Technical Specification Group Services and System Aspects
Meeting #18, New Orleans, USA, 9-12 December 2002

TSGS#18(02)0790

Source: **SA WG3**

Title: **3 CRs to 33.102 (R99, Rel-4 and Rel-5): Correction to the START formula**

Document for: **Approval**

Agenda Item: **7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020701	33.102	176		R99	Correction to the START formula	F	3.12.0	Security	S3-020689
SP-020701	33.102	177		Rel-4	Correction to the START formula	A	4.4.0	SEC1	S3-020690
SP-020701	33.102	178		Rel-5	Correction to the START formula	A	5.0.0	SEC1	S3-020691

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **176** ⌘**rev** **-** ⌘ Current version: **3.12.0** ⌘

*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:	⌘	SA WG3
Work item code:	⌘	Security
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 ⌘ The stage 3 (TS 25.331) and stage 2 (TS 33.102) specifications would not be

not approved:	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:			**X**	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

[…]

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~~2, 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~~2, 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.

[…]

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **177** ⌘**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:	⌘	SA WG3
Work item code:	⌘	SEC1
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 ⌘ The stage 3 (TS 25.331) and stage 2 (TS 33.102) specifications would not be

not approved:	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:			**X**	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

[…]

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~~2, 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~~2, 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.

[…]

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **178** ⌘**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:	⌘	SA WG3
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 ⌘ The stage 3 (TS 25.331) and stage 2 (TS 33.102) specifications would not be

not approved:	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:			**X**	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

[…]

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~~2, 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~~2, 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.

[…]