3GPP TSG CN Plenary Meeting #11, Palm Springs, U.S.A 14th - 16th March 2001

Source: TSG CN WG4

Title: CRs to R99 on Work Item Security

Agenda item: 7.3

Document for: APPROVAL

Introduction:

This document contains 8 CRs on R99 Work Item "Security", that have been agreed by TSG CN WG4, and are forwarded to TSG CN Plenary meeting #11 for approval.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
29.002	225	2	N4-010429	R99	Addition of selected UMTS algorithm indication to	F	3.7.2
					the handover procedures		
29.002	239	2	N4-010430	Rel-4	Addition of selected UMTS algorithm indication to the handover procedures	Α	4.2.1
29.002	226	2	N4-010434	R99	Addition of allowed GSM algorithms indication to the handover procedures	F	3.7.2
29.002	241	2	N4-010431	Rel-4	Addition of allowed GSM algorithms indication to the handover procedures	Α	4.2.1
29.002	242	1	N4-010432	R99	Addition of allowed UMTS algorithm indication to the handover procedures	F	3.7.2
29.002	244	1	N4-010433	Rel-4	Addition of allowed UMTS algorithm indication to the handover procedures	Α	4.2.1
29.002	243	1	N4-010435	R99	Addition of selected GSM algorithm indication to the handover procedures	F	3.7.2
29.002	245	1	N4-010436	Rel-4	Addition of selected GSM algorithm indication to the handover procedures	Α	4.2.1

Other comments: #

Tdoc N4-010429

Copina Anapon	<u>o,</u>	*/ !! 10	· —							CR-Form-v3
			СН	ANGE	REQ	UE	ST			CR-FOIIII-V3
×	29	.002	CR	225 ³	3 rev	2	Ж	Current vers	3.7.	2 **
For HELP on using this form, see bottom of this page or look at the pop-up text over the % symbols.										
Proposed change	affec	ts: ¥	(U)SIM	ME/L	ΙΕ	Rad	io Ac	cess Networ	k Core	Network X
Title:	Ad	dition o	of selected	UMTS algoi	ithm in	dication	on to	the handove	r procedures	3
Source: #	CN	14								
Work item code: ₩	Se	curity						Date: ∺	27.2.2001	
Category:	F	(Agre	ed by cons	ensus)				Release: ♯	R99	
Reason for chang	Deta be fo	F (ess A (cor B (Add C (Fur D (Edi illed exp bund in	ential correct responds to dition of feat nctional modifications of 3GPP TR 2	a correction ure), lification of fecation) f the above c 1.900.	ature) ategorie	es can		2	the following (GSM Phase (Release 199 (Release 199 (Release 199 (Release 4) (Release 5)	2) 96) 97) 98) 99)
		Curre UMTS be inc	ntly the MS S-UMTS int licated also Setting pro	er MSC SRI in case of 0	es the s NC relo	cation MTS	n. Ho inter	MTS algorithing wever, the seem MSC handower intersystem	elected algor ver, BSSMAF	ithm shall Ciphering
Summary of chang	ge: Ж									
Consequences if not approved:	*		-A does no chosen.	t know wha	UMTS	S integ	grity a	and encryptio	n algorithms	MSC-B
Clauses affected:	*	7.6.6	5, 8.4, 17.7							
Other specs affected:	¥	Te	ther core specificates the specificates the specificates and specificates the specificates are specificates and specificates are specificates and specificates are specificates are specificates and specificates are specificates and specificates are specificated		Я	8				

7.6.6.12 Selected UMTS Algorithms

This parameters identifies the UMTS integrity and optionally encryption algorithms selected by MSC-B. Coding of this parameter is defined in 3G TS 25.413.

**** NEXT MODIFIED SECTION ****

8.4 Handover services

It should be noted that the handover services used on the B-interface have not been updated for Release 99. The B-interface is not fully operational specified. It is strongly recommended not to implement the B-interface as an external interface.

8.4.1 MAP_PREPARE_HANDOVER service

8.4.1.1 Definition

This service is used between MSC-A and MSC-B (E-interface) when a call is to be handed over or relocated from MSC-A to MSC-B.

The MAP_PREPARE_HANDOVER service is a confirmed service using the primitives from table 8.4/1.

8.4.1.2 Service primitives

Table 8.4/1: MAP_PREPARE_HANDOVER

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Target Cell Id	С	C(=)		
Target RNC Id	С	C(=)		
HO-NumberNotRequired	С	C(=)		
IMSI	С	C(=)		
Integrity Protection Information	С	C(=)		
Encryption Information	С	C(=)		
Radio Resource Information	С	C(=)		
AN-APDU	С	C(=)	С	C(=)
Handover Number			С	C(=)
Relocation Number List			С	C(=)
Multicall Bearer Information			С	C(=)
Multiple Bearer Requested	С	C(=)		
Multiple Bearer Not Supported			С	C(=)
Selected UMTS Algorithms			<u>C</u>	<u>C(=)</u>
User error			С	C(=)
Provider error	·			0

8.4.1.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

Target Cell Id

For definition of this parameter see subclause 7.6.2. This parameter is only included if the service is not in an ongoing transaction. This parameter shall also be excluded if the service is a part of the Inter-MSC SRNS Relocation procedure or the inter-system handover GSM to UMTS procedure described in 3G TS 23.009.

Target RNC Id

For definition of this parameter see subclause 7.6.2. This parameter shall be included if the service is a part of the Inter-MSC SRNS Relocation procedure described in 3G TS 23.009.

HO-Number Not Required

For definition of this parameter see subclause 7.6.6.

<u>IMSI</u>

For definition of this parameter see subclause 7.6.2. This UMTS parameter shall be included if:

- it is available and
- if the access network protocol is BSSAP and
- there is an indication that the MS also supports UMTS.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Radio Resource Information

For definition of this parameter see subclause 7.6.6. This GSM parameter shall be included if the access network protocol is RANAP and there is an indication that the UE also supports GSM.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Handover Number

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at handover, unless the parameter HO-NumberNotRequired is sent. If the parameter Handover Number is returned, the parameter Relocation Number List shall not be returned.

Relocation Number List

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation, unless the parameter HO-NumberNotRequired is sent. If the parameter Relocation Number List is returned, the parameter Handover Number shall not be returned.

Multicall Bearer Information

For a definition of this parameter see subclause 7.6.2.

Multiple Bearer Requested

For a definition of this parameter see subclause 7.6.2. This parameter shall be sent when MSC-A requests multiple bearers to MSC-B.

Multiple Bearer Not Supported

For a definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation when MSC-B receives Multiple Bearer Requested parameter and MSC-B does not support multiple bearers.

Selected UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This parameters includes the UMTS integrity and optionally encryption algorithms selected by RNC under the control of MSC-B. This UMTS parameter shall be included if the service is a part of the inter MSC inter system handover from GSM to UMTS.

User error

For definition of this parameter see subclause 7.6.1. The following errors defined in subclause 7.6.1 may be used, depending on the nature of the fault:

- No handover number available.
- Target cell outside group call area;
- System failure.
- Unexpected data value.
- Data Missing.

Provider error

See definition of provider errors in subclause 7.6.1.

**** NEXT MODIFIED SECTION ****

8.4.3 MAP_PROCESS_ACCESS_SIGNALLING service

8.4.3.1 Definition

This service is used between MSC-B and MSC-A (E-interface) to pass information received on the A-interface or Iuinterface in MSC-B to MSC-A.

The MAP_PROCESS_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/3.

8.4.3.2 Service primitives

Table 8.4/3: MAP_PROCESS_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
AN-APDU	M	M(=)
Selected UMTS Algorithms	<u>C</u>	<u>C(=)</u>

8.4.3.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Selected UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This parameters includes the UMTS integrity and optionally encryption algorithms selected by RNC under the control of MSC-B. This UMTS parameter shall be included if the encapsulated PDU is BSSMAP Cipher Mode Complete and the MS is in UMTS, or an interystem handover to UMTS is performed in MSC-B.

17.7 MAP constants and data types

17.7.1 Mobile Service data types

• • • •

PrepareHO-Res ::= [3] SEQUENCE {		
handoverNumber	[0] ISDN-AddressString	OPTIONAL,
relocationNumberList	[1] RelocationNumberList	OPTIONAL,
an-APDU	[2] AccessNetworkSignalInfo	OPTIONAL,
multicallBearerInfo	[3] MulticallBearerInfo	OPTIONAL,
multipleBearerNotSupported	NULL	OPTIONAL,
selectedUMTS-Algorithms	[4] SelectedUMTS-Algorithms	OPTIONAL,
extensionContainer	[54] ExtensionContainer	OPTIONAL,
}	-	

SelectedUMTS-Algorithms ::= SEQUENCE {			
integrityProtectionAlgorithm	[0]	ChosenIntegrityProtectionAlg	orithm OPTIONAL,
encryptionAlgorithm	[1]	ChosenEncryptionAlgorithm	OPTIONAL,
extensionContainer	[2]	ExtensionContainer	OPTIONAL,
}			

```
ChosenIntegrityProtectionAlgorithm ::= OCTET STRING (SIZE (1))
-- Octet is coded according to 3G TS 25.413
```

```
ChosenEncryptionAlgorithm ::= OCTET STRING (SIZE (1))
-- Octet is coded according to 3G TS 25.413
```

ProcessAccessSignalling-Arg ::=	[3] SEQUENCE {	
an-APDU	AccessNetworkSignalInfo,	
selectedUMTS-Algorithms	[0] SelectedUMTS-Algorithms	OPTIONAL,
extensionContainer}	$[\underline{1}\theta]$ ExtensionContainer	OPTIONAL,

3GPP TSG-CN4 Meeting #07 26th February - 2nd March 2001 Sophia Antipolis, FRANCE

			CHAN	IGE R	REQ	UE	ST				CR-Form-v3
*	29.00	2 CR		226 #	rev	2	ж	Current ver	sion:	3.7.2	¥
For HELP on u	sing this	form, see	e bottom	of this pa	age or	look a	at the	e pop-up tex	t over	the ♯ sy	mbols.
Proposed change a	affects:	₩ (U)	SIM	ME/UE	=	Radi	o Ac	cess Netwo	k	Core N	etwork X
Title: #	Addition	n of allow	ved GSM	algorithr	ns ind	ication	n to t	t <mark>he handove</mark>	r proc	edures	
Source: #	CN4										
Work item code: ₩	Security	y						Date: ೫	27	.2.2001	
Category: #	F (Es	sential C	orrection	1)				Release: #	R9	9	
Reason for change	F (e A (c B (/ C (f D (E Detailed c be found E: # Dur wha furt the	essential of correspon Addition of Functional Editorial mexplanation in 3GPP Fing the lates GSM a ther Intral MSC-B I	f feature), I modifica modificatio ons of the TR 21.900 pasic UM algorithms MSC Intek	tion of fea n) above cat c).	ture) tegorie S relo wed ir hando	cation MSC ver in	the C-B.	R97 R98 R99 REL-4 REL-5	(GSI (Rela (Rela (Rela (Rela (Rela I informing	M Phase 2, ease 1996, ease 1997, ease 1999, ease 4) ease 5)	about
Summary of chang	је: Ж										
Consequences if not approved:	₩ <mark>M</mark> S	SC-B car	n not mal	ke IntraM	SC Int	ersys	tem	handover fro	om Ul	MTS to G	SM.
Clauses affected:	¥ 7.6	6, 8.4, 17	7.7								
Other specs affected:		Test spe	ore specification	าร	¥						
Other comments:	H										

7.6.6.13 Allowed GSM Algorithms

This parameters identifies the allowed GSM algorithms in MSC-B. The coding of this parameter is defined in GSM 08.08.

