TR 101 105 V5.0.0 (1997-10)

Technical Report

Digital cellular telecommunications system (Phase 2+); Fraud Information Gathering System (FIGS); Service requirements - Stage 0 (GSM 01.31 version 5.0.0)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

European Telecommunications Standards Institute

Reference
DTR/SMG-100131Q (a8c02i04.PDF)

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

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

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 ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr).

Pursuant to the ETSI Interim 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 ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Technical Specification (TS) has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).

This ETSI Technical Specification describes the requirements (at a stage 0 level) of the Fraud Information Gathering System (FIGS).

1 Scope

This GSM Technical Specification describes the requirements (at a stage 0 level) of the Fraud Information Gathering System (FIGS). FIGS provides the means for the HPLMN to monitor a defined set of subscriber activities.

The aim is to enable service providers/network operators to use FIGS, and service limitation controls such as ODB and IST, to limit their financial exposure to large unpaid bills produced on subscriber accounts whilst the subscriber is roaming outside their HPLMN. HPLMNs may also choose to send information across the Y-interface on subscriber activities whilst their subscribers are within the HPLMN.

2 Normative references

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case 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.

[1] GSM 01.04 (ETR 350): "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 02.33: "Digital cellular telecommunications system (Phase 2+); Lawful Interception - stage 1".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this specification the following definitions apply:

monitored activities: subscriber activities that must be reported to the HPLMN. These can be call related events (e.g. call-set-up, call termination) or the invocation of call related and call independent supplementary services (e.g. Call Hold, Call Waiting, Call Transfer, Call Forwarding, USSD).

Y-interface: The interface between the HPLMN and the Fraud Detection System (FDS).

J-interface: The interface between the HPLMN and the VPLMN which is used to send FIGS data from the VPLMN to the HPLMN.

K-interface: The interface between the HPLMN and the VPLMN that is used to send FIGS commands from the HPLMN to the VPLMN.

Home Network: The home PLMN including non-GSM elements such as the FDS, customer service systems and billing

3.2 Abbreviations

Abbreviations used in this report are also listed in GSM 01.04.

For the purposes of this report the following abbreviations apply:

FIGS	Fraud Information Gathering System
FDS	Fraud Detection System. This is not necessarily an automatic system but may be one that requires human intervention.
IST	Immediate Service Termination

4 Fraud Information Gathering System overview

A number of proposals have been suggested for a Subscriber Supervisory System (SSS) for which specifications were produced from May 1995 through to December 1996. Following joint review between SMG1 and SMG10, it was agreed that the system should be re-specified to take account of network operator and manufacturer needs for a Fraud Information Gathering System (FIGS). This report provides an outline of such a system.

This specification describes a method by which the Home Network can be provided with data on the activities of its subscribers in a VPLMN. The Home Network can make inferences about what the subscriber is doing and then take decisions on what the subscriber should be allowed to do. This specification does not address any Fraud Detection systems or the intelligence that is used to advise the HPLMN on the controls to be applied to a subscriber.

Figure 1 shows the flow of messages between the HPLMN and the VPLMN and between the HPLMN and the FDS.

