3GPP TSG SA WG3 Security — S3#26 **S3-020668**
19- 22 November 2002
Oxford, UK

TSG-RAN Working Group 2 Meeting #33 *R2-023258*
Sophia-Antipolis, France, 12- 15 November 2002

Title: **LS on Correction to the START formula in 33.102**
Response to:
Release: **R'99**

Source: RAN2
To: SA3
Cc:

Contact Person:
Name: Francesco Grilli
Tel. Number: +1 858 845 3742
E-mail Address: fgrilli@qualcomm.com

Attachments: Proposed_draft_CRs_to_33102

---

1. Overall Description:

RAN2 would like to point the attention of SA3 to a discrepancy between stage 2 (TS 33.102) and stage 3 (TS 25.331) security specifications.

The formula for the computation of the START values included in TS 33.102 is not consistent with the formula specified in TS 25.331. In particular, in TS 33.102 the formula includes a "+ 1" addend, while in TS 25.331 the addend in the formula is "+ 2".

"+ 2" is needed in order to avoid the reuse of the same COUNT-C. As example, when a UM radio bearer is released, the UE and UTRAN may have a different perception of the exact instant at which the UM radio bearer ceases to exist. This is due to the fact that UM PDUs are not acknowledged, and therefore it is possible that all the PDUs after the sequence number rollover are lost and not received by the UE. As a result, UTRAN would increment the HFN, while the UE would not. When that particular radio bearer is established again, the UE could select a START value that would cause the reuse of COUNT-C values, with the same radio bearer identity, the same "length", the same CK and the same "direction", i.e. all the inputs to the f8 block would be repeated. This is probably not acceptable from the security point of view. By using "+ 2" in the formula, the reuse of the same COUNT-C values is virtually eliminated, since it is almost impossible to lose two consecutive rollovers of the UM RLC sequence number.

RAN2 modified the START formula in TS 25.331 during the meeting RAN2 #27, held in Orlando, FL, USA on February 18-22, 2002. Unfortunately, at that time RAN2 forgot to inform or consult SA3 on this specific change. As a result, the March 2002 version of R'99, Rel-4 and Rel-5 TS 25.331 already includes the modified START formula ("+ 2").

RAN2 asks SA3 to modify accordingly the formula in TS 33.102 for all releases. A document including proposed draft CRs to 33.102 is attached.

RAN2 welcomes any feedback that SA3 may want to provide on this issue.

2. Actions:

To SA3 group.

ACTION: RAN2 requests SA3 to consider the changes included in the attached proposed draft CRs to TS 33.102 (R'99, Rel-4 and Rel-5) in order to align the START formulae in stage 2 (TS 33.102) and stage 3 (TS 25.331) specifications.

3. Date of Next RAN2 Meetings:

RAN2_34	17 – 21 Feb 2003	Sophia-Antipolis, France
RAN2_35	07 – 11 Apr 2003	Seoul, Korea

3GPP TSG-SA3 Meeting #nn
City, Country, Date

Tdoc ⌘S3-02nnnn

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **Draft n0** ⌘**rev** **-** ⌘ Current version: **3.11.0** ⌘

*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:	⌘	Correction to the START formula
Source:	⌘	Qualcomm
Work item code:	⌘	***Date:*** ⌘ 18 November 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)*
Rel-6	*(Release 6)*

Reason for change: ⌘ The current formula includes a "+ 1" addend, which may not guarantee against the reuse of COUNT-C for the case of unacknowledged mode radio bearers. When a UM radio bearer is released, the UE and UTRAN may have a different perception of the exact instant at which the UM radio bearer ceases to exist. This is due to the fact that UM PDUs are not acknowledged, and therefore it is possible that all the PDUs after the sequence number rollover are lost and not received by the UE. As a result, UTRAN would increment the HFN, while the UE would not. When that particular radio bearer is established again, the UE could select a START value that would cause the reuse of COUNT-C values, with the same radio bearer identity, the same "length", the same CK and the same "direction", i.e. all the inputs to the f8 block would be repeated. This is not acceptable from the security point of view.

Summary of change: ⌘ In the START formula the addend "+ 1" is changed to "+ 2".
By using "+ 2" in the formula, the reuse of the same COUNT-C values is virtually eliminated, since it is almost impossible to lose two consecutive rollovers of the UM RLC sequence number.

