INTERNATIONAL TELECOMMUNICATION UNION

ITU-T M.3210.1

(01/2001)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

Telecommunications management network

TMN management services for IMT-2000 security management

ITU-T Recommendation M.3210.1

(Formerly CCITT Recommendation)

ITU-T M-SERIES RECOMMENDATIONS

TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	**M.3000–M.3599**
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation M.3210.1

TMN management services for IMT-2000 security management

Summary

This Recommendation is one of the series of M.3200 Recommendations on TMN Management Services that provide description of management services, goals and context for management aspects of IMT-2000 networks. This Recommendation provides a profile for fraud management in an IMT-2000 mobile network. This Recommendation builds on the function sets identified in ITU-T M.3400 by defining new function sets, functions and parameters and adding additional semantics and restrictions.

Source

ITU-T Recommendation M.3210.1 was prepared by ITU-T Study Group 4 (2001-2004) and approved under the WTSA Resolution 1 procedure on 19 January 2001.

Keywords

Telecommunications Management Network (TMN), TMN Management Service, International Mobile Telecommunications: IMT-2000, Security Management, Fraud Detection and Containment, Third Generation Wireless – 3G Systems.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation M.3210.1

TMN management services for IMT-2000 security management

1 Introduction

This Recommendation provides requirements and analysis of the security management (administration) of IMT-2000. The emphasis is on the X interface between two service providers and the management services needed between the two service providers to detect and prevent fraud. The methodology used in this Recommendation is based on ITU-T M.3020.

1.1 Purpose and scope

This Recommendation describes a subset of security management services, identified in ITU-T M.3200 as a TMN managed area, for IMT-2000 management. It describes the requirements and analysis of operating the Fraud Information Gathering System (FIGS) between service providers. FIGS provides the means for the wireless service provider to monitor a defined set of subscriber activities. The aim is to enable service providers/network operators to use FIGS to limit their financial exposure to large unpaid bills produced on subscriber accounts whilst the subscriber is roaming outside their home areas.

Verification of the authenticity of the Home Network-FDS and the Visited Service Provider is beyond the scope of this management service.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Q.1701 (1999), *Framework of IMT-2000 Networks*.

[2] ITU-T Q.1711 (1999), *Network functional model for IMT-2000*.

[3] ITU-T Q.1721 (2000), *Information flows for IMT-2000 capability set 1*.

[4] ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

[5] ITU-T M.3020 (2000), *TMN interface specification methodology*.

[6] ITU-T M.3200 (1997), *TMN management services and telecommunications managed areas*: *overview*.

[7] ITU-T M.3400 (2000), *TMN management functions*.

3 Definitions

This Recommendation defines the following terms:

3.1 visited network: The foreign or Visited Network which provides subscriber with roaming service.

3.2 home network: The Home Network to which the wireless subscriber contracts service.

3.3 home network-FDS: The Fraud Detection System operated by the Home Network.

3.4 fraud report: A Fraud Report is the set of potential violations that the subscriber has performed that may indicate potential fraud. This typically captures threshold violations from the subscribers' normal patterns or criteria (like calling countries, high usage limits).

3.5 Role-related definitions

This Recommendation makes use of the following roles defined in ITU-T M.3208.1:

– service customer;

– network operator.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

FDS Fraud Detection System

FIGS Fraud Information Gathering System

GDMI Guidelines for the Definition of TMN Management Interface

IMT-2000 International Mobile Telecommunications 2000

ITU International Telecommunication Union

MS Management Services

N/A Not Applicable

NML Network Management Layer

SML Service Management Layer

TMN Telecommunications Management Network

4.1 Conventions

Symbol	Explanation
M	Mandatory
m(=)	The recipient must provide the same value in the response as provided in the request by the requestor.
O	Optional: Optionality is subject to definition according to the agreement between the two service providers, i.e. a parameter listed as optional may be made mandatory.
o(=)	Return of the value by the responder is optional; however, if the responder elects to return the value, it must be the same value supplied by the requestor in the request. Responder is not allowed to alter this field.
C	Conditional parameter: Definition of the Condition will be specified in the Notes column. A numeric suffix is used to enable reuse of the conditional statements.
c(=)	If the value is provided in the request by the requestor, the responder must provide the same value in the response.
Blank	A blank implies that the parameter is not applicable.

5 Security Management Service

5.1 Security issues

Modern telecommunication 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 (per day on a single account) can be substantial, especially when international or premium rate numbers are called. The most common types of fraud that affect 3G networks 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 the service provider. Fraudulent subscribers often avoid payment by obtaining a handset and a subscription to a 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.

5.2 Management Service description

With wireless subscribers roaming from one network operator to another (and with multiple service providers), Security Management Service becomes of paramount importance. This Recommendation specifies the Security Management related information exchanged over the x reference point between two TMN Operating System (OS)s (the Visited Network and the Home Network).

TMN relationships for IMT-2000 Security Management Service: Fraud Information Gathering are depicted in Figure 1. It shows the wireless subscriber roaming to a network of a visited service provider.