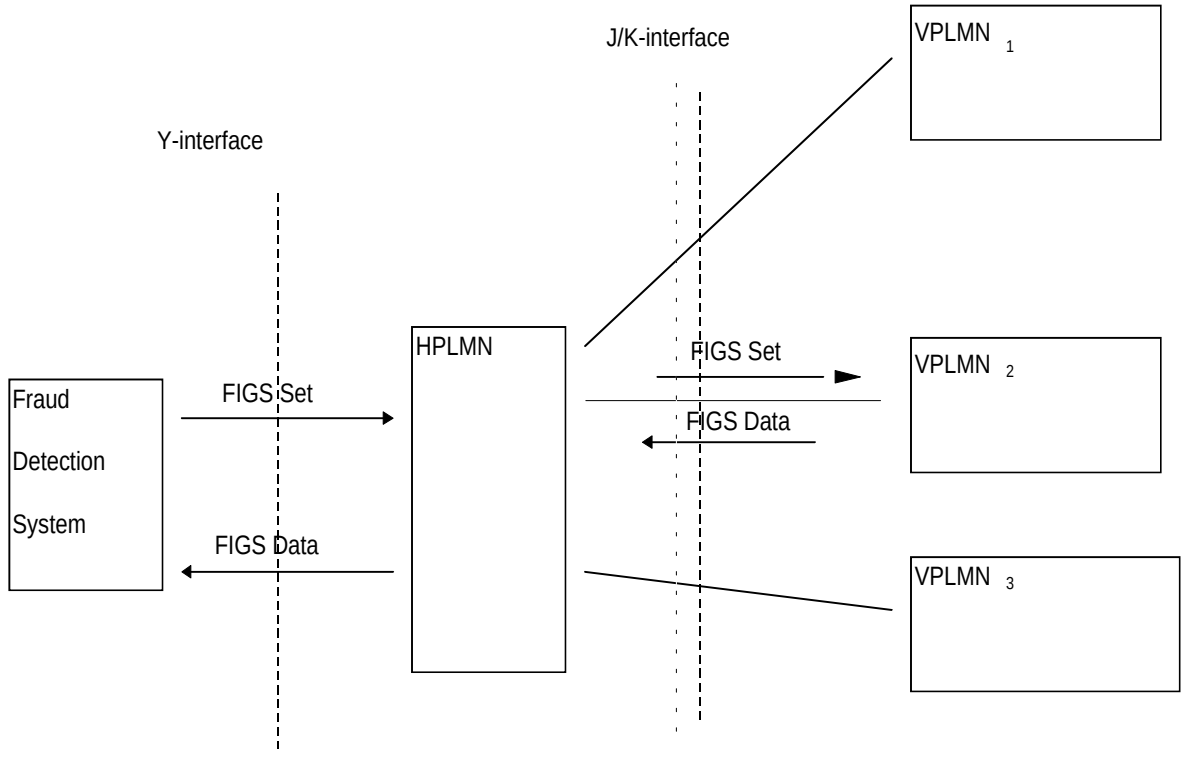

Figure 1: Flow of messages between the HPLMN and the VPLMN and between the HPLMN and the FDS

5 The need for fraud detection systems and controls

5.1 Outline of present situation

Modern telecommunications networks, particularly mobile networks provide the potential for fraudsters to make use of telecommunication services (Voice, Data, Fax etc.) without the intent to pay. A number of different scenarios are exploited and it is up to the network operator or service provider to detect misuse where it occurs and to stop it at the earliest possible opportunity.

The scale of frauds can be many thousand of ECU per day on a single account when International or Premium rate numbers are called. The most common types of fraud that effect networks like GSM are related to the ability to sell calls at below market price using stolen air-time/equipment where the user of the equipment does not intend to pay the network operator or service provider. Fraudulent subscribers often avoid payment by obtaining a handset and a subscription to a GSM network by fraudulently giving details and justifications to the network operators/service provider. If there are not good controls within the network the subscriber can make a large volume of calls to expensive destinations and accumulate a large bill.

Roaming, in co-ordination with advanced services such as call transfer and multi-party calls, complicates the issue further, requiring control of the customer within the VPLMN. Many simultaneous calls can be set up and large bills accumulated in a short time. At present no system exists within the GSM network architecture for speedily transferring information on subscriber activity from the VPLMN to the HPLMN.

In the future, SIMs may roam to non-GSM networks, further broadening the area over which control is required. It is recognised that if FIGS is implemented in non-GSM networks that suitable inter-working units will be required to translate commands and information.