**** NEXT MODIFIED SECTION ****

8.4 Handover services

It should be noted that the handover services used on the B-interface have not been updated for Release 99. The B-interface is not fully operational specified. It is strongly recommended not to implement the B-interface as an external interface.

8.4.1 MAP_PREPARE_HANDOVER service

8.4.1.1 Definition

This service is used between MSC-A and MSC-B (E-interface) when a call is to be handed over or relocated from MSC-A to MSC-B.

The MAP_PREPARE_HANDOVER service is a confirmed service using the primitives from table 8.4/1.

8.4.1.2 Service primitives

Table 8.4/1: MAP_PREPARE_HANDOVER

Parameter name	Request	Indication	Response	Confirm
Invoke Id	М	M(=)	M(=)	M(=)
Target Cell Id	С	C(=)		
Target RNC Id	С	C(=)		
HO-NumberNotRequired	С	C(=)		
IMSI	С	C(=)		
Integrity Protection Information	С	C(=)		
Encryption Information	С	C(=)		
Radio Resource Information	С	C(=)		
AN-APDU	С	C(=)	С	C(=)
Allowed GSM Algorithms	CI	<u>C(=)</u>		
Handover Number			С	C(=)
Relocation Number List			С	C(=)
Multicall Bearer Information			С	C(=)
Multiple Bearer Requested	С	C(=)		
Multiple Bearer Not Supported			С	C(=)
User error			С	C(=)
Provider error	·			0

8.4.1.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

Target Cell Id

For definition of this parameter see subclause 7.6.2. This parameter is only included if the service is not in an ongoing transaction. This parameter shall also be excluded if the service is a part of the Inter-MSC SRNS Relocation procedure or the inter-system handover GSM to UMTS procedure described in 3G TS 23.009.

Target RNC Id

For definition of this parameter see subclause 7.6.2. This parameter shall be included if the service is a part of the Inter-MSC SRNS Relocation procedure described in 3G TS 23.009.

HO-Number Not Required

For definition of this parameter see subclause 7.6.6.

<u>IMSI</u>

For definition of this parameter see subclause 7.6.2. This UMTS parameter shall be included if:

- it is available and
- if the access network protocol is BSSAP and
- there is an indication that the MS also supports UMTS.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Radio Resource Information

For definition of this parameter see subclause 7.6.6. This GSM parameter shall be included if the access network protocol is RANAP and there is an indication that the UE also supports GSM.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed GSM Algorithms

For definition of this parameter see subclause 7.6.6. This parameters includes allowed GSM algorithms. This GSM parameter shall be included if:

- the service is a part of the Inter-MSC SRNS Relocation procedure and
- Ciphering or Security Mode Setting procedure has been performed.and
- there is an indication that the MS also supports UMTS.

**** NEXT MODIFIED SECTION ****

8.4.4 MAP_FORWARD_ACCESS_SIGNALLING service

8.4.4.1 Definition

This service is used between MSC-A and MSC-B (E-interface) to pass information to be forwarded to the A-interface or Iu-interface of MSC-B.

The MAP_FORWARD_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/4.

8.4.4.2 Service primitives

Table 8.4/4: MAP_FORWARD_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
Integrity Protection Information	С	C(=)
Encryption Information	С	C(=)
Key Status	С	C(=)
AN-APDU	M	M(=)
Allowed GSM Algorithms	<u>C</u>	<u>C(=)</u>

8.4.4.3 Parameter use

For the definition and use of all parameters and errors, see subclause 7.6.1.

Invoke Id

For definition of this parameter see subclause 7.6.1.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Key Status

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed GSM Algorithms

This parameters includes allowed GSM algorithms. This GSM parameter shall be included if the encapsulated PDU is RANAP Security Mode Command and there is an indication that the UE also supports GSM.

17.7 MAP constants and data types

17.7.1 Mobile Service data types

• • • •

```
AllowedGSM-Algorithms ::= OCTET STRING (SIZE (1))

-- internal structure is coded as Algorithm identifier octet from

-- Permitted Algorithms defined in GSM 08.08

-- A node shall mark all GSM algorithms that are allowed in MSC-B
```

PrepareHO-Arg ::= [3] SEQUENCE {		
targetCellId	[0] GlobalCellId	OPTIONAL,
ho-NumberNotRequired	NULL	OPTIONAL,
targetRNCId	[1] RNCId	OPTIONAL,
an-APDU	[2] AccessNetworkSignalInfo	OPTIONAL,
multipleBearerRequested	[3] NULL	OPTIONAL,
imsi	[4] IMSI	OPTIONAL,
integrityProtectionInfo	[5] IntegrityProtectionInformat	ion OPTIONAL,
encryptionInfo	<pre>[6] EncryptionInformation</pre>	OPTIONAL,
radioResourceInformation	[7] RadioResourceInformation	OPTIONAL,
allowedGSM-Algorithms	[8] AllowedGSM-Algorithms	OPTIONAL,
extensionContainer	[9 8] ExtensionContainer	OPTIONAL,
}	_	

			CH	IAN	GE R	EQ	UE	ST				CR-	-Form-v3
	29	.002	CR	2	39 ^ж	rev	2	¥	Current ver	sion:	4.2.1	ж	
For <u>HELP</u> on u	sing	this for	m, see bo	ttom of	f this pa	ige or	look	at the	pop-up tex	t over	the # sy	mbo	ols.
Proposed change a	affec	ts: #	(U)SIM		ME/UE		Rad	io Ac	cess Netwo	rk	Core N	letwo	ork X
Title: %	Add	dition o	f selected	UMTS	algorit	hm in	dicati	on to	the handov	er pro	cedures		
Source: #	CN	4											
Work item code: ∺	Sec	curity							Date: \$	g 27	.2.2001		
Category: Ж	Α								Release: \$	R4			
Reason for change	Deta be fo	F (esse A (corr B (Add C (Fun D (Edit iled exp pund in 3	hm are us	cotion) of a correcture), diffication fication) of the ab 21.900. the integed in M SC-B in	ection in of featove cate	egorie	s can	s that	R97 R98 R99 REL-4 REL-5 MSC-A is a	(GSI) (Rele (Rele (Rele (Rele (Rele) (Rele) (ware	M Phase 2 ease 1996 ease 1997 ease 1998 ease 5) what sec	urity	se of
		UMTS be indi	-UMTS in icated also Setting pr	ter MS o in cas	C SRN se of G	C relo SM-U	catio	n. Ho inter	wever, the s MSC hando intersysten	electe ver, B	ed algorit	nm s Ciph	shall ering
Summary of chang	re: ₩												
Consequences if not approved:	ж		-A does n hosen.	ot knov	w what	UMTS	inte	grity a	and encryption	on alg	orithms N	/ISC	-B
Clauses affected:	¥	7.6.6	, 8.4, 17.7	7									
Other specs affected:	ж	Te	her core s st specific &M Specif	cations		ж							
Other comments:	Ж												

7.6.6.12 Selected UMTS Algorithms

This parameters identifies the UMTS integrity and optionally encryption algorithms selected by MSC-B. Coding of this parameter is defined in 3G TS 25.413.

**** NEXT MODIFIED SECTION ****

8.4 Handover services

It should be noted that the handover services used on the B-interface have not been updated for Release 99. The B-interface is not fully operational specified. It is strongly recommended not to implement the B-interface as an external interface.

8.4.1 MAP_PREPARE_HANDOVER service

8.4.1.1 Definition

This service is used between MSC-A and MSC-B (E-interface) when a call is to be handed over or relocated from MSC-A to MSC-B.

The MAP_PREPARE_HANDOVER service is a confirmed service using the primitives from table 8.4/1.

8.4.1.2 Service primitives

Table 8.4/1: MAP_PREPARE_HANDOVER

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Target Cell Id	С	C(=)		
Target RNC Id	С	C(=)		
HO-NumberNotRequired	С	C(=)		
IMSI	С	C(=)		
Integrity Protection Information	С	C(=)		
Encryption Information	С	C(=)		
Radio Resource Information	С	C(=)		
AN-APDU	С	C(=)	С	C(=)
Handover Number			С	C(=)
Relocation Number List			С	C(=)
Multicall Bearer Information			С	C(=)
Multiple Bearer Requested	С	C(=)		
Multiple Bearer Not Supported			С	C(=)
Selected UMTS Algorithms			<u>C</u>	<u>C(=)</u>
User error			C	C(=)
Provider error				Ò

8.4.1.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

Target Cell Id

For definition of this parameter see subclause 7.6.2. This parameter is only included if the service is not in an ongoing transaction. This parameter shall also be excluded if the service is a part of the Inter-MSC SRNS Relocation procedure or the inter-system handover GSM to UMTS procedure described in 3G TS 23.009.

Target RNC Id

For definition of this parameter see subclause 7.6.2. This parameter shall be included if the service is a part of the Inter-MSC SRNS Relocation procedure described in 3G TS 23.009.

HO-Number Not Required

For definition of this parameter see subclause 7.6.6.