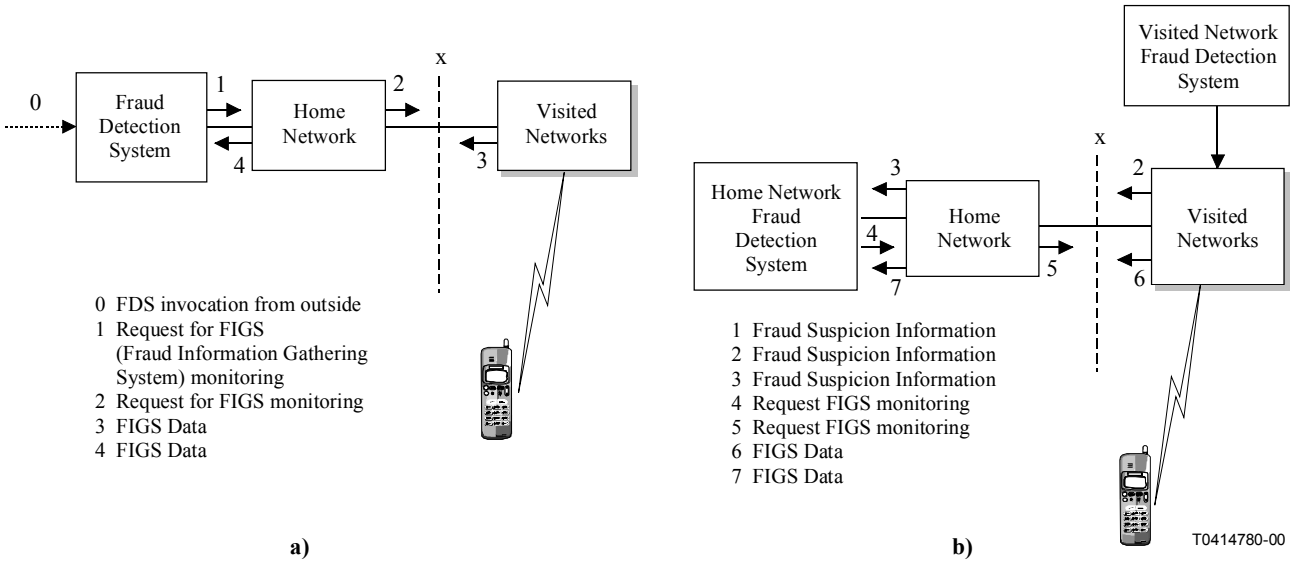

Figure 1/M.3210.1 – IMT-2000 Security Management Service: Fraud Information Gathering collaboration diagrams

In Figure 1 a), The Home Network Fraud Detection System (HN-FDS) requests the Visited Network to supply certain information about a subscriber from the time the subscriber registers in that Visited Network to the time the last of the monitored activities is finished in that Visited Network, which can be after the subscriber's deregistration from the Visited Network. The information received by the Home Network shall be passed to the Home Network-FDS. Analysis of this information may lead to further instructions transmitted to the Visited Network to act in an appropriate way.

Figure 1 b) actions are comparable to those of Figure 1 a) except that invocation of the activities is initiated by the visited service provider.

6 Management high-level requirements

The Home Network-FDS or the Visited Network can take preventive actions to control and prevent fraudulent activities, according to the security policies. The security management services described in this Recommendation are applicable across different service providers operating different or similar wireless networks. This management service provides the Visited Network and the Home Network-FDS with the capability to exchange and to control the exchange of information related to potential fraudulent activities in the Visited Network.

The Fraud Information Gathering System capabilities are categorized in Table 1:

Table 1/M.3210.1 – Minimum capabilities required for Fraud Information Gathering System

Scope	Reference	Requirement
System-wide capabilities	1	FIGS Monitoring should be activated by: 1 The Visited Network obtains requests from the Home Network-FDS for monitoring suspicious subscriber activities. 2 The Home Network-FDS receives unsolicited subscriber alerts from the Visited Network, especially if the roaming subscriber continues to obtain service from the Visited Network for extended periods of time.
	2	FIGS should not modify the Visited Network service.
	3	FIGS should not alter any standard 3G Wireless functionality seen by the customer or affect the service quality.
	4	FIGS Monitoring feature applies to all subscribed Bearer Services (e.g. Circuit, IP, etc.), TeleServices and Supplementary Services of the subscriber. It is not possible to apply FIGS independently to individual services.
	5	The information should be transferred from the Visited to the Home Network-FDS over existing communication links (e.g. TMN X interface, SS7 signalling links).
	6	A mechanism is required whereby a Visited Network can charge a Home Network-FDS for the bulk data transfer made to that Home Network-FDS.

Table 1/M.3210.1 – Minimum capabilities required for Fraud Information Gathering System *(concluded)*