5.2 General Principles

The PLMN network should be able to supply relevant information to the HPLMN network so it can make a decision on whether to terminate a call or to change the Operator Determined Barring (ODB) configuration for the specific subscriber. This decision will be carried out by the HPLMN or service provider. It is recognised that there is a limit to the type and volume of information that can be transferred between the VPLMN and the HPLMN. Therefore the requirement for the system is that distilled and standardised information must be supplied between the VPLMN and HPLMN.

5.3 Capabilities

The following minimum capabilities are required. See figure 1.

Within the Home Network:

- to mark a subscriber, defined by the IMSI or MSISDN, as being under FIGS control ("FIG Set");
- to receive from the VPLMN the data described below;
- to remove the monitoring of a subscriber’s activities ("FIGS Unset").

Within the VPLMN:

- to transmit to the HPLMN information(FIGS Data):
  - at the start of a call;
  - at the end of a call;
  - during a call` for long calls or at the mid-call invocation of supplementary services.

5.4 Service conditions

The following service conditions shall apply:

- FIGS shall not modify the VPLMN's service;
- FIGS should not alter any standard GSM functionality seen by the customer or effect the service quality;
- If the VPLMN network does not have the resources to support a FIGS Set command it shall respond accordingly to the HPLMN.

5.5 Information Delivery Time

The need for up to date information is a critical part of any fraud information system. The sooner data is transferred to the HPLMN, the sooner fraud can be stopped. Therefore the proscribed information shall be transferred from the VPLMN to the HPLMN over the J-interface within two minutes of the occurrence of a FIGS-monitored event

The information shall preferably be transferred from the VPLMN to the HPLMN over existing communication links (e.g. SS7 signalling links).

5.6 Subscriber Data Volumes

If the support of FIGS is causing overload within the VPLMN the FIGS system shall not permit the marking of new subscribers. The VPLMN should therefore handle up to a realistic limit any requests for marking of subscribers and be able to support the associated data transfer. The setting of this limit is outside the scope of this specification.

Each VPLMN should limit the number of subscribers that each HPLMN may request to be monitored using FIGS. Otherwise an HPLMN may take more than its “fair share” of the FIGS processing capability of a VPLMN.

A mechanism shall be required whereby a VPLMN can charge an HPLMN for the bulk data transfer made to that HPLMN.

6 The Y-interface

The interface between the home network and the network’s fraud detection and processing systems shall be through a specific interface called the Y-interface. This will be used to present information to the fraud detection systems. The contents of messages sent on this interface shall be specified but not the transfer mechanism. This is in line with the approach used for the X-interface as specified in GSM 02.33.

The FDS will indicate to the HPLMN (via the Y-interface) subscribers that should be subject to FIGS monitoring. This information will update the HPLMN HLR.

Information, as listed in section 5.3 gathered from the VPLMN will be transferred through the Y-interface to the FDS system. Following processing of this information, the FDS system can take no action or can advise the home network to do one of the following:

a) update ODB categories;

b) instigate an Immediate Service Termination (IST);

c) mark the subscriber as not being required to be monitored under FIGS.

7 The J and K-interfaces

The interface between the HPLMN and the VPLMN that is used to send FIGS data from the VPLMN to the HPLMN shall be through a specific interface called the J-interface. The contents of messages to be sent on this interface shall be specified but not the transfer mechanism

The interface between the HPLMN and the VPLMN that is used to send FIGS commands from the HPLMN to the VPLMN shall be through a specific interface called the K-interface. The contents of messages to be sent on this interface shall be specified but not the transfer mechanism.

8 Security of the system

It is expected that there will be a need for authentication, data integrity and confidentiality of the commands and data transferred between PLMNs.

These issues are for study under other work items within the SMG10 work programme.

Annex A:
Document history

Date	Version	Section affected	SMG
June 97	1.0.0	-	to SMG#22 for information
October 1997	2.0.0		to SMG#23 for approval

History

Document history		
V5.0.0	October 1997	Publication

ISBN 2-7437-1771-8
Dépôt légal : Octobre 1997