<u>IMSI</u>

For definition of this parameter see subclause 7.6.2. This UMTS parameter shall be included if:

- it is available and
- if the access network protocol is BSSAP and
- there is an indication that the MS also supports UMTS.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Radio Resource Information

For definition of this parameter see subclause 7.6.6. This GSM parameter shall be included if the access network protocol is RANAP and there is an indication that the UE also supports GSM.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Handover Number

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at handover, unless the parameter HO-NumberNotRequired is sent. If the parameter Handover Number is returned, the parameter Relocation Number List shall not be returned.

Relocation Number List

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation, unless the parameter HO-NumberNotRequired is sent. If the parameter Relocation Number List is returned, the parameter Handover Number shall not be returned.

Multicall Bearer Information

For a definition of this parameter see subclause 7.6.2.

Multiple Bearer Requested

For a definition of this parameter see subclause 7.6.2. This parameter shall be sent when MSC-A requests multiple bearers to MSC-B.

Multiple Bearer Not Supported

For a definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation when MSC-B receives Multiple Bearer Requested parameter and MSC-B does not support multiple bearers.

Selected UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This parameters includes the UMTS integrity and optionally encryption algorithms selected by RNC under the control of MSC-B. This UMTS parameter shall be included if the service is a part of the inter MSC inter system handover from GSM to UMTS.

User error

For definition of this parameter see subclause 7.6.1. The following errors defined in subclause 7.6.1 may be used, depending on the nature of the fault:

- No handover number available.
- Target cell outside group call area;
- System failure.
- Unexpected data value.
- Data Missing.

Provider error

See definition of provider errors in subclause 7.6.1.

**** NEXT MODIFIED SECTION ****

8.4.3 MAP_PROCESS_ACCESS_SIGNALLING service

8.4.3.1 Definition

This service is used between MSC-B and MSC-A (E-interface) to pass information received on the A-interface or Iuinterface in MSC-B to MSC-A.

The MAP_PROCESS_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/3.

8.4.3.2 Service primitives

Table 8.4/3: MAP_PROCESS_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
AN-APDU	M	M(=)
Selected UMTS Algorithms	<u>C</u>	<u>C(=)</u>

8.4.3.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Selected UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This parameters includes the UMTS integrity and optionally encryption algorithms selected by RNC under the control of MSC-B. This UMTS parameter shall be included if the encapsulated PDU is BSSMAP Cipher Mode Complete and the MS is in UMTS, or an interystem handover to UMTS is performed in MSC-B.

17.7 MAP constants and data types

17.7.1 Mobile Service data types

• • • •

PrepareHO-Res ::= [3] SEQUENCE {		
handoverNumber	[0] ISDN-AddressString	OPTIONAL,
relocationNumberList	[1] RelocationNumberList	OPTIONAL,
an-APDU	[2] AccessNetworkSignalInfo	OPTIONAL,
multicallBearerInfo	[3] MulticallBearerInfo	OPTIONAL,
multipleBearerNotSupported	NULL	OPTIONAL,
selectedUMTS-Algorithms	[4] SelectedUMTS-Algorithms	OPTIONAL,
extensionContainer	[54] ExtensionContainer	OPTIONAL,
}	-	

SelectedUMTS-Algorithms ::= SEQUENCE {			
integrityProtectionAlgorithm	[0]	ChosenIntegrityProtectionAlg	orithm OPTIONAL,
encryptionAlgorithm	[1]	ChosenEncryptionAlgorithm	OPTIONAL,
extensionContainer	[2]	ExtensionContainer	OPTIONAL,
}			

```
ChosenIntegrityProtectionAlgorithm ::= OCTET STRING (SIZE (1))

-- Octet is coded according to 3G TS 25.413
```

```
ChosenEncryptionAlgorithm ::= OCTET STRING (SIZE (1))
-- Octet is coded according to 3G TS 25.413
```

ProcessAccessSignalling-Arg :::	: [3] SEQUENCE {	
an-APDU	AccessNetworkSignalInfo,	
selectedUMTS-Algorithms	[0] SelectedUMTS-Algorithms	OPTIONAL,
extensionContainer	$[\underline{10}]$ ExtensionContainer	OPTIONAL,

Tdoc N4-010431

	CHANCE DECLIEST	CR-Form-v3
	CHANGE REQUEST	
*	29.002 CR 241 * rev 2 * Current version: 4.2.	1 *
For <u>HELP</u> on u	sing this form, see bottom of this page or look at the pop-up text over the $lpha$	symbols.
Proposed change	ffects: # (U)SIM ME/UE Radio Access Network Core	Network X
Title: 第	Addition of allowed GSM algorithms indication to the handover procedures	
Source: #	CN4	
Work item code: 第	Security	
Category: Ж	Release: # R4	
Reason for change	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) P (Editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900. B During the basic UMTS-UMTS relocation the MSC-A shall inform MSC what GSM algorithms are allowed in MSC-B. This information is needed further IntraMSC Intersystem handover in MSC-B from UMTS to GSM. the MSC-B knows what GSM algorithms are allowed to use. This indication is missing from 29.002.	22) 96) 97) 98) 99) C-B about d if there is
Summary of chang	e: #	
Consequences if not approved:	₩ MSC-B can not make IntraMSC Intersystem handover from UMTS to	GSM.
Clauses affected:	 2 , 7.6, 8.4, 17.7	
Other specs affected:	# 2, 7.6, 6.4, 17.7 # Other core specifications # Test specifications O&M Specifications	
Other comments:	# All references to GSM 08.08 should be checked from the 3G TS 29.00 specification and changed to references to 3G TS 48.008.	02

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- [1] 3G TS 21.905: "3G Vocabulary".
- [2] GSM 02.01: "Digital cellular telecommunications system (Phase 2+); Principles of telecommunication services supported by a GSM Public Land Mobile Network (PLMN)".
- [3] 3G TS 22.002: "Bearer Services Supported by a GSM Public Land Mobile Network (PLMN)".
- [4] GSM 02.03: "Digital cellular telecommunications system (Phase 2+); Teleservices Supported by a GSM Public Land Mobile Network (PLMN)".
- [5] 3G TS 22.004: "General on Supplementary Services".
- [6] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".
- [7] 3G TS 22.016: "International Mobile station Equipment Identities (IMEI)".
- [8] 3G TS 22.041: "Operator Determined Barring".
- [9] 3G TS 22.081: "Line identification supplementary services Stage 1".
- [10] 3G TS 22.082: "Call Forwarding (CF) supplementary services Stage 1".
- [11] 3G TS 22.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services Stage 1".
- [12] 3G TS 22.084: "Multi Party (MPTY) Supplementary Services Stage 1".
- [13] 3G TS 22.085: "Closed User Group (CUG) supplementary services Stage 1".
- [14] 3G TS 22.086: "Advice of charge (AoC) Supplementary Services Stage 1".
- [15] 3G TS 22.088: "Call Barring (CB) supplementary services Stage 1".
- [16] 3G TS 22.090: "Unstructured Supplementary Service Data (USSD); Stage 1".
- [17] 3G TS 23.003: "Numbering, addressing and identification".
- [18] GSM 03.04: "Digital cellular telecommunications system (Phase 2+); Signalling requirements relating to routeing of calls to mobile subscribers".
- [19] 3G TS 23.007: "Restoration procedures".
- [20] 3G TS 23.008: "Organisation of subscriber data".
- [21] 3G TS 23.009: "Handover procedures".
- [22] 3G TS 23.011: "Technical realization of Supplementary Services General Aspects".
- [23] 3G TS 23.012: "Location registration procedures".
- [24] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".
- [25] 3G TS 23.038: "Alphabets and language".
- [26] 3G TS 23.040: "Technical realization of the Short Message Service (SMS) Point to Point (PP)".

[26a]	GSM 03.71: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Functional Description; Stage 2".
[27]	3G TS 23.081: "Line Identification Supplementary Services - Stage 2".
[28]	3G TS 23.082: "Call Forwarding (CF) Supplementary Services - Stage 2".
[29]	3G TS 23.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services - Stage 2".
[30]	3G TS 23.084: "Multi Party (MPTY) Supplementary Services - Stage 2".
[31]	3G TS 23.085: "Closed User Group (CUG) Supplementary Services - Stage 2".
[32]	3G TS 23.086: "Advice of Charge (AoC) Supplementary Services - Stage 2".
[33]	3G TS 23.088: "Call Barring (CB) Supplementary Services - Stage 2".
[34]	3G TS 23.090: "Unstructured Supplementary Services Data (USSD) - Stage 2".
[35]	3G TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols - Stage 3".
[36]	3G TS 24.010: "Mobile radio interface layer 3 Supplementary Services specification - General aspects".
[37]	3G TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".
[37a]	GSM 04.71: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 location services specification".
[38]	3G TS 24.080: "Mobile radio interface layer 3 supplementary services specification - Formats and coding".
[39]	3G TS 24.081: "Line identification supplementary services - Stage 3".
[40]	3G TS 24.082: "Call Forwarding (CF) Supplementary Services - Stage 3".
[41]	3G TS 24.083: "Call Waiting (CW) and Call Hold (HOLD) supplementary services - Stage 3".
[42]	3G TS 24.084: "Multi Party (MPTY) Supplementary Services - Stage 3".
[43]	3G TS 24.085: "Closed User Group (CUG) Supplementary Services - Stage 3".
[44]	3G TS 24.086: "Advice of Charge (AoC) Supplementary Services - Stage 3".
[45]	3G TS 24.088: "Call Barring (CB) Supplementary Services - Stage 3".
[46]	3G TS 24.090: "Unstructured Supplementary Services Data - Stage 3".
[47]	GSM 08.02: "Digital cellular telecommunications system (Phase 2+); Base Station System - Mobile-services Switching Centre (BSS - MSC) interface principles".
[48]	GSM 08.06: "Digital cellular telecommunications system (Phase 2+); Signalling transport mechanism specification for the Base Station System - Mobile-services Switching Centre (BSS - MSC) interface".
[49]	3G TS 48.008GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre - Base Station System (MSC - BSS) interface; Layer 3 specification".
[49a]	GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre—Base Station System (MSC—BSS) interface Layer 3 specification".

- [49a1] GSM 08.31: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre (SMLC) Serving Mobile Location Centre (SMLC); SMLC Peer Protocol (SMLCPP)".
- [49b] GSM 08.71: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre Base Station System (SMLC BSS) interface Layer 3 specification".

