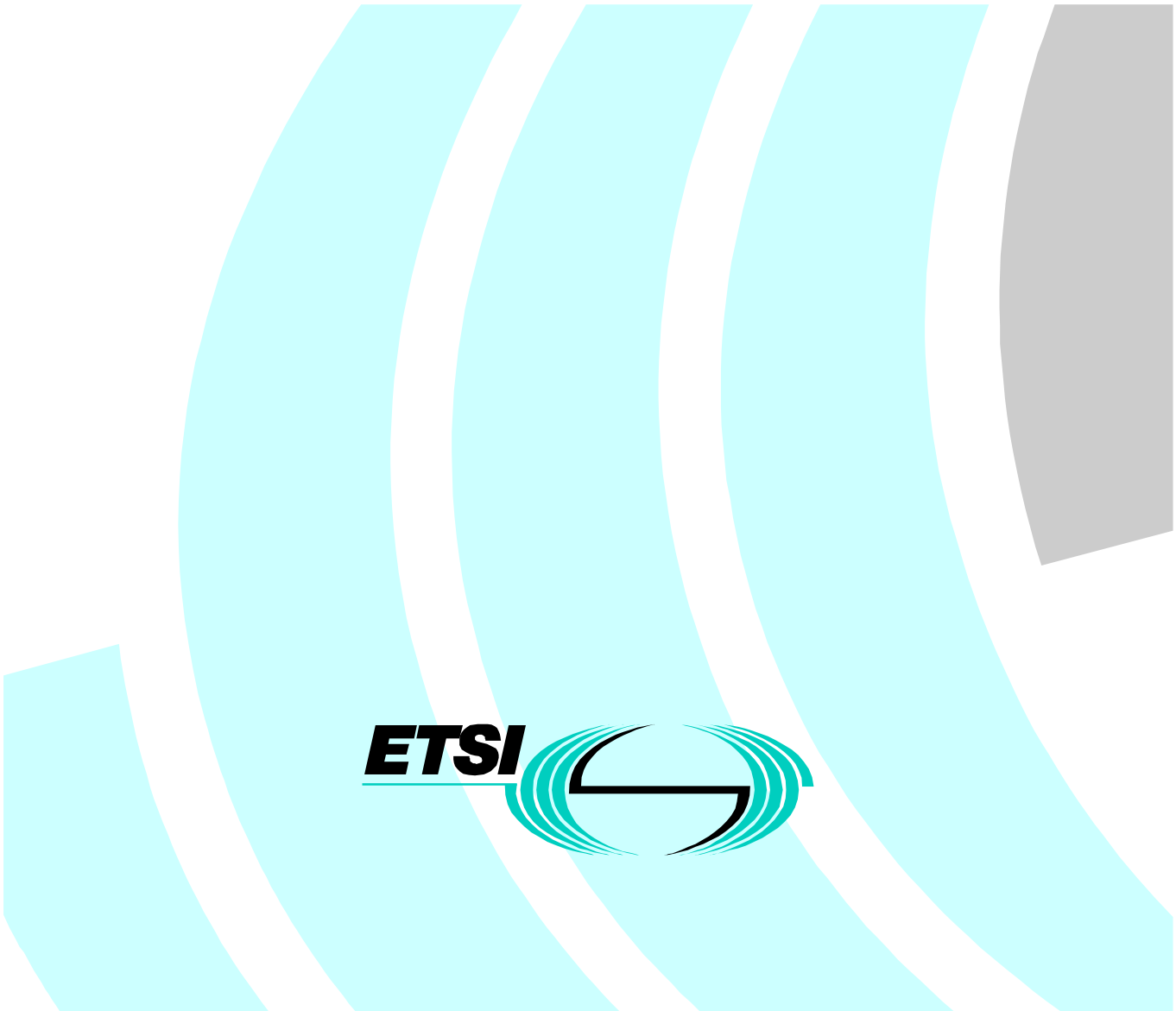
ETSI TS 101 377-2-3 V1.1.1 (2001-03)