Scope	Reference	Requirement
Home Network capabilities	7	Fraud information gathering is controlled by the Home Network-FDS and can be activated and deactivated by the Home Network-FDS only.
	8	The Home Network shall indicate the level of fraud monitoring required: **Level 1** accelerated accounting procedure, associated with a mechanism such as real time/near real time Billing. **Level 2** partial call information is gathered, but only at the beginning and the end of the call. **Level 3** full call information on subscriber activities, i.e. call start and end times, and partial call records. Notification of the invocation of Explicit Call Transfer, Call Deflection, Call Forwarding, Call Hold and Multi Party Service is also given.
	9	The Home Network-FDS shall be able to specify whether it would like call information on Mobile-Originated sessions, on Mobile-Terminated sessions, or on both.
	10	The Home Network should not permit the marking of new subscribers if the support of FIGS is causing overload within the Visited Network. The Visited Network should therefore handle up to a realistic limit any requests for marking of subscribers and should be able to support the associated data transfer. The setting of this limit is outside the scope of this Recommendation.
	11	The Home Network should mark a subscriber as being under FIGS monitoring.
	12	The Home Network should receive FIGS Data from the Visited Network.
	13	The Home Network ceases the FIGS monitoring of a subscriber's activities.
Visited Network capabilities	14	Based on roaming agreements, the Visited Network should advise the Home Network-FDS of information that suggests fraudulent activities.
	15	If the Visited Network does not have the resources to support a FIGS request, it should respond accordingly to the Home Network-FDS.
	16	Each Visited Network should limit the number of subscribers that each Home Network-FDS may request to be monitored using FIGS. Otherwise, a Home Network-FDS may take more than its "fair share" of the FIGS processing capability of a Visited Network.
	17	Information should be transferred from the Visited Network to the Home Network-FDS within two minutes of the occurrence of a FIGS-monitored event. This is because up-to-date information is a critical part of any fraud information system. The sooner data is transferred to the Home Network-FDS, the sooner fraud can be stopped.
	18	Based on roaming agreements, to transmit FIGS Data to the Home Network-FDS based on: 1 frequency requested by Home Network-FDS; 2 events specified by Home Network-FDS; and/or 3 on demand.

6.1 Management Service overview

Security Management includes the following function set groups according to ITU-T M.3400:

- Prevention;
- Detection;
- Containment and recovery;
- Security Administration.

Among the function set groups of ITU-T M.3400, this Recommendation only addresses aspects of Detection Function Set Groups in order to detect wireless fraud.

A key list of management requirements for "Security – Audits: Counts of Fraudulent Use" includes the following:

- Determination of security-related events;
- Recording of security-related events;
- Reporting of security-related events.

Several sources of detecting security violations in a wireless network exist. The processes in place in Home Network-FDS and the Visited Network use various factors such as billing usage and pattern analysis to produce security reports. The reports and events that are exchanged between the two service providers form the basis of the detection aspects of this Recommendation. The potential information contained in these reports may include: Time and date stamp, Deviation usage data, Usage data records, Alarm event reports, and Subscriber information.

6.2 Telecommunication resources

6.2.1 Fraud Information Gathering System (FIGS)

The Home Network-FDS is provided with data on the activities of subscribers in a Visited Network by way of using the Fraud Information Gathering System. The Home Network-FDS can make inferences about what the subscriber is doing and then take decisions on what the subscriber should be allowed to do. The following operations may be invoked in FIGS as described in the use cases:

1) Fraud Alert: The Visited Network invokes this operation when fraud is suspected.
2) Activate Information Gathering: This operation starts up the process of monitoring particular subscriber activities.
3) Report FIGS: This operation is invoked by the Visited Network to relay gathered information.
4) Deactivate Information Gathering: This operation concludes the process of monitoring the subscriber's activities.
5) Modify FIGS Report: This operation alters the monitoring level and/or schedule of delivering subscriber activities.
6) Advice Suspend FIGS Monitoring: This operation is invoked by the Visited Network to inform the Home Network-FDS that information gathering has been suspended.
7) Advise Resume FIGS Monitoring: This operation is invoked by the Visited Network to inform the Home Network-FDS that information gathering has been resumed after it was suspended.

6.2.2 Visited Network

A Visited Network (Visited Service Provider) can receive FIGS monitoring requests. A Visited Network can then perform some of the following actions:

– Activate FIGS monitoring for the requested roaming subscriber. The Home Network-FDS is then notified with reports as a result of the monitoring activities.

– The Visited Network may be overloaded, the request is suspended until monitoring capacity is restored and then FIGS monitoring is activated for the roaming subscriber requested.

6.2.3 Home Network Fraud Detection System (HN-FDS)

The Home Network-FDS requests FIGS monitoring from Visited Networks to start collecting data about particular subscriber activities.

The HN-FDS then schedules receipt of security event reports, as specified in an agreed-upon time interval. Alternatively, the Home Network-FDS requests security event reports at any time from the Visited Network. In either case, security information should be delivered in as close to real time as possible.