[50] GSM 09.01: "Digital cellular telecommunications system (Phase 2+); General network interworking scenarios". 3G TS 29.002: "Mobile Application Part (MAP) specification". [51] GSM 09.03: "Digital cellular telecommunications system (Phase 2+); Signalling requirements on [52] interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)". [53] GSM 09.04: "Digital cellular telecommunications system (Phase 2+); Interworking between the Public Land Mobile Network (PLMN) and the Circuit Switched Public Data Network (CSPDN)". [54] GSM 09.05: "Digital cellular telecommunications system (Phase 2+); Interworking between the Public Land Mobile Network (PLMN) and the Packet Switched Public Data Network (PSPDN) for Packet Assembly/Disassembly facility (PAD) access". [55] 3G TS 29.006: "Interworking between a Public Land Mobile Network (PLMN) and a Packet Switched Public Data Network/Integrated Services Digital Network (PSPDN/ISDN) for the support of Packet Switched data transmission services". [56] 3G TS 29.007: "Digital cellular telecommunications system (Phase 2+); General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)". GSM 09.08: "Digital cellular telecommunications system (Phase 2+); Application of the Base [57] Station System Application Part (BSSAP) on the E-interface". [58] 3G TS 29.010: "Information element mapping between Mobile Station - Base Station System and BSS - Mobile-services Switching Centre (MS - BSS - MSC) Signalling procedures and the Mobile Application Part (MAP)". [59] 3G TS 29.011: "Signalling interworking for Supplementary Services". GSM 09.31: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); [59a] Base Station System Application Part LCS Extension (BSSAP-LE)". [60] GSM 09.90: "Digital cellular telecommunications system (Phase 2+); Interworking between Phase 1 infrastructure and Phase 2 Mobile Stations (MS)". [61] GSM 12.08: "Digital cellular telecommunications system (Phase 2); Subscriber and Equipment Trace". ETS 300 102-1 (1990): "Integrated Services Digital Network (ISDN); User-network interface [62] layer 3 specifications for basic call control". [63] ETS 300 136 (1992): "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service description". ETS 300 138 (1992): "Integrated Services Digital Network (ISDN); Closed User Group (CUG) [64] supplementary service Digital Subscriber Signalling System No.one (DSS1) protocol". [65] ETS 300 287: "Integrated Services Digital Network (ISDN); Signalling System No.7; Transaction Capabilities (TC) version 2". [66] ETR 060: "Signalling Protocols and Switching (SPS); Guide-lines for using Abstract Syntax Notation One (ASN.1) in telecommunication application protocols". ITU-T Recommendation E.164: "Numbering plan for the ISDN era". [67] [68] ITU-T Recommendation E.212: "Identification plan for land mobile stations". [69] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land mobile stations". [70] ITU-T Recommendation E.214: "Structuring of the land mobile global title for the signalling connection control part". [71] CCITT Recommendation Q.699: "Interworking between the Digital Subscriber Signalling System

Layer 3 protocol and the Signalling System No.7 ISDN User part".

[72] ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Functional description of the Signalling Connection Control Part". ITU-T Recommendation Q.712: "Definition and function of SCCP messages". [73] ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; SCCP formats and [74] codes". [75] ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling Connection Control Part procedures". ITU-T Recommendation Q.716: "Specifications of Signalling System No.7; Signalling connection [76] control part (SCCP) performances". ITU-T Recommendation Q.721 (1988): "Specifications of Signalling System No.7; Functional [77] description of the Signalling System No.7 Telephone user part". [78] ITU-T Recommendation Q.722 (1988): "Specifications of Signalling System No.7; General function of Telephone messages and signals". [79] ITU-T Recommendation Q.723 (1988): "Specifications of Signalling System No.7; Formats and codes". [80] ITU-T Recommendation Q.724 (1988): "Specifications of Signalling System No.7; Signalling procedures". [81] ITU-T Recommendation Q.725 (1988): "Specifications of Signalling System No.7; Signalling performance in the telephone application". ITU-T Recommendation Q.761 (1988): "Specifications of Signalling System No.7; Functional [82] description of the ISDN user part of Signalling System No.7". [83] ITU-T Recommendation Q.762 (1988): "Specifications of Signalling System No.7; General function of messages and signals". [84] ITU-T Recommendation Q.763 (1988): "Specifications of Signalling System No.7; Formats and codes". [85] ITU-T Recommendation Q.764 (1988): "Specifications of Signalling System No.7; Signalling procedures". [86] ITU-T Recommendation Q.767: "Specifications of Signalling System No.7; Application of the ISDN user part of CCITT signalling System No.7 for international ISDN interconnections". [87] ITU-T Recommendation Q.771: "Specifications of Signalling System No.7; Functional description of transaction capabilities". ITU-T Recommendation Q.772: "Specifications of Signalling System No.7; Transaction [88] capabilities information element definitions". ITU-T Recommendation Q.773: "Specifications of Signalling System No.7; Transaction [89] capabilities formats and encoding". [90] ITU-T Recommendation Q.774: "Specifications of Signalling System No.7; Transaction capabilities procedures". ITU-T Recommendation Q.775: "Specifications of Signalling System No.7; Guide-lines for using [91] transaction capabilities". [92] ITU-T Recommendation X.200: "Reference Model of Open systems interconnection for CCITT Applications". [93] ITU-T Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)". [94] ITU-T Recommendation X.209 (1988): "Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)".

[95]	ITU-T Recommendation X.210: "Open systems interconnection layer service definition conventions".
[97]	3G TS 23.018: "Basic Call Handling".
[98]	3G TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2".
[99]	3G TS 23.079: "Support of Optimal Routeing (SOR) - Stage 2".
[100]	GSM 03.68: "Digital cellular telecommunications system (Phase 2+); - Stage 2".
[101]	GSM 03.69: "Digital cellular telecommunications system (Phase 2+); - Stage 2".
[102]	ANSI T1.113: "Signaling System No. 7 (SS7) - ISDN User Part".
[103]	3G TS 23.054 "Shared Inter Working Function (SIWF) - Stage 2".
[104]	3G TS 23.060: "General Packet Radio Service (GPRS) Description; Stage 2".
[105]	3G TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".
[106]	3G TS 29.018: "General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface layer 3 specification".
[107]	3G TS 23.093: "Technical Realization of Completion of Calls to Busy Subscriber (CCBS); Stage 2".
[108]	3G TS 23.066: "Support of Mobile Number Portability (MNP); Technical Realisation Stage 2".
[109]	ANSI T1.112 (1996): "Telecommunication – Signalling No. 7 - Signaling Connection Control Part (SCCP)".
[110]	3G TS 23.116: "Super-Charger Technical Realisation; Stage 2."
[111]	ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Signalling System No. 7 – Functional Description of the Signalling Connection Control Part".
[112]	ITU-T Recommendation Q.712: "Specifications of Signalling System No.7; Signalling System No. 7 – Definition and Function of SCCP Messages".
[113]	ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; Signalling System No. 7 – SCCP formats and codes".
[114]	ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling System No. 7 – Signalling Connection Control Part Procedures".
[115]	ITU-T Recommendation Q.716: "Specifications of Signalling System No.7; Signalling System No.7 – Signalling Connection Control Part (SCCP) Performance".
[116]	ITU-T Q.850, May 1998: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".
[117]	3G TS 22.135: "Multicall; Service description; Stage 1".
[118]	3G TS 23.135: "Multicall supplementary service; Stage 2".
[119]	3G TS 24.135: "Multicall supplementary service; Stage 3".
[120]	3G TS 25.413: "UTRAN Iu Interface RANAP Signalling".

**** NEXT MODIFIED SECTION ****

7.6.6.13 Allowed GSM Algorithms

**** NEXT MODIFIED SECTION ****

8.4 Handover services

It should be noted that the handover services used on the B-interface have not been updated for Release 99. The B-interface is not fully operational specified. It is strongly recommended not to implement the B-interface as an external interface.

8.4.1 MAP_PREPARE_HANDOVER service

8.4.1.1 Definition

This service is used between MSC-A and MSC-B (E-interface) when a call is to be handed over or relocated from MSC-A to MSC-B.

The MAP_PREPARE_HANDOVER service is a confirmed service using the primitives from table 8.4/1.

8.4.1.2 Service primitives

Table 8.4/1: MAP_PREPARE_HANDOVER

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Target Cell Id	С	C(=)		
Target RNC Id	С	C(=)		
HO-NumberNotRequired	С	C(=)		
IMSI	С	C(=)		
Integrity Protection Information	С	C(=)		
Encryption Information	С	C(=)		
Radio Resource Information	С	C(=)		
AN-APDU	С	C(=)	С	C(=)
Allowed GSM Algorithms	<u>C</u>	<u>C(=)</u>		
Handover Number			С	C(=)
Relocation Number List			С	C(=)
Multicall Bearer Information			С	C(=)
Multiple Bearer Requested	С	C(=)		
Multiple Bearer Not Supported			С	C(=)
User error			С	C(=)
Provider error				0

8.4.1.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

Target Cell Id

For definition of this parameter see subclause 7.6.2. This parameter is only included if the service is not in an ongoing transaction. This parameter shall also be excluded if the service is a part of the Inter-MSC SRNS Relocation procedure or the inter-system handover GSM to UMTS procedure described in 3G TS 23.009.

Target RNC Id

For definition of this parameter see subclause 7.6.2. This parameter shall be included if the service is a part of the Inter-MSC SRNS Relocation procedure described in 3G TS 23.009.

HO-Number Not Required

For definition of this parameter see subclause 7.6.6.

IMSI

For definition of this parameter see subclause 7.6.2. This UMTS parameter shall be included if:

- it is available and
- if the access network protocol is BSSAP and
- there is an indication that the MS also supports UMTS.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Radio Resource Information

For definition of this parameter see subclause 7.6.6. This GSM parameter shall be included if the access network protocol is RANAP and there is an indication that the UE also supports GSM.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed GSM Algorithms

For definition of this parameter see subclause 7.6.6. This parameters includes allowed GSM algorithms. This GSM parameter shall be included if:

- the service is a part of the Inter-MSC SRNS Relocation procedure and
- Ciphering or Security Mode Setting procedure has been performed.and
- there is an indication that the MS also supports UMTS.