Technical Specification

GEO-Mobile Radio Interface Specifications;
Part 2: Service specifications;
Sub-part 3: Security Aspects;
GMR-2 02.009



Reference
DTS/SES-002-02009

Keywords
GMR, GSM, GSO, interface, MES, mobile, MSS,
radio, satellite, security, S-PCN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

The information pertaining to essential IPRs is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

The attention of ETSI has been drawn to the Intellectual Property Rights (IPRs) listed below which are, or may be, or may become, Essential to the present document. The IPR owner has undertaken to grant irrevocable licences, on fair, reasonable and non-discriminatory terms and conditions under these IPRs pursuant to the ETSI IPR Policy. Further details pertaining to these IPRs can be obtained directly from the IPR owner.

The present IPR information has been submitted to ETSI and pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

IPRs:

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,715,365	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,754,974	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,226,084	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,701,390	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,826,222	US

IPR Owner: Digital Voice Systems Inc
One Van de Graaff Drive Burlington,
MA 01803
USA

Contact: John C. Hardwick
Tel.: +1 781-270-1030
Fax: +1 781-270-0166

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 377 V1.1.1	Ericsson Mobile Communication	Improvements in, or in relation to, equalisers	GB	GB 2 215 567	GB
TS 101 377 V1.1.1	Ericsson Mobile Communication	Power Booster	GB	GB 2 251 768	GB
TS 101 377 V1.1.1	Ericsson Mobile Communication	Receiver Gain	GB	GB 2 233 846	GB
TS 101 377 V1.1.1	Ericsson Mobile Communication	Transmitter Power Control for Radio Telephone System	GB	GB 2 233 517	GB

IPR Owner: Ericsson Mobile Communications (UK) Limited
The Keytech Centre, Ashwood Way
Basingstoke
Hampshire RG23 8BG
United Kingdom

Contact: John Watson
Tel.: +44 1256 864821

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 377 V1.1.1	Hughes Network Systems		US	Pending	US

IPR Owner: Hughes Network Systems
11717 Exploration Lane
Germantown, Maryland 20876
USA

Contact: John T. Whelan
Tel: +1 301-428-7172
Fax: +1 301-428-2802

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	2.4-to-3 KBPS Rate Adaptation Apparatus for Use in Narrowband Data and Facsimile Communication Systems	US	US 6,108,348	US
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Cellular Spacecraft TDMA Communications System with Call Interrupt Coding System for Maximizing Traffic ThroughputCellular Spacecraft TDMA Communications System with Call Interrupt Coding System for Maximizing Traffic Throughput	US	US 5,717,686	US
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Enhanced Access Burst for Random Access Channels in TDMA Mobile Satellite System	US	US 5,875,182	
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System	US	US 5,974,314	US
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System	US	US 5,974,315	US
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System with Mutual Offset High-argin Forward Control Signals	US	US 6,072,985	US
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System with Spot Beam Pairing for Reduced Updates	US	US 6,118,998	US

IPR Owner: Lockheed Martin Global Telecommunications, Inc.
900 Forge Road
Norristown, PA. 19403
USA

Contact: R.F. Franciose
Tel.: +1 610.354.2535
Fax: +1 610.354.7244

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

The present document is part 2, sub-part 3 of a multi-part deliverable covering Geo-Mobile Radio Interface Specification, as identified below:

Part 1: "General specifications";

Part 2: "Service specifications":

Sub-part 1: "Teleservices supported by a GMR-2 Public Satellite Mobile Network (PSMN); GMR-2 02.003";

Sub-part 2: "General on Supplementary Services; GMR-2 02.004";

Sub-part 3: "Security Aspects; GMR-2 02.009";

Sub-part 4: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services - Stage 1; GMR-2 02.083";

Sub-part 5: "Multiparty (MPTY) Supplementary Services; GMR-2 02.084";

Sub-part 6: "Service Accessibility; GMR-2 02.001";

Sub-part 7: "Operator Determined Barring (ODB); GMR-2 02.041";

Sub-part 8: "Call Barring Supplementary Services; GMR-2 02.088";

Sub-part 9: "Bearer Services (BS) supported by a GMR-2 Public Satellite Mobile Network (PSMN); GMR-2 02.002".

