3GPP TSG-T#8
Düsseldorf, Germany, 21-23 June 2000

Tdoc TP-000073

Agenda Item: 6.2.3

Source: T2

Title: R99 Change Requests

Document for: Approval

Spec	CR	Rev	Phase	Subject	Cat	Vers-Curr	Vers-New	T2-Tdoc	Workitem
21.904	001		R99	Addition of reference measurement channel	F	3.0.1	3.1.0	T2-000270	UCR
21.904	002		R99	Correction of terminology	F	3.0.1	3.1.0	T2-000269	UCR
21.904	003		R99	Deletion of PCPCH/AICH timing relation	F	3.0.1	3.1.0	T2-000340	UCR
21.904	004		R99	Reflection of changes in core specification 24.008 to v3.3.1	F	3.0.1	3.1.0	T2-000268	UCR
21.904	005		R99	Reflection of document structure changes in core specifications and correction of editorial mistakes	F	3.0.1	3.1.0	T2-000267	UCR
23.040	012		R99	Alignment in Enhanced Messaging Service	F	3.4.0	3.5.0	T2-000319	EMS
23.040	014		R99	Correction to text on SMS TimeZone	F	3.4.0	3.5.0	T2-000311	TEI
23.040	015		R99	Correction of TP-PID	F	3.4.0	3.5.0	T2-000347	TEI
23.057	003		R99	Addition of phonebook entry and addition/modification of user data update for untrusted applications	F	3.1.1	3.2.0	T2-000307	MExE
23.057	004		R99	Editorial clarifications	F	3.1.1	3.2.0	T2-000298	MExE
23.057	005		R99	ME actions on SIM insertion and/or power up	F	3.1.1	3.2.0	T2-000304	MExE
23.057	006		R99	Client/Server 'negotiation'	F	3.1.1	3.2.0	T2-000295	MExE
23.057	007		R99	Third Party Root Public Key	F	3.1.1	3.2.0	T2-000296	MExE
23.057	008		R99	Third Party root public keys management	F	3.1.1	3.2.0	T2-000291	MExE
23.057	009		R99	User permission types (visual indication)	F	3.1.1	3.2.0	T2-000300	MExE
27.007	033		R99	+CSDF and +CCLK (4 digits for year field)	B	3.4.0	3.5.0	T2-000217	TEI
27.007	034		R99	APN presentation	F	3.4.0	3.5.0	T2-000337	TEI
27.007	035		R99	+CAJOIN also serves to join an ongoing group or a broadcast call	F	3.4.0	3.5.0	T2-000271	ASCI
27.007	036		R99	+CAULEV, the uplink status presentation in a Voice Group Call	F	3.4.0	3.5.0	T2-000287	ASCI
27.007	037		R99	CME ERROR extensions for ASCI Commands	F	3.4.0	3.5.0	T2-000286	ASCI
27.007	038		R99	Correction of the description of the +CRC	F	3.4.0	3.5.0	T2-000280	ASCI
27.007	039		R99	Definition of the abbreviation of MT	F	3.4.0	3.5.0	T2-000234	ASCI
27.007	040		R99	Packet Domain QoS AT-commands	F	3.4.0	3.5.0	T2-000330	TEI
27.103	001		R99	Introduction of push and target	F	3.0.0	3.1.0	T2-000351	SYNC

3GPP TSG T2/SMG4 Meeting #9
Utrecht, The Netherlands, 15-19 May 2000

***Document* T2-000270**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

21.904	CR	001	Current Version:	3.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: T2 **Date:** 17/05/2000

Subject: Addition of reference measurement channel

Work item: UE capability requirements

Category: *(only one category shall be marked with an X)*				**Release:**		
	F	Correction	X		Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
	B	Addition of feature			Release 97	
	C	Functional modification of feature			Release 98	
	D	Editorial modification			Release 99	X
					Release 00	

Reason for change: TS25.101 was changed in v3.2.0 so that additional reference measurement channel was added and TTI was specified. This change should be reflected to this report.

Clauses affected: Annex E1

Other specs affected:				
	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

E.1 Service implementation capabilities to facilitate conformance testing of Bearer Services capabilities

NOTE: Support of the following reference measurement channels is essential depending on the Bearer Services supported by a given terminal.

Terminal service implementation capabilities:

- Down-link reference measurement channel 64 kbps (FDD), TS 25.101 clause A.3.2.
- Down-link reference measurement channel 144 kbps (FDD), TS 25.101 clause A.3.3.
- Down-link reference measurement channel 384 kbps, -20ms TTI (FDD), TS 25.101 clause A.3.4.
- Down-link reference measurement channel 384 kbps (FDD), TS 25.101 clause A.3.5
- Down-link reference measurement channel 64 kbps (TDD), TS 25.102 clause A.2.3.
- Down-link reference measurement channel 144 kbps (TDD), TS 25.102 clause A.2.4.
- Down-link reference measurement channel 384 kbps (TDD), TS 25.102 clause A.2.5.

3GPP TSG T2/SMG4 Meeting #9
Utrecht, The Netherlands, 15-19 May 2000

***Document* T2-000269**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

21.904	CR	002	Current Version:	3.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: T2 **Date:** 17/05/2000

Subject: Correction of terminology

Work item: UE capability requirements

Category: *(only one category shall be marked with an X)*			**Release:**	
F	Correction	X	Phase 2	
A	Corresponds to a correction in an earlier release		Release 96	
B	Addition of feature		Release 97	
C	Functional modification of feature		Release 98	
D	Editorial modification		Release 99	X
			Release 00	

Reason for change: Term “Carrier raster” has been used in this report. However, “Channel raster” is used in core specifications (TS25.101, 102) instead.

Clauses affected: Annex A2

Other specs affected:			
Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:


help.doc

<--------- double-click here for help and instructions on how to create a CR.

A.2 RF Baseline Implementation Capabilities

Table 1: Void

Table 2: RF baseline implementation capabilities for FDD mode E: Essential Unconditional, C: Essential Conditional, O: Optional

Capability FDD	Specification	Subclause	UE	General Comments
Chiprate 3.84 Mcps	25.101	5.1	E	
Frequency bands – 1920-1980, 2110-2170 MHz – Other spectrum	25.101	5.2	 E O	 To allow for regional variations
TX-RX Freq. Sep: - 190 MHz – Variable	25.101	5.3	 E O	 To allow for regional variations.
~~Carrier~~ Channel raster:	25.101	5.4	E	
UE maximum output power	25.101	6.2.1	E	
Output RF spectrum Emissions	25.101	6.6	E	

Table 3: RF baseline implementation capabilities for TDD mode

Capability TDD	Specification	Subclause	UE	General Comments
Chiprate 3.84 Mcps	25.102	5.1	E	
Frequency bands – 1900-1920 MHz – 2010-2025 MHz – Other spectrum	25.102	5.2	 E E O	 To allow for regional variations.
~~Carrier~~ Channel raster:	25.102	5.4	E	
UE maximum output power	25.102	6.2.1	E	
Output RF spectrum Emissions	25.102	6.6	E	

3GPP TSG T2/SMG4 Meeting #9
Utrecht, The Netherlands, 15-19 May 2000

Document T2-000340
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

21.904	CR	003	Current Version:	3.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 17/05/2000

Subject: Deletion of PCPCH/AICH timing relation

Work item: UE capability requirements

Category: *(only one category shall be marked with an X)*

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change: PCPCH/AICH timing relation (TS25.211 v3.2.0 Clause 7.4) is not required to support Physical Channels listed in A3.

Clauses affected: Annex A3

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:	
Other GSM core specifications	[ ]	→ List of CRs:	
MS test specifications	[ ]	→ List of CRs:	
BSS test specifications	[ ]	→ List of CRs:	
O&M specifications	[ ]	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

A.3 Physical Layer baseline implementation capabilities

Table 4: FDD mode Physical Layer Baseline implementation capabilities

Baseline Implementation Capability[1]	Specification	Subclause(s)	Comments
Physical Layer UE procedures and measurements:			
Support for network and access node selection	25.214	4.1, 4.2	Cell search and synchronisation
Measurements for Cell selection and reselection	25.215	5.1.1, 5.1.2, 5.1.5, 5.1.7, 5.1.11, 5.1.12	The Measurement in 5.1.2 is essential on the condition that the UE is dual mode FDD-TDD CPICH RSCP measurement
Support for network contact and registration	25.214	6.1	Random access procedure
Power control	25.214 25.215	5.1.1, 5.2.3 5.1	Open Loop PC for PRACH RSCP, SIR measurement
Channel Coding & Multiplexing	25.212	4.1, 4.2	Only support of Convolutional coding is Essential for all terminals. Turbo coding is not Essential.
Spreading and Scrambling Code Generation	25.213 25.926	4.1, 4.2.2, 4.3.1, 4.3.2, 4.3.3 5	Code allocation for PRACH Long scrambling code Scrambling code for PRACH message PRACH preamble codes For the uplink, a baseline capable UE is required to suppor a spreading factor of 256.
Code de-spreading and de-scrambling	25.213 25.926	5.1 5.2 5	
Modulation	25.213	4.4	
De-modulation	25.213	5.3	
Support for downlink Transmit Diversity	25.211	5.3.1, 5.3.3	Open Loop mode Tx diversity is essential to support baseline capability
Transport channels necessary for the above:			
Broadcast channel (BCH)	25.211	4.2.1	
Paging channel (PCH)	25.211	4.2.3	PCH is required to transport notification of a change in system information carried on BCCH.
Random access channel (RACH)	25.211	4.2.4	

1 All the baseline implementation capabilities for the FDD mode physical layer should be considered as essential for the terminal.

Forward access channel (FACH)	25.211	4.2.2	
Transport Format Combination Indicator (TFCI)	25.212	4.3.2, 4.3.3, 4.3.5.1	
Physical channels necessary for above:			
Timing relation	25.211	7.1, 7.2, 7.3, ~~7.4~~	
Common Pilot Channel (CPICH)	25.211	5.3.3.1	Primary CPICH
Primary Common Control Physical Channel (P-CCPCH)	25.211	5.3.3.2	
Secondary Common Control Physical Channel (S-CCPCH)	25.211	5.3.3.3	
Physical Random Access Channel (PRACH)	25.211	5.2.2.1	
Synchronisation Channel (SCH)	25.211	5.3.3.4	
Acquisition Indicator Channel (AICH)	25.211	5.3.3.6	

3GPP TSG-T2 meeting #9
Utrecht, The Netherlands, 15-19 May 2000

Document *T2- 000268*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

21.904	**CR**	**004**	Current Version:	3.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	Strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 17/05/2000

Subject: Reflection of changes in core specification 24.008 to v3.3.1

Work item: UE capability requirements

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: To reflect changes made to core specifications 24.008 v3.3.1 from v3.2.1 which were approved in March '00.

Clauses affected: Annex A.5

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

A.5 Layer 3 baseline implementation capabilities (non-access stratum)

Table 7: UE Baseline Implementation Capabilities for NAS
E: Essential Unconditional, C: Essential Conditional, O: Optional

Baseline Implementation Capabilities			Ref. Doc	Subclause(s)	Kind of UEs			Comments
					CS-only	PS-only	CS+PS	
UMTS CS mobility management (Optional)	MM common procedures	TMSI reallocation procedure	24.008	4.3.1	E	-	E	
		Authentication procedure	24.008	4.3.2	E	-	E	
		Identification procedure	24.008	4.3.3	E	-	E	
		IMSI detach procedure	24.008	4.3.4	E	-	E	
		Abort procedure	24.008	4.3.5	E	-	E	
		MM information procedure	24.008	4.3.6	O	-	O	
	MM specific procedure	Location updating procedure	24.008	4.4.1	E	-	E	
		Periodic updating	24.008	4.4.2	E	-	E	
		IMSI attach procedure	24.008	4.4.3	E	-	E	
		Generic Location Updating procedure	24.008	4.4.4	E	-	E	
		Core Network System Information	24.008	4.4.5	E		E	
		Paging response	24.008	4.4.6	E		E	
	MM connection management procedure	MM connection establishment initiated the mobile station	24.008	4.5.1.1	E	-	E	
		MM connection establishment for emergency calls	24.008	4.5.1.5	C	-	C	Essential If speech calls supported.
		~~Paging response procedure~~	~~04.18~~	~~3.3.2~~	~~E~~	~~-~~	~~E~~	
		MM connection establishment initiated by the network	24.008	4.5.1.3	O	-	O	
		MM connection release	24.008	4.5.3	E	-	E	
UMTS PS mobility management (Optional)	GMM common procedures	P-TMSI reallocation procedure	24.008	4.7.6	-	E	E	
		Authentication and ciphering procedure	24.008	4.7.7	-	E	E	
		Identification procedure	24.008	4.7.8	-	E	E	
		Paging procedure	24.008	4.7.9	-	E	E	
		Receiving a GMM Status message	24.008	4.7.10	-	E	E	
		~~GMM support for anonymous access~~	~~24.008~~	~~4.7.11~~	~~-~~	~~O~~	~~O~~	~~Note: This item has been deleted as a result of a decision made after Decemeber 1999~~
		GMM Information procedure	24.008	4.7.12	-	O	O	
		Service request procedure	24.008	4.7.13	-	E	E	
		Core Network System Information	24.008	4.7.14	-	E	E	

Baseline Implementation Capabilities			Ref. Doc	Subclause(s)	Kind of UEs			Comments
					CS-only	PS-only	CS+PS	
	GMM specific procedure	Intersystem change between GSM and UMTS	24.008	4.7.1.7	-	C	C	
		GPRS attach procedure	24.008	4.7.3.1	-	E	E	
		Combined GPRS attach procedure	24.008	4.7.3.2	-	-	C	Essential If class-A or B.
		MS initiated GPRS detach procedure	24.008	4.7.4.1	-	E	E	
		MS initiated Combined GPRS detach procedure	24.008	4.7.4.1.3	-	-	C	Essential If class-A or B.
		Network initiated GPRS detach procedure	24.008	4.7.4.2	-	E	E	
		Normal and periodic routing area updating Procedure	24.008	4.7.5.1	-	E	E	
		Combined routing area updating Procedure	24.008	4.7.5.2	-	-	C	Essential If class-A or B.
		~~Selective routing area updating procedure~~	~~24.008~~	~~4.7.5.3~~		~~C~~	~~C~~	~~Essential for dual mode UMTS-GSM terminals~~

3GPP TSG-T2 meeting #9
Utrecht, The Netherlands, 15-19 May 2000

Document *T2- 000267*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TR21.904	CR	005	Current Version:	3.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 17/05/2000

Subject: Reflection of document structure changes in core specifications and correction of editorial mistakes

Work item: UE capability requirements

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: To reflect changes in document structures made to core specifications which were approved in March '00. Some other editorial changes are also added.

Clauses affected: Annex A, B, C, D, E, F, G, H

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

Annex A:
Baseline Implementation Capabilities

The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

A.1 Baseline implementation capabilities to facilitate conformance testing

UE baseline implementation capabilities:

- The special conformance testing functions and the logical test interface as specified in TS 34.109.
- Up-link reference measurement channel 12.2 kbps (FDD), TS 25.101 clause A.2.1.
- Down-link reference measurement channel 12.2 kbps (FDD), TS 25.101 clause A.3.1.
- Up-link reference measurement channel 12.2. kbps (TDD), TS 25.102 clause A.2.1.
- Down-link reference measurement channel 12.2 kbps (TDD), TS 25.102 clause A.2.2.

A.2 RF Baseline Implementation Capabilities

Table 1: Void

Table 2: RF baseline implementation capabilities for FDD mode
E: Essential Unconditional, C: Essential Conditional, O: Optional

Capability FDD	Specification	Subclause	UE	General Comments
Chiprate 3.84 Mcps	25.101	5.1	E	
Frequency bands – 1920-1980, 2110-2170 MHz – Other spectrum	25.101	5.2	 E O	 To allow for regional variations
TX-RX Freq. Sep: - 190 MHz – Variable	25.101	5.3	 E O	 To allow for regional variations.
Carrier raster:	25.101	5.4	E	
UE maximum output power	25.101	6.2.1	E	
Output RF spectrum Emissions	25.101	6.6	E	

Table 3: RF baseline implementation capabilities for TDD mode

Capability TDD	Specification	Subclause	UE	General Comments
Chiprate 3.84 Mcps	25.102	5.1	E	
Frequency bands – 1900-1920 MHz – 2010-2025 MHz – Other spectrum	25.102	5.2	 E E O	 To allow for regional variations.
Carrier raster:	25.102	5.4	E	
UE maximum output power	25.102	6.2.1	E	
Output RF spectrum Emissions	25.102	6.6	E	

A.3 Physical Layer baseline implementation capabilities

Table 4: FDD mode Physical Layer Baseline implementation capabilities

Baseline Implementation Capability[1]	Specification	Subclause(s)	Comments
Physical Layer UE procedures and measurements:			
Support for network and access node selection	25.214	4.1, 4.2	Cell search and synchronisation
Measurements for Cell selection and reselection	25.215	5.1.1, 5.1.2, 5.1.4, 5.1.6, 5.1.9, 5.1.10 ~~5.1.5, 5.1.7, 5.1.11, 5.1.12~~	The Measurement in 5.1.2 is essential on the condition that the UE is dual mode FDD-TDD CPICH RSCP measurement
Support for network contact and registration	25.214	6.1	Random access procedure
Power control	25.214 25.215	5.1.1, 5.2.3 5.1	Open Loop PC for PRACH RSCP, SIR measurement
Channel Coding & Multiplexing	25.212	4.1, 4.2	Only support of Convolutional coding is Essential for all terminals. Turbo coding is not Essential.
Spreading and Scrambling Code Generation	25.213 25.926	4.1, 4.2.2, 4.3.1, 4.3.2, 4.3.3 5	Code allocation for PRACH Long scrambling code Scrambling code for PRACH message PRACH preamble codes For the uplink, a baseline capable UE is required to support a spreading factor of 256.
Code de-spreading and de-scrambling	25.213 25.926	5.1 5.2 5	
Modulation	25.213	4.4	
De-modulation	25.213	5.3	
Support for downlink Transmit Diversity	25.211	5.3.1, 5.3.3	Open Loop mode Tx diversity is essential to support baseline capability
Transport channels necessary for the above:			
Broadcast channel (BCH)	25.211	4.2.1	
Paging channel (PCH)	25.211	4.2.3	PCH is required to transport notification of a change in system information carried on BCCH.
Random access channel (RACH)	25.211	4.2.4	
Forward access channel (FACH)	25.211	4.2.2	
Transport Format Combination Indicator (TFCI)	25.212	4.3.2, 4.3.3, 4.3.5.1	
Physical channels necessary for above:			
Timing relation	25.211	7.1, 7.2, 7.3, 7.4	
Common Pilot Channel (CPICH)	25.211	5.3.3.1	Primary CPICH
Primary Common Control Physical Channel (P-CCPCH)	25.211	5.3.3.2	
Secondary Common Control Physical Channel (S-CCPCH)	25.211	5.3.3.3	
Physical Random Access Channel (PRACH)	25.211	5.2.2.1	

1 All the baseline implementation capabilities for the FDD mode physical layer should be considered as essential for the terminal.

Synchronisation Channel (SCH)	25.211	5.3.3.4	
Acquisition Indicator Channel (AICH)	25.211	5.3.3.6	

Table 5: TDD mode Physical Layer Baseline Implementation Capabilities

Baseline Implementation Capability[2]	**Specification**	**Subclause(s)**	**Comments**
Physical Layer UE procedures and measurements:			
Support for network and access node selection	25.224	6.5, 6.6	
Cell selection and reselection	25.225	6.1.1, 6.1.3, 6.1.5, 6.1.9, 7.1.1.1	
Support for network contact and registration	25.224	6.4	
Power control	25.224	6.3.3.1	
Channel Coding	25.222	6.1, 6.2	Convolutional coding is essential to support the baseline functionality.
Spreading and Scrambling Code Generation	25.223	6, 7	
Code de-spreading and de-scrambling	25.223	6, 7	
Modulation	25.223	5	
Support for downlink Transmit Diversity	25.221	6.8	
Transport channels necessary for the above:			
Synchronisation channel (SCH)	25.221	4.1.2	SCH exists for TDD mode only
Broadcast channel (BCH)	25.221	4.1.2, 6	
Paging channel (PCH)	25.221	4.1.2, 6	PCH is required to transport notification of a change in system information carried on BCCH.
Random access channel (RACH)	25.221	4.1.2, 6	
Forward access channel (FACH)	25.221	4.1.2, 6	
Physical channels necessary for above:			
Common Control Physical Channel (CCPCH)	25.221	5.3.1, 6	
Physical Random Access Channel (PRACH)	25.221	5.3.2, 6	
Physical Synchronisation Channel (PSCH)	25.221	5.4, 6	

[2] All the baseline implementation capabilities for the TDD mode physical layer should be considered as essential for the terminal.