**** NEXT MODIFIED SECTION ****

8.4.4 MAP_FORWARD_ACCESS_SIGNALLING service

8.4.4.1 Definition

This service is used between MSC-A and MSC-B (E-interface) to pass information to be forwarded to the A-interface or Iu-interface of MSC-B.

The MAP_FORWARD_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/4.

8.4.4.2 Service primitives

Table 8.4/4: MAP_FORWARD_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
Integrity Protection Information	С	C(=)
Encryption Information	С	C(=)
Key Status	С	C(=)
AN-APDU	M	M(=)
Allowed GSM Algorithms	<u>C</u>	<u>C(=)</u>

8.4.4.3 Parameter use

For the definition and use of all parameters and errors, see subclause 7.6.1.

Invoke Id

For definition of this parameter see subclause 7.6.1.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Key Status

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed GSM Algorithms

This parameters includes allowed GSM algorithms. This GSM parameter shall be included if the encapsulated PDU is RANAP Security Mode Command and there is an indication that the UE also supports GSM.

17.7 MAP constants and data types

17.7.1 Mobile Service data types

• • • •

ForwardAccessSignalling-Arg ::=	[3] SEQUENCE {	
an-APDU	AccessNetworkSignalInfo,	
integrityProtectionInfo	<pre>[0] IntegrityProtectionInforma</pre>	tion OPTIONAL,
encryptionInfo	[1] EncryptionInformation	OPTIONAL,
keyStatus	[2] KeyStatus	OPTIONAL,
allowedGSM-Algorithms	[3] AllowedGSM-Algorithms	OPTIONAL,
extensionContainer	[43] ExtensionContainer	OPTIONAL,
}	_	

```
AllowedGSM-Algorithms ::= OCTET STRING (SIZE (1))

-- internal structure is coded as Algorithm identifier octet from

-- Permitted Algorithms defined in 3G TS 48.008

-- A node shall mark all GSM algorithms that are allowed in MSC-B
```

PrepareHO-Arg ::= [3] SEQUENCE {		
targetCellId	[0] GlobalCellId	OPTIONAL,
ho-NumberNotRequired	NULL	OPTIONAL,
targetRNCId	[1] RNCId	OPTIONAL,
an-APDU	[2] AccessNetworkSignalInfo	OPTIONAL,
multipleBearerRequested	[3] NULL	OPTIONAL,
imsi	[4] IMSI	OPTIONAL,
integrityProtectionInfo	[5] IntegrityProtectionInformat	ion OPTIONAL,
encryptionInfo	<pre>[6] EncryptionInformation</pre>	OPTIONAL,
radioResourceInformation	[7] RadioResourceInformation	OPTIONAL,
allowedGSM-Algorithms	[8] AllowedGSM-Algorithms	OPTIONAL,
extensionContainer	[9 8] ExtensionContainer	OPTIONAL,
}	_	

Tdoc N4-010432

CHANGE REQUEST					CR-Form-v3			
*	29.002	CR	242 [#]	rev 1	¥	Current versi	ion: 3.7.	2 #
For <u>HELP</u> on u	sing this fo	rm, see botto	m of this pag	ge or look	at the	pop-up text	over the 🖁 🥄	symbols.
Proposed change	affects: ∺	(U)SIM	ME/UE	Rad	dio Acc	cess Network	Core	Network X
Title: 第	Addition of	of allowed UN	ATS algorithr	n indication	on to t	he handover	procedures	
Source: 第	CN4							
Work item code: ₩	Security					Date: 眯	27.2.2001	
Category: ж	F (Esse	ential correct	ion)			Release: ≭	R99	
	F (ess A (cor B (Add C (Fur D (Edr Detailed ex	dition of featui nctional modifi itorial modifica	on) correction in a re), ication of featution) he above cate	ıre)		2 R96 R97 R98 R99 REL-4	the following (GSM Phase (Release 199 (Release 199 (Release 199 (Release 4) (Release 5)	2) 96) 97) 98)
Description of the property of the MCC Ashall informs MCC Dishaut wheat UNTO all will								
Reason for change: During the basic the MSC-A shall inform MSC-B about what UMTS algorithm are allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM.								
Summary of chang	ø: Ж							
Consequences if not approved:	*							
Clauses affected:	ж <mark>7.6.6</mark>	6, 8.4, 17.7						
Other specs affected:	ж O	ther core spe est specificat &M Specifica	ions	¥				
Other comments:	ж							

7.6.6.13 Allowed UMTS Algorithms

This parameters identifies the allowed UMTS algorithms in MSC-B. Coding of this parameter is defined in 3G TS 25.413.

**** NEXT MODIFIED SECTION ****

8.4 Handover services

It should be noted that the handover services used on the B-interface have not been updated for Release 99. The B-interface is not fully operational specified. It is strongly recommended not to implement the B-interface as an external interface.

8.4.1 MAP_PREPARE_HANDOVER service

8.4.1.1 Definition

This service is used between MSC-A and MSC-B (E-interface) when a call is to be handed over or relocated from MSC-A to MSC-B.

The MAP_PREPARE_HANDOVER service is a confirmed service using the primitives from table 8.4/1.

8.4.1.2 Service primitives

Table 8.4/1: MAP_PREPARE_HANDOVER

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Target Cell Id	С	C(=)		
Target RNC Id	С	C(=)		
HO-NumberNotRequired	С	C(=)		
IMSI	С	C(=)		
Integrity Protection Information	С	C(=)		
Encryption Information	С	C(=)		
Radio Resource Information	С	C(=)		
AN-APDU	С	C(=)	С	C(=)
Allowed UMTS Algorithms	<u>C</u>	<u>C(=)</u>		
Handover Number			С	C(=)
Relocation Number List			С	C(=)
Multicall Bearer Information			С	C(=)
Multiple Bearer Requested	С	C(=)		
Multiple Bearer Not Supported			С	C(=)
User error			С	C(=)
Provider error				Ò

8.4.1.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

Target Cell Id

For definition of this parameter see subclause 7.6.2. This parameter is only included if the service is not in an ongoing transaction. This parameter shall also be excluded if the service is a part of the Inter-MSC SRNS Relocation procedure or the inter-system handover GSM to UMTS procedure described in 3G TS 23.009.

Target RNC Id

For definition of this parameter see subclause 7.6.2. This parameter shall be included if the service is a part of the Inter-MSC SRNS Relocation procedure described in 3G TS 23.009.

HO-Number Not Required

For definition of this parameter see subclause 7.6.6.

<u>IMSI</u>

For definition of this parameter see subclause 7.6.2. This UMTS parameter shall be included if:

- it is available and
- if the access network protocol is BSSAP and
- there is an indication that the MS also supports UMTS.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Radio Resource Information

For definition of this parameter see subclause 7.6.6. This GSM parameter shall be included if the access network protocol is RANAP and there is an indication that the UE also supports GSM.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if all of the following conditions apply:

- access network protocol is BSSAP and
- Integrity Protection Information and Encryption Information are not available and
- Ciphering or Security Mode Setting procedure has been performed.

Handover Number

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at handover, unless the parameter HO-NumberNotRequired is sent. If the parameter Handover Number is returned, the parameter Relocation Number List shall not be returned.

Relocation Number List

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation, unless the parameter HO-NumberNotRequired is sent. If the parameter Relocation Number List is returned, the parameter Handover Number shall not be returned.

Multicall Bearer Information

For a definition of this parameter see subclause 7.6.2.

Multiple Bearer Requested

For a definition of this parameter see subclause 7.6.2. This parameter shall be sent when MSC-A requests multiple bearers to MSC-B.

Multiple Bearer Not Supported

For a definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation when MSC-B receives Multiple Bearer Requested parameter and MSC-B does not support multiple bearers.

User error

For definition of this parameter see subclause 7.6.1. The following errors defined in subclause 7.6.1 may be used, depending on the nature of the fault:

- No handover number available.
- Target cell outside group call area;
- System failure.
- Unexpected data value.
- Data Missing.

Provider error

See definition of provider errors in subclause 7.6.1.

**** NEXT MODIFIED SECTION ****

8.4.4 MAP_FORWARD_ACCESS_SIGNALLING service

8.4.4.1 Definition

This service is used between MSC-A and MSC-B (E-interface) to pass information to be forwarded to the A-interface or Iu-interface of MSC-B.

The MAP_FORWARD_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/4.

8.4.4.2 Service primitives

Table 8.4/4: MAP_FORWARD_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
Integrity Protection Information	С	C(=)
Encryption Information	С	C(=)
Key Status	С	C(=)
AN-APDU	M	M(=)
Allowed UMTS Algorithms	С	C(=)

8.4.4.3 Parameter use

For the definition and use of all parameters and errors, see subclause 7.6.1.

Invoke Id

For definition of this parameter see subclause 7.6.1.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Key Status

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if Integrity Protection Information and Encryption Information are not available and the encapsulated PDU is BSSMAP Cipher Mode Command.