Part 3: "Network specifications";

Part 4: "Radio interface protocol specifications";

Part 5: "Radio interface physical layer specifications";

Part 6: "Speech coding specifications".

The contents of the present document are subject to continuing work within TC-SES and may change following formal TC-SES approval. Should TC-SES modify the contents of the present document it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 1.m.n

where:

- the third digit (n) is incremented when editorial only changes have been incorporated in the specification;
- the second digit (m) is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.

Introduction

GMR stands for GEO (Geostationary Earth Orbit) Mobile Radio interface, which is used for mobile satellite services (MSS) utilizing geostationary satellite(s). GMR is derived from the terrestrial digital cellular standard GSM and supports access to GSM core networks.

Due to the differences between terrestrial and satellite channels, some modifications to the GSM standard are necessary. Some GSM specifications are directly applicable, whereas others are applicable with modifications. Similarly, some GSM specifications do not apply, while some GMR specifications have no corresponding GSM specification.

Since GMR is derived from GSM, the organization of the GMR specifications closely follows that of GSM. The GMR numbers have been designed to correspond to the GSM numbering system. All GMR specifications are allocated a unique GMR number as follows:

GMR-n xx.zyy

where :

- xx.0yy (z = 0) is used for GMR specifications that have a corresponding GSM specification. In this case, the numbers xx and yy correspond to the GSM numbering scheme.
- xx.2yy (z = 2) is used for GMR specifications that do not correspond to a GSM specification. In this case, only the number xx corresponds to the GSM numbering scheme and the number yy is allocated by GMR.
- n denotes the first (n = 1) or second (n = 2) family of GMR specifications.

A GMR system is defined by the combination of a family of GMR specifications and GSM specifications as follows:

- If a GMR specification exists it takes precedence over the corresponding GSM specification (if any). This precedence rule applies to any references in the corresponding GSM specifications.

NOTE: Any references to GSM specifications within the GMR specifications are not subject to this precedence rule. For example, a GMR specification may contain specific references to the corresponding GSM specification.

- If a GMR specification does not exist the corresponding GSM specification may or may not apply. The applicability of the GSM specifications is defined in GMR-n 01.201.

1 Scope

The present document defines the security features which shall be made available in a GMR-2 PSMN, in order to provide additional protection for users of Bearer and Teleservices, together with the associated levels of protection. The present document is only concerned with the up-grading of security features in a GMR-2 PSMN. In particular, end-to-end security is outside the scope of the present document.

Bearer and Teleservices are defined in GSM 02.02 [2] and GMR-2 02.003 [3] respectively, and the security features implementation aspects are described in GMR-2 03.020 [5].

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] GMR-2 01.004 (ETSI TS 101 377-1-1): "GEO-Mobile Radio Interface Specifications; Part 1: General specifications; Sub-part 1: Abbreviations and acronyms; GMR-2 01.004".

[2] GSM 02.02 (ETSI ETS 300 501): "European digital cellular telecommunication system (Phase 2); Bearer Services (BS) supported by a GSM Public Land Mobile Network (PLMN) (GSM 02.02)".

[3] GMR-2 02.003 (ETSI TS 101 377-02-01): "GEO-Mobile Radio interface specifications; Teleservices supported by a GMR-2 Public Satellite Mobile Network (PSMN); GMR 2-02.003".

[4] GSM 02.07 (ETSI ETS 300 505 Edition 3): "Digital cellular telecommunications system (Phase 2); Mobile Station (MS) features (GSM 02.07 version 4.8.2)".

[5] GMR-2 03.020 (ETSI TS 101 377-03-10): "GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 10: Security related Network Functions; GMR-2 03.020".

[6] GSM 11.11 (ETSI ETS 300 608 Edition 8): "Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 4.20.1)".

3 Abbreviations

For the purposes of the present document, the abbreviations given in GMR-2 01.004 [1] apply.

