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

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	А	4.4.0	SEC1	S3-020690
SP-020701	33.102	178		Rel-5	Correction to the START formula	А	5.0.0	SEC1	S3-020691

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

19- 22 November 2002, Oxford, UK CR-Form-v7									
CHANGE REQUEST									
¥	33.102 CR 176 # rev - # Current version: 3.12.0 #								
For <mark>HELP</mark> on us	ing this form, see bottom of this page or look at the pop-up text over the of symbols.								
Proposed change a	ffects: UICC apps# ME X Radio Access Network X Core Network								
Title: ೫	Correction to the START formula								
Source: ೫	SA WG3								
Work item code: %	Security Date: # 18 November 2002								
	F Release: % R99 Use one of the following categories: Use one of the following releases: 2 (GSM Phase 2) A (corresponds to a correction in an earlier release) R96 (Release 1996) B (addition of feature), R97 (Release 1997) C (functional modification of feature) R98 (Release 1998) D (editorial modification) R99 (Release 1999) Detailed explanations of the above categories can Rel-4 (Release 4) be found in 3GPP TR 21.900. Rel-6 (Release 6)								
Reason for change. Summary of change	 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. acceptable from the security point of view. 								
	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	Image: State Stat								
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 poweredoff 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 <u>42</u>, i.e.:

- $\begin{array}{l} START_{CS}' = MSB_{20} \ (\ MAX \ \{ COUNT-C, \ COUNT-I \ | \ all \ radio \ bearers \ (including \ signalling) \ protected \ with \ CK_{CS} \ and \ IK_{CS} \ \}) + \frac{12}{2}. \end{array}$
- 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 <u>42</u>, i.e.:

- $$\label{eq:start_PS} \begin{split} \text{START}_{\text{PS}} &= \text{MSB}_{20} \ (\ \text{MAX} \ \{ \text{COUNT-C}, \ \text{COUNT-I} \ | \ \text{all radio bearers} \ (\text{including signalling}) \ \text{protected with} \ \text{CK}_{\text{PS}} \ \text{and} \ \text{IK}_{\text{PS}} \}) + \frac{12}{2}. \end{split}$$
- 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 SA WG3 Security — S3#26 19- 22 November 2002, Oxford, UK

19- 22 November 2	002, 07	loru	, UK									CR-Form-v7
CHANGE REQUEST												
^ж 3	<mark>3.102</mark>	CR	177	ж г	ev	-	ж	Curre	nt vers	sion:	4.4.0	Ħ
For <u>HELP</u> on using	g this forr	n, see	bottom	of this pag	ge or	look	at th	е рор-и	ıp text	over	⁻ the	mbols.
Proposed change affe	ects: U	ICC a	ррѕж	N	/IE X	Rac	lio A	ccess I	Vetwoi	rk <mark>X</mark>	Core Ne	etwork
Title: # C	orrection	to the	START	formula								
Source: # S	A WG3											
Work item code: ೫ <mark>S</mark>	EC1							Da	ate: ೫	18	Novembe	r 2002
De	Fe <u>one</u> of the F (correct A (correct B (addi C (func D (edited	ection) espond tion of tional r prial mo	ls to a cor feature), modification odification ns of the a	rrection in a on of featu) above cate	re)		elease	Use 2 R R R R R R R R		the fo (GSN (Rele (Rele (Rele (Rele (Rele	II-4 M Phase 2) pease 1996) pease 1997) pease 1998) pease 1999) pease 4) pease 5) pease 6)	
Reason for change: 3	the re When perce is due possil receiv would select same "direct	use of a UN ption of to the ole that red by I not. \ t a ST. radio tion",	f COUNT I radio be of the exit e fact that at all the the UE. When that ART valu bearer in i.e. all the	C-C for the earer is re act instan it UM PDU PDUs afte As a resu at particula ue that wo dentity, th	e case elease at at w Us are er the ult, UT ar rac ould ca e sam o the	e of u ed, the hich e not sequ RAN lio be ause ne "le f8 blo	inack e UE the U ackr uenc l wou arer the mgth ock w	and U JM rad nowledge e numb uld incr is esta reuse c ", the s	dged n TRAN io bea ged, an per roll ement blishe of COL ame C	node may rer ce nd th over the I d aga JNT-0 CK ar	uarantee a radio bea have a di eases to e erefore it are lost a HFN, while ain, the UE C values, of the san This is no	rers. fferent xist. This is nd not e the UE E could with the ne
Summary of change:	By us elimin UM R	ing "+ ated, LC se	2" in the since it is quence i	s almost i number.	the re mpos	euse sible	of th	e same	e COU	NT-C	C values is ve rollovers	
	This of If the	hange UE do	e clarifies bes not in		ering this C	and i CR, th	nere	would	be no i	intero	cedures. operability values ser	
											he CR, it y therwise.	would
Consequences if	<mark>⊮ The s</mark>	tage 3	<mark>8 (TS 25.</mark>	331) and	stage	2 (T	<mark>S 33</mark>	8 <mark>.102)</mark> s	pecific	catior	ns would r	ot 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	 Content core specifications Test specifications 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 poweredoff 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 <u>42</u>, i.e.:

- $\begin{array}{l} START_{CS}' = MSB_{20} \ (\ MAX \ \{ COUNT-C, \ COUNT-I \ | \ all \ radio \ bearers \ (including \ signalling) \ protected \ with \ CK_{CS} \ and \ IK_{CS} \ \}) + \frac{12}{2}. \end{array}$
- 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 <u>42</u>, i.e.:

- $$\label{eq:start_PS} \begin{split} \text{START}_{\text{PS}} &= \text{MSB}_{20} \ (\ \text{MAX} \ \{ \text{COUNT-C}, \ \text{COUNT-I} \ | \ \text{all radio bearers} \ (\text{including signalling}) \ \text{protected with} \ \text{CK}_{\text{PS}} \ \text{and} \ \text{IK}_{\text{PS}} \}) + \frac{12}{2}. \end{split}$$
- 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 SA WG3 Security — S3#26 19- 22 November 2002, Oxford, UK

19-22 November	2002, U		, UN								CR-Form-v7
		(CHANG	SE REQ	UE	ST	•				
ж а	3 <mark>3.102</mark>	CR	178	жrev	-	ж	Curre	nt vers	sion:	5.0.0	ж
For <mark>HELP</mark> on usi	-							-			
Proposed change af	fects: L	JICC a	pps#	ME <mark>X</mark>	Rad	A oit	ccess I	Vetwor	rk X	Core No	etwork
Title: ೫	Correctior	to the	START fo	rmula							
Source: ೫	SA WG3										
Work item code: 🕱 📒							Da	ate: ೫	18	Novembe	r 2002
D	lse <u>one</u> of t F (corr A (corr B (add C (fund D (edit	ection) respond ition of ctional crial m lanatio	ds to a correc feature), modification odification) ns of the abo	ction in an ea		elease	Use 2 e) R R R R R R		the fo (GSN (Rele (Rele (Rele (Rele (Rele (Rele	-5 Ilowing rel 1 Phase 2) ase 1996) ase 1998) ase 1999) ase 4) ase 5) ase 6)	
Reason for change:	the re When perce is du possi recei would selec same "direc	euse o a a UN eption e to th ble tha ved by d not. ' t a ST e radio ction",	f COUNT-C I radio bear of the exact e fact that U at all the PE of the UE. As When that p ART value bearer ider i.e. all the in	cludes a "+ c for the case rer is release t instant at w JM PDUs ar DUs after the s a result, U particular rac that would c ntity, the san nputs to the ecurity point	e of u ed, th hich e not sequ TRAN dio be ause ne "le f8 blo	inack e UE the U ackr uenc I wou earer the u ength ock w	Anowled and U JM rad nowledge e numb is esta reuse o ", the s	dged n TRAN jo beau ged, au per roll ement blishe of COU ame C	node may rer ce nd the over a the H d aga JNT-C CK an	radio bea have a d ases to e erefore it are lost a IFN, while in, the UI values, d the san	rers. fferent xist. This is nd not e the UE E could with the ne
Summary of change.	By us elimin UM F	sing "+ nated, RLC se	2" in the fo since it is a equence nu	the addend prmula, the r Ilmost impos mber. Ige Analysis	euse sible	of th	e same	e COU	NT-C		
	If the	UE do	bes not imp	ne ciphering lement this (N, in any ca	CR, tl	nere	would	be no i	intero	perability	
				ementations supporting							would
Consequences if	<mark>ដ The ទ</mark>	stage 3	3 (TS 25.33	1) and stage	2 (T	<mark>S 33</mark>	8 <mark>.102)</mark> s	pecific	cation	<mark>s would r</mark>	ot 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	 Content core specifications Test specifications 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 poweredoff 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 <u>42</u>, i.e.:

- $\begin{array}{l} START_{CS}' = MSB_{20} \ (\ MAX \ \{ COUNT-C, \ COUNT-I \ | \ all \ radio \ bearers \ (including \ signalling) \ protected \ with \ CK_{CS} \ and \ IK_{CS} \ \}) + \frac{12}{2}. \end{array}$
- 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 <u>42</u>, i.e.:

- $$\label{eq:start_PS} \begin{split} \text{START}_{\text{PS}} &= \text{MSB}_{20} \ (\ \text{MAX} \ \{ \text{COUNT-C}, \ \text{COUNT-I} \ | \ \text{all radio bearers} \ (\text{including signalling}) \ \text{protected with} \ \text{CK}_{\text{PS}} \ \text{and} \ \text{IK}_{\text{PS}} \}) + \frac{12}{2}. \end{split}$$
- 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.

[...]