Source: TSG CN WG 1

Title: CR to R99 (with mirror CRs) on Work Item Security towards 24.008

Agenda item: 7.2

Document for: APPROVAL

Introduction:

This document contains **3** CRs, **R99 with mirror CRs to** Work Item "**Security**", that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #18 for approval.

Spec	CR#	Re	CA	Rel	Tdoc Title	Meeting	TDoc #	C_Version
24.008	705	2	F	R99	Cell barring after Network authentication rejection from the UE	N1-26	N1-022150	3.13.0
24.008	706	1	Α	Rel-4	Cell barring after Network authentication rejection from the UE	N1-26	N1-022074	4.8.0
24.008	707	1	Α	Rel-5	Cell barring after Network authentication rejection from the UE	N1-26	N1-022075	5.5.0

3GPP TSG-CN1 Meeting #26 Miami Beach, Florida, USA, 23 – 27 September 2002

roy of Tdoc N1-022073)

Miami Beach, Flo	orida, USA,	23 – 27 Sep	tember 2	2002	(rev of Tdoc N1-022073		
CHANGE REQUEST							
ж	24.008 CF	705	≋ rev	2 #	Current version: 3.13.0 #		
For <u>HELP</u> on us	sing this form, s	ee bottom of thi	is page or l	look at the	e pop-up text over the % symbols.		
Proposed change affects: UICC apps# ME X Radio Access Network Core Network							
Title: #	Cell barring a	fter Network aut	hentication	rejection	n from the UE		
Source: #	ETSI- NEC To	<mark>echnologies (U</mark>	K) LTD				
Work item code: ₩	security				Date: 第 26/09/2002		
Category: 第	F (correction A (corresponding B (addition C (function D (editorial	onds to a correction of feature), all modification of modification) attions of the above	on in an earl feature)		Release: # R99 Use one of the following releases: 2 (GSM Phase 2) e) 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	connection when they This proces 24.008 nov then it shou MS shall tr which lead	and bar the curre determine that the dure can be found wwords "If the M ald abort the RR c eat the cell where	nt cell or ce e network had in chapter and S deems that connection a e the first fail	Ils. The properties failed at 8.1.4a and at the netword the PS led AUTHATION FA	se of this procedure is to release the RRC rocedure is requested by upper layers in authentication check". It is an Access Stratum procedure. Work has failed the authentication check, is signalling connection. Additionally, the HENTICATION REQUEST message AILURE was received as barred."		
Summary of chang	RAN meets 2G cell bar	ing, 24.008 should	d give the re e taken into	eference to account, s	, and has just been created during last of this 25.331 RAN defined procedure. Since network authentication is a R99 stratum.		
Consequences if not approved:		ld still be contrade			08 and 25.331 UE decribed behaviours eck.		
Clauses affected:	 4.3.2.6.1	, 4.7.7.6.1					
Other specs affected:		ner core specific st specifications		*			

	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.

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.3.2.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3214 or T3216 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it shall request RR or RRC to release the RR connection and the PS signalling connection, if any, and bar the active cell or cells (see 3GPP TS 25.331 and 3GPP TS 04.18), should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected..

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.7.7.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3318 or T3320 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it shall request RR or RRC to release the RR connection and the PS signalling connection, if any, and bar the active cell or cells (see 3GPP TS 25.331 and 3GPP TS 04.18), should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