17.7 MAP constants and data types

17.7.1 Mobile Service data types

• • • •

PrepareHO-Arg ::= [3] SEQUENCE {		
targetCellId	[0] GlobalCellId	OPTIONAL,
ho-NumberNotRequired	NULL	OPTIONAL,
targetRNCId	[1] RNCId	OPTIONAL,
an-APDU	[2] AccessNetworkSignalInfo	OPTIONAL,
multipleBearerRequested	[3] NULL	OPTIONAL,
imsi	[4] IMSI	OPTIONAL,
integrityProtectionInfo	[5] IntegrityProtectionInformati	on OPTIONAL,
encryptionInfo	<pre>[6] EncryptionInformation</pre>	OPTIONAL,
radioResourceInformation	[7] RadioResourceInformation	OPTIONAL,
allowedUMTS-Algorithms	[8] AllowedUMTS-Algorithms	OPTIONAL,
extensionContainer	[<u>9</u> 8] ExtensionContainer	OPTIONAL,
}	_	

AllowedUMTS-Algorithms ::= SEQUENCE {		
integrityProtectionAlgorithms	[0]	PermittedIntegrityProtectionAlgorithms
OPTIONAL,		
encryptionAlgorithms	[1]	PermittedEncryptionAlgorithms OPTIONAL,
extensionContainer	[2]	ExtensionContainer OPTIONAL,
}		

PermittedIntegrityProtectionAlgorithms ::= OCTET STRING (SIZE (2..maxPermittedIntegrityProtectionAlgorithmsLength)) -- Octets are coded according to Permitted Integrity Protection Algorithms in Integrity -- Protection Information information element in 3G TS 25.413

maxPermittedIntegrityProtectionAlgorithmsLength INTEGER ::= 9

```
PermittedEncryptionAlgorithms ::=

OCTET STRING (SIZE (2..maxPermittedEncryptionAlgorithmsLength))

-- Octets are coded according to Permitted Encryption Algorithms in Encryption

-- Information information element in 3G TS 25.413
```

maxPermittedEncryptionAlgorithmsLength INTEGER ::= 9

ProcessAccessSignalling-Arg	::= [3] SEQUENCE {	
an-APDU	AccessNetworkSignalInfo,	
allowedUMTS-Algorithms	[0] AllowedUMTS-Algorithms	OPTIONAL,
extensionContainer}	$[\underline{10}]$ ExtensionContainer	OPTIONAL,

26th February - 2 [™] March 2001 Sophia Antipolis, FRANCE						
	CHANGE REQUEST					
*	29.002 CR 243 * rev 1 * Current version: 3.7.2 *					
For HELP on u	sing this form, see bottom of this page or look at the pop-up text over the % symbols	:.				
Proposed change	ffects: 第 (U)SIM ME/UE Radio Access Network Core Networ	k X				
Title: #	Addition of selected GSM algorithm indication to the handover procedures					
Source: 第	CN4					
Work item code: ₩	Security Date: # 27.2.2001					
Category: Ж	F (Agreed by consensus) 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 1999) R99 (Release 1999) REL-4 (Release 4) REL-5 (Release 5)); 				
Reason for change	* * The principle of the interMSC handover is that MSC-A is aware what security					
	algorithm are used in MSC-B.					
Summary of chang	e: #					
Consequences if not approved:	# MSC-A does not know what algorithm MSC-B has chosen or in the worst case whether the connection is ciphered at all.	е				
Clauses affected:	% 7.6.6, 8.4, 17.7					
viauses allected.	00 7.0.0, 0.7, 17.7					

Other core specifications

Test specifications O&M Specifications

Other specs affected:

Other comments:

 \mathfrak{R}

7.6.6.13 Selected GSM Algorithm

This parameter identifies the GSM algorithm selected by GSM BSC controlled by MSC-B. Coding of this parameter is defined in GSM 08.08.

**** NEXT MODIFIED SECTION ****

8.4.3 MAP_PROCESS_ACCESS_SIGNALLING service

8.4.3.1 Definition

This service is used between MSC-B and MSC-A (E-interface) to pass information received on the A-interface or Iuinterface in MSC-B to MSC-A.

The MAP_PROCESS_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/3.

8.4.3.2 Service primitives

Table 8.4/3: MAP PROCESS ACCESS SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
AN-APDU	M	M(=)
Selected GSM Algorithm	CI	<u>C(=)</u>

8.4.3.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Selected GSM algorithm

For definition of this parameter see subclause 7.6.6. This parameter shall be present if the encapsulated PDU is Security Mode Complete and MS is in GSM access.

**** NEXT MODIFIED SECTION ****

17.7 MAP constants and data types

17.7.1 Mobile Service data types

•••

ProcessAccessSignalling-Arg ::= [3] SEQUENCE {		
an-APDU	AccessNetworkSignalInfo,	
selectedGSM-Algorithm	[0] SelectedGSM-Algorithm	OPTIONAL,
extensionContainer	[1 0] ExtensionContainer	OPTIONAL,
}	_	

```
SelectedGSM-Algorithm ::= OCTET STRING (SIZE (1))

-- internal structure is coded as Algorithm identifier octet from Chosen Encryption

-- Algorithm defined in GSM 08.08

-- A node shall mark only the selected GSM algorithm
```

 \mathfrak{R}

 \mathfrak{R}

Other specs affected:

Other comments:

Other core specifications

Test specifications **O&M Specifications**

CHANGE REQUEST # 29.002 CR 244 # rev 1 # Current version: 4.2.1 # For HELP on using this form, see bottom of this page or look at the pop-up text over the # symbols.	26th February - Sophia Antipol	2 nd March 2001 FRANCE	
For HELP on using this form, see bottom of this page or look at the pop-up text over the \$\mathbb{R}\$ symbols. Proposed change affects: \$\mathbb{R}\$ (U)SIM ME/UE Radio Access Network Core Network 7. Title: \$\mathbb{R}\$ Addition of allowed UMTS algorithm indication to the handover procedures Source: \$\mathbb{R}\$ CN4 Work item code: \$\mathbb{R}\$ Security Date: \$\mathbb{R}\$ 27.2.2001 Category: \$\mathbb{A}\$ Release: \$\mathbb{R}\$ R4 Use one of the following categories: Use one of the following releases: F (essential correction) 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-5 (Release 5) Reason for change: \$\mathbb{R}\$ During the basic the MSC-A shall inform MSC-B about what UMTS algorithm are allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM. Summary of change: \$\mathbb{R}\$ Consequences if mot approved:		•	CR-Form-v
Proposed change affects: \$\mathbb{R}\$ (U)SIM	*	29.002 CR 244 **	rev 1 % Current version: 4.2.1
Title:	For <u>HELP</u> on	sing this form, see bottom of this pag	ge or look at the pop-up text over the ₩ symbols.
Source: Work item code: Security Date: Z7.2.2001 Category: A Release: R4 Use one of the following categories: Use one of the following releases: F (essential correction) 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-5 (Release 5) Reason for change: During the basic the MSC-A shall inform MSC-B about what UMTS algorithm are allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM. Summary of change: Consequences if mot approved:	Proposed change	affects: # (U)SIM ME/UE	Radio Access Network Core Network
Work item code: Security Date: Page 27.2.2001 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) Potailed explanations of the above categories can be found in 3GPP TR 21.900. Reason for change: During the basic the MSC-A shall inform MSC-B about what UMTS algorithm are allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM. Summary of change: Consequences if mot approved:	Title:	Addition of allowed UMTS algorithm	n indication to the handover procedures
Category: A Release: Rel	Source:	CN4	
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) P (Editorial modification) D (Editorial modification) E (Functional modification) R (Elease 1998) D (Editorial modification) R (Elease 1999) D (Editorial modification) R (Elease 1999) D (Editorial modification) R (Elease 1999) R (Elease 1999) R (Elease 1999) R (Elease 4) E (Elease 5) R (Elease 6) R (Elease 7) R (Elease 7) R (Elease 7) R (Elease 7) R (Elease 6) R (Elease 7) R (Elease 1998) R	Work item code:	Security	<i>Date:</i>
F (essential correction) A (corresponds to a correction in an earlier release) B (Addition of feature), C (Functional modification) D (Editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900. Reason for change: During the basic the MSC-A shall inform MSC-B about what UMTS algorithm are allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM. Summary of change: Consequences if mot approved:	Category:	Α	Release: ₩ R4
allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM. Summary of change: Consequences if # not approved:		F (essential correction) A (corresponds to a correction in a B (Addition of feature), C (Functional modification of feature) D (Editorial modification) Detailed explanations of the above cate	2 (GSM Phase 2) an earlier release) R96 (Release 1996) R97 (Release 1997) ure) R98 (Release 1998) R99 (Release 1999) gories can REL-4 (Release 4)
allowed in MSC-B. This indication is missing from 29.002 in case the user has GSM SIM. Summary of change: Consequences if # not approved:	Passan for abone	. # During the basic the MSC-A sk	and inform MSC-R about what LIMTS algorithm are
Consequences if # not approved:	Reason for chang	allowed in MSC-B.	
Consequences if # not approved:	Summary of chan	e: #	
	Consequences if		
		¥ 766 84 177	

 \mathfrak{R}

7.6.6.13 Allowed UMTS Algorithms

This parameters identifies the allowed UMTS algorithms in MSC-B. Coding of this parameter is defined in 3G TS 25.413.

**** NEXT MODIFIED SECTION ****

8.4 Handover services

It should be noted that the handover services used on the B-interface have not been updated for Release 99. The B-interface is not fully operational specified. It is strongly recommended not to implement the B-interface as an external interface.

8.4.1 MAP_PREPARE_HANDOVER service

8.4.1.1 Definition

This service is used between MSC-A and MSC-B (E-interface) when a call is to be handed over or relocated from MSC-A to MSC-B.

The MAP_PREPARE_HANDOVER service is a confirmed service using the primitives from table 8.4/1.

8.4.1.2 Service primitives

Table 8.4/1: MAP_PREPARE_HANDOVER

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Target Cell Id	С	C(=)		
Target RNC Id	С	C(=)		
HO-NumberNotRequired	С	C(=)		
IMSI	С	C(=)		
Integrity Protection Information	С	C(=)		
Encryption Information	С	C(=)		
Radio Resource Information	С	C(=)		
AN-APDU	С	C(=)	С	C(=)
Allowed UMTS Algorithms	<u>C</u>	<u>C(=)</u>		
Handover Number			С	C(=)
Relocation Number List			С	C(=)
Multicall Bearer Information			С	C(=)
Multiple Bearer Requested	С	C(=)		
Multiple Bearer Not Supported	•		С	C(=)
User error	_		С	C(=)
Provider error				0

8.4.1.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

Target Cell Id

For definition of this parameter see subclause 7.6.2. This parameter is only included if the service is not in an ongoing transaction. This parameter shall also be excluded if the service is a part of the Inter-MSC SRNS Relocation procedure or the inter-system handover GSM to UMTS procedure described in 3G TS 23.009.

Target RNC Id

For definition of this parameter see subclause 7.6.2. This parameter shall be included if the service is a part of the Inter-MSC SRNS Relocation procedure described in 3G TS 23.009.

HO-Number Not Required

For definition of this parameter see subclause 7.6.6.

<u>IMSI</u>

For definition of this parameter see subclause 7.6.2. This UMTS parameter shall be included if:

- it is available and
- if the access network protocol is BSSAP and
- there is an indication that the MS also supports UMTS.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the access network protocol is BSSAP.

