3GPP TSG SA WG3 Security — S3#11 **S3-000156**

22-24 February, 2000

Mainz, Germany

Source: **Vodafone**

Title: **CRs from S1 on GPRS encryption**

Document for: **Discussion/Decision**

The following is an extract from the draft report of the S1 meeting 9-11 Feb 2000:

5.2.3 Support of encryption in GPRS

Document 110/00 contained a CR to 02.07 on Support of encryption in GPRS mobile stations R97, and document 111/00 contained a similar CR for R'98. The point here is to add the requirement for encryption for GPRS. It was questioned if these changes had been seen by S3. The answer was that the chairman of S3 had seen these, and that the requirement has been expressed by S3, but that the changes have not been seen by S3.

In R'99 02.07 has been absorbed by document 22.101. The equivalent changes therefore have been included in 22.101 and were presented in document 112/00. In addition the same requirements was introduced into 22.060 in document 113/00.

Of note is the difference between CS and PS domains.

The documents 110/00 and 111/00 were approved subject to checking by delegates with their companies. If there are no comments they will be sent to S3 and, subject to the package being completed by S3, sent to SA#7 for approval.

Attached: S1-000110, S1-000111, S1-000112, S1-000113

Document ***TSG S1 (00) 110***

3GPP TSG SA1
Sophia Antipolis, France, 9-11 Feb 2000

CHANGE REQUEST

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

02.07 **CR** Current Version: 6.1.0

SMG specification number ↑ *↑ CR number as allocated by support team*

For submision to SMG#
list SMG meeting no. here ↑

for approval ☒
for information □
(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM □ ME ☒ UTRAN □ Core Network □
(at least one should be marked with an X)

Source: Vodafone AirTouch **Date:** 9-02-2000

Subject: Support of encryption in GPRS mobile stations

3G Work item:

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

F	Correction	□
A	Corresponds to a correction in a 2G specification	□
B	Addition of feature	☒
C	Functional modification of feature	□
D	Editorial modification	□

Reason for change: Currently it is not explicitly stated that support for encryption and no-encryption modes is mandatory for GPRS terminals. Networks may be operating either with encryption on or off and therefore terminals must support both modes to ensure consistent access when roaming.

Clauses affected: 2, new B.1.xx

Other specs affected:

Other 3G core specifications	☒	→ List of CRs:	
Other 2G 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:

***** First Modified Section *****

2 Requirements for implementing MS features

MS features are qualified as mandatory or optional. Mandatory features have to be implemented as long as they are relevant to the MS type, and will be subject to Type Approval when applied according to GSM 11.10 [13]. Whether or not an optional feature is implemented is left to the manufacturers' discretion. The method of implementation of all MS features must be done in accordance with the appropriate GSM specifications. For all present and future MS features, manufacturers have the responsibility to ensure that the MS features will neither conflict with the air interface nor cause any interference to the network or any other MS or its own MS, and these requirements shall be recognized during the Type Approval process.

In the following tables 1, 2 and 3 the basic, supplementary and additional MS features are listed. Mandatory features are marked by "M". Optional features are marked by "0".

Additional MS features not listed in table 3 are permitted without the requirement for this table to be amended, provided that these new features do not affect the mandatory air interface requirements.

Unless otherwise stated for a particular feature, the feature supported by the Subscriber Identity Module (SIM) takes priority over the same feature supported by the Mobile Equipment (ME).