A.4 Layer 2/3 baseline implementation capabilities (access stratum)

Table 6: Baseline implementation capabilities for Layer 2/3 (access stratum)

Baseline Implementation Capability[3]	**Specification**	**Subclause(s)**	**Comments**
UE procedures:			
The procedures below require support of the RLC protocol described in 25.322, with the exception of RLC header compression.			
Support for PLMN selection Support for location registration	25.304	5.1, 5.4, 10.4, 10.5, 10.6, 10.7	
Cell selection and reselection	25.304	5.2, 10.8	
System information reception	25.304 25.331	6.1, 10.1, 10.2 8.1.1, 10.2.49, 10.2.50, 10.3.8.1, ~~10.1.3,~~ ~~10.1.6~~	The following messages are required: - System information message - BCCH modification info" in the Paging type 1 message - System Information Change Indication message
Paging	25.303 25.304 25.331	6.5, 6.6 8, 10.3 8.1.2, ~~10.1.3.1,~~ ~~10.1.3.2~~10.2.16, 10.2.17	The following message are required: - Paging type 2 message - Paging type 1 message
Idle mode measurements procedure	25.304	7	
RRC connection establishment	25.303 25.331	6.1.1 8.1.3, ~~10.1.4.6,~~ ~~10.1.4.7,~~ ~~10.1.4.8,~~ ~~10.1.4.9~~10.2.38, 10.2.41, 10.2.42, 10.2.43	The following messages are required: - RRC connection request message - RRC connection set up message - RRC connection set-up complete message - RRC connection reject message
RRC Status	25.331	~~10.1.7.7~~10.2.44	The following message is required: - RRC status message
RRC connection release	25.303 25.331	6.1.3 8.1.4, ~~10.1.4.4,~~ ~~10.1.4.5~~10.2.39, 10.2.40	The following messages are required: - RRC connection release message - RRC connection release complete message
Support for higher layer messages on signalling connection	25.303	6.1.2	
Initial Direct transfer	25.331	8.1.8 ~~10.1.7.4~~10.2.10	The following message is required: - Initial Direct transfer message
Downlink Direct transfer	25.331	8.1.9 ~~10.1.7.8~~10.2.6	The following messages are required: - Downlink Direct transfer message
Uplink Direct transfer	25.331	8.1.10 ~~10.1.7.9~~10.2.59	The following message - Uplink Direct transfer message

[3] All the baseline implementation capabilities for L2/3 should be considered as essential for the terminal.

Cell update	25.303 25.331	6.4.2 ~~10.1.1.4~~10.2.4, ~~10.1.1.5~~10.2.5, ~~10.1.1.13~~10.2.33	The following messages are required: - Cell update message - Cell update confirm message - RNTI reallocation complete message
UE capability	25.303 25.331	6.7.1 8.1.6 10.2.56~~10.1.54~~ 10.2.57~~10.1.55~~ 10.2.58~~10.1.56~~	The following messages are required: - UE capability enquiry message - UE capability information message - UE capability information confirm message
Security mode control	25.331	8.1.12 10.2.45~~10.1.7.5,~~ 10.2.46~~10.1.7.6~~	The following messages are required: - Security mode command message - Security mode complete message
RNTI reallocation	25.331	8.3.3 10.2.32~~10.1.31~~ 10.2.33~~10.1.32~~	The following messages are required: - RNTI reallocation message - RNTI reallocation complete message
Measurement control	25.331	8.4.1 8.4.2 ~~10.1.12~~10.2.13 ~~10.1.13~~10.2.14 ~~10.1.14~~10.2.15	The following messages are required: - Measurement control message - Measurement control failure message - Measurement report message
Logical channels necessary for the above procedures:			
Synchronisation control channel (SCCH)	25.301	5.3	SCCH exists for TDD mode only
Broadcast control channel (BCCH)	25.301 ~~25.321~~	5.3 ~~9.2.1.2~~	BCCH is mapped to BCH. No MAC header is required.
Paging control channel (PCCH)	25.301	~~6.3~~5.3	PCCH is needed for notification of the change in system information on BCCH. It may also be needed by the CN MM protocol for reasons other than UE terminated services. There is no Mac header for PCCH.
Common control channel (CCCH)	25.301 25.321	5.3 9.2.1.4	MAC-PDU for mapping CCCH to RACH/FACH
Dedicated control channel (DCCH)	25.301 25.321	5.3 9.2.1.1	MAC-PDU for mapping DCCH to RACH/FACH
Transport channels necessary for the above procedures			
Synchronisation channel (SCH)	25.301	5.2	SCH exists for TDD mode only
Broadcast channel (BCH)	25.301	5.2	
Paging channel (PCH)	25.301	5.2	
Random access channel (RACH)	25.301 25.321	5.2 11.2	RACH transmission procedure
Forward access channel (FACH)	25.301	5.2	

A.5 Layer 3 baseline implementation capabilities (non-access stratum)

Table 7: UE Baseline Implementation Capabilities for NAS E: Essential Unconditional, C: Essential Conditional, O: Optional

Baseline Implementation Capabilities			Ref. Doc	Subclause(s)	Kind of UEs			Comments
					CS-only	PS-only	CS+PS	
UMTS CS mobility management (Optional)	MM common procedures	TMSI reallocation procedure	24.008	4.3.1	E	-	E	
		Authentication procedure	24.008	4.3.2	E	-	E	
		Identification procedure	24.008	4.3.3	E	-	E	
		IMSI detach procedure	24.008	4.3.4	E	-	E	
		Abort procedure	24.008	4.3.5	E	-	E	
		MM information procedure	24.008	4.3.6	O	-	O	
	MM specific procedure	Location updating procedure	24.008	4.4.1	E	-	E	
		Periodic updating	24.008	4.4.2	E	-	E	
		IMSI attach procedure	24.008	4.4.3	E	-	E	
		Generic Location Updating procedure	24.008	4.4.4	E	-	E	
	MM connection management procedure	MM connection establishment initiated the mobile station	24.008	4.5.1.1	E	-	E	
		MM connection establishment for emergency calls	24.008	4.5.1.5	C	-	C	Essential If speech calls supported.
		Paging response procedure	04.18	3.3.2	E	-	E	
		MM connection establishment initiated by the network	24.008	4.5.1.3	O	-	O	
		MM connection release	24.008	4.5.3	E	-	E	
UMTS PS mobility management (Optional)	GMM common procedures	P-TMSI reallocation procedure	24.008	4.7.6	-	E	E	
		Authentication and ciphering procedure	24.008	4.7.7	-	E	E	
		Identification procedure	24.008	4.7.8	-	E	E	
		Paging procedure	24.008	4.7.9	-	E	E	
		Receiving a GMM Status message	24.008	4.7.10	-	E	E	
		GMM support for anonymous access	24.008	4.7.11	-	O	O	Note: This item has been deleted as a result of a decision made after Decemeber 1999
		GMM Information procedure	24.008	4.7.12	-	O	O	
		Service request procedure	24.008	4.7.13	-	E	E	
	GMM specific procedure	GPRS attach procedure	24.008	4.7.3.1	-	E	E	
		Combined GPRS attach procedure	24.008	4.7.3.2	-	-	C	Essential If class-A or B.
		MS initiated GPRS detach procedure	24.008	4.7.4.1	-	E	E	
		MS initiated Combined GPRS detach procedure	24.008	4.7.4.1.3	-	-	C	Essential If class-A or B.
		Network initiated GPRS detach procedure	24.008	4.7.4.2	-	E	E	

Baseline Implementation Capabilities			Ref. Doc	Subclause(s)	Kind of UEs			Comments
					CS-only	PS-only	CS+PS	
		Normal and periodic routing area updating Procedure	24.008	4.7.5.1	-	E	E	
		Combined routing area updating Procedure	24.008	4.7.5.2	-	-	C	Essential If class-A or B.
		Selective routing area updating procedure	24.008	4.7.5.3		C	C	Essential for dual mode UMTS-GSM terminals

A.6 Security baseline implementation capabilities

Table 8: UE Baseline Implementation Capabilities in the security domain

Security feature			Essential/optional capabilities	Subclause In TS 33.102
User Identity Confidentiality			-----	5.1.1
	Identification by temporary identities and confidential transport of other USIM information.		<Essential Unconditional>	6.1
	Identification by a permanent identity *Note: This functionality is implemented in the USIM and is transparent to the UE.*	Use of IMUI and other USIM information in cleartext	<Essential Unconditional>	6.2
		Transport of an encrypted IMUI and other USIM information.	<Essential Unconditional> *Note: The use of the enhanced mechanism is detemined by the HE.*	6.2
Entity Authentication			-----	5.1.2
	Authentication and key agreement	The authentication and key agreement protocol	<Essential Unconditional>	6.3
		Authentication and key agreement algorithms. *Note: Algorithms are implemented on the USIM.*	<Optional> *Note: The algorithms are determined by the HE.*	
Confidentiality			-----	5.1.3
	Access Link Data confidentiality		<Essential Unconditional>	6.6
	Encryption indication		<Essential Unconditional>	5.5
Hooks for network wide encryption			<Essential Unconditional>	~~8.2~~5.4.2, 6.7
Data integrity			-----	5.1.4
	Access link data integrity		<Essential Unconditional>	6.5
Mobile Equipment Identification			<Essential Unconditional> *Note: Includes capability of having IMEI and capability of reporting it to the network.*	5.1.5
User-to-USIM Authentication			<Essential Unconditional>	5.3.1
USIM-Terminal Link			<Optional>	5.3.2
Secure messaging between the USIM and the network			<Optional> *Note: Security features are HE and application specific*	5.4.1, 8.1
Interoperation between 3GPP and GSM systems			<Essential Conditional> UEs that support GSM SIM or a GSM SIM application on the UICC shall include functions that allow conversion of security parameters from GSM to UMTS to access a 3G system. <Essential Conditional> 3G/GSM dual system terminals shall use the GSM security parameters derived through a conversion function in the USIM application with files required for GSM access when they access to GSM system. If this is not available, a GSM SIM application on the UICC or 2G chip card shall be used.	6.8.1 6.8.2

A.7 USIM baseline implementation capabilities

Table 9: Baseline Implementation Capabilities in the USIM domain

Baseline Implementation Capability	**Specification**	**Clause(s)**	**Essential/Optional** **Comments**
Physical Characteristics			
Support for the card sizes; “ID-1 UICC” and/or “Plug-in UICC”	31.101	4.1, 4.2	<Essential Unconditional>
Provisions of Contacts	31.101	4.4	<Essential Unconditional>
Electrical specifications of the UICC – Terminal interface			
Support for electrical specifications; 3V and 1.8V	31.101	5	<Essential Unconditional>
Initial communication establishment procedures			
Initial communication establishment procedures	31.101	6	<Essential Unconditional>
Protocols			
Transmission protocols T=0 and T=1	31.101	7	<Essential Unconditional> T=0 and T=1 are essential for the Terminal. T=0 is essential for the UICC. <Optional> T=1 is optional for the UICC.
Structure of commands and responses	31.101.	10	<Essential Unconditional>
Generic commands	31.101	11.1	<Essential Unconditional>
Transmission oriented commands	31.101	12	<Essential Unconditional>
Application independent protocol	31.101	14	<Essential Unconditional>
Application independent procedures			
Procedures from USIM initialisation to network registration	31.102	5.1, 5.2	<Essential Unconditional> Capabilities to access the related files with network registration (ex. Files which contain IMSI, RACH access control parameters, forbidden PLMNs and location area information)
Subscription related procedures	31.102	5.3	<Essential Conditional>
Security features			
Authentication and Key agreement procedure	31.102	6.1	<Essential Unconditional>
USIM commands	31.102	7	<Essential Unconditional> Except Subclause 7.1.1.2 <Essential Conditional> Subclause 7.1.1.2 GSM security context Capabilities to access 2G network

Annex B:
Speech Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support the default speech service. The references in this annex are to 3GPP documents agreed for release '99 in March~~December~~ 2000~~1999~~. The referenced section numbers may change with future versions.

B.1 Physical layer implementation capabilities to support the default speech service

Table 10: FDD mode Physical Layer Service implementation capabilities for support of AMR speech service

Service Implementation Capability	Specification	Subclause(s)	Comments
Physical Layer UE procedures and measurements:			
Support of Handover	25.215 25.212	5.1, 6.1 4.4	Support of soft handover is Essential for all speech capable UE. Support of Inter-Frequency handover is Essential for all speech capable UE. Terminals shall support measurements commensurate with their mode/system capabilities, to facilitate inter-frequency, inter-mode & inter-system handover.
Power control	25.214 25.215	5.1.2, 5.2.1 ~~5.1.8, 5.1.9~~5.1.7	Support of closed loop power control is Essential for all speech capable UE. ~~Note: Physical channel BER measurement in 25.215 subclause 5.1.9 is not required according to decision made after December 1999.~~
Error detection	25.212	4.2.1	Support of 0, 8, 12 and 16 bits CRC per transport block is essential for all UE. Support of 24 bits CRC per transport block is optional.
Channel Coding	25.212	4.2.3	Support of no coding and convolutional coding with rates ½ and 1/3 is essential for all UE.
Multiplexing	25.212 25.926	4.2.4 – 4.2.14 5.1	Uplink. In single service case, with only AMR and a dedicated signalling channel, it is Essential for all terminals to support at minimum 4 transport channels in uplink, of which 1-3 is reserved for AMR and 1 for dedicated signalling. Support of TTI=20 ms for all AMR transport channels except dedicated signalling channel is Essential for all terminals. Downlink In single service case, with only AMR and a dedicated signalling channel, it is Essential for all terminals to support at minimum 4 transport channels in downlink, of which 1-3 is reserved for AMR and 1 for dedicated signalling. Support of TTI=20 ms for all AMR transport channels except dedicated signalling channel is Essential for all terminals.

Service Implementation Capability	Specification	Subclause(s)	Comments
Transport format detection	25.212 25.926	4.3 5.1	In downlink, the support of transport format detection with TFCI is essential for all terminals both with fixed and flexible TrCH positions. In downlink, when SF=128 and fixed TrCH positions is used in the single service case, with only AMR and dedicated signalling channel, the support of blind transport format detection is essential for all terminals. In the single service case, with only AMR and dedicated signalling channel, it is essential for all terminals to support at minimum 2*(8+1+1)=20 transport format combinations during the connection in uplink and downlink, of which 8 is reserved for AMR modes, 1 for SID frame, 1 for DTX and the multiplication of 2 is due to dedicated signalling channel having two possible rates (e.g. on/off).
Spreading and Scrambling Code Generation	25.213	4.2.1, 4.3	For the single service case, with only AMR and dedicated signalling channel, it is essential for all terminals to support SF=256, SF=128 and SF=64 in uplink.
Code de-spreading and de-scrambling	25.213	5.1, 5.2	It is essential for all terminals to support SF=128 and SF=256 in downlink
Support for downlink Transmit Diversity	25.211 25.214	5.3.1, 5.3.2 ~~8~~7	Support of open loop and closed loop transmit diversity is Essential for all terminals.
Support for Site Selection Diversity Transmission	25.214	5.2.1.4	Support of SSDT is Essential for all terminals.
Transport channels required:			
Dedicated channel (DCH)	25.211	4.1.1, 6	
Physical channels required:			
Dedicated Physical Data Channel (DPDCH)	25.211	5.2.1, 5.3.2, 6	
Dedicated Physical Control Channel (DPCCH)	25.211	5.2.1, 5.3.2, 6	

Table 11: TDD mode Physical Layer Service implementation capabilities for support of the AMR speech service

Service Implementation Capability	Specification	Sub/Clause(s)	Comments
Physical Layer UE procedures and measurements:			
Handover	25.225	5	Support of Intra and Inter Frequency hard handover is essential for all terminals. Terminals shall support measurements commensurate with their mode/system capabilities, to facilitate inter-frequency, inter-mode & inter-system handover.
Dynamic Channel Allocation	25.225	5	Terminals shall support measurement of SIR in different timeslots.
Power control	25.224 25.225	4.3 5	Support of closed loop control for DL power. Support of open loop control for UL power.
Error detection	25.222	6.2.1	Support of 0, 8, 12 and 16 bits CRC per transport block is essential for all terminals
Channel Coding	25.222	6.2.3	Support of no coding and convolutional coding with rates ½ and 1/3 is essential for all terminals.
Multiplexing	25.222 25.926	6.2.4 – 6.2.13 5.1	Uplink. In single service case, with only AMR and dedicated signalling channel, it is essential for all terminals to support at minimum 4 transport channels in uplink, of which 1-3 is reserved for AMR and 1 for dedicated signalling. Downlink. In single service case, with only AMR and dedicated signalling channel, it is essential for all terminals to support at minimum 4 transport channels in downlink, of which 1-3 is reserved for AMR and 1 for dedicated signalling. <Note: This assumes that fast mode control is required to be signalled in the downlink direction only. >
Transport format detection	25.222 25.926	6.2.13 5.1	The support of transport format detection with a TFCI length of 0, 4, 8, 16 and 32 bits is essential for all terminals. Support of 1024 transport format combinations is essential for all terminals
Spreading and Scrambling Code Generation	25.223	6	Terminals shall support spreading factors 8 and 16 for uplink transmission. Simultaneous transmission of up to two codes shall be supported.
Code de-spreading and de-scrambling	25.223	6	Terminals shall support simultaneous reception of up to 2 codes using spreading factor 16 for speech.
Support for Downlink Transmit diversity	25.221 25.224	5.2.4 4.8	Support channel estimation on different midambles
Timing Advance	25.224	4.4	Support of TA adjustment according to higher layer signalling
Discontinuous transmission	25.224	4.7	Each mobile must be capable to switch of transmission in those physical channels which are not needed to transmit the instantaneous TFC.
Transport channels necessary for the above:			
DCH	25.221	4.1.1, 6	
Physical channels necessary for above:			
Dedicated Physical Channel (DPCH)	25.221	5.2, 6	

B.2 Layer 2/3 Implementation Capabilities to support the default speech service

Table 12: Speech Service Implementation Capability for Layer 2/3 (access stratum)

Service Implementation Capability	Specification	Subclause(s)	Comments
UE procedures:			
RRC connection re-establishment	25.331	8.1.5 ~~10.1.4.1~~10.2.35, ~~10.1.4.2~~10.2.36, ~~10.1.4.3~~10.2.37	The following messages are required: - RRC connection re-establishment message - RRC connection re-establishment complete message - RRC connection re-establishment request message
Radio bearer establishment	25.303 25.331	6.2.1.1 8.2.1 ~~10.1.28~~10.2.29 ~~10.1.29~~10.2.30 ~~10.1.30~~10.2.31	The following messages are required~~The required messages are~~: - Radio Bearer Setup message - Radio Bearer Setup Complete message - Radio Bearer Setup Failure message
Radio bearer reconfiguration	25.303 25.331	~~6.2.1.2~~6.2.1.3 8.2.2 ~~10.1.22~~10.2.23 ~~10.1.23~~10.2.24 ~~10.1.24~~10.2.25	The following message are required: - Radio Bearer Reconfiguration message - Radio Bearer Reconfiguration complete message - Radio Bearer Reconfiguration Failure message
Radio bearer release	25.303 25.331	~~6.2.1.3~~6.2.1.2 8.2.3 ~~10.1.2~~10.2.26 ~~10.1.26~~10.2.27 ~~10.1.27~~10.2.28	The following messages are required: - Radio Bearer Release message - Radio Bearer Release Complete message - Radio Bearer Release Failure message
Transport channel reconfiguration	25.303 25.331	6.2.2 8.2.4 ~~10.1.49~~10.2.51 ~~10.1.50~~10.2.52 ~~10.1.51~~10.2.53	The following messages are required: - Transport channel reconfiguration message - Transport channel reconfiguration complete message - Transport channel reconfiguration failure message
Transport format combination control	25.303 25.331	6.2.4 8.2.5 ~~10.1.52~~10.2.54 ~~10.1.53~~10.2.55	The following messages are required: - Transport format combination control message - Transport format combination control failure message

Service Implementation Capability	Specification	Subclause(s)	Comments
UE procedures:			
Physical channel reconfiguration	25.303 25.331	6.2.3 ~~8.2.5~~8.2.6 ~~10.1.17~~10.2.18 ~~10.1.18~~10.2.19 ~~10.1.19~~10.2.20	The following messages are required: - Physical channel reconfiguration message - Physical channel reconfiguration complete message - Physical channel reconfiguration failure message
Active set update in soft handover	25.303 25.331	6.4.1 6.4.4 6.4.5 6.4.6 8.3.4 ~~10.1.1~~10.2.1 , ~~10.1.2,~~10.2.2 ~~10.1.3~~10.2.3	The following messages are required: - Active Set Update message - Active Set Update Complete message - Active Set Update Failure message
Inter-system handover	25.303 25.331	6.4.9 6.4.10 8.3.6 8.3.7 8.3.8 8.3.9 9.4 9.5 9.6 ~~10.1.10~~10.2.11 ~~10.1.11~~10.2.12	The following messages are required: - Inter-system handover command message - Inter-system handover failure message Note: support of Inter-system handover is required for multi-mode terminals only.
Hard handover	25.303 25.331	6.4.7 8.3.5	
Downlink outer loop control	25.331	8.2.9 ~~10.1.7~~10.2.7	The following message is required: - Downlink Outer Loop Control message
Logical channels required in addition to those required for the baseline functionality, for the above procedures:			
Dedicated traffic channel (DTCH)	25.301	5.3	
Transport channels required in addition to those required for the baseline functionality, for the above procedures			
Dedicated channel (DCH)	25.301	5.2	