6.3 Fraud Information Gathering use cases

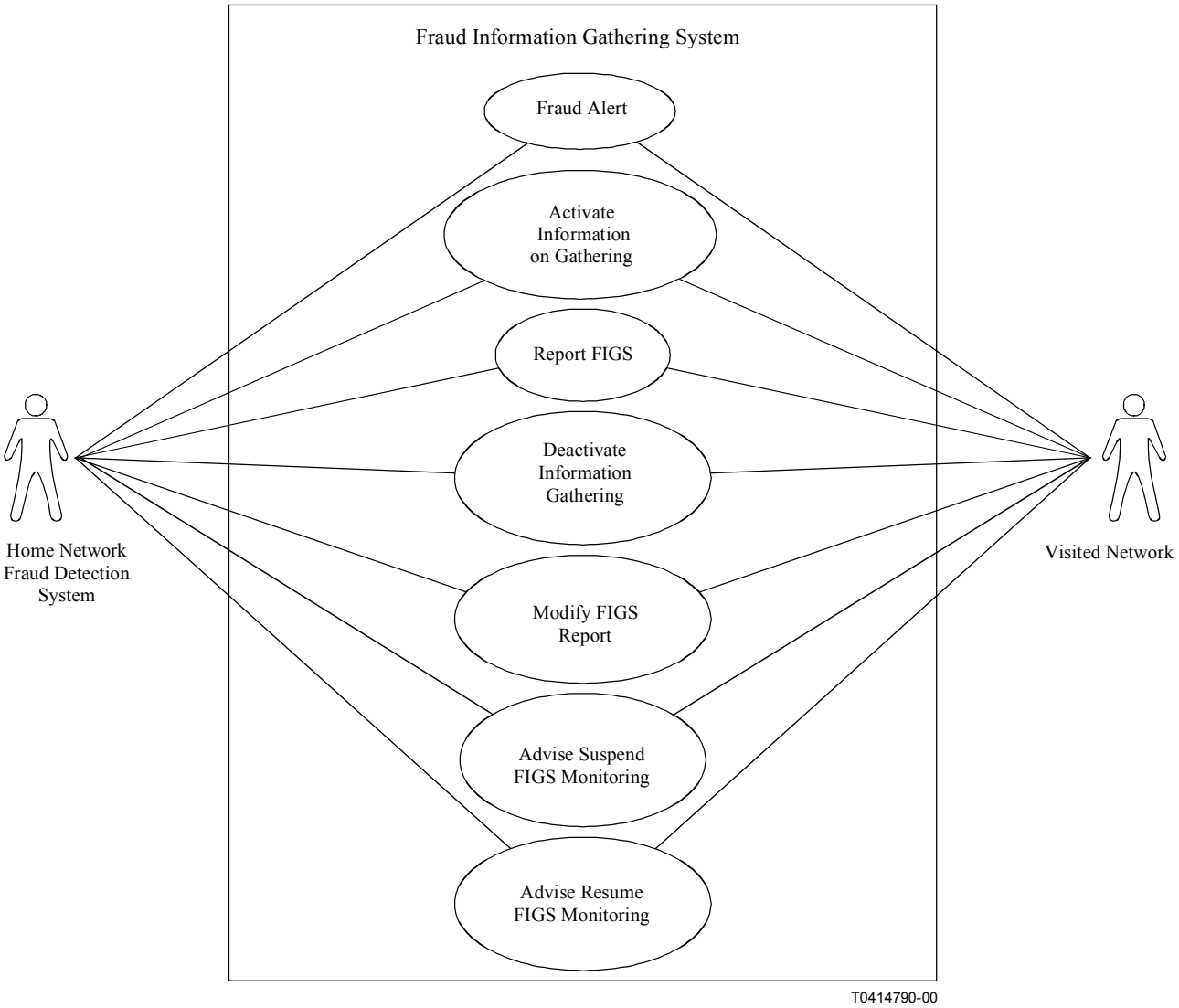

Figure 2/M.3210.1 – FIGS use cases

6.3.1 Fraud Alert use case

Name	Fraud Alert
Summary	This operation is invoked by the Visited Network suspecting fraud to inform Home Network-FDS of need to initiate FIGS monitoring.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	Subscriber fraud suspected.
Begins When	Subscriber roams to Visited Network.
Description	After a particular subscriber roam in a Visited Network, the Visited Network may inform the subscriber Home Network-FDS that it suspects fraudulent use. This alert may be the result of the roaming subscriber following an unusual usage pattern, for example.
Ends When	N/A
Exceptions	N/A
Post-Conditions	FIGS Monitoring requested. Fraud no longer suspected. Subscriber device deactivated.
Traceability	This use case fulfils the following requirements: 1 (Table 1)

6.3.2 Activate Information Gathering use case

Name	Activate Information Gathering
Summary	This operation initiates the request to start up the process of monitoring particular subscriber activities.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	Subscriber fraud suspected.
Begins When	Receive request from either: – Home Network-FDS, or – Visited Network request
Description	The Home Network-FDS may find it necessary to monitor a particular subscriber. This decision may be in response to the Visited Network Fraud Alert message.
Ends When	Home Network-FDS request to terminate subscriber monitoring.
Exceptions	Visited Network is unable to initiate monitoring.
Post-Conditions	Fraud no longer suspected. Subscriber device deactivated.
Traceability	This use case fulfils the following requirements: 1, 8, 9, 10, 12 and 15 (Table 1)

6.3.3 Report FIGS use case

Name	Report FIGS
Summary	This operation is invoked by the Visited Network to relay gathered information to the Home Network-FDS.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	Subscriber fraud suspected.
Begins When	Subscriber roams to Visited Network.
Description	The Visited Network accumulates information about roaming subscriber usage for the Home Network-FDS. This information is only gathered based on the Home Network request to activate the subscriber monitoring. This information is then transmitted to the home network based on the set criteria.
Ends When	When FIGS monitoring is deactivated or FIGS is suspended because of Visited Network overload.
Exceptions	N/A
Post-Conditions	Fraud no longer suspected. Subscriber device deactivated.
Traceability	This use case fulfils the following requirements: 2, 3, 4, 5, 6, 7, 12, 13, 14, 15, 17 and 18 (Table 1)

