Technical Specification Group Services and System Aspects
Meeting #16, Marco Island, Florida, 10-13 June 2002

TSGS#16(02)0344

Source: **SA WG3**

Title: **CRs to 33.102: Clarification of sequence number management (Release 1999 / Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020344	33.102	173		R99	Clarification of sequence number management	F	3.11.0	Security	S3-020308
SP-020344	33.102	174		Rel-4	Clarification of sequence number management	A	4.3.0	SEC1	S3-020309

3GPP TSG SA WG3 Security — S3#23 **S3-020308**
14 - 17 May 2002, Victoria, Canada

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.102** **CR** **173** ⌘ **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:	⌘	SA WG3
Work item code:	⌘	Security
Date:	⌘	17 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 interoperability guidelines do not properly identify the requirements on the IND length.
Summary of change:	⌘	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.4
Other specs affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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.

3GPP TSG SA WG3 Security — S3#23 **S3-020309**
14 - 17 May 2002, Victoria, Canada

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.102** **CR** **174** ⌘ **rev** **-** ⌘ Current version: **4.3.0** ⌘

*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:	⌘	SA WG3
Work item code:	⌘	SEC1
Date:	⌘	17 May 2002
Category:	⌘	**A**
Release:	⌘	REL-4

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 interoperability guidelines do not properly identify the requirements on the IND length.
Summary of change:	⌘	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.4
Other specs affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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.