B.3 Layer 3 (non-access stratum) implementation capabilities to support the default speech service

Table 12: UE Speech Service Implementation Capability for Layer 3 Non-Access Stratum
E: Essential Unconditional, C: Essential Conditional, O: Optional

		Service Implementation Capabilities			Ref. Doc	**Subclause(s)**	Tele-service for Terminals	Comments
							Speech (w/ E. call)	
	Layer 3 specification	UMTS Call Control (Optional)	Mobile originating call Establishment		24.008	5.2.1	C	Essential for speech service
			Mobile terminating call Establishment		24.008	5.2.2	C	Essential for speech service
			Call clearing	Exception conditions	24.008	5.4.2	C	Essential for speech service
				Clearing initiated by the mobile station	24.008	5.4.3	C	Essential for speech service
				Clearing initiated by the network	24.008	5.4.4	C	Essential for speech service
			In-band tones and announcements		24.008	5.5.1	C	Essential for speech service
			Status procedure		24.008	5.5.3	C	Essential for speech service
			Call re-establishment, mobile station side		24.008	5.5.4	C	Essential for speech service
			Progress		24.008	5.5.6	C	Essential for speech service
			DTMF protocol control procedure (send DTMF to PLMN direction)		24.008	5.5.7	C	Essential for speech service

Annex C:
SMS Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support SMS. The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

C.1 Physical layer implementation capabilities to support the SMS service

Table 13: FDD mode Physical Layer Service implementation capabilities for support of SMS service

Service Implementation Capability	Specification	Subclause(s)	Comments
Physical Layer UE procedures and measurements:			
Support of Handover	25.215 25.212	5.1, 6.1 4.4	Support of handover may be required depending on how SMS is implemented.
Power control	25.214 25.215	5.1.2, 5.2.1 ~~5.1.8, 5.1.9~~5.1.7	Support of closed loop power control may be required depending on how SMS is implemented. ~~Note: Physical channel BER measurement in 25.215 subclause 5.1.9 is not required according to decision made after December 1999.~~
Error detection	25.212	4.2.1	Support of 0, 8, 12, ~~-~~and 16 bits CRC per transport block is essential for all terminals.
Channel Coding	25.212	4.2.3	
Multiplexing	25.212	4.2.4 – 4.2.14	In SMS service case, it is Essential for all terminals to support at minimum 1 transport channels in uplink, of which is reserved dedicated signalling. In SMS service case, it is Essential for all terminals to support at minimum 1 transport channels in downlink, of which is reserved for dedicated signalling.
Transport format detection	25.212	4.3	In downlink, the support of transport format detection with TFCI is essential for all terminals both with fixed and flexible TrCH positions.
Spreading and Scrambling Code Generation	25.213	4.2.1, 4.3	
Code de-spreading and de-scrambling	25.213	5.1, 5.2	
Support for downlink Transmit Diversity	25.211 25.214	5.3.1, 5.3.2 ~~8~~7	Support of closed loop transmit diversity may be required depending on implementation.
Support for Site Selection Diversity Transmission	25.214	5.2.1.4	Support of SSDT may be required depending on implementation.
Transport channels required in addition to those required for the baseline functionality, for the above procedures:			
Downlink Shared Channel (DSCH)	25.211	4.2.6, 6	Conditional on Implementation
Common Packet Channel (CPCH)	25.211	4.2.5, 6	Conditional on Implementation
Dedicated Channel (DCH)	25.211	4.1.1, 6	Conditional on Implementation
Physical channels required in addition to those required for the baseline functionality, for the above procedures:			
Physical Common Packet Channel (PCPCH)	25.211	5.2.2.2,6	Conditional on Implementation
Physical Downlink Shared Channel (PDSCH)	25.211	5.3.3.5,6	Conditional on implementation
Dedicated Physical Data Channel (DPDCH)	25.211	5.2.1, 5.3.2, 6	Conditional on implementation
Dedicated Physical Control Channel (DPCCH)	25.211	5.2.1, 5.3.2, 6	Conditional on implementation

C.2 Layer 2/3 Implementation Capabilities to support SMS Service

Table14: SMS Service Implementation Capabilities Layer 2/3 (access stratum)

SMS Service Implementation Capabilities	Specification	Subclause(s) [i]	Comments
UE procedures:			
RRC connection re-establishment	25.331	~~10.1.4.1,~~ ~~10.1.4.2,~~ ~~10.1.4.3~~10.2.35 10.2.36 10.2.37	The following messages are required: - RRC connection re-establishment message - RRC connection re-establishment complete message - RRC connection re-establishment request message
Active set update in soft handover	25.303 25.331	6.4.1 6.4.4 6.4.5 6.4.6 8.3.4 ~~10.1.1~~ ~~10.1.2~~ ~~10.1.3~~10.2.1 10.2.2 10.2.3	If handover is supported, the following are required: - Active Set Update message - Active Set Update Complete message - Active Set Update Failure message ~~is required.~~
Inter-system handover	25.303 25.331	6.4.9 6.4.10 8.3.6 8.3.7 8.3.8 8.3.9 9.4 9.5 9.6 ~~10.1.10~~ ~~10.1.11~~10.2.11 10.2.12	If handover is supported, the following are required: - Inter-system handover command message - Inter-system handover failure message Note: support of Inter-system handover is required for multi-mode terminals only.
Hard handover	25.303 25.331	6.4.7 8.3.5	Dependent on whether handover is supported.
Downlink outer loop control	25.331	8.2.9 ~~10.1.7~~10.2.7	Supported of the Downlink Outer Loop Control message may be required depending on how SMS is implemented.
Logical channels required in addition to those required for the baseline functionality, for the above procedures:			
Dedicated Traffic Channel (DTCH)	25.301	5.3	DTCH is conditional on implementation.
Transport channels required in addition to those required for the baseline functionality, for the above procedures			
Dedicated Channel (DCH)	25.301	5.2	DCH is conditional on implementation.

C.3 SMS-PP Layer 3 (non access stratum)

Table 15: UE Service Implementation Capability for SMS-PP Layer3 (non access stratum)
E: Essential unconditional, C: essential Conditional, O: Optional, N/A: Not Applicable

	Service Implementation Capabilities			Ref. Doc	Subclause(s)	Service for UE		Comments
						SMS-PP		
						CS	PS	
Layer 3 specification (procedures)	CM-procedure	Connection establishment procedures		24.011	5.3.1	C	N/A	
		RP Data Unit (RPDU) transfer procedures	RPDU transfer for CS	24.011	5.3.2.1	C	N/A	
			RPDU transfer for GPRS	24.011	5.3.2.2	N/A	C	
		Connection release procedures		24.011	5.3.3	C	N/A	
		Procedures for abnormal cases		24.011	5.3.4	C	C	
	hort Message ely Procedure	TP Data Unit(TPDU) Relay Procedure		24.011	6.3.1	C	C	
		Notification relay procedures		24.011	6.3.3	C	C	
		Procedures for abnormal cases		24.011	6.3.4	C	C	

Annex D:
CBS Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support CBS. The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

D.1 Physical layer implementation capabilities to support the CBS service

Table 16: FDD mode Physical Layer Service implementation capabilities for support of CBS service

Service Implementation Capability	Specification	Subclause(s)	Comments
Physical Layer UE procedures and measurements:			
Error detection	25.212	4.2.1	Support of 0, 8, 12 and 16 bits CRC per transport block is essential for all terminals.
Channel Coding	25.212	4.2.3.	
Multiplexing	25.212	4.2.4 – 4.2.14	

D.2 Layer 2/3 Implementation Capabilities to support CBS Service

Table 17: CBS Service Implementation Capability for Layer 2/3 (access stratum)

Service Implementation Capability	Specification	Subclause(s)	Comments
UE procedures:			
BMC message reception	25.324	9.4 ~~10.1~~ 10.2 10.3	The following messages are required: - BMC CBC Message~~ is required.~~ - BMC Schedule Message~~ is required.~~
Logical channels required in addition to those required for the baseline functionality, for the above procedures:			
Common traffic channel (CTCH)	25.301	5.3	

Annex E:
Bearer Services Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support Bearer Services. The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

E.1 Service implementation capabilities to facilitate conformance testing of Bearer Services capabilities

NOTE: Support of the following reference measurement channels is essential depending on the Bearer Services supported by a given terminal.

Terminal service implementation capabilities:

- Down-link reference measurement channel 64 kbps (FDD), TS 25.101 clause A.3.2.
- Down-link reference measurement channel 144 kbps (FDD), TS 25.101 clause A.3.3.
- Down-link reference measurement channel 384 kbps (FDD), TS 25.101 clause A.3.4.
- Down-link reference measurement channel 64 kbps (TDD), TS 25.102 clause A.2.3.
- Down-link reference measurement channel 144 kbps (TDD), TS 25.102 clause A.2.4.
- Down-link reference measurement channel 384 kbps (TDD), TS 25.102 clause A.2.5.

E.2 Physical layer implementation capabilities to support Bearer service

Table 18: FDD mode Physical Layer Service implementation capabilities for support of Bearer service

Service Implementation Capability	Specification	Subclause(s)	Comments
Physical Layer UE procedures and measurements:			
Handover	25.215 25.212	5.1, 6.1 4.4	Support of soft handover is Essential for all UE. Support of Inter-Frequency handover is Essential for all UE. Terminals shall support measurements commensurate with their mode/system capabilities, to facilitate inter-frequency, inter-mode & inter-system handover.
Power control	25.214 25.215	5.1.2, 5.2.1 ~~5.1.8, 5.1.9~~5.1.7	Support of closed loop power control is Essential for all UE. ~~Note: Physical channel BER measurement in 25.215 subclause 5.1.9 is not required according to decision made after December 1999.~~
Error detection	25.212	4.2.1	Support of 0, 8, 12 and 16 bits CRC per transport block is essential for all terminals.
Channel coding & Multiplexing	25.212 25.926	4.2.3, 4.2.4-4.2.14 5.1	Turbo coding is essential only for block sizes of greater than 320 bits.
Spreading and Scrambling Code Generation	25.213	4.2.1, 4.3	
Code de-spreading and de-scrambling	25.213	5.1, 5.2	
Support for downlink Transmit Diversity	25.211 25.214	5.3.1, 5.3.2 ~~8~~7	Support of open loop and closed loop transmit diversity is Essential for all terminals.
Support for Site Selection Diversity Transmission	25.214	5.2.1.4	Support of SSDT is Essential for all terminals.
Transport channels required in addition to those required for the baseline functionality, for the above procedures:			
Downlink Shared Channel (DSCH)	25.211	4.2.6, 6	Conditional on Implementation
Common Packet Channel (CPCH)	25.211	4.2.5, 6	Conditional on Implementation
Dedicated channel (DCH)	25.211	4.1.1, 6	Conditional on Implementation
Physical channels required in addition to those required for the baseline functionality, for the above procedures:			
Physical Common Packet Channel (PCPCH)	25.211	5.2.2.2,6	Conditional on Implementation
Physical Downlink Shared Channel (PDSCH)	25.211	5.3.3.5,6	Conditional on implementation
Dedicated Physical Data Channel (DPDCH)	25.211	5.2.1 5.3.2, 6	Conditional on Implementation
Dedicated Physical Control Channel (DPCCH)	25.211	5.2.1 5.3.2, 6	Conditional on Implementation

E.3 Layer 2/3 Implementation Capabilities to support Bearer Services

Table 19: Bearer Services Service Implementation Capabilities Layer 2/3 (access stratum)

Bearer Services Service Implementation Capabilities	Specification	Subclause(s) [ii]	Comments
UE procedures:			
RRC connection re-establishment	25.331	~~10.1.4.1,~~ ~~10.1.4.2,~~ ~~10.1.4.3~~10.2.35 10.2.36 10.2.37	The following messages are required: - RRC connection re-establishment message - RRC connection re-establishment complete message - RRC connection re-establishment request message
Radio bearer establishment	25.303 25.331	6.2.1.1 8.2.1 ~~10.1.28~~ ~~10.1.29~~ ~~10.1.30~~10.2.29 10.2.30 10.2.31	The following messages are required: - Radio Bearer Setup message - Radio Bearer Setup Complete message - Radio Bearer Setup Failure message
Radio bearer reconfiguration	~~25.331~~25.303 ~~25.303~~25.331	~~8.2.2~~6.2.1.3 ~~6.2.1.3~~8.2.2 ~~10.1.22~~ ~~10.1.23~~ ~~10.1.24~~10.2.23 10.2.24 10.2.25	The following messages are required: - Radio Bearer Reconfiguration message - Radio Bearer Reconfiguration complete message - Radio Bearer Reconfiguration Failure message
Radio bearer release	25.303 25.331	6.2.1.2 8.2.3 ~~10.1.2~~ ~~10.1.26~~ ~~10.1.27~~10.2.26 10.2.27 10.2.28	The following messages are required: - Radio Bearer Release message - Radio Bearer Release Complete message - Radio Bearer Release Failure message
Transport channel reconfiguration	25.303 25.331	6.2.2 8.2.4 ~~10.1.49~~ ~~10.1.50~~ ~~10.1.51~~10.2.51 10.2.52 10.2.53	The following messages are required: - Transport channel reconfiguration message - Transport channel reconfiguration complete message - Transport channel reconfiguration failure message
Transport format combination control	25.303 25.331	6.2.4 8.2.5 ~~10.1.52~~ ~~10.1.53~~10.2.54 10.2.55	The following messages are required: - Transport format combination control message - Transport format combination control failure message

Bearer Services Service Implementation Capabilities	Specification	Subclause(s) [ii]	Comments
UE procedures:			
Physical channel reconfiguration	25.303 25.331	6.2.3 ~~8.2.5~~8.2.6 ~~10.1.17~~ ~~10.1.18~~ ~~10.1.19~~10.2.18 10.2.19 10.2.20	The following messages are required: - Physical channel reconfiguration message - Physical channel reconfiguration complete message - Physical channel reconfiguration failure message
URA update	25.303 25.331	6.4.3 8.3.2 ~~10.1.1.11~~ ~~10.1.1.12~~10.2.61 10.2.62	The following messages are required: - URA update message - URA update confirm message
Active set update in soft handover	25.303 25.331	6.4.1 6.4.4 6.4.5 6.4.6 8.3.4 ~~10.1.1~~ ~~10.1.2~~ ~~10.1.3~~10.2.1 10.2.2 10.2.3	The following messages are required: - Active Set Update message - Active Set Update Complete message - Active Set Update Failure message
Inter-system handover	25.303 25.331	6.4.9 6.4.10 8.3.6 8.3.7 8.3.8 8.3.9 9.4 9.5 9.6 ~~10.1.10~~ ~~10.1.11~~10.2.11 10.2.12	The following messages are required: - Inter-system handover command message - Inter-system handover failure message is required. Note: support of Inter-system handover is required for multi-mode terminals only.
Hard handover	25.303 25.331	6.4.7 8.3.5	
Downlink outer loop control	25.331	8.2.9 ~~10.1.7~~10.2.7	The following message is required: - Downlink Outer Loop Control message
PDCP – PDU transfer	25.323	5.4	PDCP-PDU is Essential for UE which have packet switched data service
Logical channels required in addition to those required for the baseline functionality, for the above procedures:			
Common Traffic Channel (CTCH)	25.301	5.3	Conditional on Implementation
Dedicated traffic channel (DTCH)	25.301	5.3	Conditional on Implementation
Transport channels required in addition to those required for the baseline functionality, for the above procedures			
Downlink Shared Channel (DSCH)	25.301	5.2	Conditional on Implementation
Common Packet Channel (CPCH)	25.301	5.2	Conditional on Implementation
Dedicated channel (DCH)	25.301	5.2	Conditional on Implementation

E.4 Layer 3 (non access stratum)

Table 20: UE Service Implementation Capability for Layer3 (non access stratum)

E: Essential unconditional, C: essential Conditional, O: Optional

	Service Implementation Capabilities			Ref. Doc	Subclause(s)	Bearer service for Terminals		Comments
						Circuit SW data	Packet SW data	
Layer 3 specification	UMTS Call Control	Mobile originating call Establishment		24.008	5.2.1	C	-	
		Mobile terminating call Establishment		24.008	5.2.2	C	-	
		Network initiated MO call (CCBS)		24.008	5.2.3	O	-	
		Call clearing	Exception conditions	24.008	5.4.2	C	-	
			Clearing initiated by the mobile station	24.008	5.4.3	C	-	
			Clearing initiated by the network	24.008	5.4.4	C	-	
		In-band tones and announcements		24.008	5.5.1	C	-	
		Status procedure		24.008	5.5.3	C	-	
		DTMF protocol control procedure		24.008	5.5.7	O	-	
	MTS Session anagement	PDP context activation		24.008	6.1.3.1	-	C	
		Secondary PDP context activation procedure		24.008	6.1.3.2		O	
		PDP context modification procedure		24.008	6.1.3.3	-	C	
		PDP context deactivation procedure		24.008	6.1.3.4	-	C	
		Receiving a SM STATUS message by a SM entity		24.008	6.1.3.6	-	C	

Annex F:
Supplementary Services Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support Supplementary Services. The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

F.1 Supplementary Service Layer 3 (non access stratum)

Table 21: UE Service Implementation Capability for Supplementary Service Layer3 (non access stratum)

E: Essential unconditional, C: essential Conditional, O: Optional

	Service Implementation Capabilities			Ref. Doc	Subclause(s)	SS for UE	Comments
						Call Forward, Advise of Change, USSD, Explicit Call transfer, and others	
Layer 3 specification	UMTS Call Control	Mobile originating call Establishment		24.008	5.2.1	C	CC is related upon each SS operations. *: Conditional, If CCBS is supported.
		Mobile terminating call Establishment		24.008	5.2.2	C	
		Network initiated MO call (CCBS)		24.008	5.2.3	C*	
		Call clearing	Exception conditions	24.008	5.4.2	C	
			Clearing initiated by the mobile station	24.008	5.4.3	C	
			Clearing initiated by the network	24.008	5.4.4	C	
		In-band tones and announcements		24.008	5.5.1	C	
		Status procedure		24.008	5.5.3	C	
		DTMF protocol control procedure		24.008	5.5.7	C	
	Supplementary Service	Generic Procedure for the control of SS (CALL RELATED)		24.010	2.2.4	O	SA defines support items. See each specific procedure depending on supporting services. The procedures are defined in the TS24.072, 24.08x-series, 24.09x-series CC is Related upon each SS operation.
					2.2.6.1	O	
					2.2.7.1	O	
					2.2.8.1	O	
		Generic Procedure for the control of SS (CALL INDEPENDENT)		24.010	2.2.5	C	
					2.2.6.2	C	
					2.2.7.2	C	
					2.2.8.2	C	
		SS Support procedure		24.010	3	C	
		Password management		24.010	4	C (depending on supporting services)	
		Supplementary service cross phase compatibility		24.010	5	C (depending on supporting services)	

Annex G:
USAT Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support Supplementary Services. The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

G.1 USIM implementation to support USAT

Table 22: USIM Implementation Capabilities to support USAT

Service Implementation Capability	Specification	Sub/Subclauses	Essential/Optional Comments
USIM Application Toolkit			
USAT commands	31.101	11.2	<Essential Conditional>
Support for USAT feature	31.111	5	<Essential Conditional>
Proactive/Envelope commands	31.111	6, 7	<Essential Conditional>

Annex H:
LCS Service Implementation Capabilities

This annex identifies Service Implementation Capabilities that are required to support the LCS Service Capability. The references in this annex are to 3GPP documents agreed for release '99 in March 2000~~December 1999~~. The referenced section numbers may change with future versions.