4 General

The use of radio communications for transmission to the mobile subscribers makes PSMNs particularly sensitive to:

- misuse of their resources by unauthorized persons using manipulated Mobile Earth Stations, who try to impersonate authorized subscribers; and
- eavesdropping of the various information which are exchanged on the radio path.

It can be seen that PSMNs intrinsically do not provide the same level of protection to their operators and subscribers as the traditional telecommunication networks provide. This fact leads to the need to implement security features in a GMR-2 PSMN in order to protect:

1) the access to the mobile services;
2) any relevant item from being disclosed at the radio path, mainly in order to ensure the privacy of user-related information.

Two levels of protection are therefore assumed:

- where security features are provided, as defined in clause 3, the level of protection at the radio path of the corresponding items is as good as the level of protection provided in the fixed networks;
- where no special provision is made, the level of protection at the radio path is null.

5 Security features provided in a GMR-2 PSMN

The following security features are considered:

- subscriber identity (IMSI) authentication;
- user data confidentiality on physical connections;
- connectionless user data confidentiality;
- signalling information element confidentiality.

The implementation of these four security features is mandatory on both the fixed infrastructure side and the MES side. This means that all GMR-2 PSMNs and all MESs shall be able to support every security feature. Use of these four security features is at the discretion of the operator for its own subscribers while on the HPSMN. For roaming subscribers, use of these four security features is mandatory unless otherwise agreed by all the affected PSMN operators (see also clause 5.3.3).

5.1 Subscriber identity confidentiality

5.1.1 Definition

The subscriber identity confidentiality feature is the property that the IMSI is not made available or disclosed to unauthorized individuals, entities or processes. This feature is not implemented in the current version of GMR-2.

5.1.2 Purpose

If implemented this feature would provide for the privacy of the identities of the subscribers who are using GMR-2 PSMN resources (e.g. a traffic channel or any signalling means).

5.1.3 Functional requirements

If implemented this feature would necessitate the confidentiality of the subscriber identity (IMSI) when it is transferred in signalling messages (see clause 5.5) together with specific measures to preclude the possibility to derive it indirectly from listening to specific information, such as addresses, at the radio path.

If implemented the means used to identify a mobile subscriber on the radio path would consist of a local number called Temporary Mobile Subscriber Identity (TMSI).

If implemented , the subscriber identity confidentiality feature would apply for all signalling sequences on the radio path. However, in the case of location register failure, or in case the MES had no TMSI available, open identification would be allowed on the radio path.

5.2 Subscriber identity authentication

5.2.1 Definition

International Mobile Subscriber identity (IMSI) authentication is the corroboration by the land-based part of the system that the subscriber identity (IMSI), transferred by the mobile subscriber within the identification procedure at the radio path, is the one claimed.

5.2.2 Purpose

The purpose of this authentication security feature is to protect the network against unauthorized use. It enables also the protection of the GMR-2 PSMN subscribers by denying the possibility for intruders to impersonate authorized users.

5.2.3 Functional requirements

The authentication of the GMR-2 PSMN subscriber identity may be triggered by the network when the subscriber applies for:

- a change of subscriber-related information element in the VLR or HLR (including some or all of: location updating involving change of VLR, registration or erasure of a supplementary service); or
- an access to a service (including some or all of: set-up of mobile originating or terminated calls, activation or deactivation of a supplementary service); or
- first network access after restart of MSC/VLR; or
- in the event of cipher key sequence number mismatch.

Physical security means must be provided to preclude the possibility to obtain sufficient information to impersonate or duplicate a subscriber in a GMR-2 PSMN, in particular by deriving sensitive information from the mobile earth station equipment.

If, on an access request to the GMR-2 PSMN, the subscriber identity authentication procedure fails and this failure is not due to network malfunction, then the access to the GMR-2 PSMN shall be denied to the requesting party.

5.2.4 Authentication during a malfunction of the network

If an MES is registered and has been successfully authenticated, whether active or not active on a call, calls are permitted (including continuation and hand-over).

