Technical Specification Group Services and System Aspects
Meeting #14, Kyoto, Japan, 17-20 December 2001

TSGS#14(01)0610

Source: **SA WG3**

Title: **2 CRs to 33.102: SQN_{MS} retrieval in AuC during resynchronisation (Rel-99 and Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
21.133	160		Rel-99	F	SQN_{MS} retrieval in AuC during resynchronisation.	3.9.0	3.10.0	S3-010457
21.133	161		Rel-4	A	SQN_{MS} retrieval in AuC during resynchronisation.	4.2.0	4.3.0	S3-010458

3GPP TSG SA WG3 Security — S3#20 **S3-010457**

16-19 October 2001, Sidney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.102** **CR** **160** ⌘ ev **-** ⌘ Current version: **3.9.0** ⌘

*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 ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	SQN_{MS} retrieval in AuC during resynchronisation.
Source:	⌘	SA WG3
Work item code:	⌘	SEC-1
Date:	⌘	19 September 2001
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:	⌘	During resynchronisation the function f5* shall be used at both USIM and AuC for the concealment of SQN_{MS}.
Summary of change:	⌘	Correct mistake in Clause 6.3.5, where f5 is used in stead of f5*.
Consequences if not approved:	⌘	Inconsistent specification.

Clauses affected:	⌘	6.3.5
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications ⌘
Other comments:	⌘	

6.3.5 Re-synchronisation procedure

A VLR/SGSN may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the VLR/SGSN sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- *AUTS* received by the VLR/SGSN in the response to that request, as described in subsection 6.3.3.

An VLR/SGSN will not react to unsolicited "synchronisation failure indication" messages from the MS.

The VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

1. The HE/AuC retrieves SQN_{MS} from Conc(SQN_{MS}) by computing Conc(SQN_{MS}) $\oplus$ $f5^{*}_{K}(RAND)$~~,~~.
2. The HE/AuC checks if SQN_{HE} is in the correct range, i.e. if the next sequence number generated SQN_{HE} using would be accepted by the USIM.
3. If SQN_{HE} is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).
4. The HE/AuC verifies *AUTS* (cf. subsection 6.3.3.).
5. If the verification is successful the HE/AuC resets the value of the counter SQN_{HE} to $SQN_{MS.}$
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter SQN_{HE} was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SQN_{HE}. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an authentication data request with synchronisation failure indication it deletes the old ones for that user in the VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC. Figure 12 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in section 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response* (as described in this section).

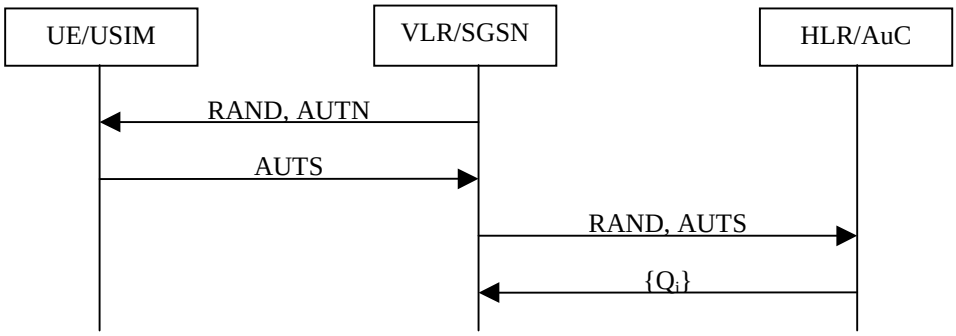

Figure 12: Resynchronisation mechanism

3GPP TSG SA WG3 Security — S3#20 **S3-010458**

16-19 October 2001, Sidney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.102** **CR** **161** ⌘ ev **-** ⌘ Current version: **4.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	SQN_{MS} retrieval in AuC during resynchronisation.
Source:	⌘	SA WG3
Work item code:	⌘	SEC-1
Date:	⌘	19 September 2001
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:	⌘	During resynchronisation the function f5* shall be used at both USIM and AuC for the concealment of $SQN_{MS.}$
Summary of change:	⌘	Correct mistake in Clause 6.3.5, where f5 is used in stead of f5*.
Consequences if not approved:	⌘	Inconsistent specification.

Clauses affected:	⌘	6.3.5
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

6.3.5 Re-synchronisation procedure

A VLR/SGSN may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the VLR/SGSN sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- *AUTS* received by the VLR/SGSN in the response to that request, as described in subsection 6.3.3.

An VLR/SGSN will not react to unsolicited "synchronisation failure indication" messages from the MS.

The VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

1. The HE/AuC retrieves SQN_{MS} from Conc(SQN_{MS}) by computing Conc(SQN_{MS}) $\oplus$ $f5^*_K(RAND)$~~,~~.
2. The HE/AuC checks if SQN_{HE} is in the correct range, i.e. if the next sequence number generated SQN_{HE} using would be accepted by the USIM.
3. If SQN_{HE} is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).
4. The HE/AuC verifies *AUTS* (cf. subsection 6.3.3.).
5. If the verification is successful the HE/AuC resets the value of the counter SQN_{HE} to $SQN_{MS.}$
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter SQN_{HE} was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SQN_{HE}. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an authentication data request with synchronisation failure indication it deletes the old ones for that user in the VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC. Figure 12 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in section 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response* (as described in this section).

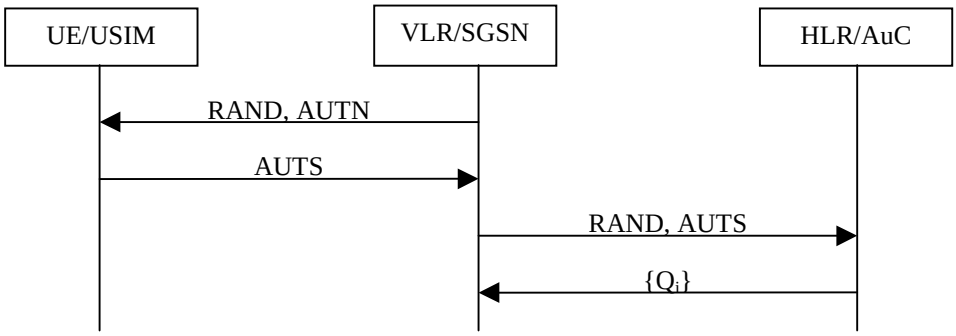

Figure 12: Resynchronisation mechanism