Table 1: Basic MS features

	Name	Mandatory (M) Optional (O)	
1.1	Display of Called Number	M*	
1.2	Indication of Call Progress Signals	M*	
1.3	Country/PLMN Indication	M*	
1.4	Country/PLMN Selection	M	
1.5	Keypad	O	(note 1)
1.6	IMEI	M	
1.7	Short Message	M	(note 4)
1.8	Short Message Overflow Indication	M	
1.9	DTE/DCE Interface	O	
1.10	ISDN "S" Interface	O	
1.11	International Access Function ("+" key)	O	(note 1)
1.12	Service Indicator	M*	
1.13	Autocalling restriction capabilities		(note 2)
1.14	Emergency Calls capabilities	M	(note 3)
1.15	Dual Tone Multi Frequency function (DTMF)	M	(note 5)
1.16	Subscription Identity Management	M	
1.17	On/Off switch	O	
1.18	Subaddress	O	
1.19	Support of Encryption A5/1 and A5/2	M	
1.20	Support of GPRS Encryption	M	(note 6)
1.21~~0~~	Short Message Service Cell Broadcast	M	
1.22~~1~~	Short Message Service Cell Broadcast DRX	O	
1.23~~2~~	Service Provider Indication	O	
1.24~~3~~	Support of the extended SMS CB channel	O	
1.25~~4~~	Support of Additional Call Set-up MMI Procedures	O	
1.26~~5~~	Network Identity and Timezone	O	
1.27~~6~~	Ciphering Indicator	M*	
1.28~~7~~	Network's indication of alerting in the MS	O	(NI Alert in MS)
1.29~~8~~	Network initiated Mobile Originated connection	O	

Descriptions are given in annex B.

* Mandatory where a human interface is provided, i.e. may be in-appropriate for MS driven by external equipment.

NOTE 1: The physical means of entering the characters 0-9, +, * and # may be keypad, voice input device, DTE or others, but it is mandatory that there shall be the means to enter this information.

NOTE 2: MTs with capabilities for Autocalling, or to which call initiating equipment can be connected via the "R" or "S" interface, shall restrict repeated call attempts according to the procedures described in annex A.

NOTE 3: Emergency calls shall be possible according to Teleservice 12 (see GSM 02.03 [2] and GSM 02.30 [7]). This feature is only required to be provided by ME supporting Telephony.

NOTE 4: Support of reception by the ME and storage of SMS MT in the SIM is mandatory, but its display is optional. Reception and storage of a message shall be indicated by the MS.

NOTE 5: The use of DTMF is only mandatory when the speech teleservice is being used or during the speech phase of alternate speech/data and alternate speech/facsimile teleservices.

NOTE 6: The implementation of a GPRS encryption algorithm is mandatory for terminals supporting GPRS

Table 2: Supplementary MS features

	Name	Mandatory (M) Optional (O)
2.1	Control of Supplementary Services	(note 1)

NOTE 1: See annex B, subclause B.2.1.

Descriptions are given in annex B to GSM 02.07.

*****Next Modified Section *****

B.1.18 Sub-Address

This feature allows the mobile to append and/or receive a sub-address to a Directory Number, for use in call set-up, and in those supplementary services that use a Directory Number.

B.1.19 Support of encryption A5/1 and A5/2

Provision is made for support of up to 7 different algorithms, and the support of no encryption. It is mandatory for A5/1, A5/2 and non encrypted mode to be implemented on mobile stations. Other algorithms are optional.

B.1.20 Support of GPRS encryption

Provision is made for support of up to 7 different algorithms, and the support of no encryption. It is mandatory for a GPRS encryption algorithm and non encrypted mode to be implemented on mobile stations supporting GPRS.

B.1.21~~0~~ Short Message Service Cell Broadcast

The Short Message Service Cell Broadcast enables the mobile station to receive short messages from a message handling system.
The short message service cell broadcast teleservice is described in specification GSM 02.03 [2].

Document ***TSG SG (00) 111***

3GPP TSG SA1
Sophia Antipolis, France, 9-11 Feb 2000

CHANGE REQUEST

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

02.07 **CR** Current Version: 7.1.0

SMG specification number ↑ *↑ CR number as allocated by support team*

For submision to SMG SMG# for approval ☒ *(only one box should*
list SMG meeting no. here ↑ for information □ *be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM □ ME ☒ UTRAN □ Core Network □
(at least one should be marked with an X)

Source: Vodafone-AirTouch **Date:** 9-02-2000

Subject: Support of encryption in GPRS mobile stations

3G Work item:

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

F	Correction	□
A	Corresponds to a correction in a 2G specification	□
B	Addition of feature	☒
C	Functional modification of feature	□
D	Editorial modification	□

Reason for change: Currently it is not explicitly stated that support for encryption and no-encryption modes is mandatory for GPRS terminals. Networks may be operating either with encryption on or off and therefore terminals must support both modes to ensure consistent access when roaming.