H.1 Physical layer implementation capabilities to support LCS

Table 23: FDD mode physical layer implementation capabilities to support LCS

Measurements and Procedures	Specification	Subclause	Comment
Idle Periods for IDPL location method	25.214 25.215	~~10~~8 ~~5.1.2~~5.1.10	General IPDL procedure SFN-SFN Observed Time Difference
UE GPS Timing of Cell Frames for LCS	25.215	~~5.1.15~~5.1.13	

H.2 Layer 2/3 access stratum implementation capabilities to support LCS

Table 24: FDD mode layer 2/3 non-access stratum implementation capabilities to support LCS

Measurements and Procedures	Specification	Subclause	Comment
SFN-SFN Observed time difference	25.302	~~9.1.16~~9.2.15	Essential only for support of ODTOA based mechanisms

H.3 Layer 3 non-access stratum implementation capabilities to support LCS

Table 25: FDD mode layer ~~2/~~3 non-access stratum implementation capabilities to support LCS

Measurements and Procedures	Specification	Subclause	Status	Comment
Mobile station Classmark 2	24.008	10.5.1.6	C	Essential if LCS is supported

Annex I:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
17/03/00	T#7	TP-000026			New	2.0.0	3.0.0
28/03/00					Editorial modification by MCC	3.0.0	3.0.1

3GPP TSG-T2 #9 / ETSI SMG4
Utrecht, The Netherlands, 15-19 May 2000

***Document* TSGT2000319**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.040	**CR**	**012**	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: T2 **Date:** 16 May 2000

Subject: Alignment in Enhanced Messaging Service

Work item: EMS

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:
This CR proposes a correction of the default alignment value for EMS. In the specification the default alignment is set to left. This is not always true. Some languages for example Arabic do not normally use left alignment as default. To solve this problem, this CR proposes to assign a new alignment value, “language dependent”. If this value is used the alignment should be set according to the normal alignment for that language. This new value should be used as default.

It also performs and editorial correction to section 9.2.3.24.10.1.2

Clauses affected:
9.2.3.24.10.1.1
9.2.3.24.10.1.2

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.2.3.24.10.1.1 Text Formatting

The Information-Element-Data octet(s) shall be coded as follows.

Octet 1 Start position of the text formatting. Set to the number of characters after the formatting shall be applied from the beginning of the SM data.

This octet shall be coded as an integer value in the range 0 (beginning of the SM data) to the maximum number of characters included in the SM data of one single SM or one segment of a concatenated SM

Octet 2 Text formatting length. Gives the number of formatted characters

This octet shall be coded as an integer value in the range 1 to the maximum number of characters for which the formatting applies in one single SM or one segment of a concatenated SM.Octet 3 formatting mode value coded as following :

Octet 3 : Bit 7 Bit 6 Bit 5 Bit 4 Bit 3 Bit 2 Bit 1 Bit 0

Bit 1	Bit 0	*Alignment
0	0	Left ~~(default)~~
0	1	Center
1	0	Right
1	1	Language dependent (default) ~~*reserved*~~

*in case formatting text is inserted on the same line as previous non formatting text or with a different mode value, the alignment value shall be set to the same value as the previous formatted predefined object.

Bit 3	Bit 2	Font Size
0	0	Normal (default)
0	1	Large
1	0	Small
1	1	*reserved*

Bit 4	Style **bold**
1	Bold on
0	Bold off

Bit 5	Style *Italic*
1	Italic on
0	Italic off

Bit 6	Style Underlined
1	Underlined on
0	Underlined off

Bit 7	Style ~~Strikethrough~~
1	Strikethrough on
0	Strikethrough off

If bit 4,5,6 and 7 are set to 0, it will mean normal style (default).

9.2.3.24.10.1.2 Predefined Sound

The Information-Element-Data octet(s) shall be coded as follows.

Octet 1 position indicating in the SM data the instant after which the sound shall be played. It will be set to the number of characters from the beginning of the SM data after which the sound shall be played.

Octet 2	This octet shall be coded as an integer value in the range 0 (beginning of the SM data) to the maximum number of characters included in the SM data of one single SM or one segment of a concatenated SM sound number. Shall be encoded as a integer value.

3GPP T2/SMG4 Meeting #9
Maarsen, NL, 15-19 May 2000

***Document* T2-000311**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.040	CR	014	Current Version:	3.4.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*

(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: T2 **Date:** 16/05/2000

Subject: Correction to text on SMS TimeZone

Work item: TEI

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: The current text has been identified as ambiguous, as at least one implementor believed that the time zone field did not need to change for summer and winter times. The added text clarifies and provides a specific example which should prevent any future misinterpretation.

Clauses affected: 9.2.3.11

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:


help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.2.3.11 TP-Service-Centre-Time-Stamp (TP-SCTS)

The TP-Service-Centre-Time-Stamp field is given in semi-octet representation, and represents the local time in the following way:

	Year:	Month:	Day:	Hour:	Minute:	Second:	Time Zone
Digits: (Semi-octets)	2	2	2	2	2	2	2

The Time Zone indicates the difference, expressed in quarters of an hour, between the local time and GMT. In the first of the two semi-octets, the first bit (bit 3 of the seventh octet of the TP-Service-Centre-Time-Stamp field) represents the algebraic sign of this difference (0: positive, 1: negative).

The Service-Centre-Time-Stamp, and any other times coded in this format that are defined in the present document, represent the time local to the sending entity.

If the MS has knowledge of the local time zone, then any time received (e.g. Service-Centre-Time-Stamp) at the MS may be displayed in the local time rather than the time local to the sending entity. Messages shall be stored as received without change to any time contained therein.

The Time Zone code enables the receiver to calculate the equivalent time in GMT from the other semi-octets in the Service-Centre-Time-Stamp, or indicate the time zone (GMT, GMT+1H etc.), or perform other similar calculations as required by the implementation. The value contained in the Time Zone field must take into account daylight saving time, such that when the sending entity changes from regular (winter) time to daylight saving (summer) time, there is a change to the value in the Time Zone field, for example in the UK the winter setting is 00000000 and the summer setting is 01000000.

If the MS receives a non-integer value in the SCTS, it shall assume that the digit is set to 0 but shall store the entire field exactly as received.

3GPP T2/SMG4 Meeting #9
Utrecht, Netherland, 15-19 05 2000

***Document* T2-000347**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.040	**CR**	**015**	Current Version:	3.4.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 18.05.2000

Subject: Correction of TP-PID

Work item: TEI

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Correction of TP-PID because of misleading description.

Clauses affected: 9.2.3.9

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments: In case of approval of this CR different implementations and behaviour of various mobile phones can be avoided.


help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.2.3.9 TP-Protocol-Identifier (TP-PID)

The TP-Protocol-Identifier parameter serves the purposes indicated in subclause 3.2.3. It consists of one octet, and the bits in the octet are used as follows:

The MS shall interpret reserved or unsupported values as the value 00000000 but shall store them exactly as received.

The SC may reject messages with a TP-Protocol-Identifier containing a reserved value or one which is not supported.

bits	usage
7 6	
0 0	Assigns bits 0..5 as defined below
0 1	Assigns bits 0..5 as defined below
1 0	reserved
1 1	Assigns bits 0-5 for SC specific use

In the case where bit 7 = 0 and bit 6 = 0,

bit 5 indicates telematic interworking:
value = 0 : no interworking, but SME-to-SME protocol
value = 1 : telematic interworking

In the case of telematic interworking, the following five bit patterns in bits 4..0 are used to indicate different types of telematic devices:

4.. .0	
00000	implicit - device type is specific to this SC, or can be concluded on the basis of the address
00001	telex (or teletex reduced to telex format)
00010	group 3 telefax
00011	group 4 telefax
00100	voice telephone (i.e. conversion to speech)
00101	ERMES (European Radio Messaging System)
00110	National Paging system (known to the SC)
00111	Videotex (T.100 [20] /T.101 [21])
01000	teletex, carrier unspecified
01001	teletex, in PSPDN
01010	teletex, in CSPDN
01011	teletex, in analog PSTN
01100	teletex, in digital ISDN
01101	UCI (Universal Computer Interface, ETSI DE/PS 3 01-3)
01110..01111	(reserved, 2 combinations)
10000	a message handling facility (known to the SC)
10001	any public X.400-based message handling system
10010	Internet Electronic Mail
10011..10111	(reserved, 5 combinations)
11000..11110	values specific to each SC, usage based on mutual agreement between the SME and the SC (7 combinations available for each SC)
11111	A GSM/UMTS mobile station. The SC converts the SM from the received TP-Data-Coding-Scheme to any data coding scheme supported by that MS (e.g. the default).

If bit 5 has value 1 in an SMS-SUBMIT PDU, it indicates that the SME is a telematic device of a type which is indicated in bits 4..0, and requests the SC to convert the SM into a form suited for that device type. If the destination network is ISDN, the SC must also select the proper service indicators for connecting to a device of that type.

If bit 5 has value 1 in an SMS-DELIVER PDU, it indicates that the SME is a telematic device of a type which is indicated in bits 4..0.

If bit 5 has value 0 in an SMS-DELIVER PDU, the value in bits 4..0 identifies the SM-AL protocol being used between the SME and the MS.

Note that for the straightforward case of simple MS-to-SC short message transfer the Protocol Identifier is set to the value 0.

In the case where bit 7 = 0, bit 6 = 1, bits 5..0 are used as defined below

5 0	
000000	Short Message Type 0
000001	Replace Short Message Type 1
000010	Replace Short Message Type 2
000011	Replace Short Message Type 3
000100	Replace Short Message Type 4
000101	Replace Short Message Type 5
000110	Replace Short Message Type 6
000111	Replace Short Message Type 7
001000..011101	Reserved
011110	Enhanced Message Service (EMS. Refer subclause 3.10)
001000..011110	Reserved
011111	Return Call Message
100000..111011	Reserved
111100	ANSI-136 R-DATA
111101	ME Data download
111110	ME De-personalization Short Message
111111	(U)SIM Data download

A short message type 0 indicates that the ME must acknowledge receipt of the short message but may discard its contents.

The Replace Short Message feature is optional for the ME and the (U)SIM but if implemented it shall be performed as described here.

For MT short messages, on receipt of a short message from the SC, the MS shall check to see if the associated Protocol Identifier contains a Replace Short Message Type code.

If such a code is present, then the MS shall check the originating address and replace any existing stored message having the same Protocol Identifier code and originating address with the new short message and other parameter values. If there is no message to be replaced, the MS shall store the message in the normal way. The MS may also check the SC address as well as the Originating Address. However, in a network which has multiple SCs, it is possible for a Replace Message type for a SM to be sent via different SCs and so it is recommended that the SC address should not be checked by the MS unless the application specifically requires such a check.

If a Replace Short Message Type code is not present then the MS shall store the message in the normal way.

In MO short messages the SC reacts similarly but only the address of the originating MS or any other source is checked.

The Enhanced Message Service PID value shall be set in a MO enhanced short message unless there is a need to set the PID to any other value (e.g. for telematic interworking). In the event where the message contains one or more IE that could not be understood by the receiving SME, this PID value may be used to assist the receiving SME and/or the SMSC to identify such a message (e.g. for diagnostic purposes). It is not a mandatory requirement for the SMSC or receiving SME to process this PID value or for the SMSC to pass the value to the receiving SME.

A Return Call Message indicates to the MS to inform the user that a call (e.g. a telephone call) can be established to the address specified within the TP-OA. The RP-OA contains the address of the SC as usual. The message content (if present) gives displayable information (e.g. the number of waiting voice messages). The message is handled in the same way as all other messages of the Replace Short Message Types.

The ME De-personalization Short Message is a ME-specific message which instructs the ME to de-personalities the ME (see 3G TS 22.022 [25]). The TP-DCS shall be set to Uncompressed, Default Alphabet, and Message Class 1 (ME-specific), which corresponds to a bit coding of 00010001. The TP-UD field contains de-personalization information coded according to 3G TS 22.022 [25]. This information shall not be displayed by an ME which supports the scheme. The acknowledgement to this message is a SMS-DELIVER-REPORT for RP-ACK in which the TP-User-Data shall be coded according to 3G TS 22.022 [25].

(U)SIM Data download is a facility whereby the ME must pass the short message in its entirety including all SMS elements contained in the SMS deliver to the (U)SIM using the mechanism described in GSM TS 11.11 [16] and 3G TS 31.102 [30]. The DCS shall be set to 8 bit message class 2 (either bit coding 1111 0110 or 00010110). The entire user data field is available for (U)SIM Data download. If the DCS is not set to 8-bit message class 2 then the message shall be handled in the normal way by the ME.

ME Data download is a facility whereby the ME shall process the short message in its entirety including all SMS elements contained in the SMS deliver to the ME. The DCS ~~shall~~should normally be set to message class 1. If the DCS is set to message class 1 and no application in the ME exists, which is able to process the short message, the ME may discard the short message. The entire user data field is available for ME data download. The TPDU parameters required for the SMS-DELIVER should be passed transparently by all involved SCs, so no TPDU parameter in the entire short message is modified, other than the changes required to convert an SMS-SUBMIT into an SMS-DELIVER.

ANSI-136 R-DATA is a facility whereby the ME must pass the short message in its entirety, including all elements contained in the SMS DELIVER, to the (U)SIM using the mechanism described in GSM TS 11.14 [16] and 3G TS 31.102 [30]. The DCS shall be set to 8-bit message class 2 (either bit coding 11110110 or 00010110). If the DCS is not set to 8-bit message class 2 then the message shall be handled in the normal way by the ME.

3GPP TSG-T2 #9 / ETSI SMG4
Utrecht, NETHERLANDS
15 - 19 May 2000

T2-000307

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	003	Current Version:	3.1.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T#8 *list expected approval meeting # here ↑*

for approval [X] for information [ ]

strategic [ ] non-strategic [ ] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 04.04.2000

Subject: Addition of phonebook entry and addition/modification of user data update for untrusted applications

Work item: MExE

Category: *(only one category shall be marked with an X)*

F	Correction	[X]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[ ]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change:

To be in line with WAP WTA specification, unrusted MExE executables must also have permission to add a phonebook entry. Further, there are several use cases in the world where the executable, although being untrusted, could assist the user for updating also other data: task lists, ringing tones, calendar data.

However, because the executable is untrusted, the strict security rules must be applied. The user must be displayed both the application name and the data to be handled by the provisioned functionality in the terminal and not by the executable itself. User must give permission for all data updates performed by the untrusted executable.

Clauses affected: 8.2.1.

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments: Refer to WAP Wireless Telephony Application Interface Specification, chapter "Public WTAI".


help.doc

<--------- double-click here for help and instructions on how to create a CR.

8.2.1 MExE executable ~~p~~Permissions for untrusted MExE executables

Clause 8.2 identifies the permissions for MExE executables in the 3 domains (operator, MS manufacturer and Third Party). The permissions do not apply to untrusted MExE executables which are not permitted to execute within the domains.

In order to facilitate untrusted MExE executables having some limited access to MExE MS functionality beyond their very limited privileges, the following specific access permissions in Table 3 are extended to untrusted MExE executables:-

- User interface

  An untrusted, uninstalled MExE executable (e.g. an applet) can access the user interface output (display) and input (keyboard, mouse, ..) without user permission, but the sending of user data to a server to which the MExE executables has a session connection (e.g. as part of a browser sesssion) requires user permission.

  An installed untrusted MExE executable shall only be able to access the user interface output (display) and input (keyboard, mouse, ..) with user permission. (Clearly, for the usability of untrusted MExE executables such as games, blanket user permission should be sought and given, and this is permissible.)

- File

  File access is not permitted for untrusted MExE executables, except that untrusted MExE executables can access files only in the MExE executable's own directory.

- Initiate a voice/data connection

  Untrusted MExE executables shall be able to make calls under the following conditions.

  In addition to an untrusted MExE executable possibly displaying the number to be called to the user, the number to be called shall be presented to the user for permission by a provisioned functionality of the MExE MS and not by the MExE executable itself. (This facility would support, for example, "click to dial" button/links in an untrusted MExE executable, and a MExE MS provisioned functionality then represents the number to the user for confirmation.)

- Generate DTMF

  Untrusted MExE executables shall be able to generate DTMF tones under the following conditions.

  An untrusted MExE executable is only permitted to send DTMF tones in a currently active call. The request to generate DTMF tones in the currently active call, shall result in the characters which the tones represent being presented to the user for permission by a provisioned functionality of the MExE MS.

- <u>Add phonebook entry</u>

  <u>Untrusted MExE executables shall be able to add a phonebook entry (i.e. name and number only) under the following conditions.</u>

  <u>The name and the number to be added shall be displayed to the user for permission by a provisioned functionality of the MExE MS and not by the MExE executable itself. The phonebook entry shall not be added without user permission. The function shall not be able to modify or delete any phonebook entry.</u>

The untrusted MExE executables permitted to use the above facilities shall be MExE executables the user has downloaded himself, and not be MExE executables that have been pushed to the user. MExE executables/applets on the MExE MS due to the user having visited a particular web site are considered to be MExE executables that the user had downloaded himself.

Untrusted MExE executables shall not be permitted access to any other functions.

3GPP TSG-T WG2#9

Maarssen, Netherlands, 15-19 May 2000

TSGT2#9(2000)298

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	004	Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: T2 **Date:** 17.05.2000

Subject: Editorial clarifications

Work item: MExE

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

Clauses affected: 8.7, 8.8

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.2.3 Required and optional JavaPhone APIs

The JavaPhone APIs extend the PersonalJava APIs to provide functionality unique to telephony devices. Java MExE devices shall support the Wireless Profile of the JavaPhone API specification [4]. Java MExE devices shall support all APIs specified as required by the Wireless Profile in the JavaPhone API specification. All APIs that are optional in the Wireless Profile shall be optional in Java MExE devices.

6.2.3.1 Application installation

Java MExE devices shall support the following JAR file manifest entries (as described in the JavaPhone specification) as described below:

- Implementation-Title
  the Implementation-Title shall be used in any textual description of the application which is displayed in the UI element used to launch the application. E.g. the text displayed with an icon.
- Main-Icon
  the use of icons to launch applications is optional, however if icons are used as elements to launch the application, then the icon file within the JAR file named by the Main-Icon attribute shall be displayed, and may be scaled if desired.
- Main-Class and Class-Path
  when the application is launched, the MExE Java VM shall be supplied with the classpath and shall call the main() method in the class named by the Main-Class attribute.

6.2.3.2 Power

Java MExE devices shall support the Power Monitor package (javax.power.monitor) as specified by the JavaPhone API to access the power level of the device and receive notifications concerning changes in power states.

Note that the Power Monitor package does not specify the minimum required events that should be generated under certain circumstances. A MExE Java device shall at least implement the following event generation:

- BatteryCritical

  shall be generated when the battery is at a critically low level.

- BatteryNormal

  shall be generated when the battery is no longer low.

All the other event generation should be supported by the implementation.

6.2.4 Required and optional MExE APIs

A Java MExE device shall not be required to support any other Java APIs.

A Java MExE device may optionally support any other Java APIs which comply with the MExE security requirements in table 3, such as:

- OCF SmartCard API OpenCard, available from [21]. If the ME supports smartcards other than the SIM, and the smartcard is open to 3rd party applications, then the opencard.core.terminal section of the OpenCard API may be used to access the card.

6.2.5 Mandated services and applications

6.2.5.1 WAP browser support

To provide backward compatibility to MExE classmark 1, i.e. allow access to services designed for MExE classmark 1 devices, classmark 2 devices must feature a pre-installed or pre-loaded WAP browser that is capable of rendering at least the following content formats:

- tokenised WML documents (“WML decks”)

- WMLscript bytecode

- A WAP service in a MExE classmark 2 MS, shall execute in the same manner as it executes in a MExE classmark 1 MS, and is subject to the same security requirements as in a MExE classmark 1 MS.

~~A WAP service in a MExE classmark 2 MS shall execute in the same manner as it executes in a MExE classmark 1 MS.~~

Other WML formats (such as textual WML documents or textual WMLscripts) are optional.

The MExE MS shall enable ~~T~~the pre-installed/pre-loaded WAP browser ~~may~~ to be upgraded, replaced or extended by transferring, a replacement, extension or plug-in mechanism to the MS. Depending on user preferences identified in the user profile and the terminal capabilities, the pre-installed or pre-loaded WAP browser may be overwritten or the new browser stored in a different location.

3GPP TSG-T2 #9 / ETSI SMG4

Utrecht, Netherlands, 15-19 May 2000

TSGT2#9(00)0304

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	005	Current Version:	3.1.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 10.05.2000

Subject: ME actions on SIM insertion and/or power up

Work item: MExE

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Correction

Clauses affected: 8.5.1.1

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

8.5.1.1 ME actions on SIM insertion and/or power up.

The requirements in this sub-clause ensure that the operator domain on the ME belongs to the same operator as the operator that issued the SIM inserted in the ME and, if there is an operator root public key (ORPK) on the SIM, that trusted operator applications on the terminal were verified using that ORPK.

The ME shall support the use and management of an Operator root public key (ORPK) on the SIM. Note that this does not apply to MExE release 98.

~~*Editor's note: This line not to apply to release 98 spec*~~

On power up of the terminal, the terminal shall behave as dictated by figure 6 below.

