Technical Specification Group Services and System Aspects **TSGS#12(01)0319** Meeting #12, Stockholm, Sweden, 18-21 June 2001

Source: SA WG3

Title: 2 CRs to 33.102: THRESHOLD Check at RRC connection

establishment (R99, Rel-4)

Document for: Approval

Agenda Item: 7.3.3

Spec	CR	Rev	Phase	Cat	Subject	Version-	Version	Doc-2nd-
						Current	-New	Level
33.102	153		R99	F	THRESHOLD Check at RRC connection establishment	3.8.0	3.9.0	S3-010272
33.102	154		Rel-4	Α	THRESHOLD Check at RRC connection establishment	4.0.0	4.1.0	S3-010271

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

		CHANG	E REQ	UEST			CR-Form-v3
X	33.102 C	R 153	₩ rev	- #	Current versi	3.8.0	¥
For <u>HELP</u> on us	ing this form, s	see bottom of th	nis page or	look at th	e pop-up text	over the 🕱 syn	nbols.
Proposed change a	ffects: # (U)SIM <mark>X</mark> M	IE/UE X	Radio Ad	cess Network	Core Ne	twork
Title: ₩	THRESHOLD	Check at RRC	connection	n establis	hment.		
Source: #	SA WG3						
Work item code: ₩	SEC1				Date: ♯	23-May-01	
Category: 第	F				Release: #	R99	
	F (essentia A (corresp B (Addition C (Functio D (Editoria	following categorial correction) onds to a correct of feature), nal modification of I modification) ations of the abov P TR 21.900.	tion in an ear		2 R96 R97 R98 R99 REL-4	the following rele (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5)	ases:
Reason for change	establish	message" mig ment so it migh THRESHOLD	nt contain a	valid KSI			
Summary of chang	光 Main cha - -		nges, value is che l keys of co	rrepondin	g CN domain	on release (ST are set to inva	
Consequences if not approved:		HRESHOLD is al RRC connect		its purpo	se and old ke	ys are used in	an
Clauses affected:	₩ 6.4.3						
Other specs affected:	Test s	core specificati pecifications Specifications	ions 光				
Other comments:							

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement, which generates cipher/integrity keys, is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established that values are read from the USIM.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are compared with the maximum value, THRESHOLD. If $START_{CS}$ and/or $START_{PS}$ have reached the maximum value (THRESHOLD), the ME marks the START value in the USIM for the corresponding core network domain(s) as invalid by setting the $START_{CS}$ and/or $START_{PS}$ to THRESHOLD, deletes the cipher key and the integrity key stored on the USIM and sets the KSI to invalid (refer to subclause 6.4.4). Otherwise, the $START_{CS}$ and $START_{PS}$ are stored in the USIM. The maximum value THRESHOLD is set by the operator and stored in the USIM.

When the next RRC connection is established, that START values are read from the USIM. Then, the ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if START_{CS} and/or START_{PS} has reached a the maximum value THRESHOLD, for the corresponding core network domain(s) set by the operator and stored in the USIM at the next RRC connection request message sent out. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

CHANGE REQUEST						
*	33.102 CR 154					
For <u>HELP</u> on us	sing this form, see bottom of this page or look at the pop-up text over the 🛱 symbols.					
Proposed change a	affects: (U)SIM X ME/UE X Radio Access Network Core Network					
Title: #	THRESHOLD Check at RRC connection establishment.					
Source: #	SA WG3					
Work item code: ₩	SEC1 Date: # 23-May-01					
Category: Ж	Release: # REL-4					
	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	e: # Initial "L3 message" might be prepared before request of RRC connection					
	establishment so it might contain a valid KSI even when the START values have reached THRESHOLD (R2-010981).					
Summary of chang	 Main changes includes: Edictorial changes, THRESHOLD value is checked at RRC connection release (START value, KSI and keys of correponding CN domain are set to invalid and deleted if THRESHOLD is reached). 					
Consequences if not approved:	# Use of THRESHOLD is not serving its purpose and old keys are used in an additional RRC connection.					
Clauses affected:	% 6.4.3					
Other specs affected:	# Other core specifications # Test specifications O&M Specifications					
Other comments:	x					

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement, which generates cipher/integrity keys, is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established that values are read from the USIM.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are compared with the maximum value, THRESHOLD. If $START_{CS}$ and/or $START_{PS}$ have reached the maximum value (THRESHOLD), the ME marks the START value in the USIM for the corresponding core network domain(s) as invalid by setting the $START_{CS}$ and/or $START_{PS}$ to THRESHOLD, deletes the cipher key and the integrity key stored on the USIM and sets the KSI to invalid (refer to subclause 6.4.4). Otherwise, the $START_{CS}$ and $START_{PS}$ are stored in the USIM. The maximum value THRESHOLD is set by the operator and stored in the USIM.

When the next RRC connection is established, that START values are read from the USIM. Then, the ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if START_{CS} and/or START_{PS} has reached a the maximum value THRESHOLD, for the corresponding core network domain(s) set by the operator and stored in the USIM at the next RRC connection request message sent out. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.