6.3.4 Deactivate Information Gathering use case

Name	Deactivate Information Gathering
Summary	This operation is invoked by the Home Network-FDS to request terminating the process of monitoring the visiting subscriber's activities.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	Either case is reached: • Subscriber fraud not suspected. • Subscriber finished roaming.
Begins When	Receive request from the Home Network-FDS.
Description	Request is accepted and passed to the Visited Network.
Ends When	N/A
Exceptions	N/A
Post-Conditions	Fraud no longer suspected. Subscriber device deactivated.
Traceability	This use case fulfils the following requirements: 7, and 13 (Table 1)

6.3.5 Modify FIGS Report use case

Name	Modify schedule for delivering Fraud Information
Summary	The Home Network-FDS sends request to the Visited Network asking to modify the frequency of delivering monitoring reports.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	• FIGS monitoring is in progress for a subscriber. • Home FDS requires subscriber activities to be monitored at a different level or on a different schedule than those identified in the roaming agreement.
Begins When	Receive request from the Home Network-FDS.
Description	The Home Network-FDS may find it necessary to change: a) the schedule of delivering the monitoring reports of a particular subscriber; b) the level of fraud monitoring required.
Ends When	Request is accepted and passed to the Visited Network.
Exceptions	Visited System cannot process request.
Post-Conditions	New delivery schedule or monitoring level is established.
Traceability	This use case fulfils the following requirements: 8 and 18 (Table 1)

6.3.6 Advise Suspend FIGS Monitoring use case

Name	Advise Suspend FIGS Monitoring
Summary	This operation is invoked by the Visited Network to inform the Home Network-FDS of suspending the collection of FIGS information because of resource shortage.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	Subscriber fraud suspected and Visited Network resources are short.
Begins When	Visited Network resources cannot meet the demand to monitor existing roaming subscribers.
Description	The Visited Network monitoring resources may suffer from resource shortage. This may be the result of increased activities of a large number of roamers being monitored, for example. Consequently, a message is sent to some of the subscribers' Home Network informing them that monitoring is being suspended.
Ends When	Visited Network normal condition is restored and a message advising the Home Network of resuming the monitoring gets sent.
Exceptions	N/A
Post-Conditions	Fraud no longer suspected. Subscriber device deactivated.
Traceability	This use case fulfils the following requirements: 10, 15 and 16 (Table 1)

6.3.7 Advise Resume FIGS Monitoring use case

Name	Advise Resume FIGS Monitoring
Summary	This operation is invoked by the Visited Network to inform the Home Network-FDS of the resumption of collecting FIGS information.
Actor(s)	1) Home Network-FDS 2) Visited Network
Pre-Conditions	Subscriber Fraud suspected.
Begins When	Subscriber roams to Visited Network.
Description	Visited Network resources are restored and can resume monitoring existing tagged roaming subscribers.
Ends When	Subscriber monitoring is ended or Visited Network FIGS System overload reoccurs.
Exceptions	N/A
Post-Conditions	Fraud no longer suspected. Subscriber device deactivated.
Traceability	This use case fulfils the following requirements: 10, 15 and 16 (Table 1)

7 Management Functions analysis

This clause provides the high-level description for the FIGS Security Management service. That is, it provides the messages needed to support the management functions for requesting and collecting security-related information between service providers.

7.1 Fraud Information Gathering Function set

FIGS Function set supports a service provider request and reporting of usage data from other service provider. Table 2 lists FIGS functions to illustrate the management activity originator and recipient.

Table 2/M.3210.1 – FIGS function sets interactions

	Function	Originator	Responder
1	Fraud Alert function	Visited Network	Home Network-FDS
2	Activate Information Gathering function	Home Network-FDS	Visited Network
3	Report FIGS function	Visited Network	Home Network-FDS
4	Deactivate Information Gathering function	Home Network-FDS	Visited Network
5	Modify FIGS reporting schedule function	Home Network-FDS	Visited Network
6	Advise Suspend FIGS Monitoring function	Visited Network	Home Network-FDS
7	Advise Resume FIGS Monitoring function	Visited Network	Home Network-FDS

7.2 Object Classes and State Chart

The state machine describing FIGS related interaction is illustrated in the diagram in Figure 3. As messages are exchanged between the Visited Network and the Home Fraud Detection System, the message link between them may be situated in one of the states listed (see Figure 4).