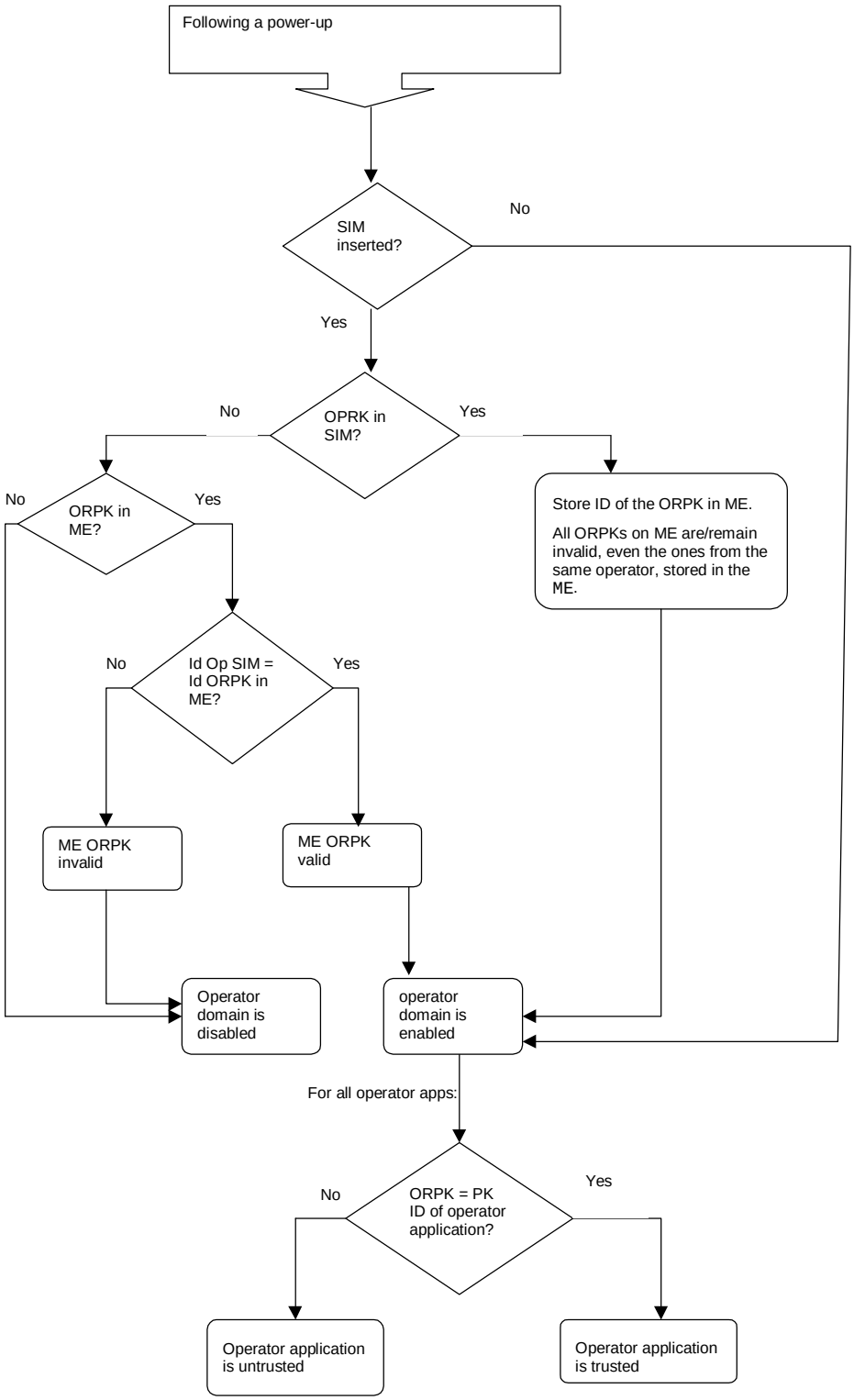


Figure 6: Terminal behaviour on power up

*Editor's n*Note that : Oin DCS1900 the MCC+MNC is 6 digits, but elsewhere it is 5 digits. The ME needs to know how many digits to use, however this is outside the scope of this specification. This problem may have been solved already. The identity of the root public key has to be defined.

The terminal shall only read the SIM ORPK from the SIM when required and shall not store a SIM ORPK on the terminal.

When an operator root public key stored on the ME is marked as invalid, all operator applications verified using that root public key or by certificates verified by a chain that terminates with that root public key, shall cease operation as soon as possible and shall be marked as untrusted.

3GPP TSG-T WG2#9

Maarssen, Netherlands, 15-19 May 2000

TSGT2#9(2000)295

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	006	Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: T2 **Date:** 26.04.2000

Subject: Client/Server 'negotiation'

Work item: MExE

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Current text concerning CC/PP based capability negotiation is misleading and could be misinterpreted.

Clauses affected: 4.4

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments: Refer to WAP UAProf specification and W3C Consortium CC/PP notes.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

4.4 Capability and content negotiation

Interaction between the MExE MS and the MSE shall be supported by the use of the hypertext transfer protocol HTTP/1.1 [9], or an HTTP/1.1 derived protocol (e.g. WSP as defined in Wireless Application Protocol [6]). Communication between the MExE MS and the MSE supports:-

- Capability negotiation

  The MExE MS connects to the MSE by using HTTP/1.1 or an HTTP/1.1 derived protocol. Capability negotiation between the MExE MS and the MSE only takes place for the first time after the MExE MS has connected to the MSE, and the MSE is informed about the MExE MS. Without this first initial contact from the MExE MS, the MSE has no knowledge of the MExE MS, and thereafter the MSE may connect to the MExE MS by using HTTP/1.1 or an HTTP/1.1 derived protocol.

  Capability negotiation represents the mechanism by which the MExE MS and the MSE interact to inform each other of the specific mechanisms, capabilities and support which each is able to provide or support within the scope of a MExE service interaction. The capability negotiation normally takes place prior to any content transfer between the two entities.

  Capability negotiation is used by the MExE MS~~E~~ to ~~request~~ inform the MS~~' MEx~~E of its capabilities~~, to which a response may be returned by the MExE MS. Information is normally requested by the MSE and supplied by the MExE MS, however t~~. The MExE MS may ~~also~~ be informed by the MSE of its use~~current view~~ of the MExE MS's capabilities. The MExE MS may also spontaneously inform the MSE of its capabilities ~~without initially being requested to send them~~ (i.e. following a change in MExE support, such as removal of MExE MS from a docking station with its keyboard, mouse and monitor). ~~The~~ A subset of characteristics which may be ~~requested and~~ transferred between the MExE MS and the MSE during the capability negotiation are identified in subclause 4.4.1 Capability negotiation characteristics.

- Content negotiation

  Content negotiation represents the means by which the MExE MS and the MSE inform each other of the requested and available form of content. If needed, the content negotiation may take place following capability negotiation between the two. The methods for content negotiation are the basic HTTP/1.1. or WSP methods explained in [9] and [6].

  Content negotiation is used to select the best representation of an entity when there are multiple representations of the entity available from the MSE. The entity (e.g. a service, an image, etc) is located behind a URI, and the application in the MExE MS connects to the URI by using HTTP/1.1 or an HTTP/1.1 derived protocol. The best representation of an entity can be decided by the server (server-driven negotiation) or by the client application (agent-driven negotiation).

Both the capability and the content negotiation has the same purpose: to optimise the content according to client's capabilities. The term "content negotiation" has been used e.g. in the HTTP specification and the HTTP/1.1. and the WSP contain headers to perform the content negotiation. However, the capability negotiation in MExE aims at extending the basic HTTP and WSP methods for content negotiation. MExE terminal is free to use both the existing HTTP/WSP content negotiation methods and the new MExE capability negotiation methods.

The content negotiation transferred between the MExE MS and the MSE is identified in subclause 4.4.2 Client Capability Report onwards.

4.4.1 Capability negotiation characteristics

Method for capability negotiation is based on the CC/PP specification made by W3C, [16]. The properties and the actual schema is based on the WAP UAProf group specification [17]. The Composite Capability/ Preferences Profiles framework is intended to provide an efficient mechanism for enabling enhanced content and service negotiation through a standardised format for user agent profiles. The use of Resource Description Framework (RDF) in CC/PP allows for interoperable encoding of the profile metadata in XML and supports multiple vocabularies to provide for future extensibility. WAP UAProf is based on the CC/PP framework. The purpose of the UAProf is to specify

- an RDF based schema and vocabulary for CC/PP in the context of WAP UAProf that includes the class definitions and semantics of attributes described in a user agent profile, and

- guidelines for schema extensibility to support a composite profile that enables future additions to the vocabulary and schema.

Not all capabilities have to be reported in the request to the server but instead, the client may point to ~~an~~ URL(s) where the server may fetch the properties. An MSE may, or may not, use the client capability information.

The generic set of capabilities which may be negotiated between the client and the server consists of the subsequently identified properties in the UAProf schema, [17]. A MExE terminal shall support (but not be limited to) the following properties in the UAProf schema for capability negotiation::-

- MexeClassmark
- MexeSpec
- Vendor
- Model
- Screensize
- ScreenSizeChar
- ColorCapable
- AudioInputEncoder
- VideoInputEncoder
- PointingResolution
- `CcppAccept-Language`
- Keyboard
- SoftwareNumber
- SupportedBearers

It is not required that a MExE terminal shall send all the above properties together when sending a request, however it shall be possible for the MExE terminal to send one or more of the above properties ~~if subsequently requested by the server~~, with user permission.

Generally, the combination of user profile and ME logic will determine the information sent in the capability negotiation from the MExE device to the MExE Service Environment. As an example, for the support of VideoInputEncoder ~~location~~ information the user's profile controls if and when VideoInputEncoder ~~location~~ information may be sent to the MExE Service Environment (e.g. never sent, always sent, only after user confirmation).

The capability negotiation process shall be used by the client to permit transfer of capabilities from the client to the server. By transferring its capabilities, the client will support efficient use of resources both over the radio interface as well as in the client or server. Capability negotiation shall be performed prior to transfer over the radio interface to verify as far as possible the ability of the client to support any services to be downloaded.

In order to transfer the capability information between the MExE MS and the MSE, CC/PP method is used with the schema defined in the WAP UAProf working group.

3GPP TSG-T2 #9 / ETSI SMG4

Utrecht, Netherlands, 15-19 May 2000

TSGT2#9(00)0296

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	007	Current Version:	3.1.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*

(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: T2 **Date:** 10.05.2000

Subject: Third Party Root Public Key

Work item: MExE

Category: *(only one category shall be marked with an X)*

			Release:		
F	Correction	X		Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Minor clarification

Clauses affected: 8.5.3

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

8.5.3 Third party root public key

The ME shall support secure storage for at least one certificate containing a third party root public key. The ME shall support the use and management of Third Party root public keys on the SIM. The ME may contain root public key (s) generated by CA(s) implicitly trusted by the user. The user will be able to securely install (using a secure transport) or remove Third Party root public keys at any time using a system administrative tool.

The Manufacturer, Operator and Administrator may at their discretion, securely install certificates containing Third Party root public key(s) on behalf of the user, e.g. at the time of manufacture by the Manufacturer. See section 8.14 for details of Administrator control of Third Party certificate download.

If a Third Party public key is deleted or becomes invalid, then the certificate chain to MExE executables previously executing in the Third Party Domain certified by that public key will become "untrusted".

There may be any number of Third Party root public keys on the MS.

The third party domain administrator (user or other body) shall be able to enable and disable Third Party root public keys by using CCM. The process of adding/removing public keys and enabling/disabling public key are independent.

All third party certificates shall be subject to restrictions imposed by valid certificate configuration messages.

See clause 8.8 for the management of Third Party root public keys on the SIM.

3GPP TSG-T WG2#9

Maarssen, Netherlands, 15-19 May 2000

TSGT2#9(2000)291

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	008	Current Version:	3.0.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 10.03.2000

Subject: Third Party root public keys management

Work item: MExE

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Modification of example of Third Party root public keys management, because Administrator has no right to **delete** root public keys.

Clauses affected: 8.7, 8.8

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

8.7 Certificate configuration message (CCM)

The MExE device shall use the CCM to determine the third party certificates (and only the Third Party certificates) that are trusted for use on the MExE MS. The CCM shall only be used to enable or disable third party certificates and can not be used to delete certificates. The CCM may be periodically fetched or downloaded to a MExE device by the Administrator to dynamically configure the third party list using the mechanisms defined in section 8.15.2. The Certificate Configuration Message shall be as shown in Figure 8. This message is essentially a simplified version of a certificate revocation list to satisfy a particular use case. More complex usage requires a full certificate revocation list.

The MExE device may additionally support other means of enabling/disabling root certificates.

8.~~12.~~7.1 CCM Numbering convention

Bits are grouped into octets. The bits of an octet are shown horizontally and are numbered from 0 to 7. Multiple octets are shown vertically and are numbered from 0 to n.

8.~~12.~~7.2 CCM Order of transmission

Frames are transferred in units of octets, in ascending numerical octet order (i.e., octet 0, 1, …, n-1, n). The order of bit transmission is specific to the underlying protocols used to transport the CCM.

8.~~12.~~7.3 CCM Field mapping convention

When a field is contained within a single octet, the lowest bit number of the field represents the lowest-order value. When a field spans more than one octet, the order of bit values within each octet progressively decreases as the octet number increases. In that part of the field contained in a given octet the lowest bit number represents the lowest-order value.

For example, a 16 bit number can be represented as shown in Figure 7.

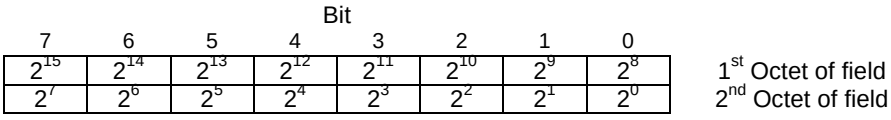


Figure 7: Field mapping convention

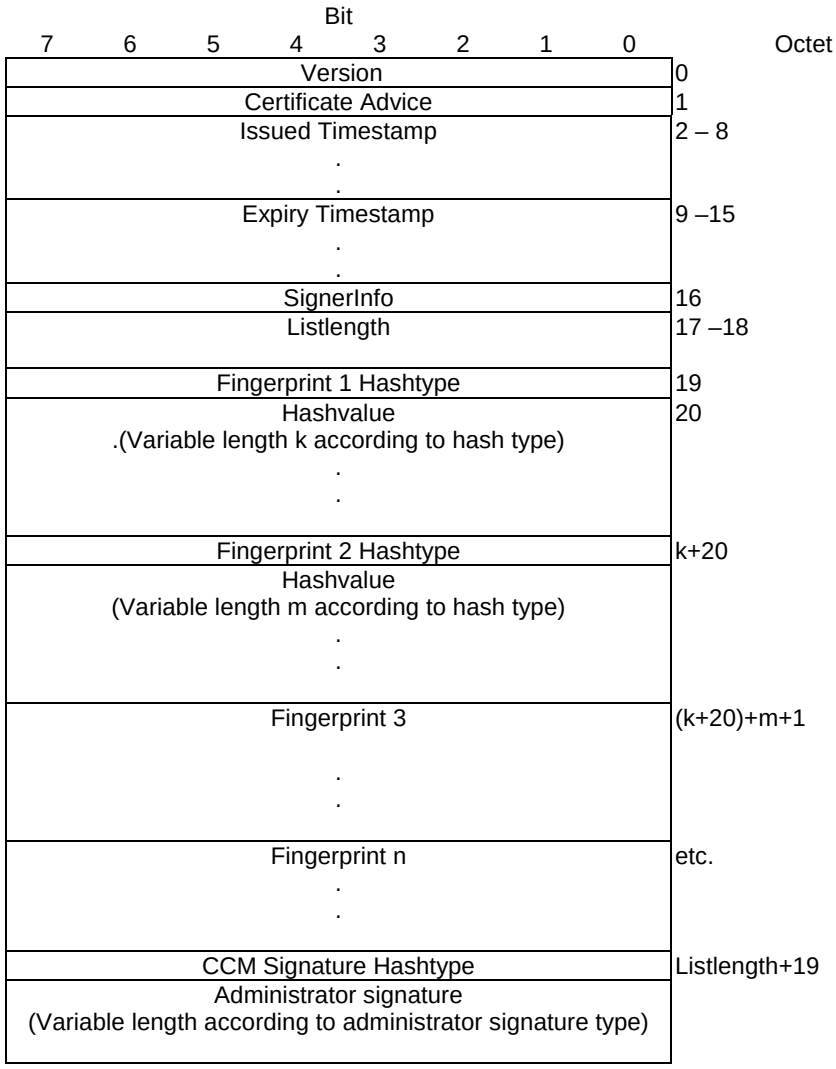


Figure 8 Format of a CCM

version = For MExE-98 the CCM format version is 0. All other values are reserved for future use.

certificateAdvice = enumerated { enable all present and future Third Party certificates (0), disable all present and future Third Party certificates (1), enable present list only (2),enable CCM list (3), disable CCM list (4) }. All other values are reserved for future use.

Issue and Expiry Timestamps = Fields used to identify the issue and expiry date of the CCM. The issue timestamp indicates a time before the current time of day (GMT) when a CCM message must be considered invalid. The expiry timestamp (GMT) identifies the time when a CCM is to be deemed no longer valid. The receiver shall use these parameters to detect a replay attack. A MExE MS maintains information on the last valid CCM message received. A replay attack is an attacker replaying a previous valid CCM message to a MS in order to change the security settings. This is particularly dangerous for CCM messages used to enable certificates. Administrators should try and set the expiration time to be no longer than the next expected system update time of CCM information. CCM messages used to enable-all (rather than disable-all) certificates should be very short lived as the danger of these being used in a replay attack should be considered serious.

The encoding of time (GMT) shall be coded as an OCTET SEQUENCE of seven octets in length as follows:

Octet 0	1	2	3	4	5	Octet 6
Year		Month	Day	Hour	Minute	Second

Element	Size (bits)	Range
Year	16	$(0 – 65535)_{10}$
Month	8	$(1 – 12)_{10}$
Day	8	$(1 - 31)_{10}$
Hour	8	$(0- 23)_{10}$
Minute	8	$(0 – 59)_{10}$
Second *	8	$(0 – 60)_{10}$

*Note: The second field range includes the value 60 in order to accommodate leap seconds.

For example, 1st January, 2001 00:00:30 would be encoded as: 07 d1 01 01 00 00 1E.

SignerInfo = one octet indicating the type of signer information for this CCM. The only currently defined value is device-admin = 0. In this case, no further signer information follows as it is implicit. All other values are reserved for future use.

listLength = The total length of the fingerprint list not including the final CCM signature. Shall be zero when certificateAdvice = enable-all or disable-all.

hashType = enumerated { signature (0), MD5 (1), SHA-1 (2) } All other values are reserved for future use.

hashLength = The number of octets output by the selected hash type (16 for MD5 [23] and 20 for SHA-1 [24]).

The list entries shall contain certificate *fingerprints* in the form of hashes of the encoded signed certificates. The full hash output for the specified algorithm shall be used to generate the fingerprint. A list generator shall check to insure that no two list entries match when creating a list. For an X509v3 [26] or X9.68 (currently being drafted) certificate the fingerprint hash shall be computed over the ASN.1 encoded signed certificate object, first octet to last octet. For WTLS certificates the hash shall be computed over the signed WTLS certificate in network transmission format, first octet to last octet.

The signature type and length shall be indicated by the administrator certificate, which shall be present on the device. If no administrator certificate is on the device or the signature does not verify the message shall be rejected.

Upon receipt of a valid certificate configuration message the MExE device shall go through the third party certificate list, computing fingerprints if they are not stored with the certificate, enabling or disabling each certificate according to the following conditions

- certificateAdvice is enable-all all Third Party certificates shall be enabled
- certificateAdvice is disable-all all Third Party certificates shall be disabled
- certificateAdvice is enable present list only enable all Third Party certificates currently on device, do not enable any future certificates (this option allow the list to be frozen at time of manufacture) until Administrator changes
- certificateAdvice is enable-list if its fingerprint occurs in the CCM, it shall be enabled, otherwise it shall be disabled
- certificateAdvice is disable-list if its fingerprint occurs in the CCM, it shall be disabled, otherwise it shall be enabled

For future releases, the setting of fine grained permissions for each certificate is expected to be supported.

An implementation shall keep track of the domain that authorised a given application. If a CCM message is received while MExE applications are currently running the implementation shall check to ensure any applications no longer in a trusted domain have their permissions re-configured appropriately and actions that are no longer permissible are terminated.

8.7.~~1~~4 Authorised CCM download mechanisms

The download of third party certificate lists by a remote administrator shall be performed by using a secure mechanism as defined below. The download mechanisms shall use HTTP over IP and/or the WAP Protocol. The URL from which the CCM is downloaded shall be in the administrator certificate if the CCM was not downloaded with the Administrator certificate. The format for storing the URL information with the certificate shall be as shown in figure 9:

Urltype	CharacterSet	UrlLength	URL

Figure 9: CCM Message URL storage format

Urltype= one byte, enumerated {WAP (0), HTTP (1)}. All other values are reserved for future use

CharacterSet = one byte, Internet Assigned Numbers Authority assigned character set.