Isolated Impact Change Analysis.

This change clarifies the ciphering and integrity protection procedures.
If the UE does not implement this CR, there would be no interoperability problems, since UTRAN, in any case, should use the START values sent by the UE.

It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.

Consequences if not approved:	⌘	The stage 3 (TS 25.331) and stage 2 (TS 33.102) specifications would not be aligned. If the UE implements the current formula included in 33.102, the UE could expose the ciphering mechanism to some security attacks due to the reuse of the same COUNT-C values in the DL.

Clauses affected:	⌘	6.4.8			
		Y	**N**		
Other specs affected:	⌘	**X**		Other core specifications	⌘ TS 25.331 already implements this correction
				Test specifications	To be verified by SA3
			X	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.

[…]

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a $START_{CS}$ value for the CS cipher/integrity keys and a $START_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the $START_{CS}$ and the $START_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting $START_{CS}$ and $START_{PS}$ to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection) and the RLC SN (for ciphering) are initialised to 0.

During an ongoing radio connection, the $START_{CS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data radio bearers protected using CK_{CS} and/or $IK_{CS,}$ incremented by 1, i.e.:

$START_{CS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{CS} and IK_{CS}}) + ~~1~~2.

- If current $START_{CS} < START_{CS}'$ then $START_{CS} = START_{CS}'$, otherwise $START_{CS}$ is unchanged.

Likewise, during an ongoing radio connection, the $START_{PS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$START_{PS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{PS} and IK_{PS}}) + ~~1~~2.

- If current $START_{PS} < START_{PS}'$ then $START_{PS} = START_{PS}'$, otherwise $START_{PS}$ is unchanged.

If any of the COUNT-C or COUNT-I assigned to the radio bearers of the same CN domain reaches its maximum value, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates $START_{CS}$ and $START_{PS}$ in the USIM with the current values.

During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.

[…]

3GPP TSG-SA3 Meeting #nn ***Tdoc ⌘S3-02nnnn***
City, Country, Date

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **Draft n0** ⌘**rev** **-** ⌘ Current version: **4.4.0** ⌘

*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:	⌘	Correction to the START formula
Source:	⌘	Qualcomm
Work item code:	⌘	***Date:*** ⌘ 18 November 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)*
Rel-6	*(Release 6)*

Reason for change: ⌘ The current formula includes a "+ 1" addend, which may not guarantee against the reuse of COUNT-C for the case of unacknowledged mode radio bearers. When a UM radio bearer is released, the UE and UTRAN may have a different perception of the exact instant at which the UM radio bearer ceases to exist. This is due to the fact that UM PDUs are not acknowledged, and therefore it is possible that all the PDUs after the sequence number rollover are lost and not received by the UE. As a result, UTRAN would increment the HFN, while the UE would not. When that particular radio bearer is established again, the UE could select a START value that would cause the reuse of COUNT-C values, with the same radio bearer identity, the same "length", the same CK and the same "direction", i.e. all the inputs to the f8 block would be repeated. This is not acceptable from the security point of view.

Summary of change: ⌘ In the START formula the addend "+ 1" is changed to "+ 2".
By using "+ 2" in the formula, the reuse of the same COUNT-C values is virtually eliminated, since it is almost impossible to lose two consecutive rollovers of the UM RLC sequence number.

Isolated Impact Change Analysis.

This change clarifies the ciphering and integrity protection procedures.
If the UE does not implement this CR, there would be no interoperability problems, since UTRAN, in any case, should use the START values sent by the UE.

It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.

Consequences if not approved:	⌘	The stage 3 (TS 25.331) and stage 2 (TS 33.102) specifications would not be aligned. If the UE implements the current formula included in 33.102, the UE could expose the ciphering mechanism to some security attacks due to the reuse of the same COUNT-C values in the DL.

Clauses affected:	⌘	6.4.8			
		Y	**N**		
Other specs	⌘	**X**		Other core specifications	⌘ TS 25.331 already implements this correction
affected:				Test specifications	To be verified by SA3
			X	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.

[…]

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a $START_{CS}$ value for the CS cipher/integrity keys and a $START_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the $START_{CS}$ and the $START_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting $START_{CS}$ and $START_{PS}$ to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection) and the RLC SN (for ciphering) are initialised to 0.