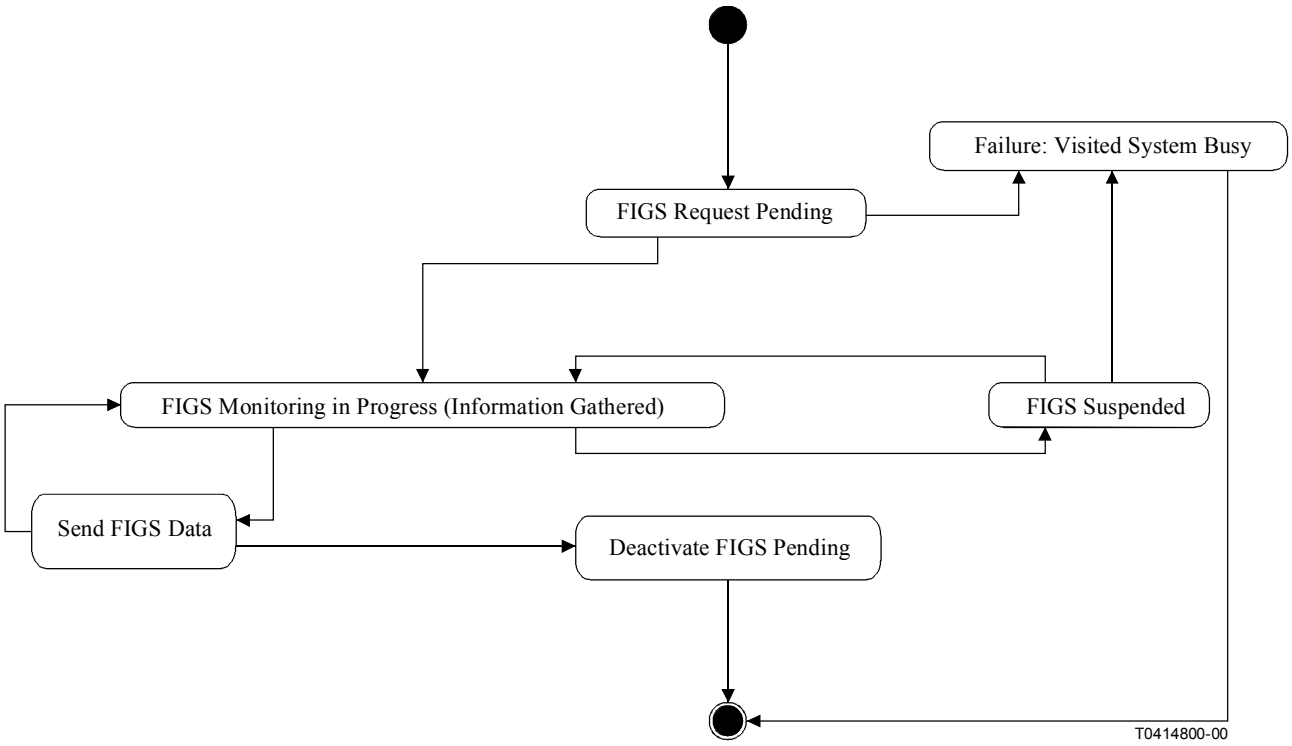

Figure 3/M.3210.1 – FIGS state diagram

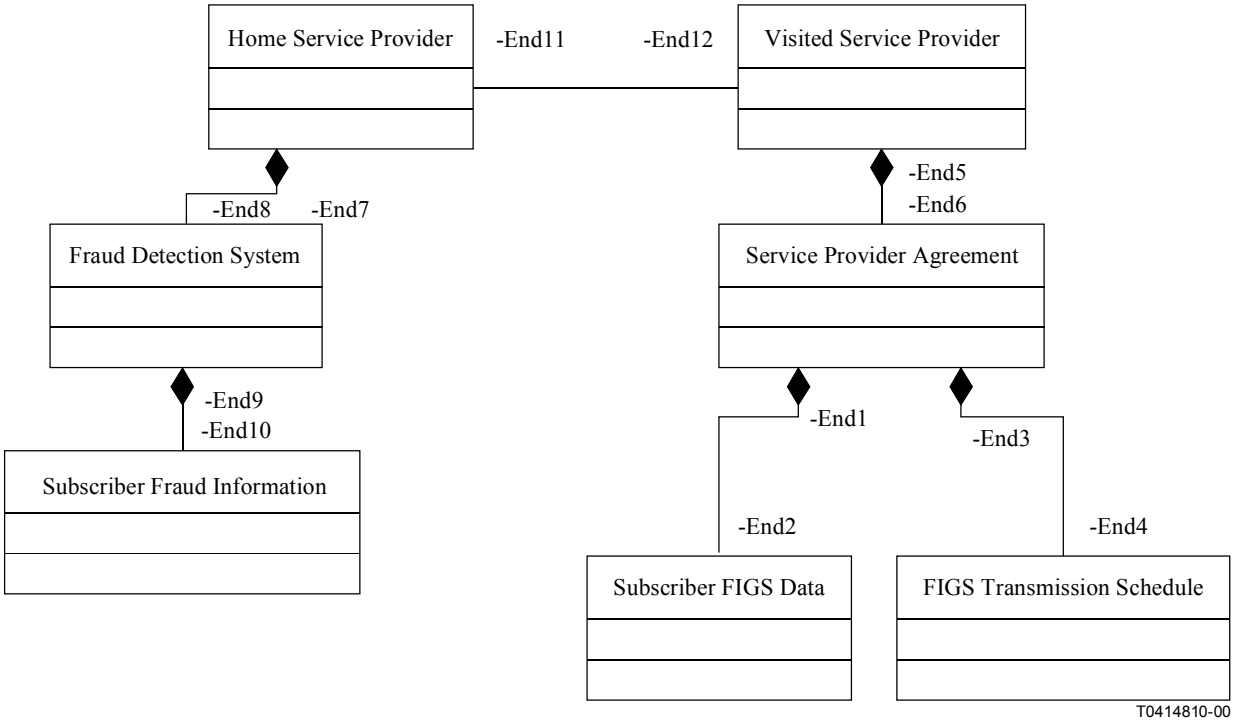

Figure 4/M.3210.1 – FIGS class diagram

7.3 Fraud Information Gathering functions and sequence diagrams

7.3.1 Fraud Alert function

After a particular subscriber roam in a Visited Network, the Visited Network may inform the subscriber Home Network-FDS that it suspects fraudulent use. This alert may be the result of the roaming subscriber following an unusual usage pattern, for example, as in Figure 5:

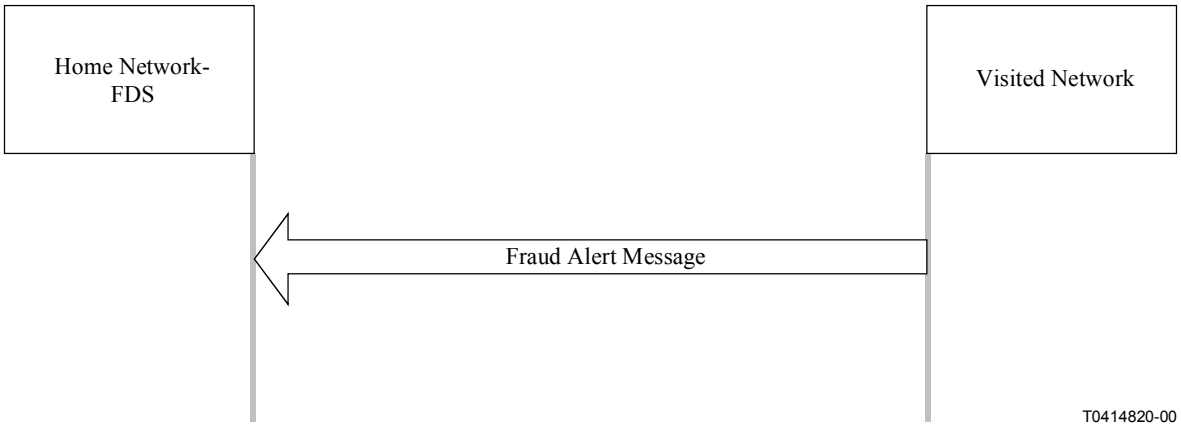

Figure 5/M.3210.1 – Alert Message flow

Consequently, the Home Network-FDS is informed. In the scenario shown in Figure 5, the Visited Network informs the Visited Network of a particular roaming subscriber.

7.3.1.1 Information flow

The information exchanged for Fraud Alert is detailed in Table 3.

Table 3/M.3210.1 – Fraud Alert exchanged information

	Home Network-FDS	Visited Network	Notes
3G User Identification List		m	List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number).
Electronic Serial Number		m	The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.

7.3.2 Activate Information Gathering function

The Home Network-FDS may find it necessary to monitor a particular subscriber. This decision may be in response to the Visited Network Fraud Alert message for example. In this scenario, the Home Network-FDS requests from the Visited Network to monitor a particular roaming subscriber. The Visited Network is required to acknowledge the receipt of this request.

The request to activate information gathering is only initiated by the Home Network-FDS and transmitted to the Visited Network as shown in Figure 6.

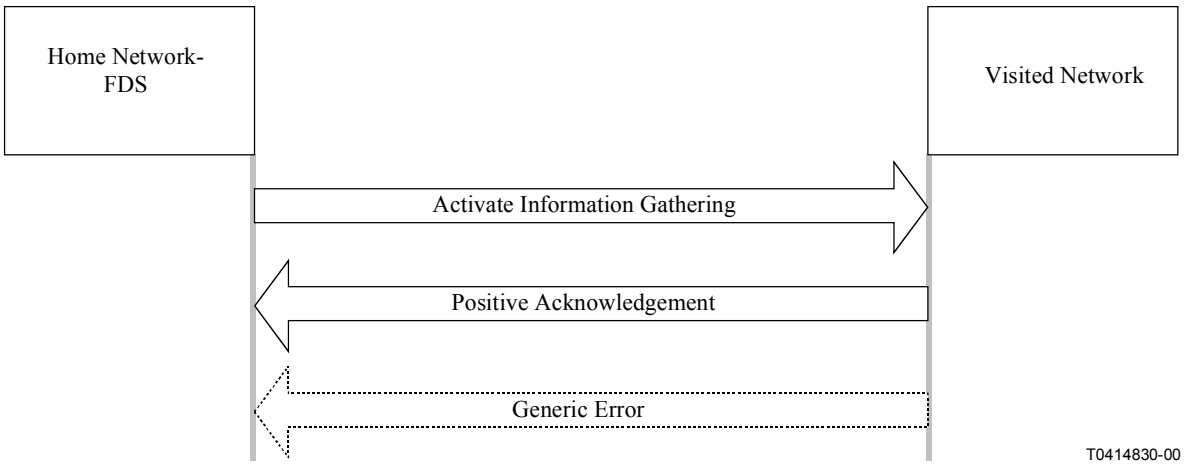

Figure 6/M.3210.1 – Message flow to activate FIGS

7.3.2.1 Information flow

The information exchanged for Activate FIGS is detailed in Table 4.

Table 4/M.3210.1 – Activate FIGS exchanged information

	Home Network-FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number).
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Activate FIGS reason	c		Reason Code: – Fraud is suspected; – Other.
Level of Monitoring Required	m		Level of Monitoring: Level 1 – (near) real time billing; Level 2 – partial call records; Level 3 – full call records.
Confirmation		m	Result code: R0: other; R1: success; R2: unknown subscriber(s).

7.3.3 Report FIGS function

The Visited Network accumulates information about roaming subscriber usage for the Home Network-FDS. This information is only gathered based on the Home Network request to activate the subscriber monitoring.

In this scenario, shown in Figure 7, the Visited Network sends the Home Network-FDS particular roaming subscriber information periodically.

