ETSI TR 141 031 V9.0.0 (2010-02)

Technical Report

Digital cellular telecommunications system (Phase 2+);
Fraud Information Gathering System (FIGS);
Service requirements;
Stage 0
(3GPP TR 41.031 version 9.0.0 Release 9)

Reference
RTR/TSGS-0341031v900

Keywords
GSM, SECURITY

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

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://webapp.etsi.org/IPR/home.asp).

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 Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This Technical Report 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 Operator Determined Barring (ODB) and Immediate Service Termination (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 collect information on subscriber activities whilst their subscribers are within the HPLMN.

2 Normative 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] GSM 01.04: "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 report 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, Unstructured Supplementary Service Data).

Home Network: The home PLMN including non-GSM elements such as the Fraud Detection System (FDS), customer service systems and billing.

3.2 Abbreviations

Abbreviations used in this report are 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 report 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 report 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.

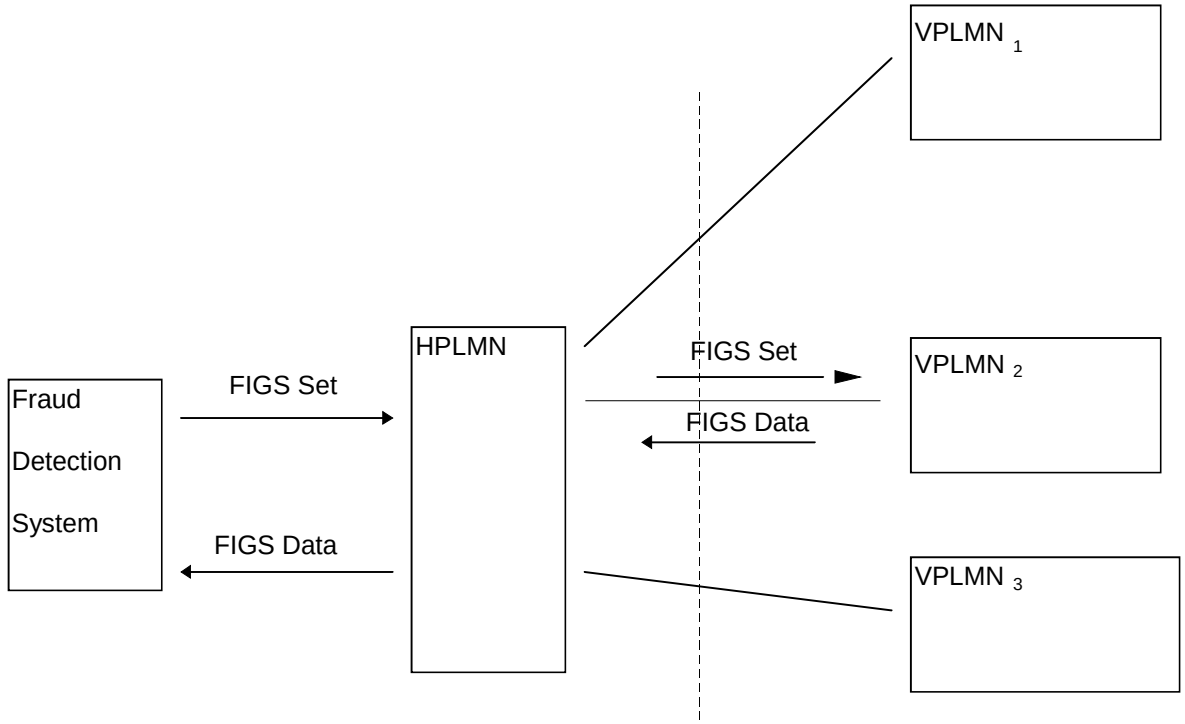

Figure 1: Flow of messages between the HPLMN and the VPLMN and between the HPLMN and the FDS

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 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 report.

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 Interface between HPLMN and FDS

The interface between the home network and the network''s fraud detection and processing systems shall be through a specific 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 subscribers that should be subject to FIGS monitoring. This information will update the HPLMN HLR.

Information, as listed in subclause 5.3 gathered from the VPLMN will be transferred 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 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:
Change History

Change history						
SMG#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
						No Phase 1 version
SMG#22	01.31				1.0.0	To SMG#22 for information
SMG#23	01.31				2.0.0	To SMG#23 for approval
SMG#23	01.31	2.0.0		R96	5.0.0	TS approved by SMG#23
SMG#25	01.31	5.0.0		R98	7.0.0	The report was converted to version 7.0.0 because the work item is related to Release 98. Version 5.x.y was withdrawn (SMG#25)
SMG#26	01.31	7.0.0	A001	R98	7.0.1	CR 01.31-A001 (Editorial) approved by SMG#26
		7.0.1	-	R99	8.0.0	The report was converted to version 8.0.0 because the work item is related to Release 99.
Change history						
TSG SA#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
SP-11	01.31	8.0.0	-	Rel-4	41.031 v 4.0.0	Upgrade to Release 4 (3GPP numbering)
	41.031	4.0.0	-	Rel-4	4.0.1	May 2001: change from TS layout to TR layout.
SP-16	41.031	4.0.1	-	Rel-5	5.0.0	June 2002: Upgrade to Release 5
SP-26	41.031	5.0.0	-	Rel-6	6.0.0	December 2004: Upgrade to Release 6
SP-36	41.031	6.0.0	-	Rel-7	7.0.0	June 2007: Upgrade to Release 7
SP-42	41.031	7.0.0	-	Rel-8	8.0.0	December 2008: Upgrade to Release 8
SP-46	41.031	8.0.0	-	Rel-9	9.0.0	December 2009: Upgrade to Release 9

History

Document history		
V9.0.0	February 2010	Publication