Clauses affected: 2, new B.1.xx

Other specs affected:

Other 3G core specifications	□	→	List of CRs:
Other 2G 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:

***** First Modified Section *****

2 Requirements for implementing MS features

MS features are qualified as mandatory or optional. Mandatory features have to be implemented as long as they are relevant to the MS type, and will be subject to Type Approval when applied according to GSM 11.10 [13]. Whether or not an optional feature is implemented is left to the manufacturers' discretion. The method of implementation of all MS features must be done in accordance with the appropriate GSM specifications. For all present and future MS features, manufacturers have the responsibility to ensure that the MS features will neither conflict with the air interface nor cause any interference to the network or any other MS or its own MS, and these requirements shall be recognized during the Type Approval process.
In the following tables 1, 2 and 3 the basic, supplementary and additional MS features are listed. Mandatory features are marked by "M". Optional features are marked by "0".
Additional MS features not listed in table 3 are permitted without the requirement for this table to be amended, provided that these new features do not affect the mandatory air interface requirements.
Unless otherwise stated for a particular feature, the feature supported by the Subscriber Identity Module (SIM) takes priority over the same feature supported by the Mobile Equipment (ME).

Table 1: Basic MS features

	Name	**Mandatory (M) Optional (O)**	
1.1	Display of Called Number	M*	
1.2	Indication of Call Progress Signals	M*	
1.3	Country/PLMN Indication	M*	
1.4	Country/PLMN Selection	M	
1.5	Keypad	O	(note 1)
1.6	IMEI	M	
1.7	Short Message	M	(note 4)
1.8	Short Message Overflow Indication	M	
1.9	DTE/DCE Interface	O	
1.10	ISDN "S" Interface	O	
1.11	International Access Function ("+" key)	O	(note 1)
1.12	Service Indicator	M*	
1.13	Autocalling restriction capabilities		(note 2)
1.14	Emergency Calls capabilities	M	(note 3)
1.15	Dual Tone Multi Frequency function (DTMF)	M	(note 5)
1.16	Subscription Identity Management	M	
1.17	On/Off switch	O	
1.18	Subaddress	O	
1.19	Support of Encryption A5/1 and A5/2	M	
1.20	Support of GPRS Encryption	M	(note 6)
1.21~~0~~	Short Message Service Cell Broadcast	M	
1.22~~1~~	Short Message Service Cell Broadcast DRX	O	
1.23~~2~~	Service Provider Indication	O	
1.24~~3~~	Support of the extended SMS CB channel	O	
1.25~~4~~	Support of Additional Call Set-up MMI Procedures	O	
1.26~~5~~	Network Identity and Timezone	O	
1.27~~6~~	Ciphering Indicator	M*	
1.28~~7~~	Network's indication of alerting in the MS	O	(NI Alert in MS)
1.29~~8~~	Network initiated Mobile Originated connection	O	
1.30~~29~~	Support of Localised Service Area	O	

Descriptions are given in annex B.

* Mandatory where a human interface is provided, i.e. may be in-appropriate for MS driven by external equipment.

NOTE 1: The physical means of entering the characters 0-9, +, * and # may be keypad, voice input device, DTE or others, but it is mandatory that there shall be the means to enter this information.

NOTE 2: MTs with capabilities for Autocalling, or to which call initiating equipment can be connected via the "R" or "S" interface, shall restrict repeated call attempts according to the procedures described in annex A.

NOTE 3: Emergency calls shall be possible according to Teleservice 12 (see GSM 02.03 [2] and GSM 02.30 [7]). This feature is only required to be provided by ME supporting Telephony.

NOTE 4: Support of reception by the ME and storage of SMS MT in the SIM is mandatory, but its display is optional. Reception and storage of a message shall be indicated by the MS.

