ETSI/TC GSM
Date : June, 1993
Released by : ETSI/PT 12

UPDATE NOTE

Recommendation GSM 02.09

Security Aspects

Previously released version 1992: 3.0.1
Updated version June 1993: 3.1.0

1. Reason for Change

Change Request 02.09-5 for GSM Phase 1 - approved at SMG#6 bis, Issy-les-Moulineaux is included.

2. Details of Change

Page 7 has been changed to include addition of IMEI security requirements.

3. Instructions to update GSM Recommendation

Whole version 3.1.0 is included.

ETSI GSM

Released by: ETSI PT12

Release date: May, 1993

Recommendation: GSM 02.09

Title: SECURITY ASPECTS

List of contents :

Original language: English

Number of pages: 8

1. SCOPE

Bearer and Teleservices, as respectively defined in GSM Recommendations 02.02 and 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 this Recommendation is to define the security features which are to be available in a GSM PLMN, together with the associated levels of protection. This Recommendation is only concerned by those security features which aim at the up-grading of the security in a GSM PLMN. In particular, end-to-end security is out the scope of this Recommendation.

The implementation aspects of security features are described in GSM Recommendations 03.20 and 03.21. Network performances aspects are dealt with in GSM Recommendation 03.05.

The terms related to security aspects used in the relevant GSM Recommendations are in accordance with the ISO definitions in the field of security and protection (ISO 7498 proposed draft Addendum N[2).

Editorial Note: Physical security aspects and the necessity of further defining provisions and/or procedures for secure production and distribution of the hardware which contains the identities require further study.

2. GENERAL

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

- misuse of their resources by unauthorized persons using manipulated Mobile Stations, who try to impersonate authorized Subscribers; and
- eavesdropping of the various informations which are exchanged on the radiopath.

It can be seen that PLMNs intrinsically do not provide for 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 radiopath, mainly in order to insure the privacy of users related information.

Two level of protection are therefore assumed :

- where security features are provided, as defined in Section 3, the level of protection at the radiopath of the corresponding items is as good as the level of protection provided in the fixed networks;
- where no special provision is made for, the level of protection at the radiopath is null. All items which are not dealt with in Section 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. Also, the usey of the five security features is mandatory, with the exception of Notes 2 and 3 in Table 1.

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 subscriber who are using GSM PLMN resources (e.g. a traffic channel or any signalling means). It allows for the improvement y 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. Operational requirements

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

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

The subscriber identity confidentiality feature shall apply for all signalling sequences on the radiopath, according to Note 3 of Table 1. However, in the case of location register failure, or in case the MS has no TMSI available, open identification is allowed on the radiopath.

3.2. Subscriber Identity Authentication

3.2.1. Definition

Subscriber identity (IMSI) authentication is the corroboration by they land-based part of the system that the subscriber identity (IMSI or TMSI), transferred by the mobile subscriber within the identification procedure at the radiopath,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. Operational requirements

The authentication of the GSM PLMN subscriber identity is applied at each registration, each call set-up attempt (mobile originating or terminated calls) according to Note 2 of Table

1, and before performing some supplementary services activation, deactivation, registration or erasure.

The authentication of the GSM PLMN subscriber identity is also required at those location up-dating procedures which cause changes of the Mobile Station Roaming Number. Authentication in the remaining cases of location up-dating (e.g. simple change of LAI) is left to the network operator discretion.

In particular, authentication is not mandatory prior to IMSI attach and detach procedures.

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, 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 succesfully authenticated, whether active or not active on a call, calls are permitted (including continuation and hand-over). The Home PLMN will receive the charge.

If an MS has already been registered (and therefore been alreadyy 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. The Home PLMN will receive the charge.

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 insure the privacy of the user information on traffic channels.

3.3.3. Operational requirements

This feature applies for both voice and non-voice communications.It is considered as a network function involved in the provision of all telecommunication services.

Note 1: End-to-end protection of user data is of the responsability of the users. In order to allow for such protection mechanisms, the system shall provide for transparent data circuits.

Note 2: It is noted that in some countries the GSM operators will require a specific license for the use of encryption user data.

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 insure the privacy of the user information on signalling channels (e.g. short messages).

3.4.3. Operational requirements

Note1: End-to-end protection of connectionless user data is of the responsability of users.

Note 2: It is noted that in some countries the GSM operators will require a specific license for the use of encryption user data.

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 mobile stations 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 insure the privacy of users related signalling elements.

3.5.3. Operational requirements

This feature applies on selected fields of signalling messages which are exchanged between mobile stations and base stations.

The four signalling information elements which directly control the connection establishment (protocol discriminator, call reference, message type and mobile subscriber identity (IMSI or TMSI)) are not protected.

The following signalling information elements related to the user are protected:

- International Mobile Equipment Identity (IMEI);
- International Mobile Subscriber Identity (IMSI);
- User identity (e.g. in the case of payphone operation) (For further study);
- Calling subscriber directory number (mobile terminating calls) ;
- Called subscriber directory number (mobile originated calls).

The need for protection of signalling information elements to protect the network against illicit use non covered by authentication is under study.

Both IMSI and IMEI require physical protection.

Physical protection means that manufacturers shall take necessary and sufficient measures to ensure the programming and mechanical security of the IMEI. The manufacturer shall also ensure that the knowledge of how to change the IMEI (where applicable) remains securely under his control.

3.6. Overview of GSM PLMN Security Features

Table 1/GSM 02.09 shows the different security features in a GSM PLMN. It shows also the status of implementation required in the fixed infrastructure of the GSM PLMNs and in the MSs, and the status of its usage.

Security Features	Mandatory/Optional (M/O) Status			Technical and Operational Framework
	PLMN	MS	Use	
1. Subscriber Id. (IMSI) Confidentiality	M	M	M	See Section 3.1 and see Note 3.
2. Subscriber Id. Authentication	M	M	M	See Section 3.2 and see Note 2.
3. User Data (voice and non-voice) Confidentiality on Physical Connection.	M	M	M	See Section 3.3 and see Note 1.
4. Connectionless User Data Confidentiality :				See Section 3.4 and see Note 1.
- Point to point	M	M	M	
- Broadcast	-	-	-	Not applicable.
5. Signalling Information Element Confidentiality	M	M	M	See Section 3.5.

TABLE 1/GSM 02.09, GSM PLMN Security features

Note 1: It is noted that in some countries the GSM operators will require a specific license for the use of encryption of user data.

Note 2 : The frequency with which a particular PLMN applies the authentication procedure at call set-up to its own subscribers is under its own responsability. However, a PLMN shall apply the authentication procedure to visiting subscribers at least as often as this feature is applied to these subscribers in their Home PLMN. Bilateral agreements are permitted.

If in the future this reduced authentication procedure is found to compromise the security level on any other network, authentication on every call set-up shall be mandatorily invoked again.

Note 3: The use of subscriber identity confidentiality is a choice left to each PLMN operator. However a PLMN operator shall apply subscriber identity confidentiality to all visiting subscriber from a given PLMN if this feature is applied in that PLMN. Bilateral agreement are permitted.