Radio Resource Information

For definition of this parameter see subclause 7.6.6. This GSM parameter shall be included if the access network protocol is RANAP and there is an indication that the UE also supports GSM.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if all of the following conditions apply:

- access network protocol is BSSAP and
- Integrity Protection Information and Encryption Information are not available and
- <u>Ciphering or Security Mode Setting procedure has been performed.</u>

Handover Number

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at handover, unless the parameter HO-NumberNotRequired is sent. If the parameter Handover Number is returned, the parameter Relocation Number List shall not be returned.

Relocation Number List

For definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation, unless the parameter HO-NumberNotRequired is sent. If the parameter Relocation Number List is returned, the parameter Handover Number shall not be returned.

Multicall Bearer Information

For a definition of this parameter see subclause 7.6.2.

Multiple Bearer Requested

For a definition of this parameter see subclause 7.6.2. This parameter shall be sent when MSC-A requests multiple bearers to MSC-B.

Multiple Bearer Not Supported

For a definition of this parameter see subclause 7.6.2. This parameter shall be returned at relocation when MSC-B receives Multiple Bearer Requested parameter and MSC-B does not support multiple bearers.

User error

For definition of this parameter see subclause 7.6.1. The following errors defined in subclause 7.6.1 may be used, depending on the nature of the fault:

- No handover number available.
- Target cell outside group call area;
- System failure.
- Unexpected data value.
- Data Missing.

Provider error

See definition of provider errors in subclause 7.6.1.

**** NEXT MODIFIED SECTION ****

8.4.4 MAP_FORWARD_ACCESS_SIGNALLING service

8.4.4.1 Definition

This service is used between MSC-A and MSC-B (E-interface) to pass information to be forwarded to the A-interface or Iu-interface of MSC-B.

The MAP_FORWARD_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/4.

8.4.4.2 Service primitives

Table 8.4/4: MAP_FORWARD_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
Integrity Protection Information	С	C(=)
Encryption Information	С	C(=)
Key Status	С	C(=)
AN-APDU	M	M(=)
Allowed UMTS Algorithms	С	C(=)

8.4.4.3 Parameter use

For the definition and use of all parameters and errors, see subclause 7.6.1.

Invoke Id

For definition of this parameter see subclause 7.6.1.

Integrity Protection Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Encryption Information

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

Key Status

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if available and if the encapsulated PDU is BSSMAP Cipher Mode Command.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Allowed UMTS Algorithms

For definition of this parameter see subclause 7.6.6. This UMTS parameter shall be included if Integrity Protection Information and Encryption Information are not available and the encapsulated PDU is BSSMAP Cipher Mode Command.

17.7 MAP constants and data types

17.7.1 Mobile Service data types

....

PrepareHO-Arg ::= [3] SEQUENCE {		
targetCellId	[0] GlobalCellId	OPTIONAL,
ho-NumberNotRequired	NULL	OPTIONAL,
targetRNCId	[1] RNCId	OPTIONAL,
an-APDU	[2] AccessNetworkSignalInfo	OPTIONAL,
multipleBearerRequested	[3] NULL	OPTIONAL,
imsi	[4] IMSI	OPTIONAL,
integrityProtectionInfo	[5] IntegrityProtectionInformat	ion OPTIONAL,
encryptionInfo	<pre>[6] EncryptionInformation</pre>	OPTIONAL,
radioResourceInformation	[7] RadioResourceInformation	OPTIONAL,
allowedUMTS-Algorithms	[8] AllowedUMTS-Algorithms	OPTIONAL,
extensionContainer	[9 8] ExtensionContainer	OPTIONAL,
}		

AllowedUMTS-Algorithms ::= SEQUENCE {		
integrityProtectionAlgorithms	[0]	PermittedIntegrityProtectionAlgorithms
OPTIONAL,		
encryptionAlgorithms	[1]	PermittedEncryptionAlgorithms OPTIONAL,
extensionContainer	[2]	ExtensionContainer OPTIONAL,
}		

PermittedIntegrityProtectionAlgorithms ::= OCTET STRING (SIZE (2..maxPermittedIntegrityProtectionAlgorithmsLength)) -- Octets are coded according to Permitted Integrity Protection Algorithms in Integrity -- Protection Information information element in 3G TS 25.413

maxPermittedIntegrityProtectionAlgorithmsLength INTEGER ::= 9

```
PermittedEncryptionAlgorithms ::=

OCTET STRING (SIZE (2..maxPermittedEncryptionAlgorithmsLength))

-- Octets are coded according to Permitted Encryption Algorithms in Encryption

-- Information information element in 3G TS 25.413
```

maxPermittedEncryptionAlgorithmsLength INTEGER ::= 9

ProcessAccessSignalling-Arg :::	: [3] SEQUENCE {	
an-APDU	AccessNetworkSignalInfo,	
allowedUMTS-Algorithms	<pre>[0] AllowedUMTS-Algorithms</pre>	OPTIONAL,
extensionContainer	[1 0] ExtensionContainer	OPTIONAL,
}		

			CH	IANC	GE R	EQ	UE	ST			(CR-Form-v3
ж	29.0	002	CR	2	<mark>45</mark> [∺]	rev	1	Ħ	Current ver	sion: 4.	2.1	*
For HELP on t	using th	is forn	n, see bo	ttom of	this pa	ge or	look a	at the	e pop-up tex	t over the	₩ sym	bols.
Proposed change	affects	: X	(U)SIM		ME/UE		Radi	о Ас	cess Netwo	k Co	ore Net	twork X
Title: #	Addit	tion of	selected	I GSM a	algorith	m indi	catior	n to tl	he handover	procedur	es	
Source: #	CN4											
Work item code: ₩	Secu	ırity							Date: ♯	27.2.20	01	
Category:	B A								Release: #	R4		
	F A B C D Detaile	esser) (corre (Addit (Func (Edito	ne followin intial corre esponds to tion of fea tional mo orial modif anations of GPP TR 2	ection) o a correcture), dification of the ab	ection in n of feat	ture)		elease	2	f the follown (GSM Pha (Release (Release (Release (Release (Release	ase 2) 1996) 1997) 1998) 1999)	ases:
Reason for change			nciple of m are us			hando	ver is	that	MSC-A is a	ware wha	t securi	ity
Summary of chang	ge: #											
Consequences if not approved:			A does n er the co						3 has chose	n or in the	worst	case
Clauses affected:	ж	2. 7.6	6, 8.4, 1 ⁻	7.7								
Other specs affected:	*	Oth	er core s	specifica	ations	ж						

All references to GSM 08.08 should be checked from the 3G TS 29.002

specification and changed to references to 3G TS 48.008.

O&M Specifications

Other comments:

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- [1] 3G TS 21.905: "3G Vocabulary".
- [2] GSM 02.01: "Digital cellular telecommunications system (Phase 2+); Principles of telecommunication services supported by a GSM Public Land Mobile Network (PLMN)".
- [3] 3G TS 22.002: "Bearer Services Supported by a GSM Public Land Mobile Network (PLMN)".
- [4] GSM 02.03: "Digital cellular telecommunications system (Phase 2+); Teleservices Supported by a GSM Public Land Mobile Network (PLMN)".
- [5] 3G TS 22.004: "General on Supplementary Services".
- [6] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".
- [7] 3G TS 22.016: "International Mobile station Equipment Identities (IMEI)".
- [8] 3G TS 22.041: "Operator Determined Barring".
- [9] 3G TS 22.081: "Line identification supplementary services Stage 1".
- [10] 3G TS 22.082: "Call Forwarding (CF) supplementary services Stage 1".
- [11] 3G TS 22.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services Stage 1".
- [12] 3G TS 22.084: "Multi Party (MPTY) Supplementary Services Stage 1".
- [13] 3G TS 22.085: "Closed User Group (CUG) supplementary services Stage 1".
- [14] 3G TS 22.086: "Advice of charge (AoC) Supplementary Services Stage 1".
- [15] 3G TS 22.088: "Call Barring (CB) supplementary services Stage 1".
- [16] 3G TS 22.090: "Unstructured Supplementary Service Data (USSD); Stage 1".
- [17] 3G TS 23.003: "Numbering, addressing and identification".
- [18] GSM 03.04: "Digital cellular telecommunications system (Phase 2+); Signalling requirements relating to routeing of calls to mobile subscribers".
- [19] 3G TS 23.007: "Restoration procedures".
- [20] 3G TS 23.008: "Organisation of subscriber data".
- [21] 3G TS 23.009: "Handover procedures".
- [22] 3G TS 23.011: "Technical realization of Supplementary Services General Aspects".
- [23] 3G TS 23.012: "Location registration procedures".
- [24] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".
- [25] 3G TS 23.038: "Alphabets and language".
- [26] 3G TS 23.040: "Technical realization of the Short Message Service (SMS) Point to Point (PP)".

[26a]	GSM 03.71: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Functional Description; Stage 2".
[27]	3G TS 23.081: "Line Identification Supplementary Services - Stage 2".
[28]	3G TS 23.082: "Call Forwarding (CF) Supplementary Services - Stage 2".
[29]	3G TS 23.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services - Stage 2".
[30]	3G TS 23.084: "Multi Party (MPTY) Supplementary Services - Stage 2".
[31]	3G TS 23.085: "Closed User Group (CUG) Supplementary Services - Stage 2".
[32]	3G TS 23.086: "Advice of Charge (AoC) Supplementary Services - Stage 2".
[33]	3G TS 23.088: "Call Barring (CB) Supplementary Services - Stage 2".
[34]	3G TS 23.090: "Unstructured Supplementary Services Data (USSD) - Stage 2".
[35]	3G TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols - Stage 3".
[36]	3G TS 24.010: "Mobile radio interface layer 3 Supplementary Services specification - General aspects".
[37]	3G TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".
[37a]	GSM 04.71: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 location services specification".
[38]	3G TS 24.080: "Mobile radio interface layer 3 supplementary services specification - Formats and coding".
[39]	3G TS 24.081: "Line identification supplementary services - Stage 3".
[40]	3G TS 24.082: "Call Forwarding (CF) Supplementary Services - Stage 3".
[41]	3G TS 24.083: "Call Waiting (CW) and Call Hold (HOLD) supplementary services - Stage 3".
[42]	3G TS 24.084: "Multi Party (MPTY) Supplementary Services - Stage 3".
[43]	3G TS 24.085: "Closed User Group (CUG) Supplementary Services - Stage 3".
[44]	3G TS 24.086: "Advice of Charge (AoC) Supplementary Services - Stage 3".
[45]	3G TS 24.088: "Call Barring (CB) Supplementary Services - Stage 3".
[46]	3G TS 24.090: "Unstructured Supplementary Services Data - Stage 3".
[47]	GSM 08.02: "Digital cellular telecommunications system (Phase 2+); Base Station System - Mobile-services Switching Centre (BSS - MSC) interface principles".
[48]	GSM 08.06: "Digital cellular telecommunications system (Phase 2+); Signalling transport mechanism specification for the Base Station System - Mobile-services Switching Centre (BSS - MSC) interface".
[49]	3G TS 48.008GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre - Base Station System (MSC - BSS) interface; Layer 3 specification".
[49a]	GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre—Base Station System (MSC—BSS) interface Layer 3 specification".