UrlLength = one byte unsigned integer, length of the URL in octets.

The format for storing the URL information in the certificate shall be defined as part of the enhanced administrator mechanism.

When the administrator is changed, then the CCM shall also be changed. If there is URL information with the certificate as described in figure 9, then the new CCM shall be obtained using the URL. If the Administrator certificate was downloaded in a JAR file, the CCM shall be obtained from the same JAR file.

8.8 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE MS

All applications in the Domain are to be signed by a key which shall be verified back to a Third Party root public key on the MExE MS. The Third Party root public keys shall be managed (e.g. addition/ ~~deletion/~~mark trusted/mark untrusted~~/change fine grained access privileges~~) by an administrator that is designated by the owner of the MExE MS using the MExE administrator provisioning mechanism. A mechanism is required to be provided to enable the owner of the device to dynamically assign an administrator. The mechanism shall support the following cases:

- the user is the owner
- the owner is at a remote location. In this case the owner could be the operator, a service provider or a third party.
- the owner of the MExE-SIM wants to be a temporary administrator.

3GPP TSG-T2 #9 / ETSI SMG4

Utrecht, Netherlands, 15-19 May 2000

TSGT2#9(00)0300

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

23.057	CR	009	Current Version:	3.1.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*

(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: T2 **Date:** 10.05.2000

Subject: User permission types (visual indication)

Work item: MExE

Category: *(only one category shall be marked with an X)*

			Release:	
F	Correction	X	Phase 2	
A	Corresponds to a correction in an earlier release		Release 96	
B	Addition of feature		Release 97	
C	Functional modification of feature		Release 98	
D	Editorial modification		Release 99	X
			Release 00	

Reason for change: Correction

Clauses affected: 8.3

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

8.3 User permission types

The term "user permission" is defined to mean that the user can give permission for a specific action in one of the ways defined in Table 4. Support of blanket permission and single action permission is mandatory, but support of session permission is optional.

All prompts for user permission as described in Table 4 must display a user friendly name identifying the signer of the corresponding MExE executable, if available. The user shall be able to request to see the "subject" field of the certificate of the signer ("subject" here refers to the "subject" fields of WTLS and X.509 certificates and an equivalent field for any other format of certificate). If an application, for which user permission is being sought, is untrusted, the fact that the application is untrusted shall be at least visually indicated to the user, if the ME is capable of visual indication, whenever user permission is sought. Other means of indication are additionally permitted. If the ME is not capable of visual indication, or is not designed for use by a human user, other means of indication shall be used.

The user shall be prompted for user permission relating to all action groups listed in the Table 3 that are required by the MExE executable. If a prompt for permission relates to more than one action, e.g. networking and user data, then it shall list the individual action group permissions which will be granted, though the action group permissions can all be granted with a single user action. This condition applies to any prompts relating to user permissions in Table 4.

Note that blanket permission cannot be used for uninstalled MExE executables e.g. applets, WMLS.

3GPP TSG-T2 meeting #9
Utrecht, The Netherlands, 15-19 May 2000

Document *T2- 000217*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007	**CR**	**033**	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 18/05/2000

Subject: +CSDF,+CCLK and +CALA(4 digits for year field)

Work item: Technical Enahncements

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature	X		Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: To allow 4 digits for year field

Clauses affected: 6.22 8.15 8.16

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.22 Settings date format +CSDF

Table 29: +CSDF parameter command syntax

Command	Possible response(s)
+CSDF=[[<mode>][,<auxmode>]]	*+CME ERROR: <err>*
+CSDF?	+CSDF:<mode>[,<auxmode>] *+CME ERROR: <err>*
+CSDF=?	+CSDF:(list of supported <mode>s) [, (list of supported <auxmode>s)] *+CME ERROR: <err>*

Description

This command sets the date format via MMI of the date information presented to the user, which is specified by use of the <mode> parameter . The <mode> affects the date format on the phone display and doesn't affect the date format of the AT command serial interface. The command also sets the date format of the TE-TA interface, which is specified by use of the <auxmode> parameter. (e.g. the <auxmode> affects the <time> of +CCLK and +CALA.) If the parameter is omitted ("+CSDF =","+CSDF =<mode>","+CSDF=,<auxmode>"),then this sets the default value.

Defined values

<mode>:

NOTE: It is manufacturer specific which modes that are supported.

1 DD-MMM-YYYY

NOTE: Presentation of MMM is language dependent.

2 DD-MM-YY

3 MM/DD/YY

4 DD/MM/YY

5 DD.MM.YY

6 YYMMDD

7 YY-MM-DD

8-255 Manufacturer specific

<auxmode>:

1 yy/MM/dd (default)

2 yyyy/MM/dd

also all other values are reserved by this TS

NOTE: The <time> format of +CCLK and +CALA "yy/MM/dd,hh:mm:ss±zz" when <auxmode>=1 and it is "yyyy/MM/dd,hh:mm:ss±zz" when <auxmode>=2. If ME does not support time zone information then the three last characters may be omitted. (see +CCLK command)

Implementation

Optional

8.15 Clock +CCLK

Table 70: +CCLK parameter command syntax

Command	Possible response(s)
+CCLK=<time>	*+CME ERROR: <err>*
+CCLK?	+CCLK: <time> *+CME ERROR: <err>*
+CCLK=?	

Description

Set command sets the real-time clock of the ME. If setting fails in an ME error, +CME ERROR: <err> is returned. Refer subclause 9.2 for <err> values.

Read command returns the current setting of the clock.

Defined values

<time>: string type value; format is "yy/MM/dd,hh:mm:ss±zz", where characters indicate year (two last digits), month, day, hour, minutes, seconds and time zone (indicates the difference, expressed in quarters of an hour, between the local time and GMT; range -47...+48). E.g. 6th of May 1994, 22:10:00 GMT+2 hours equals to "94/05/06,22:10:00+08"

NOTE: If ME does not support time zone information then the three last characters of <time> are not returned by +CCLK?. The format of <time> is specified by use of the +CSDF command.

Implementation

Optional.

8.16 Alarm +CALA

Table 71: +CALA parameter command syntax

Command	Possible response(s)
+CALA=<time>[,<n>[,<type>[,<text>[,<recurr>[,<silent>]]]]]	*+CME ERROR: <err>*
+CALA?	[+CALA: <time>,<n1>,<type>,[<text>],[<recurr>],<silent> [<CR><LF>+CALA: <time>,<n2>,<type>,[<text>],[<recurr>],<silent> [...]]] *+CME ERROR: <err>*
+CALA=?	+CALA: (list of supported <n>s),(list of supported <type>s),<tlength>,<rlength>,(list of supported <silent>s) *+CME ERROR: <err>*

Description

Set command sets an alarm time in the ME. There can be an array of different types of alarms, and each alarm may cause different text to be displayed in the ME display. If setting fails in an ME error, +CME ERROR: <err> is returned. Refer subclause 9.2 for <err> values.

To set up a recurrent alarm for one or more days in the week, the <recurr>-parameter may be used.

When an alarm is timed out and executed, the unsolicited result code +CALV: <n> is always returned, even if the alarm is set up to be silent.

Read command returns the list of current active alarm settings in the ME.

Test command returns supported array index values, alarm types, and maximum length of the text to be displayed.

Defined values

<time>: refer +CCLK,+CSDF

NOTE: If the <recurr>-parameter is used, the <time>-parameter must not contain a date.

<n>, <n1>, <n2>: integer type value indicating the index of the alarm; default is manufacturer specific

<type>: integer type value indicating the type of the alarm (e.g. sound, volume, LED); values and default are manufacturer specific

<text>: string type value indicating the text to be displayed when alarm time is reached; maximum length <tlength>

<tlength>: integer type value indicating the maximum length of <text>

<recurr>: string type value indicating day of week for the alarm in one of the following formats:

"<1..7>[,<1..7>[…]]" – Sets a recurrent alarm for one or more days in the week. The digits 1 to 7 corresponds to the days in the week, Monday (1), …, Sunday (7).
Example: The string "1,2,3,4,5" may be used to set an alarm for all weekdays.

"0" – Sets a recurrent alarm for all days in the week.

<rlength>: integer type value indicating the maximum length of <recurr>

<silent>: Integer type value indicating if the alarm is silent or not. If set to 1 the alarm will be silent and the only result from the alarm is the unsolicited result code +CALV. If set to 0 the alarm will not be silent.

Implementation

Optional.

3GPP TSG-T2 meeting #9
Utrecht, The Netherlands, 15-19 May 2000

Document *T2- 000337*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007	**CR**	**034**	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 18/05/2000

Subject: APN presentation

Work item: Technical Enahncements

Category: *(only one category shall be marked with an X)*

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change:

In order to indicate the Access Point Name (APN) to the user, the IE of APN had been already added to the air-message" REQUEST PDP CONTEXT ACTIVATION", as specified in TS 24.008 for R'99, which is sent by the network to the MS to initiate the activation of a PDP context.

In order to indicate APN to the user when NW requests PDP context activation, it is necessary that the expand result code "+CRING: <text>" is added. Because there is no way to indicate APN from TA to TE. This CR enables to indicate <text> from TA to TE and APN is indicated to the user by the use of <text> field.

In order to use "+CRING: <text>" with backward compatibility, it is necessary to add <mode>=2 to <mode>-parameter.

Clauses affected: 6.11, ANNEX B

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.11 Cellular result codes +CRC

Table 1: +CRC parameter command syntax

Command	Possible response(s)
+CRC=[<mode>]	
+CRC?	+CRC: <mode>
+CRC=?	+CRC: (list of supported <mode>s)

Description

Set command controls whether or not the extended format of incoming call indication or GPRS network request for PDP context activation is used. When enabled, an incoming call is indicated to the TE with unsolicited result code +CRING: <type>(<mode>=1) or +CRING: <text>(<mode>=2) instead of the normal RING.

Test command returns values supported by the TA as a compound value.

NOTE: Similar command may be found in TIA IS-99 [15] and TIA IS-135 [16].

Defined values

<mode>:

0 disables extended format

1 enables extended format (+CRING: <type>)

2 enables extended format (+CRING: <text>)

<type>:

ASYNC [,<priority>[,<subaddr>,<satype>]]	asynchronous transparent
SYNC [,<priority>[,<subaddr>,<satype>]]	synchronous transparent
REL ASYNC [,<priority>[,<subaddr>,<satype>]]	asynchronous non-transparent
REL SYNC [,<priority>[,<subaddr>,<satype>]]	synchronous non-transparent
FAX [,<priority>[,<subaddr>,<satype>]]	facsimile (TS 62)
VOICE [,<priority>[,<subaddr>,<satype>]]	normal voice (TS 11)
VOICE/*XXX* [,<priority>[,<subaddr>,<satype>]]	voice followed by data (BS 81) (*XXX* is ASYNC, SYNC, REL ASYNC or REL SYNC)
ALT VOICE/*XXX* [,<priority>[,<subaddr>,<satype>]]	alternating voice/data, voice first (BS 61)
ALT *XXX*/VOICE [,<priority>[,<subaddr>,<satype>]]	alternating voice/data, data first (BS 61)
ALT VOICE/FAX [,<priority>[,<subaddr>,<satype>]]	alternating voice/fax, voice first (TS 61)
ALT FAX/VOICE [,<priority>[,<subaddr>,<satype>]]	alternating voice/fax, fax first (TS 61)
GPRS <PDP_type>, <PDP_addr>[, <L2P>]	GPRS network request for PDP context activation
VGC <GCA>, <GId>, <ackflag> [,<priority>]	voice group call (TS 91)
VBC <GCA>, <GId>, <ackflag> [,<priority>]	voice broadcast call (TS 92)

The optional <priority> indicates the eMLPP priority level of the incoming call by paging, notification or setup message. The priority level values are as defined in eMLPP specification 3G TS 22.067 [57].

<subaddr>: string type subaddress of format specified by <satype>

<satype>: type of subaddress octet in integer format (refer 3G TS 24.008 [57] subclause 10.5.4.8)

<PDP_type> and <PDP_addr> are as defined in the Define PDP Context (+CGDCONT) command. The optional <L2P> proposes a layer 2 protocol to use between the MT and the TE. It is defined in the Enter GPRS Data Mode (+CGDATA) command. If the MT is unable to announce to the TE the network's request (for example it is in V.25ter online data state) the MT shall reject the request. No corresponding unsolicited result code shall be issued when the MT returns to a command state.

<GCA> is a part of the group call reference as specified in 3G TS 23.003 [7] and indicates group call area.

<GId> is a part of the group call reference as specified in 3G TS 23.003 [7] and indicates group call identification.The <ackflag>=1 proposes that a predefined confirmation procedure is to be used after the call is ended. For <ackflag>=0 no confirmation procedure is required.

<text>: string type field which is manufacturer specific and gives additional information; character set as specified by command Select TE Character Set +CSCS

Implementation

Mandatory when data or fax circuit mode calls implemented or for a ME supporting AT commands only and eMLPP or VGCS or VBS is implemented.

Annex B (normative): Summary of result codes

V.25ter [14] result codes which can be used in GSM/UMTS and codes defined in the present document:

Table B.1: Result codes

Verbose result code (V.25ter command V1 set)	Numeric (V0 set)	Type	Description
+CALV	as verbose	unsolicited	refer subclause 8.16
+CCCM: <ccm>	as verbose	unsolicited	refer subclause 7.16
+CCWA: <number>,<type> ,<class> [,<alpha>]	as verbose	unsolicited	refer subclause 7.12
+CCWV	as verbose	unsolicited	refer subclause 8.28
+CDEV: <elem>,<text>	as verbose	unsolicited	refer subclause 8.10
+CDIP:<number>,<type>[,<subaddr>,<satype>]	as verbose	unsolicited	refer subclause 7.9
+CIEV: <ind>,<value>	as verbose	unsolicited	refer subclause 8.10
+CKEV: <key>,<press>	as verbose	unsolicited	refer subclause 8.10
+CLAV: <code>	as verbose	unsolicited	refer subclause 8.
+CLIP: <number> ,<type>[,<subaddr> ,<satype>[,<alpha>]]	as verbose	unsolicited	refer subclause 7.6
+CME ERROR: <err>	as verbose	final	refer subclause 9.2
+COLP: <number> ,<type>[,<subaddr> ,<satype>[,<alpha>]]	as verbose	intermediate	refer subclause 7.8
+CR: <type>	as verbose	intermediate	refer subclause 6.9
+CREG: <stat>[,<lac> ,<ci>]	as verbose	unsolicited	refer subclause 7.2
+CRING: <type>	as verbose	unsolicited	refer subclause 6.11
+CRING: <text>	as verbose	unsolicited	refer subclause 6.11
+CSSI: <code1> [,<index>]	as verbose	intermediate	refer subclause 7.17
+CSSU: <code2> [,<index>[,<number>, <type>[,<subaddr>, <satype>]]]	as verbose	unsolicited	refer subclause 7.17
+CTZV: <tz>	as verbose	unsolicited	refer subclause 8.40
+CUSD: <m>[,<str>,<dcs>]	as verbose	unsolicited	refer subclause 7.15
+DR: <type>	as verbose	intermediate	refer subclause 6.13
+ILRR: <rate>	as verbose	intermediate	refer subclause 4.3
BUSY	6	final	busy signal detected
CONNECT	1	intermediate	connection has been established
CONNECT <text>	manufacturer specific	intermediate	as CONNECT but manufacturer specific <text> gives additional information (e.g. connection data rate)
ERROR	4	final	command not accepted

NO ANSWER	7	final	connection completion timeout
NO CARRIER	3	final	connection terminated
NO DIALTONE	5	final	no dialtone detected
OK	0	final	acknowledges execution of a command line
RING	2	unsolicited	incoming call signal from network

3GPP TSG T WG2 #9 / ETSI SMG4
Utrecht, NETHERLANDS
15 - 19 May 2000

Document* *T2-000271

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007	**CR**	**035**	Current Version:	3.4.0

↑ *CR number as allocated by MCC support team*

For submission to: TSG-T#8 *list expected approval meeting # here* ↑

for approval [X]
For information [ ]

Strategic [ ]
non-strategic [ ]
(for SMG use only)

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 10-05-2000

Subject: +CAJOIN also serves to join an ongoing group or a broadcast call

Work item: ASCI

Category: *(only one category shall be marked with an X)*

F	Correction	[X]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[ ]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change: This AT command should applied in case of incoming group or broadcast call but also in case of a group or broadcast call held through a +CAREJ

Clauses affected: 11.1.1

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

11.1.1 Accept an incoming Voice Group or Voice Broadcast Call +CAJOIN

Table 1: CAJOIN parameter command syntax

Command	Possible Response(s)
+CAJOIN=<service>, <GId> ,<GCA>	*+CME ERROR: <err>*
CAJOIN=?	

Description

The execute command accepts an incoming or ongoing voice group or voice broadcast call. ~~indicated by a RING or +CRING, the command is applicable as long the indication is pending.~~

See command +CALCC to get a list of current voice group or voice broadcast calls.

Defined Values

<GId>: a digit string that specifies the group identification for the incoming voice group or voice broadcast call.

<GCA>: a digit string that specifies the group call area identification for the incoming voice group or voice broadcast call.

<service> (tele-service):

17 voice group call

18 voice broadcast call

Implementation

Mandatory for a ME supporting AT commands only and VGCS or VBS is implemented.

3GPP TSG T WG2 #9 / ETSI SMG4
Utrecht, NETHERLANDS
15 - 19 May 2000

Document* *T2-000287

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007 **CR** **036** Current Version: 3.4.0

↑ *CR number as allocated by MCC support team*

For submission to: TSG-T#8 for approval [X] Strategic [ ]
list expected approval meeting # here ↑ For information [ ] non-strategic [ ] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: T2 **Date:** 16-05-2000

Subject: +CAULEV, the uplink status presentation in a Voice Group Call

Work item: ASCI

Category: *(only one category shall be marked with an X)*

F	Correction	[X]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[ ]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change: The purpose of the command is to manage the presentation of the uplink status when it has changed rather than each time the UPLINK_FREE message is received. The UPLINK_FREE message is received too often and the old solution doesn't function properly.
If there is no active VBS/VGCS call, no uplink status should be returned by the read command otherwise the information indicated is wrong.

Clauses affected: 11.1.5

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

11.1.5 Voice Group Call Uplink Status Presentation +CAULEV

Table 1: CAULEV parameter command syntax

Command	Possible Response(s)
+CAULEV=[<mode>]	*+CME ERROR: <err>*
+CAULEV?	+CAULEV: <mode>[,<status>] *+CME ERROR: <err>*
+CAULEV=?	+CAULEV: (list of supported <mode>s)

Description

The set command enables or disables the presentation of uplink access status for an active VGCS call. When enabled the unsolicited response +CAULEV: <status> is returned from MT to TE whenever the call uplink status changes.~~after every UPLINK_FREE or UPLINK_BUSY message received from the network.~~

Read command returns the current uplink <status> and the selected <mode>.

The test command returns values supported as a compound value.

Defined Values

<mode>: status of unsolicited result response presentation

0 disabled (default)

1 enabled

<status>: network uplink access status

0 uplink free

1 uplink busy

Implementation

Mandatory for a ME supporting AT commands only and VGCS is implemented.

3GPP TSG T WG2 #9 / ETSI SMG4
Utrecht, NETHERLANDS
15 - 19 May 2000

Document* *T2-000286

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007 **CR** **037** Current Version: 3.4.0

↑ *CR number as allocated by MCC support team*

For submission to: TSG-T#9 *list expected approval meeting # here ↑*

for approval [X] For information [ ]

Strategic [ ] non-strategic [ ] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 16-05-2000

Subject: CME ERROR extensions for ASCI Commands

Work item: ASCI

Category: *(only one category shall be marked with an X)*

F	Correction	[X]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[ ]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change: CME ERROR values are already referenced in 27.007 R99 but they are missing in sub-clause "9 Mobile Equipement errors".

Clauses affected: New sub-clause 9.2.3

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

9 Mobile Equipment errors

9.1 Report Mobile Equipment error +CMEE

Table 1: +CMEE parameter command syntax

Command	Possible response(s)
+CMEE=[<n>]	
+CMEE?	+CMEE: <n>
+CMEE=?	+CMEE: (list of supported <n>s)

Description

Set command disables or enables the use of result code +CME ERROR: <err> as an indication of an error relating to the functionality of the ME. When enabled, ME related errors cause +CME ERROR: <err> final result code instead of the regular ERROR final result code. ERROR is returned normally when error is related to syntax, invalid parameters, or TA functionality.

Test command returns values supported by the TA as a compound value.

Defined values

<n>:

0 disable +CME ERROR: <err> result code and use ERROR instead

1 enable +CME ERROR: <err> result code and use numeric <err> values (refer next subclause)

2 enable +CME ERROR: <err> result code and use verbose <err> values (refer next subclause)

Implementation

Mandatory for <n> values 0 and 1.