If an MES has already been registered (and therefore been already authenticated) and can not be successfully re-authenticated due to the network malfunction (e.g. the HPSMN was not able to provide authentication pairs RAND, SRES), calls are permitted.

If an MES attempts to register and can not be successfully authenticated due to the network malfunction, calls are not permitted.

If the MES is not registered, or ceases to be registered, a new registration need to be performed, and the preceding cases apply.

5.3 User data confidentiality on physical connections (Voice and Non-voice)

5.3.1 Definition

The user data confidentiality feature on physical connections is the property that the user information exchanged on traffic channels is not made available or disclosed to unauthorized individuals, entities or processes.

5.3.2 Purpose

The purpose of this feature is to ensure the privacy of the user information on traffic channels.

5.3.3 Functional requirements

Encryption will normally be applied to all voice and non-voice communications. Although a standard algorithm will normally be employed, it is permissible for the mobile earth station and/or PSMN infrastructure to support more than one algorithm. In this case, the infrastructure is responsible for deciding which algorithm to use (including the possibility not to use encryption, in which case confidentiality is not applied).

When necessary, the MES shall signal to the network indicating which of up to seven ciphering algorithms it supports. The serving network then selects one of these that it can support (based on an order of priority pre-set in the network), and signals this to the MES. The MES and network then use the selected algorithm. The network shall not provide service to an MES that indicates that it does not support any of the ciphering algorithm(s) required by GSM 02.07 [4].

The ME has to check if the user data confidentiality is switched on, by using one of the seven algorithms as defined in GSM 02.07 [4]. In the event that the ME detects that this is not the case, or ceases to be the case (e.g. during handover), then an indication is given to the user.

This ciphering indicator feature may be disabled by the SIM (see GSM 11.11[6]).

In case the SIM does not support the feature that disables the ciphering indicator, then the ciphering indicator feature in the ME shall be enabled by default.

The nature of the indicator and the trigger points for its activation are for the ME manufacturer to decide.

During the establishment of a call the trigger point shall be at call initiation at the latest. In the case of hand-over the trigger point shall be the completion of hand-over at the latest.

The manufacturer may provide the means to enable the user to temporarily disable the feature. This should be done in such a way that the user can protect it from misuse.

5.4 Connectionless user data confidentiality

5.4.1 Definition

The connectionless user data confidentiality feature is the property that the user information which is transferred in a connectionless packet mode over a signalling channel is not made available or disclosed to unauthorized individuals, entities or processes.

5.4.2 Purpose

The purpose of this feature is to ensure the privacy of the user information on signalling channels (e.g. short messages).

5.4.3 Functional requirements

NOTE: Short Messaging user data confidentiality requirements apply only to point-to-point data transfers since SMS Cell Broadcast is not provided in this version of GMR-2.

5.5 Signalling information element confidentiality

5.5.1 Definition

The signalling information element confidentiality feature is the property that a given piece of signalling information which is exchanged between MESs and base stations is not made available or disclosed to unauthorized individuals, entities or processes.

5.5.2 Purpose

The purpose of this feature is to ensure the privacy of users related signalling elements.

5.5.3 Functional requirements

When used, this feature applies on selected fields of signalling messages which are exchanged between MESs and base stations.

The signalling information elements included in the message used to establish the connection (protocol discriminator, connection reference, message type and MES identity (IMSI or IMEI according to the circumstance)) are not protected.

The following signalling information elements related to the user are protected whenever used after connection establishment:

- International Mobile Equipment Identity (IMEI);
- International Mobile Subscriber Identity (IMSI);
- Calling subscriber directory number (mobile terminating calls);
- Called subscriber directory number (mobile originated calls).

The IMEI requires physical protection against being removed, replaced or its contents being changed by unauthorized individuals. The IMSI is stored securely within the SIM.

The security policy for the Software Version Number (SVN) is such that it cannot be readily changed by the user, but can be updated with changes to the software. The security of the SVN shall be separate from that of the IMEI.

History

Document history		
V1.1.1	March 2001	Publication