During an ongoing radio connection, the $START_{CS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data radio bearers protected using CK_{CS} and/or $IK_{CS,}$ incremented by 1, i.e.:

$START_{CS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{CS} and IK_{CS}}) + 1.

- If current $START_{CS} < START_{CS}'$ then $START_{CS} = START_{CS}'$, otherwise $START_{CS}$ is unchanged.

Likewise, during an ongoing radio connection, the $START_{PS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$START_{PS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{PS} and IK_{PS}}) + ~~1~~2.

- If current $START_{PS} < START_{PS}'$ then $START_{PS} = START_{PS}'$, otherwise $START_{PS}$ is unchanged.

If any of the COUNT-C or COUNT-I assigned to the radio bearers of the same CN domain reaches its maximum value, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates $START_{CS}$ and $START_{PS}$ in the USIM with the current values.

During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.

[…]

3GPP TSG-SA3 Meeting #nn ***Tdoc ⌘S3-02nnnn***
City, Country, Date

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **Draft n0** ⌘**rev** **-** ⌘ Current version: **5.0.0** ⌘

*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:	⌘	Correction to the START formula
Source:	⌘	Qualcomm
Work item code:	⌘	***Date:*** ⌘ 18 November 2002
Category:	⌘ **A**	***Release:*** ⌘ Rel-5

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: ⌘ The current formula includes a "+ 1" addend, which may not guarantee against the reuse of COUNT-C for the case of unacknowledged mode radio bearers. When a UM radio bearer is released, the UE and UTRAN may have a different perception of the exact instant at which the UM radio bearer ceases to exist. This is due to the fact that UM PDUs are not acknowledged, and therefore it is possible that all the PDUs after the sequence number rollover are lost and not received by the UE. As a result, UTRAN would increment the HFN, while the UE would not. When that particular radio bearer is established again, the UE could select a START value that would cause the reuse of COUNT-C values, with the same radio bearer identity, the same "length", the same CK and the same "direction", i.e. all the inputs to the f8 block would be repeated. This is not acceptable from the security point of view.

Summary of change: ⌘ In the START formula the addend "+ 1" is changed to "+ 2".
By using "+ 2" in the formula, the reuse of the same COUNT-C values is virtually eliminated, since it is almost impossible to lose two consecutive rollovers of the UM RLC sequence number.

Isolated Impact Change Analysis.

This change clarifies the ciphering and integrity protection procedures.
If the UE does not implement this CR, there would be no interoperability problems, since UTRAN, in any case, should use the START values sent by the UE.

It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.

Consequences if not approved:	⌘	The stage 3 (TS 25.331) and stage 2 (TS 33.102) specifications would not be aligned. If the UE implements the current formula included in 33.102, the UE could expose the ciphering mechanism to some security attacks due to the reuse of the same COUNT-C values in the DL.

Clauses affected:	⌘	6.4.8			
		Y	**N**		
Other specs	⌘	**X**		Other core specifications	⌘ TS 25.331 already implements this correction
affected:				Test specifications	To be verified by SA3
			X	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.

[…]

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a $START_{CS}$ value for the CS cipher/integrity keys and a $START_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the $START_{CS}$ and the $START_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting $START_{CS}$ and $START_{PS}$ to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection) and the RLC SN (for ciphering) are initialised to 0.

During an ongoing radio connection, the $START_{CS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data radio bearers protected using CK_{CS} and/or $IK_{CS,}$ incremented by 1, i.e.:

$START_{CS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{CS} and IK_{CS}}) + 1.

- If current $START_{CS} < START_{CS}'$ then $START_{CS} = START_{CS}'$, otherwise $START_{CS}$ is unchanged.

Likewise, during an ongoing radio connection, the $START_{PS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$START_{PS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{PS} and IK_{PS}}) + ~~1~~2.

- If current $START_{PS} < START_{PS}'$ then $START_{PS} = START_{PS}'$, otherwise $START_{PS}$ is unchanged.

If any of the COUNT-C or COUNT-I assigned to the radio bearers of the same CN domain reaches its maximum value, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates $START_{CS}$ and $START_{PS}$ in the USIM with the current values.

During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.

[…]