9.2 Mobile Equipment error result code +CME ERROR

The operation of +CME ERROR: <err> result code is similar to the regular ERROR result code: if +CME ERROR: <err> is the result code for any of the commands in a command line, none of the following commands in the same command line is executed (neither ERROR nor OK result code shall be returned as a result of a completed command line execution). The format of <err> can be either numeric or verbose. This is set with command +CMEE (refer previous subclause).

NOTE: ITU-T V.25ter [14] command V does not affect the format of this result code.

<err> values (numeric format followed by verbose format):

9.2.1 General errors

0 phone failure

1 no connection to phone

2 phone-adaptor link reserved

3 operation not allowed

4 operation not supported

5 PH-SIM PIN required

6 PH-FSIM PIN required

7 PH-FSIM PUK required

10 SIM not inserted

11 SIM PIN required

12 SIM PUK required

13 SIM failure

14 SIM busy

15 SIM wrong

16 incorrect password

17 SIM PIN2 required

18 SIM PUK2 required

20 memory full

21 invalid index

22 not found

23 memory failure

24 text string too long

25 invalid characters in text string

26 dial string too long

27 invalid characters in dial string

30 no network service

31 network timeout

32 network not allowed - emergency calls only

40 network personalisation PIN required

41 network personalisation PUK required

42 network subset personalisation PIN required

43 network subset personalisation PUK required

44 service provider personalisation PIN required

45 service provider personalisation PUK required

46 corporate personalisation PIN required

47 corporate personalisation PUK required

100 unknown

9.2.2 GPRS-related errors

9.2.2.1 Errors related to a failure to perform an Attach

Numeric	Text
103	Illegal MS (#3)
106	Illegal ME (#6)
107	GPRS services not allowed (#7)
111	PLMN not allowed (#11)
112	Location area not allowed (#12)
113	Roaming not allowed in this location area (#13)

(Values in parentheses are GSM 04.08 cause codes.)

9.2.2.2 Errors related to a failure to Activate a Context

Numeric	Text
132	service option not supported (#32)
133	requested service option not subscribed (#33)
134	service option temporarily out of order (#34)
149	PDP authentication failure

(Values in parentheses are GSM 04.08 cause codes.)

9.2.2.3 Other GPRS errors

Numeric	Text
150	invalid mobile class
148	unspecified GPRS error

Other values in the range 101 - 150 are reserved for use by GPRS

9.2.3 VBS / VGCS and eMLPP -related errors

Numeric	Text
151	VBS/VGCS not supported by the network
152	No service subscription on SIM
153	No subscription for group ID
154	Group Id not activated on SIM
155	No matching notification
156	VBS/VGCS call already present
157	Congestion
158	Network failure
159	Uplink busy
160	No access rights for SIM file
161	No subscription for priority
162	operation not applicable or not possible

Other values in the range 151 - 170 are reserved for use by VBS/VGCS and eMLPP

Also all other values below 256 are reserved

Implementation
Mandatory for numeric format codes applicable to implemented command set.

9.3 Informative examples

An example of TA responses with all three +CMEE values when ME manufacturer identification is requested but ME is not connected to the TA:

```
AT+CMEE=0    (+CME ERROR shall not be used)
OK
AT+CGMI
ERROR
AT+CMEE=1    (use numeric <err>)
OK
AT+CGMI
+CME ERROR: 1
AT+CMEE=2    (use verbose <err>)
OK
AT+CGMI
+CME ERROR: no connection to phone
```

3GPP TSG T WG2 #9 / ETSI SMG4
Utrecht, NETHERLANDS
15 - 19 May 2000

Document* *T2-000280

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007 **CR** **038** Current Version: 3.4.0

↑ *CR number as allocated by MCC support team*

For submission to: TSG-T#8 *list expected approval meeting # here ↑*

for approval [X] For information [ ]

Strategic [ ] non-strategic [ ] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 16-05-2000

Subject: Correction of the description of the +CRC

Work item: ASCI

Category: *(only one category shall be marked with an X)*

F	Correction	[X]	**Release:**	Phase 2	[ ]
A	Corresponds to a correction in an earlier release	[ ]		Release 96	[ ]
B	Addition of feature	[ ]		Release 97	[ ]
C	Functional modification of feature	[ ]		Release 98	[ ]
D	Editorial modification	[ ]		Release 99	[X]
				Release 00	[ ]

Reason for change: There is no mention of VBS and VGCS calls for the description of +CRC
The function of the command for the services VBS/VGCS is unclear unless the event for the +CRING indication is included in the description of the command.

Clauses affected: 6.11

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

6.11 Cellular result codes +CRC

Table 1: +CRC parameter command syntax

Command	Possible response(s)
+CRC=[<mode>]	
+CRC?	+CRC: <mode>
+CRC=?	+CRC: (list of supported <mode>s)

Description

Set command controls whether or not the extended format of incoming call indication or GPRS network request for PDP context activation or notification for VBS/VGCS calls is used. When enabled, an incoming call is indicated to the TE with unsolicited result code +CRING: <type> instead of the normal RING.

Test command returns values supported by the TA as a compound value.

NOTE: Similar command may be found in TIA IS-99 [15] and TIA IS-135 [16].

Defined values

<mode>:

0 disables extended format

1 enables extended format

<type>:

ASYNC [,[<priority>][,<subaddr>,<satype>]]	asynchronous transparent
SYNC [,[<priority>][,<subaddr>,<satype>]]	synchronous transparent
REL ASYNC [,[<priority>][,<subaddr>,<satype>]]	asynchronous non-transparent
REL SYNC [,[<priority>][,<subaddr>,<satype>]]	synchronous non-transparent
FAX [,[<priority>][,<subaddr>,<satype>]]	facsimile (TS 62)
VOICE [,[<priority>][,<subaddr>,<satype>]]	normal voice (TS 11)
VOICE/*XXX* [,[<priority>][,<subaddr>,<satype>]]	voice followed by data (BS 81) (*XXX* is ASYNC, SYNC, REL ASYNC or REL SYNC)
ALT VOICE/*XXX* [,[<priority>][,<subaddr>,<satype>]]	alternating voice/data, voice first (BS 61)
ALT *XXX*/VOICE [,[<priority>][,<subaddr>,<satype>]]	alternating voice/data, data first (BS 61)
ALT VOICE/FAX [,[<priority>][,<subaddr>,<satype>]]	alternating voice/fax, voice first (TS 61)
ALT FAX/VOICE [,[<priority>][,<subaddr>,<satype>]]	alternating voice/fax, fax first (TS 61)
GPRS <PDP_type>, <PDP_addr>[, <L2P>]	GPRS network request for PDP context activation
VGC <GCA>, <GId>, <ackflag> [,<priority>]	voice group call (TS 91)
VBC <GCA>, <GId>, <ackflag> [,<priority>]	voice broadcast call (TS 92)

<PDP_type> and <PDP_addr> are as defined in the Define PDP Context (+CGDCONT) command. The optional <L2P> proposes a layer 2 protocol to use between the MT and the TE. It is defined in the Enter GPRS Data Mode (+CGDATA) command. If the MT is unable to announce to the TE the network's request (for example it is in V.25ter online data state) the MT shall reject the request. No corresponding unsolicited result code shall be issued when the MT returns to a command state.

<GCA> is a part of the group call reference as specified in GSM 03.03 and indicates group call area.

<GId> is a part of the group call reference as specified in GSM 03.03 and indicates group call identification.The <ackflag>=1 proposes that a predefined confirmation procedure is to be used after the call is ended. For <ackflag>=0 no confirmation procedure is required.

Implementation

Mandatory when data or fax circuit mode calls implemented.

3GPP TSG T WG2 #9 / ETSI SMG4
Utrecht, NETHERLANDS
15 - 19 May 2000

Document* *T2-000234

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.007 **CR** **039** Current Version: 3.4.0

↑ *CR number as allocated by MCC support team*

For submission to: TSG-T#9 *list expected approval meeting # here ↑*

for approval [X] For information [ ]

Strategic [ ] non-strategic [ ] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 10-05-2000

Subject: Definition of the abbreviation of MT

Work item: ASCI

Category: *(only one category shall be marked with an X)*

F	Correction	[X]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[ ]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change: To avoid any doubt on signification of MT :
Either Mobile Terminating either Mobile Termination

Clauses affected: 3.1

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

3.1 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AT	ATtention; this two-character abbreviation is always used to start a command line to be sent from TE to TA
BCD	Binary Coded Decimal
ETSI	European Telecommunications Standards Institute
HSCSD	High Speed Circuit Switched Data
IHOSS	Internet Hosted Octet Stream Service
IMEI	International Mobile station Equipment Identity
IRA	International Reference Alphabet (ITU-T T.50 [13])
IrDA	Infrared Data Association
ISO	International Standards Organisation
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector
ME	Mobile Equipment, e.g. a GSM phone (equal to MS; Mobile Station)
MoU	Memorandum of Understanding (GSM operator joint)
MT	Mobile Termination
OSP	Octet Stream Protocol
OSP:IHOSS	Octet Stream Protocol for Internet Hosted Octet Stream Service
PCCA	Portable Computer and Communications Association
RDI	Restricted Digital Information
RLP	Radio Link Protocol
SIM	Subscriber Identity Module
TA	Terminal Adaptor, e.g. a GSM data card (equal to DCE; Data Circuit terminating Equipment)
TE	Terminal Equipment, e.g. a computer (equal to DTE; Data Terminal Equipment)
TIA	Telecommunications Industry Association
UDI	Unrestricted Digital Information

3GPP TSG T2/SMG 4 Meeting #9
Utrecht, Netherlands 15-19 May 2000

***Document* T2-000330**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

3G 27.007	CR	040	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T2 **Date:** 2000-05-10

Subject: Packet Domain QoS AT-commands

Work item: TEI

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2
A	Corresponds to a correction in an earlier release			Release 96
B	Addition of feature			Release 97
C	Functional modification of feature			Release 98
D	Editorial modification			Release 99 X
				Release 00

Reason for change:

This CR updates the +CGEQREQ, +CGEQMIN and +CGEQNEG commands in order to make them in line with the current R'99 QoS IE, as specified in 24.008.

- 'Maximum bitrate' and 'Guaranteed bitrate' are duplicated and renamed in order to allow for separate parameters for up- and downlink.
- 'SDU format information' is not used for packet domain, removed.
- 'Allocation/Retention Priority' is not negotiated from the mobile terminal, removed.

In addition this CR makes some clarifications concerning parameter types and valid parameter values.

These commands are not available in earlier releases (i.e. R98 and backwards) so there will be no backward compatibility problems.

Clauses affected: 10.1.6, 10.1.7, 10.1.8

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

10.1.6 3G Quality of Service Profile (Requested) +CGEQREQ

Table 1: +CGEQREQ parameter command syntax

Command	Possible Response(s)
+CGEQREQ=[<cid> [,<Traffic class> [,<Maximum bitrate UL> [,<Maximum bitrate DL> [,<Guaranteed bitrate UL> [,<Guaranteed bitrate DL> [,<Delivery order> [,<Maximum SDU size> ~~[,<SDU format information>~~ [,<SDU error ratio> [,<Residual bit error ratio> [,<Delivery of erroneous SDUs> [,<Transfer delay> [,<Traffic handling priority> ~~[,<Allocation/Retention Priority>~~]]]]]]]]]]]]]	OK ERROR
+CGEQREQ?	+CGEQREQ: <cid>, <Traffic class> ,<Maximum bitrate UL> ,<Maximum bitrate DL> ,<Guaranteed bitrate UL> ,<Guaranteed bitrate DL> ,<Delivery order> ,<Maximum SDU size> ~~,<SDU format information>~~ ,<SDU error ratio> ,<Residual bit error ratio> ,<Delivery of erroneous SDUs> ,<Transfer delay> ,<Traffic handling priority> ~~,<Allocation/Retention Priority>~~ [<CR><LF>+CGEQREQ: <cid>, <Traffic class> ,<Maximum bitrate UL> ,<Maximum bitrate DL> ,<Guaranteed bitrate UL> ,<Guaranteed bitrate DL> ,<Delivery order> ,<Maximum SDU size> ~~,<SDU format information>~~ ,<SDU error ratio> ,<Residual bit error ratio> ,<Delivery of erroneous SDUs> ,<Transfer delay> ,<Traffic handling priority> ~~,<Allocation/Retention Priority>~~ […]]
+CGEQREQ=?	+CGEQREQ: <PDP_type>, (list of supported <Traffic class>s) ,(list of supported <Maximum bitrate UL>s), (list of supported <Maximum bitrate DL>s), (list of supported <Guaranteed bitrate UL>s), (list of supported <Guaranteed bitrate DL>s),(list of supported <Delivery order>s) ,(list of supported <Maximum SDU size>s) ~~,(list of supported <SDU format information>s)~~ ,(list of supported <SDU error ratio>s) ,(list of supported <Residual bit error ratio>s) ,(list of supported <Delivery of erroneous SDUs>s) ,(list of supported <Transfer delay>s) ,(list of supported <Traffic handling priority>s) ~~,(list of supported <Allocation/Retention Priority>s)~~ [<CR><LF>+CGEQREQ: <PDP_type>, (list of supported <Traffic class>s) ,(list of supported <Maximum bitrate UL>s), (list of supported <Maximum bitrate DL>s), (list of supported <Guaranteed bitrate UL>s), (list of supported <Guaranteed bitrate DL>s),(list of supported <Delivery order>s) ,(list of supported <Maximum SDU size>s) ~~,(list of~~

Command	Possible Response(s)
	~~supported <SDU format information>s)~~ ,(list of supported <SDU error ratio>s) ,(list of supported <Residual bit error ratio>s) ,(list of supported <Delivery of erroneous SDUs>s) ,(list of supported <Transfer delay>s) ,(list of supported <Traffic handling priority>s) ~~,(list of supported <Allocation/Retention Priority>s)~~ […]]

Description

This command allows the TE to specify a UMTS Quality of Service Profile that is used when the MT sends an Activate PDP Context Request message to the network.

The set command specifies a profile for the context identified by the (local) context identification parameter, <cid>. The specified profile will be stored in the MT and sent to the network only at activation or MS-initiated modification of the related context. Since this is the same parameter that is used in the +CGDCONT and +CGDSCONT commands, the +CGEQREQ command is effectively an extension to these commands. The QoS profile consists of a number of parameters, each of which may be set to a separate value.

A special form of the set command, +CGEQREQ= <cid> causes the requested profile for context number <cid> to become undefined.

The read command returns the current settings for each defined context.

The test command returns values supported as a compound value. If the MT supports several PDP types, the parameter value ranges for each PDP type are returned on a separate line.

Defined values

<cid>: a numeric parameter which specifies a particular PDP context definition (see +CGDCONT and +CGDSCONT commands).

The following parameters are defined in 3G TS 23.107 [46] -

<Traffic class>: a numeric parameter that ~~i~~indicates the type of application for which the UMTS bearer service is optimised.
0 - conversational
1 - streaming
2 - interactive
3 - background
Other values are reserved.

<Maximum bitrate UL>: a numeric parameter that indicates the maximum number of kbits/s delivered to UMTS (up-link traffic) at a SAP. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQREQ=…,32, …).

<Maximum bitrate DL>: a numeric parameter that ~~i~~indicates the maximum number of kbits/s delivered by UMTS (down-link traffic) at a SAP ~~within a period of time, divided by the duration of the period~~. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQREQ=…,32, …).

<Guaranteed bitrate UL>: a numeric parameter that indicates the guaranteed number of kbits/s delivered to UMTS (up-link traffic) at a SAP (provided that there is data to deliver). As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQREQ=…,32, …).

<Guaranteed bitrate DL>: a numeric parameter that ~~i~~indicates the guaranteed number of kbits/s delivered by UMTS (down-link traffic) at a SAP ~~within a period of time~~ (provided that there is data to deliver) ~~, divided by the duration of the period~~. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQREQ=…,32, …).

<Delivery order>: a numeric parameter that ~~I~~indicates whether the UMTS bearer shall provide in-sequence SDU delivery or not.
0 - no ~~(default if value is omitted)~~
1 - yes
Other values are reserved.

<Maximum SDU size>: a numeric parameter (1,2,3,…) that ~~I~~indicates the maximum allowed SDU size in octets~~bits~~.

~~<SDU format information>: List of possible exact sizes of SDUs in bits. If the list contains more than one value, colons separate the values.~~

<SDU error ratio>: a string parameter that ~~I~~indicates the target value for the fraction of SDUs lost or detected as erroneous. SDU error ratio is defined only for conforming traffic. The value is specified as 'mEe'. As an example a target SDU error ratio of $5 \cdot 10^{-3}$ would be specified as '5E3' (e.g. AT+CGEQREQ=…,"5E3",…).

<Residual bit error ratio>: a string parameter that ~~I~~indicates the target value for the undetected bit error ratio in the delivered SDUs. If no error detection is requested, Residual bit error ratio indicates the bit error ratio in the delivered SDUs. The value is specified as 'mEe'. As an example a target residual bit error ratio of $5 \cdot 10^{-3}$ would be specified as '5E3' (e.g. AT+CGEQREQ=…,"5E3",…).

<Delivery of erroneous SDUs>: a numeric parameter that ~~I~~indicates whether SDUs detected as erroneous shall be delivered or not.
0 - no ~~(default if value is omitted)~~
1 - yes
Other values are reserved.

<Transfer delay>: a numeric parameter (0,1,2,…) that ~~I~~indicates the targeted time between request to transfer an SDU at one SAP to its delivery at the other SAP, in milliseconds. ~~Transfer delay is specified for one or more fixed SDU sizes. If transfer delay values are specified for more than one fixed SDU size the values shall be separated by commas and be in the same order as the corresponding fixed SDU sizes specified in the <SDU format information> parameter.~~

<Traffic handling priority>: ~~N~~a numeric parameter (1,2,3,…) that specifies the relative importance for handling of all SDUs belonging to the UMTS bearer compared to the SDUs of other bearers.

~~<Allocation/Retention Priority>: Numeric parameter (1,2,3,…) that specifies the relative importance compared to other UMTS bearers for allocation and retention of the UMTS bearer.~~

<PDP_type>: (see +CGDCONT and +CGDSCONT commands).

If a value is omitted for a particular class then the value is considered to be unspecified.

Implementation

Optional. If the command is not implemented then all the values are considered to be unspecified.

10.1.7 3G Quality of Service Profile (Minimum acceptable) +CGEQMIN

Table 2: +CGEQMIN parameter command syntax

Command	Possible Response(s)
+CGEQMIN=[<cid> [,<Traffic class> [,<Maximum bitrate UL> [,<Maximum bitrate DL> [,<Guaranteed bitrate UL> [,<Guaranteed bitrate DL> [,<Delivery order> [,<Maximum SDU size> ~~[,<SDU format information>~~ [,<SDU error ratio> [,<Residual bit error ratio> [,<Delivery of erroneous SDUs> [,<Transfer delay> [,<Traffic handling priority> ~~[,<Allocation/Retention Priority>~~]]]]]]]]]]]]]	OK ERROR
+CGEQMIN?	+CGEQMIN: <cid>, <Traffic class> ,<Maximum bitrate UL>, <Maximum bitrate

Command	Possible Response(s)
	DL> ,<Guaranteed bitrate UL> ,<Guaranteed bitrate DL>, <Delivery order> ,<Maximum SDU size> ~~,<SDU format information>~~ ,<SDU error ratio> ,<Residual bit error ratio> ,<Delivery of erroneous SDUs> ,<Transfer delay> ,<Traffic handling priority> ~~,<Allocation/Retention Priority>~~ [<CR><LF>+CGEQMIN: <cid>, <Traffic class> ,<Maximum bitrate UL> ,<Maximum bitrate DL> ,<Guaranteed bitrate UL> ,<Guaranteed bitrate DL>, <Delivery order> ,<Maximum SDU size> ~~,<SDU format information>~~ ,<SDU error ratio> ,<Residual bit error ratio> ,<Delivery of erroneous SDUs> ,<Transfer delay> ,<Traffic handling priority> ~~,<Allocation/Retention Priority>~~ […]]
+CGEQMIN=?	+CGEQMIN: <PDP_type>, (list of supported <Traffic class>s) ,(list of supported <Maximum bitrate UL>s) ,(list of supported <Maximum bitrate DL>s), (list of supported <Guaranteed bitrate UL>s), (list of supported <Guaranteed bitrate DL>s) ,(list of supported <Delivery order>s) ,(list of supported <Maximum SDU size>s) ~~,(list of supported <SDU format information>s)~~ ,(list of supported <SDU error ratio>s) ,(list of supported <Residual bit error ratio>s) ,(list of supported <Delivery of erroneous SDUs>s) ,(list of supported <Transfer delay>s) ,(list of supported <Traffic handling priority>s) ~~,(list of supported <Allocation/Retention Priority>s)~~ [<CR><LF>+CGEQMIN: <PDP_type>, (list of supported <Traffic class>s) ,(list of supported <Maximum bitrate UL>s), (list of supported <Maximum bitrate DL>s) ,(list of supported <Guaranteed bitrate UL >s), (list of supported <Guaranteed bitrate DL >s) ,(list of supported <Delivery order>s) ,(list of supported <Maximum SDU size>s) ~~,(list of supported <SDU format information>s)~~ ,(list of supported <SDU error ratio>s) ,(list of supported <Residual bit error ratio>s) ,(list of supported <Delivery of erroneous SDUs>s) ,(list of supported <Transfer delay>s) ,(list of supported <Traffic handling priority>s) ~~,(list of supported <Allocation/Retention Priority>s)~~ […]]

Description

This command allows the TE to specify a minimum acceptable profile, which is checked by the MT against the negotiated profile returned in the Activate/Modify PDP Context Accept message.