- [49a1] GSM 08.31: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre (SMLC) Serving Mobile Location Centre (SMLC); SMLC Peer Protocol (SMLCPP)".
- [49b] GSM 08.71: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre Base Station System (SMLC BSS) interface Layer 3 specification".

[50] GSM 09.01: "Digital cellular telecommunications system (Phase 2+); General network interworking scenarios". 3G TS 29.002: "Mobile Application Part (MAP) specification". [51] GSM 09.03: "Digital cellular telecommunications system (Phase 2+); Signalling requirements on [52] interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)". [53] GSM 09.04: "Digital cellular telecommunications system (Phase 2+); Interworking between the Public Land Mobile Network (PLMN) and the Circuit Switched Public Data Network (CSPDN)". [54] GSM 09.05: "Digital cellular telecommunications system (Phase 2+); Interworking between the Public Land Mobile Network (PLMN) and the Packet Switched Public Data Network (PSPDN) for Packet Assembly/Disassembly facility (PAD) access". [55] 3G TS 29.006: "Interworking between a Public Land Mobile Network (PLMN) and a Packet Switched Public Data Network/Integrated Services Digital Network (PSPDN/ISDN) for the support of Packet Switched data transmission services". [56] 3G TS 29.007: "Digital cellular telecommunications system (Phase 2+); General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)". GSM 09.08: "Digital cellular telecommunications system (Phase 2+); Application of the Base [57] Station System Application Part (BSSAP) on the E-interface". [58] 3G TS 29.010: "Information element mapping between Mobile Station - Base Station System and BSS - Mobile-services Switching Centre (MS - BSS - MSC) Signalling procedures and the Mobile Application Part (MAP)". [59] 3G TS 29.011: "Signalling interworking for Supplementary Services". GSM 09.31: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); [59a] Base Station System Application Part LCS Extension (BSSAP-LE)". [60] GSM 09.90: "Digital cellular telecommunications system (Phase 2+); Interworking between Phase 1 infrastructure and Phase 2 Mobile Stations (MS)". [61] GSM 12.08: "Digital cellular telecommunications system (Phase 2); Subscriber and Equipment Trace". ETS 300 102-1 (1990): "Integrated Services Digital Network (ISDN); User-network interface [62] layer 3 specifications for basic call control". [63] ETS 300 136 (1992): "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service description". ETS 300 138 (1992): "Integrated Services Digital Network (ISDN); Closed User Group (CUG) [64] supplementary service Digital Subscriber Signalling System No.one (DSS1) protocol". [65] ETS 300 287: "Integrated Services Digital Network (ISDN); Signalling System No.7; Transaction Capabilities (TC) version 2". [66] ETR 060: "Signalling Protocols and Switching (SPS); Guide-lines for using Abstract Syntax Notation One (ASN.1) in telecommunication application protocols". ITU-T Recommendation E.164: "Numbering plan for the ISDN era". [67] [68] ITU-T Recommendation E.212: "Identification plan for land mobile stations". [69] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land mobile stations". [70] ITU-T Recommendation E.214: "Structuring of the land mobile global title for the signalling connection control part". [71] CCITT Recommendation Q.699: "Interworking between the Digital Subscriber Signalling System

Layer 3 protocol and the Signalling System No.7 ISDN User part".

[72] ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Functional description of the Signalling Connection Control Part". ITU-T Recommendation Q.712: "Definition and function of SCCP messages". [73] ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; SCCP formats and [74] codes". [75] ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling Connection Control Part procedures". ITU-T Recommendation Q.716: "Specifications of Signalling System No.7; Signalling connection [76] control part (SCCP) performances". ITU-T Recommendation Q.721 (1988): "Specifications of Signalling System No.7; Functional [77] description of the Signalling System No.7 Telephone user part". [78] ITU-T Recommendation Q.722 (1988): "Specifications of Signalling System No.7; General function of Telephone messages and signals". [79] ITU-T Recommendation Q.723 (1988): "Specifications of Signalling System No.7; Formats and codes". [80] ITU-T Recommendation Q.724 (1988): "Specifications of Signalling System No.7; Signalling procedures". [81] ITU-T Recommendation Q.725 (1988): "Specifications of Signalling System No.7; Signalling performance in the telephone application". ITU-T Recommendation Q.761 (1988): "Specifications of Signalling System No.7; Functional [82] description of the ISDN user part of Signalling System No.7". [83] ITU-T Recommendation Q.762 (1988): "Specifications of Signalling System No.7; General function of messages and signals". [84] ITU-T Recommendation Q.763 (1988): "Specifications of Signalling System No.7; Formats and codes". [85] ITU-T Recommendation Q.764 (1988): "Specifications of Signalling System No.7; Signalling procedures". [86] ITU-T Recommendation Q.767: "Specifications of Signalling System No.7; Application of the ISDN user part of CCITT signalling System No.7 for international ISDN interconnections". [87] ITU-T Recommendation Q.771: "Specifications of Signalling System No.7; Functional description of transaction capabilities". ITU-T Recommendation Q.772: "Specifications of Signalling System No.7; Transaction [88] capabilities information element definitions". ITU-T Recommendation Q.773: "Specifications of Signalling System No.7; Transaction [89] capabilities formats and encoding". [90] ITU-T Recommendation Q.774: "Specifications of Signalling System No.7; Transaction capabilities procedures". ITU-T Recommendation Q.775: "Specifications of Signalling System No.7; Guide-lines for using [91] transaction capabilities". [92] ITU-T Recommendation X.200: "Reference Model of Open systems interconnection for CCITT Applications". [93] ITU-T Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)". [94] ITU-T Recommendation X.209 (1988): "Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)".

[95]	ITU-T Recommendation X.210: "Open systems interconnection layer service definition conventions".
[97]	3G TS 23.018: "Basic Call Handling".
[98]	3G TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2".
[99]	3G TS 23.079: "Support of Optimal Routeing (SOR) - Stage 2".
[100]	GSM 03.68: "Digital cellular telecommunications system (Phase 2+); - Stage 2".
[101]	GSM 03.69: "Digital cellular telecommunications system (Phase 2+); - Stage 2".
[102]	ANSI T1.113: "Signaling System No. 7 (SS7) - ISDN User Part".
[103]	3G TS 23.054 "Shared Inter Working Function (SIWF) - Stage 2".
[104]	3G TS 23.060: "General Packet Radio Service (GPRS) Description; Stage 2".
[105]	3G TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".
[106]	3G TS 29.018: "General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface layer 3 specification".
[107]	3G TS 23.093: "Technical Realization of Completion of Calls to Busy Subscriber (CCBS); Stage 2".
[108]	3G TS 23.066: "Support of Mobile Number Portability (MNP); Technical Realisation Stage 2".
[109]	ANSI T1.112 (1996): "Telecommunication – Signalling No. 7 - Signaling Connection Control Part (SCCP)".
[110]	3G TS 23.116: "Super-Charger Technical Realisation; Stage 2."
[111]	ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Signalling System No. 7 – Functional Description of the Signalling Connection Control Part".
[112]	ITU-T Recommendation Q.712: "Specifications of Signalling System No.7; Signalling System No. 7 – Definition and Function of SCCP Messages".
[113]	ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; Signalling System No. 7 – SCCP formats and codes".
[114]	ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling System No. 7 – Signalling Connection Control Part Procedures".
[115]	ITU-T Recommendation Q.716: "Specifications of Signalling System No.7; Signalling System No. 7 – Signalling Connection Control Part (SCCP) Performance".
[116]	ITU-T Q.850, May 1998: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".
[117]	3G TS 22.135: "Multicall; Service description; Stage 1".
[118]	3G TS 23.135: "Multicall supplementary service; Stage 2".
[119]	3G TS 24.135: "Multicall supplementary service; Stage 3".
[120]	3G TS 25.413: "UTRAN Iu Interface RANAP Signalling".

**** NEXT MODIFIED SECTION ****

7.6.6.13 Selected GSM Algorithm

**** NEXT MODIFIED SECTION ****

8.4.3 MAP_PROCESS_ACCESS_SIGNALLING service

8.4.3.1 Definition

This service is used between MSC-B and MSC-A (E-interface) to pass information received on the A-interface or Iuinterface in MSC-B to MSC-A.

The MAP_PROCESS_ACCESS_SIGNALLING service is a non-confirmed service using the primitives from table 8.4/3.

8.4.3.2 Service primitives

Table 8.4/3: MAP_PROCESS_ACCESS_SIGNALLING

Parameter name	Request	Indication
Invoke Id	M	M(=)
AN-APDU	M	M(=)
Selected GSM Algorithm	C	<u>C(=)</u>

8.4.3.3 Parameter use

Invoke Id

For definition of this parameter see subclause 7.6.1.

AN-APDU

For definition of this parameter see subclause 7.6.9.

Selected GSM algorithm

For definition of this parameter see subclause 7.6.6. This parameter shall be present if the encapsulated PDU is Security Mode Complete and MS is in GSM access.

**** NEXT MODIFIED SECTION ****

17.7 MAP constants and data types

17.7.1 Mobile Service data types

....

ProcessAccessSignalling-Arg ::=	[3] SEQUENCE {	
an-APDU	AccessNetworkSignalInfo,	
selectedGSM-Algorithm	<pre>[0] SelectedGSM-Algorithm</pre>	OPTIONAL,
extensionContainer	[1 0] ExtensionContainer	OPTIONAL,
}	_	

```
SelectedGSM-Algorithm ::= OCTET STRING (SIZE (1))

-- internal structure is coded as Algorithm identifier octet from Chosen Encryption

-- Algorithm defined in 3G TS 48.008

-- A node shall mark only the selected GSM algorithm
```