NOTE 5: The use of DTMF is only mandatory when the speech teleservice is being used or during the speech phase of alternate speech/data and alternate speech/facsimile teleservices.

NOTE 6: The implementation of GPRS encryption algorithm is mandatory for terminals supporting GPRS

Table 2: Supplementary MS features

	Name	Mandatory (M) Optional (O)
2.1	Control of Supplementary Services	(note 1)

NOTE 1: See annex B, subclause B.2.1.

Descriptions are given in annex B to GSM 02.07.

*****Next Modified Section *****

B.1.18 Sub-Address

This feature allows the mobile to append and/or receive a sub-address to a Directory Number, for use in call set-up, and in those supplementary services that use a Directory Number.

B.1.19 Support of encryption A5/1 and A5/2

Provision is made for support of up to 7 different algorithms, and the support of no encryption. It is mandatory for A5/1, A5/2 and non encrypted mode to be implemented on mobile stations. Other algorithms are optional.

B.1.20 Support of GPRS encryption

Provision is made for support of up to 7 different algorithms, and the support of no encryption. It is mandatory for a GPRS encryption algorithm and non encrypted mode to be implemented on mobile stations supporting GPRS.

B.1.21~~0~~ Short Message Service Cell Broadcast

The Short Message Service Cell Broadcast enables the mobile station to receive short messages from a message handling system.
The short message service cell broadcast teleservice is described in specification GSM 02.03 [2].

3GPP SA WG1
Sophia Antipolis, France **7-9/2/00**

Document ***TSG S1 (00) 112***

3G CHANGE REQUEST

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

22-101 **CR** Current Version: 3.8.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submision to TSG SA# for approval ☒ *(only one box should*
list TSG meeting no. here ↑ for information □ *be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM □ ME ☒ UTRAN □ Core Network □
(at least one should be marked with an X)

Source: Vodafone Airtouch **Date:** 09/02/00

Subject: Support of encryption in PS mobile stations

3G Work item:

Category:	F	Correction	□
	A	Corresponds to a correction in a 2G specification	□
(only one category	B	Addition of feature	☒
shall be marked	C	Functional modification of feature	□
with an X)	D	Editorial modification	□

Reason for change: Currently it is not explicitly stated that support for encryption and no-encryption modes is mandatory for PS terminals. Networks may be operating either with encryption on or off and therefore terminals must support both modes to ensure consistent access when roaming.

Clauses affected: 13

Other specs affected:	Other 3G core specifications	☒	→ List of CRs:	23-060
	Other 2G 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:

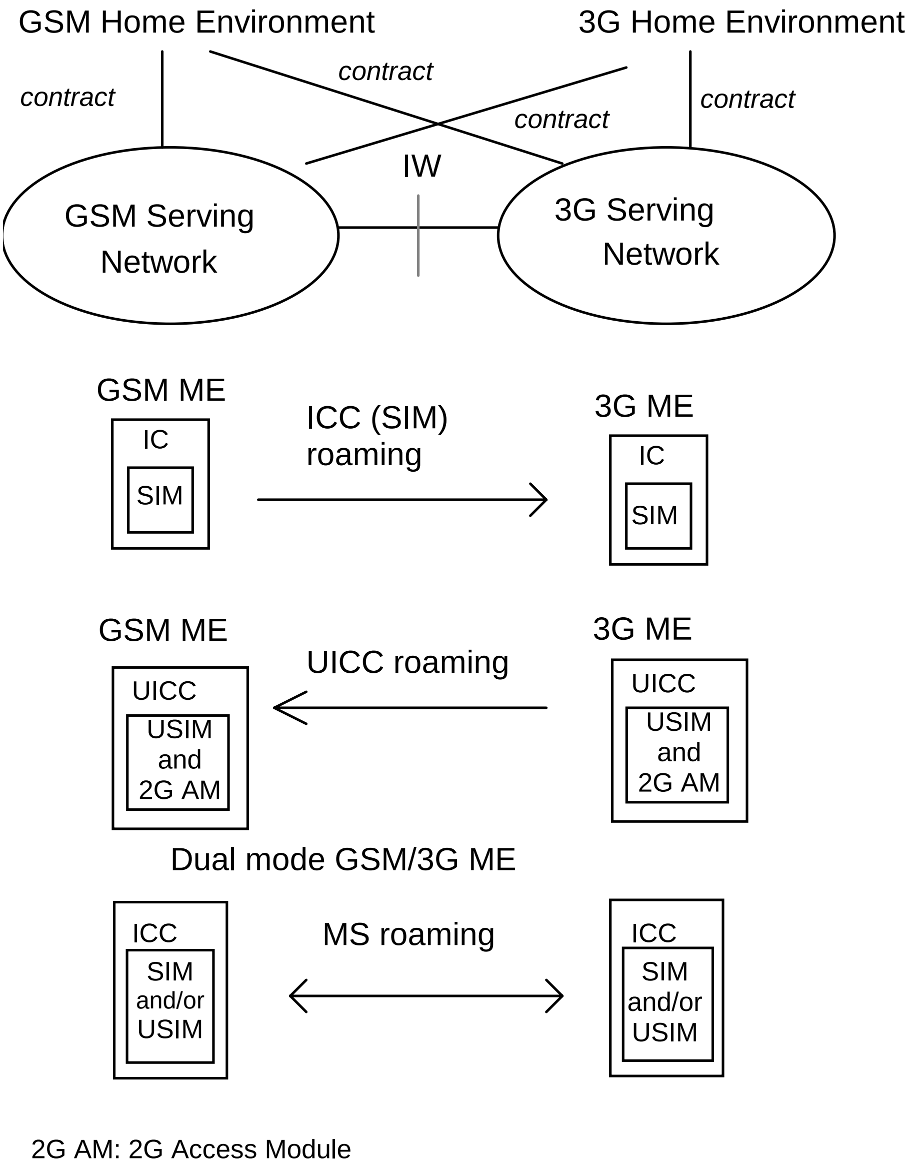

Figure 4 Roaming Users

13 Types of features of UEs

3GPP specifications should support a wide variety of user equipment, i.e. setting any limitations on terminals should be avoided as much as possible. For example user equipment like hand-portable phones, personal digital assistants and laptop computers can clearly be seen as likely terminals.

In order not to limit the possible types of user equipment they are not standardised. The UE types could be categorised by their service capabilities rather than by their physical characteristics. Typical examples are speech only UE, narrowband data UE, wideband data UE, data and speech UE, etc..

In order to enhance functionality split and modularity inside the user equipment the interfaces of UE should be identified. Interfaces like UICC-interface, PCMCIA-interface and other PC-interfaces, including software interfaces, should be covered by references to the applicable interface standards.

UEs have to be capable of supporting a wide variety of teleservices and applications provided in PLMN environment. Limitations may exist on UEs capability to support all possible teleservices and information types (speech, narrowband data, wideband data, video, etc.) and therefore functionality to indicate capabilities of a UE shall be specified. UEs should be capable of supporting new supplementary services without any changes in UE.

The basic mandatory UE requirements are:

- Encrypted terminal-UICC interface;
- Support for GSM phase 2 and 2+ SIM cards, phase 1 5V SIM cards shall not be supported;
- Home environment and serving network registration and deregistration;
- Location update;
- Originating or receiving a connection oriented or a connectionless service;
- An unalterable equipment identification; IMEI, see TS 22.016 [12];
- Basic identification of the terminal capabilities related to services such as; the support for software downloading, application execution environment/interface, MExE terminal class, supported bearer services.
- Terminals capable for emergency calls shall support emergency call without a SIM/USIM.
- Support for the execution of algorithms required for encryption, for CS and PS services. Support for non encrypted mode is required;
- Support for the method of handling automatic calling repeat attempt restrictions as specified in TS 22.001 [4];
- At least one capability type shall be standardised for mobile terminals supporting the GRAN and UTRAN radio interfaces.
- Under emergency situations, it may be desirable for the operator to prevent UE users from making access attempts (including emergency call attempts) or responding to pages in specified areas of a network, see TS 22.011 [11];
- Ciphering Indicator for terminals with a suitable display;
- The ciphering indicator feature allows the ME to detect that ciphering is not switched on and to indicate this to the user. The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;
- Support for PLMN selection.