The set command specifies a profile for the context identified by the (local) context identification parameter, <cid>. The specified profile will be stored in the MT and checked against the negotiated profile only at activation or MS-initiated modification of the related context. Since this is the same parameter that is used in the +CGDCONT and +CGDSCONT commands, the +CGEQMIN command is effectively an extension to these commands. The QoS profile consists of a number of parameters, each of which may be set to a separate value.

A special form of the set command, +CGEQMIN= <cid> causes the minimum acceptable profile for context number <cid> to become undefined. In this case no check is made against the negotiated profile.

The read command returns the current settings for each defined context.

The test command returns values supported as a compound value. If the MT supports several PDP types, the parameter value ranges for each PDP type are returned on a separate line.

Defined values

<cid>: a numeric parameter which specifies a particular PDP context definition (see +CGDCONT and +CGDSCONT commands).

The following parameters are defined in 3G TS 23.107 [46] -

<Traffic class>: a numeric parameter that i~~I~~ndicates the type of application for which the UMTS bearer service is optimised.
0 - conversational
1 - streaming
2 - interactive
3 - background
Other values are reserved.

<Maximum bitrate UL>: a numeric parameter that indicates the maximum number of kbits/s delivered to UMTS (up-link traffic) at a SAP. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQMIN=…,32, …).

<Maximum bitrate DL>: a numeric parameter that i~~I~~ndicates the maximum number of kbits/s delivered by UMTS (down-link traffic) at a SAP ~~within a period of time, divided by the duration of the period~~. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQMIN=…,32, …).

<Guaranteed bitrate UL>: a numeric parameter that indicates the guaranteed number of kbits/s delivered to UMTS (up-link traffic) at a SAP (provided that there is data to deliver). As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQMIN=…,32, …).

<Guaranteed bitrate DL>: a numeric parameter that i~~I~~ndicates the guaranteed number of kbits/s delivered by UMTS (down-link traffic) at a SAP ~~within a period of time~~ (provided that there is data to deliver)~~, divided by the duration of the period~~. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQMIN=…,32, …).

<Delivery order>: a numeric parameter that i~~I~~ndicates whether the UMTS bearer shall provide in-sequence SDU delivery or not.
0 - no ~~(default if value is omitted)~~
1 - yes
Other values are reserved.

<Maximum SDU size>: a numeric parameter (1,2,3,…) that i~~I~~ndicates the maximum allowed SDU size in octets~~bits~~.

~~<SDU format information>: List of possible exact sizes of SDUs in bits. If the list contains more than one value, the values shall be separated by colons.~~

<SDU error ratio>: a string parameter that i~~I~~ndicates the target value for the fraction of SDUs lost or detected as erroneous. SDU error ratio is defined only for conforming traffic. The value is specified as 'mEe'. As an example a target SDU error ratio of $5 \cdot 10^{-3}$ would be specified as '5E3'~~.~~ (e.g. AT+CGEQMIN=…,"5E3",…).

<Residual bit error ratio>: a string parameter that i~~I~~ndicates the target value for the undetected bit error ratio in the delivered SDUs. If no error detection is requested, Residual bit error ratio indicates the bit error ratio in the delivered SDUs. The value is specified as 'mEe'. As an example a target residual bit error ratio of $5 \cdot 10^{-3}$ would be specified as '5E3' (e.g. AT+CGEQMIN=…,"5E3",…).

<Delivery of erroneous SDUs>: a numeric parameter that i~~I~~ndicates whether SDUs detected as erroneous shall be delivered or not.
0 - no ~~(default if value is omitted)~~
1 - yes
Other values are reserved.

<Transfer delay>: a numeric parameter (0,1,2,…) that i~~I~~ndicates the targeted time between request to transfer an SDU at one SAP to its delivery at the other SAP, in milliseconds. ~~Transfer delay is specified for one or more fixed SDU sizes. If transfer delay values are specified for more than one fixed SDU size the values shall be separated by commas and be in the same order as the corresponding fixed SDU sizes specified in the <SDU format information> parameter.~~

<Traffic handling priority>: a ~~N~~numeric parameter (1,2,3,…) that specifies the relative importance for handling of all SDUs belonging to the UMTS bearer compared to the SDUs of other bearers.

~~<Allocation/Retention Priority>: Numeric parameter (1,2,3,…) that specifies the relative importance compared to other UMTS bearers for allocation and retention of the UMTS bearer.~~

<PDP_type>: (see +CGDCONT and +CGDSCONT commands).

If a value is omitted for a particular class then the value is considered to be unspecified.

Implementation

Optional. If the command is not implemented then no check is made against the negotiated profile.

10.1.8 3G Quality of Service Profile (Negotiated) +CGEQNEG

Table 3: +CGEQNEG action command syntax

Command	Possible Response(s)
+CGEQNEG =[<cid>[,<cid>[,…]]]	+CGEQNEG: <cid>, <Traffic class> ,<Maximum bitrate UL>, <Maximum bitrate DL> ,<Guaranteed bitrate UL>, <Guaranteed bitrate DL> ,<Delivery order> ,<Maximum SDU size> ~~,<SDU format information>~~ ,<SDU error ratio> ,<Residual bit error ratio> ,<Delivery of erroneous SDUs> ,<Transfer delay> ,<Traffic handling priority> ~~,<Allocation/Retention Priority>~~ [<CR><LF>+CGEQNEG: <cid>, <Traffic class> ,<Maximum bitrate UL>, <Maximum bitrate DL> ,<Guaranteed bitrate UL>, <Guaranteed bitrate DL> ,<Delivery order> ,<Maximum SDU size> ~~,<SDU format information>~~ ,<SDU error ratio> ,<Residual bit error ratio> ,<Delivery of erroneous SDUs> ,<Transfer delay> ,<Traffic handling priority> ~~,<Allocation/Retention Priority>~~ […]]
+CGEQNEG=?	+CGEQNEG: (list of <cid>s associated with active contexts)

Description

This command allows the TE to retrieve the negotiated QoS profiles returned in the Activate PDP Context Accept message.

The execution command returns the negotiated QoS profile for the specified context identifiers, <cid>s. The QoS profile consists of a number of parameters, each of which may have a separate value.

The test command returns a list of <cid>s associated with active contexts.

Defined values

<cid>: a numeric parameter which specifies a particular PDP context definition (see +CGDCONT and +CGDSCONT commands).

The following parameters are defined in 3G TS 23.107 [46] -

<Traffic class>: a numeric parameter that i~~I~~ndicates the type of application for which the UMTS bearer service is optimised.
0 - conversational
1 - streaming
2 - interactive
3 - background
Other values are reserved.

<Maximum bitrate UL>: a numeric parameter that indicates the maximum number of kbits/s delivered to UMTS (up-link traffic) at a SAP. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQNEG=…,32, …).

<Maximum bitrate DL>: a numeric parameter that i~~I~~ndicates the maximum number of kbits/s delivered by UMTS (down-link traffic) at a SAP ~~within a period of time, divided by the duration of the period.~~ As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQNEG=…,32, …).

<Guaranteed bitrate UL>: a numeric parameter that indicates the guaranteed number of kbits/s delivered to UMTS (up-link traffic) at a SAP (provided that there is data to deliver). As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQNEG=…,32, …).

<Guaranteed bitrate DL>: a numeric parameter that iIndicates the guaranteed number of kbits/s delivered by UMTS (down-link traffic) at a SAP ~~within a period of time~~ (provided that there is data to deliver)~~, divided by the duration of the period~~. As an example a bitrate of 32kbit/s would be specified as '32' (e.g. AT+CGEQNEG=…,32, …).

<Delivery order>: a numeric parameter that iIndicates whether the UMTS bearer shall provide in-sequence SDU delivery or not.
0 - no ~~(default if value is omitted)~~
1 - yes
Other values are reserved.

<Maximum SDU size>: a numeric parameter that (1,2,3,…) iIndicates the maximum allowed SDU size in octets~~bits~~.

~~<SDU format information>: List of possible exact sizes of SDUs in bits. If the list contains more than one value, colons separate the values.~~

<SDU error ratio>: a string parameter that iIndicates the target value for the fraction of SDUs lost or detected as erroneous. SDU error ratio is defined only for conforming traffic. The value is specified as 'mEe'. As an example a target SDU error ratio of $5 \cdot 10^{-3}$ would be specified as '5E3' (e.g. AT+CGEQNEG=…,"5E3",…).

<Residual bit error ratio>: a string parameter that iIndicates the target value for the undetected bit error ratio in the delivered SDUs. If no error detection is requested, Residual bit error ratio indicates the bit error ratio in the delivered SDUs. The value is specified as 'mEe'. As an example a target residual bit error ratio of $5 \cdot 10^{-3}$ would be specified as '5E3' (e.g. AT+CGEQNEG=…,"5E3",…).

<Delivery of erroneous SDUs>: a numeric parameter that iIndicates whether SDUs detected as erroneous shall be delivered or not.
0 - no ~~(default if value is omitted)~~
1 - yes
Other values are reserved.

<Transfer delay>: a numeric parameter (0,1,2,…) that iIndicates the targeted time between request to transfer an SDU at one SAP to its delivery at the other SAP, in milliseconds. ~~Transfer delay is specified for one or more fixed SDU sizes. If transfer delay values are specified for more than one fixed SDU size the values shall be separated by commas and be in the same order as the corresponding fixed SDU sizes specified in the <SDU format information> parameter.~~

<Traffic handling priority>: a ~~N~~numeric parameter (1,2,3,…) that specifies the relative importance for handling of all SDUs belonging to the UMTS bearer compared to the SDUs of other bearers.

~~<Allocation/Retention Priority>: Numeric parameter (1,2,3,…) that specifies the relative importance compared to other UMTS bearers for allocation and retention of the UMTS bearer.~~

If a value is omitted for a particular class then the value is considered to be unspecified.

Implementation

Optional.

3GPP TSG-2 meeting #9 **Document** ***T2-000351***

Utrecht, Netherlands, 15-19 May 2000

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.103	CR	001	Current Version:	3.0.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: Ericsson **Date:** 16 May 2000

Subject: Introduction of PUSH and TARGET

Work item: SYNC

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

Improvements of the functionality, partially due to improvements in the OBEX protocol, have been made.

- Name of request parameters removed, i.e. no “”OBEX=...”
- Use Base64 instead of URL-encoding for encoding the binary data
- User ID sent in response to the connect request instead of being sent at start of sync. Sync is now initialised using OBEX PUSH.
- Making use of the OBEX Connection ID in order to enable simultaneous sessions.
- TARGET includes request to sync. with e.g. the calendar.
- WHO contains assigned session ID

Clauses affected: Chapter 6 and 7(Tunnelling of OBEX)

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:


help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.2 Client/Server

The client will always call the server with OBEX headers as http POST data. The reason for using POST is that there is a size limit for sending data in the URL, using the GET method. Using the POST method also avoids problems with special characters, using binary POST (binary POST is not supported in Wap1.1, however. Another solution is provided below). Every client request implies permission for the server to request a client task in it's response.

~~The client will always call the server with one parameter (except for the initial connect request), using the POST method. The reason for using POST is that there is a size limit for sending data in the URL, using the GET method. Using the POST method also avoids problems with special characters, using binary POST (binary POST is not supported in Wap1.1, however. Another solution is provided below). The parameter should be named **obex**. The connect request calls the server with one parameter, **userid**, wich contains the user name. Every client request implies permission for the server to request a client task in it's response.~~

~~**Name**~~	~~**Size**~~	~~**Description**~~
~~Obex~~	~~-~~	~~This parameter contains the obex headers sent from the client to the server. The format is plain text (in future versions of WAP, binary will be used).~~
~~Userid~~	~~-~~	~~This parameter contains the user name. The format is plain text.~~

6.3 Binary POST

As binary POST is not supported in WAP1.1, the OBEX headers are ~~URL~~base64-encoded and sent as plain text.

~~Example:~~

~~Obex header:~~	~~82 00 0A 01 02 03 04 05 06 07~~
~~Transferred as:~~	~~"obex=%82%00%0A%01%02%03%04%05%06%07"~~

This could result in sending ~~almost three~~ 33% more than ~~times~~ the ammount of data neccesary. ~~Printable character codes will not result in any overhead though~~. The solution is however only temporary, awaiting WAP binary POST.

6.4 The secure connection

The authentication process only guaranties that the client and the server can rely on each others identity during the connection process. The connection that is established is not secure and could easily be tapped for information. It is therefore desired to encrypt all data that is sent between the client and the server. 3GPP currently does not guarantee strong enough encryption so we will ensure data is secure and untampered.

In the case of a synchronization of a mobile calendar over 3GPP, there are actually two different transports that has to be considered. First it is the transport from the mobile device to the 3GPP gateway. Then there is the transport from the gateway to the web server. The transport from the mobile device to the gateway is sent over GSM, which is fairly well encrypted. The transport from the gateway to the web server is not protected in any way though. To solve this problem a third party products for corporate extranet solutions could be used. These products should be transparent from the mobile device and set up the required SSL connection.

6.5 Connect

The connect sequence sets up the connection from the mobile device to the web server. The session id has to be assigned in the first response from the server, as more request/response pairs are needed to complete the authentication procedure. The Connect procedure is always invoked by the client.

	~~Data~~	~~Description~~
~~Request →~~	~~userid=<user name>~~	~~The mobile device calls the web server, using the POST method to send the user name.~~
~~Response ←~~	~~<WAN UUID > <obex connect with authenticate challenge>~~	~~The web server responds with a 16 byte session id and the obex headers for connect with authenticate challange.~~
~~Request →~~	~~obex=<WAN UUID ><obex unauthorized with authenticate challenge>~~	~~The mobile device responds to the connect request by sending an unauthorized response with authernticate challenge, forcing the web server to authenticate itself.~~
~~Response ←~~	~~<obex connect with authenticate challenge and authentication response>~~	~~The web server verifies the mobile device and authenticates itself.~~
~~Request →~~	~~obex=<WAN UUID ><obex success with authenticate response>~~	~~The mobile device verifies the web server and sends an obex success.~~
~~Response ←~~	~~...~~	~~The web server now starts acting like the a client to the mobile device, sending PUT and GET operations to the mobile device.~~

	Data	Description
Request →	<OBEX push>	The mobile device alerts the web server, sending an empty obex push.
Response ←	<obex connect with authenticate challenge, WAN UUID and target >	The web server responds with a 16 byte session id and the obex headers for connect with authenticate challange. The server also sends an obex target header, indicating calendar synchronisation.
Request →	<obex unauthorized with authenticate challenge containg user name in realm, WAN UUID and who header >	The mobile device responds to the connect request by sending an unauthorized response with authernticate challenge, forcing the web server to authenticate itself. Username is sent as realm. Who header with assigned connection id.
Response ←	<obex connect with authenticate challenge and authentication response , and connectionid>	The web server verifies the mobile device and authenticates itself.
Request →	<obex success with authenticate response, WAN UUID and connectionid>	The mobile device verifies the web server and sends an obex success.
Response ←	...	The web server now starts acting like the a client to the mobile device, sending PUT and GET operations to the mobile device.

6.6 Disconnect

Disconnection can either be invoked by the client or be invoked by the server as a last response. The client's session is then destroyed in the server. A third case is that the connection is lost for other reasons, e.g. power failure by the client. In this case, the session should be timed out automatically.

6.6.1 Client disconnection

The client normally should not invoke the disconnection. Should the client however need to disconnect, the following sequence should be used:

	Data	Description
Response ←	…	The web server asks the mobile device to perform some operation.
Request →	<obex disconnect, WAN UUID >~~obex=<WAN UUID ><obex disconnect>~~	The mobile device send an obex disconnect to the web server.
Response ←	-	The web server destroys the session and responds with an empty response.

6.6.2 Server disconnection

When the server is done synchronizing its content, it should disconnect the client. The following sequence should be used:

	Data	Description
Response ←	<obex disconnect><obex connectionid>	The web server send an obex disconnect to the mobile device and destroys the session.
	-	The mobile device disconnects and sends no more requests to the web server.

6.7 Put

The PUT operation sends a named vCalendar object from the server to the mobile device. The PUT operation can only be invoked by the web server.

	Data	Description
Response ←	<obex put~~>~~, connectionid>	The web server sends a put request to the mobile device.
Request →	<obex put response, WAN UUID >~~obex=<WAN UUID ><obex put response>~~	The mobile device performs the put operation and responds with the resulting obex data.

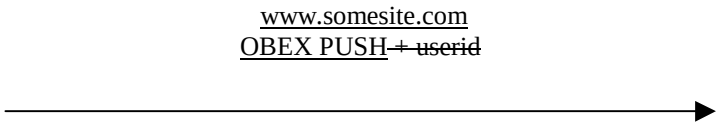
6.8 Get

The GET operation retrieves a named vCalendar object from the mobile device. The GET operation can only be invoked by the web server.

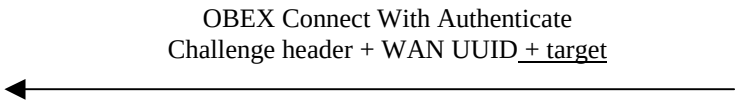
	Data	Description
Response ←	<obex get><obex target>	The web server sends a get request to the mobile device.
Request →	<WAN UUID ><obex get response>~~obex=<WAN UUID ><obex get response>~~	The mobile device performs the get operation and responds with the resulting obex data.

7 Use Case

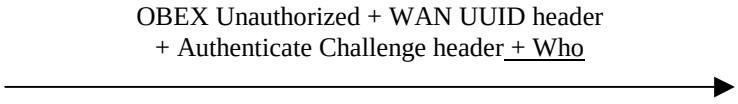
The user chose “remote sync” and is prompted for the URL, for example www.somesite.com, userid and password. ~~The userid will be sent to the server.~~ The userid and the password will be saved in the local storage oif the mobile device.



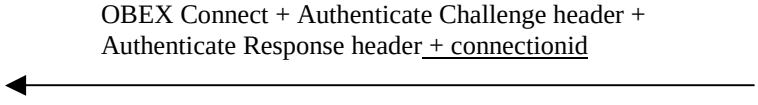
When the WAP server receives this, it will try to establish an OBEX connection with the mobile device, acting as a primary from an OBEX point of view. An OBEX Connect request with a WAN UUID header and an Authentication challenge header will be sent. The WAN UUID header will contain a unique16 byte UUID that will be used to identify this session. The server also sends a obex target header, indicating that a syncronization is in progress.



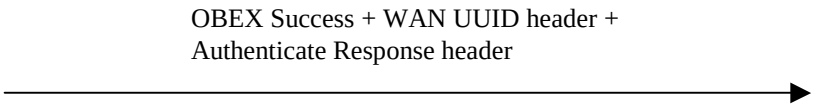
When the phone receives the OBEX connect, it will respond with an OBEX Unauthorized response and an Authenticate Challenge of it’s own.The user id is sent in the realm field in the obex authorize header. From now on, the given UUID must be present when a request is sent from the phone to the WAP server. This is the only way that the server can recognize the phone. The UUID will be identified with the WAN UUID header, which means that the phone identifies itself with the given UUID. The client also assigns a connection id that is sent in an obex who header in every request.



Receiving this, the WAP server resends the same command as last time but this time also adds the Authenticate Response header. The server always sends an obex target header, containg the connection id.



If the OBEX secondary at this stage verifies the received request-digest with the one generated by itself, the client is authenticated and the response will be an OBEX Success with an Authenticate Response header.



At this stage the OBEX connection is up and the actual synchronization can start. We are now in the middle of a WAP request/response pair and the WAP server response will now contain a OBEX Get command, asking for the mobile's Change Log. The steps following are identical to the ones in a local synchronization from an OBEX and IrMC point of view, the only real difference is the use of the WAN UUID header when sending from the mobile. Worth mentioning is that this form of remoted synchronization is not suited for a slow sync [see reference 2]. The user is supposed to do the first synchronization locally, using for example cable or IR.