3GPP TSG-CN1 Meeting #25

Miami Beach, Fl	orida	a, US	A, 23 –	· 27 Sep	tember	2002	2		(rev c	of Tdoc N	1-022049)
CHANGE REQUEST							CR-Form-v7				
ж	24.	800	CR <mark>70</mark>	6	∺ rev	1	æ	Current vers	sion:	4.8.0	ж
For <u>HELP</u> on u	sing ti	nis for	m, see bot	ttom of thi	s page o	r look a	at the	e pop-up text	t over	the # syl	mbols.
Proposed change affects: UICC apps# ME X Radio Access Network Core Network											
Title:	Cell	barrin	g after Ne	twork aut	hentication	n reje	ction	from the UE			
Source: #	ETS	I- NE	C Techno	logies (U	K) LTD						
Work item code: ₩	seci	urity						Date: ₩	26/	08/2002	
Category: ₩	Use of I	(corr (corr (add (fund (edit ed exp	he following ection) responds to lition of feat ctional modifi orial modifi lanations o BGPP TR 2	a correction a correction if ication of cation)	on in an ea feature)		elease	Release: # Use <u>one</u> of 2 e) R96 R97 R98 R99 Rel-4 Rel-5 Rel-6	the for (GSN) (Rele (Rele (Rele (Rele (Rele		
Reason for change		connect when the This profession of the 24.008 then it MS shawhich	tion and bathey determined the control of the contr	or the curre ine that the in be found is "If the M rt the RR c cell where ding of AU	nt cell or de network in chapte. S deems the connection of the first f	cells. Thas fail r 8.1.4a hat the and the ailed ACATIO	the proled are and network PS AUTH	ocedure is required and authentication is an Access to ork has failed signalling content (ENTICATIO) allure was a signallure	uested on checon Strature the au inection N REC	I by upper ck". In proceduration. Addition QUEST me	layers re. on check, onally, the essage
Summary of chang		RAN n 2G cell	neeting, 24.	.008 should 11 has to be	d give the e taken int	referen o accou	ice to unt, si	this 25.331 R	AN de	efined prod	cedure.
Consequences if not approved:			would still he network					8 and 25.331 lek.	UE de	cribed beh	aviours
Clauses affected:	ж	4.3.2	.6.1, 4.7.7	.6.1							
Other specs affected:	ж	Y N X X	Other cor			*					

	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.

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.3.2.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3214 or T3216 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it shall request RR or RRC to release the RR connection and the PS signalling connection, if any, and bar the active cell or cells (see 3GPP TS 25.331 and 3GPP TS 44.018), should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.7.7.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3318 or T3320 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it shall request RR or RRC to release the RR connection and the PS signalling connection, if any, and bar the active cell or cells (see 3GPP TS 25.331 and 3GPP TS 44.018), should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

3GPP TSG-CN1 Meeting #25 Helsinki, Finland, 29 July – 2 August

(rev of Tdoc N1-022050)

reisiliki, Fililalia, 29 July – 2 August (rev or 1000 NT-022050)							
CR-Form-v7 CHANGE REQUEST							
*	24.008 CR 707	5.5.0 *					
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 X Radio Access Network Core Network							
Title: 第	Cell barring after Network authentication rejection from the UE						
Source: #	ETSI- NEC Technologies (UK) LTD						
Work item code: ₩	security Date: 26	/08/2002					
Category: ₩	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) P (editorial modification) Release P (Release) Release Rel	oll-5 ollowing releases: M Phase 2) ease 1996) ease 1997) ease 1998) ease 1999) ease 4) ease 5)					
	 25.331 newly defines this procedure: "The purpose of this procedure connection and bar the current cell or cells. The procedure is requeste when they determine that the network has failed an authentication che This procedure can be found in chapter 8.1.4a and is an Access Stratu 24.008 now words "If the MS deems that the network has failed the a then it should abort the RR connection and the PS signalling connecti MS shall treat the cell where the first failed AUTHENTICATION RE which lead to sending of AUTHENTICATION FAILURE was received A contradiction can be seen between the two descriptions. As far as this procedure is Access Stratum related, and has just been connected to the second the second treatment of the procedure is Access Stratum related, and has just been connected to the second treatment of the procedure is Access Stratum related, and has just been connected to the procedure is Access Stratum related, and has just been connected to the procedure is Access Stratum related, and has just been connected to the procedure is Access Stratum related. 	d by upper layers eck". m procedure. uthentication check, on. Additionally, the EQUEST message red as barred."					
	RAN meeting, 24.008 should give the reference to this 25.331 RAN of 2G cell barring still has to be taken into account, since network authorissue, and can also take place within a 2G access stratum.	ntication is a R99					
Consequences if not approved:	# There would still be contradictions between 24.008 and 25.331 UE de when the network has failed an authentication check.	ecribed behaviours					
Clauses affected:	34.3.2.6.1, 4.7.7.6.1						
Other specs affected:	Y N X Other core specifications Test specifications						

	X O&M Specifications	
Other comments:	X	

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.

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

If the MS deems that the network has failed the authentication check, then it shall request RR or RRC to release the RR connection and the PS signalling connection, if any, and bar the active cell or cells (see 3GPP TS 25.331 and 3GPP TS 44.018). abort the RR connection and the PS signalling connection and treat the cell where the first failed AUTHENTICATION REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

******* NEXT MODIFIED SECTION ***********

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

If the MS deems that the network has failed the authentication check, then it shall request RR or RRC to release the RR connection and the PS signalling connection, if any, and bar the active cell or cells (see 3GPP TS 25.331 and 3GPP TS 44.018), abort the RR connection and the PS signalling connection and treat the cell where the first failed AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.