ETSI EN 300 920 V7.1.1 (2000-08)

European Standard (Telecommunications series)

Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 version 7.1.1 Release 1998)

Reference
REN/SMG-010209Q7R1

Keywords
Digital cellular telecommunications system,
Global System for Mobile communications (GSM)

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

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, 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).

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.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Special Mobile Group (SMG).

The present document defines security features within the digital cellular telecommunications system.

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

Version 7.x.y

where:

7 GSM Phase 2+ Release 1998;

x the second digit is incremented for changes of substance, i.e. technical enhancements, corrections, updates, etc.;

y the third digit is incremented when editorial only changes have been incorporated in the specification.

National transposition dates	
Date of adoption of this EN:	14 July 2000
Date of latest announcement of this EN (doa):	31 October 2000
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 April 2001
Date of withdrawal of any conflicting National Standard (dow):	30 April 2001

1 Scope

Bearer and Teleservices, as respectively defined in GSM 02.02 and GSM 02.03, are the objects which the GSM PLMN operators offer to their customers. Besides these basic telecommunications services, features which aim at up-grading these basic services need also to be offered. Due to the use of radiocommunications in a PLMN, which are of a special nature compared to classical distribution transmission techniques used in the fixed networks, such a category of features is related to security aspects.

In a GSM PLMN, both the users and the network operator have to be protected against undesirable intrusion of third parties. However, measures should be provided for in order to insure maximum protection of the rights of the individuals concerns. As a consequence, a security feature is either a supplementary service to Tele or Bearer services, which can be selected by the subscriber, or a network function involved in the provision of one or several telecommunication services.

The purpose of the present document is to define the security features which are to be available in a GSM PLMN, together with the associated levels of protection. The present document is only concerned with those security features which aim at the up-grading of the security in a GSM PLMN. In particular, end-to-end security is outside the scope of the present document.

The implementation aspects of security features are described in GSM 03.20.

1.1 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 02.02: "Digital cellular telecommunications system (Phase 2+); Bearer Services (BS) supported by a GSM Public Land Mobile Network (PLMN)".

[3] GSM 02.03: "Digital cellular telecommunications system (Phase 2+); Teleservices supported by a GSM Public Land Mobile Network (PLMN)".

[4] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[5] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

1.2 Abbreviations

Abbreviations used in the present document are listed in GSM 01.04.

2 General

The use of radiocommunications for transmission to the mobile subscribers makes PLMNs particularly sensitive to:

- misuse of their resources by unauthorized persons using manipulated Mobile 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 PLMNs 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 GSM PLMN in order to protect:

i) the access to the mobile services;

ii) 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. All items which are not dealt with in clause 3 are therefore considered to need no protection.

3 Security features provided in a GSM PLMN

The following security features are considered:

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

The implementation of these five security features is mandatory on both the fixed infrastructure side and the MS side. This means that all GSM PLMNs and all MSs shall be able to support every security feature. Use of these five security features is at the discretion of the operator for its own subscribers while on the HPLMN. For roaming subscribers, use of these five security features is mandatory unless otherwise agreed by all the affected PLMN operators (see also subclause 3.3.3).

3.1 Subscriber identity confidentiality

3.1.1 Definition

The subscriber identity confidentiality feature is the property that the IMSI is not made available or disclosed to unauthorized individuals, entities or processes.

3.1.2 Purpose

This feature provides for the privacy of the identities of the subscribers who are using GSM PLMN resources (e.g. a traffic channel or any signalling means). It allows for the improvement of all other security features (e.g. user data confidentiality) and provides for the protection against tracing the location of a mobile subscriber by listening to the signalling exchanges on the radio path.

3.1.3 Functional requirements

This feature necessitates the confidentiality of the subscriber identity (IMSI) when it is transferred in signalling messages (see subclause 3.5) together with specific measures to preclude the possibility to derive it indirectly from listening to specific information, such as addresses, at the radio path.

The means used to identify a mobile subscriber on the radio path consists of a local number called Temporary Mobile Subscriber Identity (TMSI), described in GSM 03.20.

When used, the subscriber identity confidentiality feature shall apply for all signalling sequences on the radio path. However, in the case of location register failure, or in case the MS has no TMSI available, open identification is allowed on the radio path.

3.2 Subscriber identity authentication

3.2.1 Definition

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

3.2.2 Purpose

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

3.2.3 Functional requirements

The authentication of the GSM PLMN 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 GSM PLMN, in particular by deriving sensitive information from the mobile station equipment.

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

3.2.4 Authentication during a malfunction of the network

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

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

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

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

3.3.1 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.

3.3.2 Purpose

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

3.3.3 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 station and/or PLMN 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 MS 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 preset in the network), and signals this to the MS. The selected algorithm is then used by the MS and network. The network shall not provide service to an MS which indicates that it does not support any of the ciphering algorithm(s) required by GSM 02.07.

The ME has to check if the user data confidentiality is switched on using one of the seven algorithms as defined in GSM 02.07. 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).

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 handover the trigger point shall be the completion of handover 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.

3.4 Connectionless user data confidentiality

3.4.1 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.

3.4.2 Purpose

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

3.4.3 Functional requirements

NOTE: Protection of connectionless user data is not applicable to SMS Cell Broadcast.

3.5 Signalling information element confidentiality

3.5.1 Definition

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

3.5.2 Purpose

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

3.5.3 Functional requirements

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

The signalling information elements included in the message used to establish the connection (protocol discriminator, connection reference, message type and MS identity (IMSI, TMSI 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 IMSI is stored securely within the SIM.

The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type approved after 1st June 2002.

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.

Annex A (informative): Change history

SMG#	VERS	NEW_VERS	CR	SUBJECT
S03	4.0.0	4.1.0	003	Clarifications
S05	4.1.0	4.2.0	004	Control of encryption
S12	4.2.0	4.3.0	A001	Security policy for SVN
s22	4.3.0	4.4.0	A003	Correction of User data confidentiality feature
s22	5.0.1	5.1.0	A004	Correction of User data confidentiality feature
S20	4.5.0	5.0.1		Upgrade to Phase 2+ version 5.0.0
S27	5.0.1	6.0.0		Upgrade to Release 1997 version 6.0.0
S29		7.0.0		Upgrade to Release 1998 version 7.0.0
-	7.0.0	7.0.1		Version update to 7.0.1 for publication
S31	7.0.1	7.1.0	A008r2	Modification of section 3.5.3 to enhance IMEI security
	7.1.0	7.1.1		Version update to 7.1.1 for Publication

History

Document history			
V7.0.0	August 1999	One-step Approval Procedure	OAP 9956: 1999-08-25 to 1999-12-24
V7.0.1	January 2000	Publication	
V7.1.0	March 2000	One-step Approval Procedure	OAP 20000714: 2000-03-15 to 2000-07-14
V7.1.1	August 2000	Publication	