3GPP TSG-SA WG3 Meeting #18
Phoenix, USA, 21st – 24th May 2001

S3-010195
(Part ½: R99 CR)

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **3.8.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Calculation and Wrap-around of START value
Source:	⌘	Ericsson
Work item code:	⌘	R99 Security Architecture
Date:	⌘	21-May-01
Category:	⌘	**D**
Release:	⌘	R99

Use one of the following categories:
F *(essential 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:	⌘	Clarifications on the handling of wrap-around of START values and in its calculation.
Summary of change:	⌘	According to 25.331 (chapter 8.5.9), during the calculation of the START value for a CN domain 'x' (being STARTx' the new calculated value of START) … *"if the current STARTx < STARTx´, then STARTx = STARTx´, otherwise STARTx is unchanged".* This is done in order to keep START values always increasing. This note is now added in 33.102. If the calculated value of START wraps around, START value shall be kept at its maximum value.
Consequences if not approved:	⌘	R2 and S3 specs will not be aligned. Additionally wrap-around conditions in START values will not be considered.

Clauses affected:	⌘	6.4.8		
Other specs affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	25.331
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, 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.

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

If the calculated value of START wraps around, START value shall be kept at 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-SA WG3 Meeting #18
Phoenix, USA, 21st – 24th May 2001

S3-010195
(Part 2/2: Rel-4 CR)

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Calculation and Wrap-around of START value
Source:	⌘	Ericsson
Work item code:	⌘	Security Architecture
Date:	⌘	21-May-01
Category:	⌘	**D**
Release:	⌘	R4

Use one of the following categories:
F *(essential 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:	⌘	Clarifications on the handling of wrap-around of START values and in its calculation.
Summary of change:	⌘	According to 25.331 (chapter 8.5.9), during the calculation of the START value for a CN domain 'x' (being STARTx' the new calculated value of START) … *"if the current STARTx < STARTx´, then STARTx = STARTx´, otherwise STARTx is unchanged".* This is done in order to keep START values always increasing. This note is now added in 33.102. If the calculated value of START wraps around, START value shall be kept at its maximum value.
Consequences if not approved:	⌘	R2 and S3 specs will not be aligned. Additionally wrap-around conditions in START values will not be considered.

Clauses affected:	⌘	6.4.8		
Other specs affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	25.331
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, 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.

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

If the calculated value of START wraps around, START value shall be kept at 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.