Annex A describes a number of features which may optionally be supported by the ME.

TSG-SA Working Group 1 meeting #7
Sophia Antipolis, France

TSG S1 (00) 113
Agenda Item: 5.2

CHANGE REQUEST No :

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

Technical Specification / Report UMTS 22.060 Version: 3.2.0

Submitted to TSG_SA	7	for approval	X	without presentation ("non-strategic")	
list TSG plenary meeting no. here ↑		for information		with presentation ("strategic")	X

PT SMG CR cover form is available from: http://docbox.etsi.org/tech-org/smg/Document/smg/tools/CR_form/crf28_1.zip

Proposed change affects: USIM □ TE □ Network ☒
(at least one should be marked with an X)

Work item:

Source: Vodafone Airtouch **Date:** 09/02/00

Subject: Support of encryption in GPRS mobile stations

Category:

(one category And one release Only 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			UMTS 99	X

Reason for change: Currently it is not explicitly stated that support for encryption and no-encryption modes is mandatory for GPRS terminals. Networks may be operating either with encryption on or off and therefore terminals must support both modes to ensure consistent access when roaming.

Clauses affected: 5.4.3

Other specs Affected:

Other releases of same spec		→ List of CRs:	
Other core specifications	X	→ List of CRs:	21.101
MS test specifications / TBRs		→ 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.

5.4.3 Security services

The use of radio communications for transmission to/from subscribers in mobile networks makes them particularly sensitive to:

1) misuse of their resources by unauthorized persons using manipulated MSs;

2) eavesdropping on the information being exchanged on the radio path.

Therefore, to protect the system in the two cases mentioned above, the following security features are provided for GPRS:

- MS authentication; i.e., the confirmation by the land-based part of the system that the subscriber identity, transferred by the MS within the identification procedure on the radio path, is the one claimed. The purpose of this authentication is to protect the network against unauthorized use. It also enables the protection of GPRS subscribers by denying intruders the ability to impersonate authorized users;

- access control; i.e., the network can support restrictions on access by or to different GPRS subscribers, such as restrictions by location, screening lists, and so on;

- user identity confidentiality; i.e., the property that the user identity on the radio link is not made available or disclosed to unauthorized individuals, entities or processes. The purpose is to provide privacy of identities of the subscribers who are using GPRS radio resources. It allows for the improvement of other security features, e.g., user information confidentiality, and also provides for the protection against tracing the location of a mobile subscriber by listening to the signalling exchanges on the radio path;

- user information confidentiality; i.e., the property that the user information is not made available or disclosed to unauthorized individuals, entities or processes. The purpose is to provide for confidentiality of user data, i.e., protection of the message part pertaining to layers 3 and above, that passes over the radio path.

Both user identity and user data shall be protected as shown in table 6:

Table 6: Protection of user identity and user data

Service	User Identity Protection	User Data Protection
PTP	Yes	Yes
PTM-Multicast (receiver)	Yes [a)]	No[b)]
PTM-Group Call	Yes	Yes

a) The individual identities of the group members that actually receive the PTM-M traffic, are not transferred on the radio path and furthermore are also not known to the network. This is an important aspect for those applications where it is imperative that the location of the user cannot under any circumstances be traced. However, the group identity and the identity of the service requester are sent unciphered on the radio path.

b) This does not preclude end-to-end ciphering of user data by the PTM-M application, this however, is outside the scope of this specification.

Security mechanisms available for existing teleservices and bearer services should be used if possible.

Terminals supporting GPRS shall implement a GPRS encryption algorithm. Support for non encrypted mode is also required.

5.4.4 Packet size