:
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. To give an example: if the policy stipulates that authentication vectors older than x time units shall be rejected then L has to be set to x.

User anonymity: the value of SQN does not allow to trace the user over longer periods. Therefore, there may be no need to conceal SQN by an anonymity key as specified in section 6.3.

C.3.4 Guidelines for the allocation of the index values in the array scheme

- **General rule**: index values *IND* used in the array scheme, according to Annex C.1.2, shall be allocated cyclically within its range 0, ... , *a-1*. This means that the index value *IND* used with the previously generated authentication vector is stored in SQN_{HE} , and the next authentication vector shall use index value *IND +1 mod a*.

It may be useful to allow exceptions to this general rule when additional information is available. This includes:

- Authentication vectors distributed within the same batch shall have the same index value.

  In future releases, the Authentication Data Request MAP message may contain information about the requesting serving node and the domain (CS or PS) from which the request originates. Note that this information may also be available from other sources, depending on the implementation of the HLR and the HLR/AuC interface. If this information is available it is recommended to use it in the following way. Support for this use is, however, not required for an implementation to claim compliance to Annex C.

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

- If the new request comes from the same serving node as the previous request, then the index value used for the new request shall be the same as was used for the previous request.

C.4 Guidelines for interoperability in a multi-vendor environment

The specification of a sequence number management scheme affects only the USIM and the AuC which are both under the control of one operator. Therefore, the specification of such a scheme is entirely at the discretion of an operator. Nevertheless, certain operators may not want to define a scheme of their own. Instead, they may want to rely on vendors implementing one of the schemes according to the profiles in C.3 or variants thereof. If these operators have multiple vendors for USIMs and/or AuCs, and the operators wish to move subscribers from the AuC of one vendor to that supplied by another one implementing a different scheme then this will work smoothly only when the following guidelines are adhered to by all the sequence number management schemes implemented in the operator's domain.

- The array mechanism specified in C.1.2 and C.2 is used in the USIM to verify SQNs. The length of the IND used by the USIM to index the array shall be not less than the length of the IND used by the AuC when allocating index values. However, we recommend that the same IND length of 5 bits is used in USIMs and AuCs. This is the same IND length as proposed for all profiles in C.3.

- Relation to Annex F: if the AMF field is used to signal further parameters relevant to sequence number management (age limit L) then the formats of the AMF and its interpretation by the USIM must be the same for all implementations in the operator's domain.

- Δ is larger than a specified minimum.
  This is necessary to accommodate schemes as in C.3.2 according to note 7 of C.2.3.
  We propose $\Delta \geq 2^{28}$.

- There are no requirements on the synchronicity of clocks in different AuCs for the time-based schemes. For the entirely time-based scheme, the following is recommended when moving users from one AuC to another one: The DIF value is updated in an appropriate manner when moving subscribers from an AuC to another AuC. More specifically, assume a user is moved from AuC1 to AuC2. If AuC1 is of profile 3 and AuC2 is of any profile then AuC1 sends GLC+DIF as SEQ_HE to AuC2. In the receiving end, if AuC2 is of profile 3 while AuC1 is of any profile then AuC2 sets DIF value for this user as DIF = SEQ_HE - GLC.