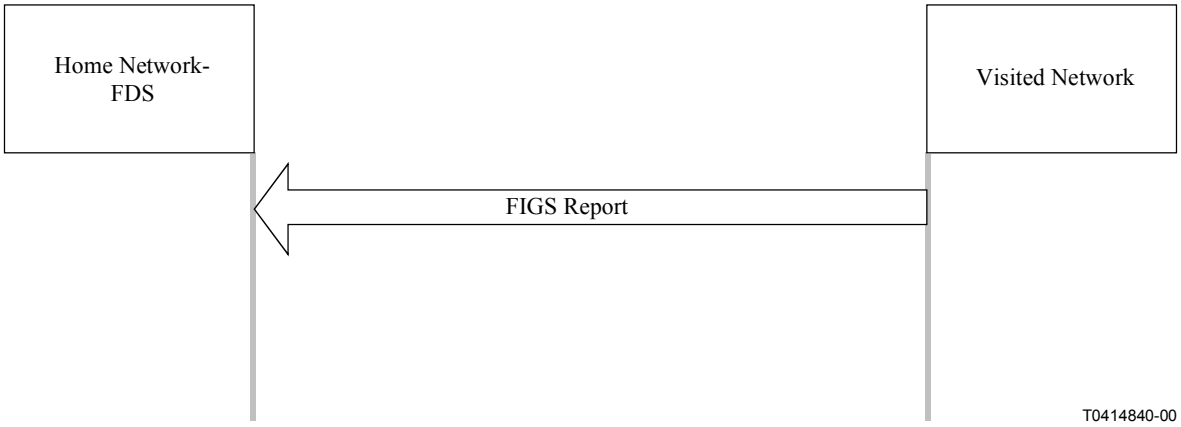

Figure 7/M.3210.1 – Message flow to send information

7.3.3.1 Information flow

The Report FIGS information is detailed in Table 5.

Table 5/M.3210.1 – Report FIGS information

	Home Network-FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
FIGS Report	c		Reason code: – Fraud is suspected; – Other.
Confirmation		m	Result code: R0: other; R1: success; R2: unknown subscriber(s).

7.3.4 Deactivate Information Gathering function

The Home Network-FDS may find it necessary to terminate monitoring a particular subscriber. This decision may be a result of determining that a subscriber usage pattern is verified to be ordinary. In this scenario, the Home Network-FDS requests from the Visited Network to terminate the monitoring of a particular roaming subscriber. The Visited Network is required to acknowledge the receipt of this request and to terminate the monitoring.

The request to deactivate information gathering is only initiated by the Home Network-FDS and transmitted to the Visited Network as shown in Figure 8.

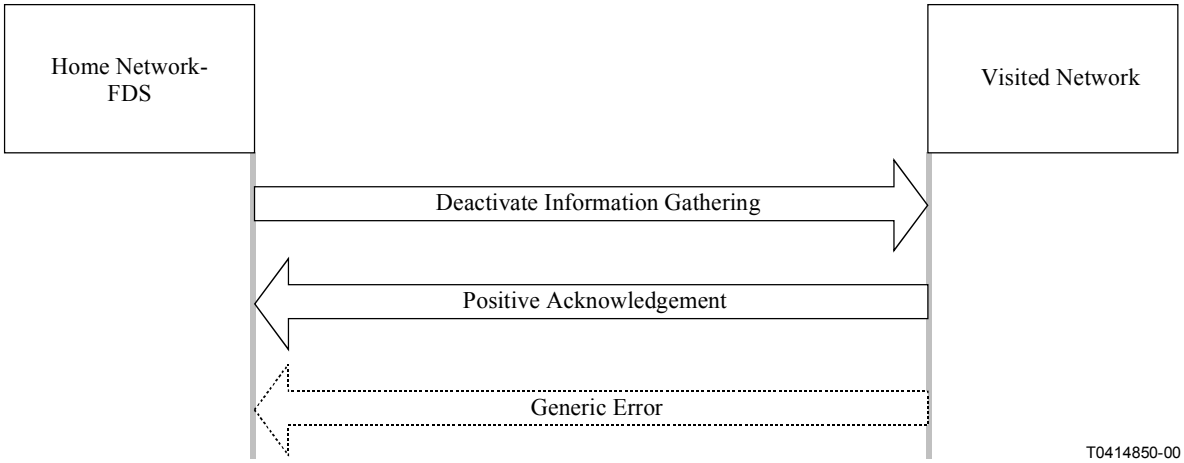

Figure 8/M.3210.1 – Message flow to deactivate FIGS

7.3.4.1 Information flow

The Deactivate FIGS information exchanged is detailed in Table 6.

Table 6/M.3210.1 – Deactivate FIGS exchanged information

	Home Network-FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number).
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Deactivate FIGS reason	c		Reason code: – Fraud is detected – Subscriber suspended. – No Fraud is concluded.
Confirmation		m	Result code: R0: other; R1: success; R2: unknown subscriber(s).

7.3.5 Modify FIGS Report function

The Home Network-FDS may find it necessary to change the schedule of delivering the monitoring reports of a particular subscriber. This decision may be a result of overload condition.

In this scenario, shown in Figure 9, the Home Network-FDS requests from the Visited Network to change the reporting schedule. The Visited Network is required to acknowledge the receipt of this request and to alter the reporting schedule.

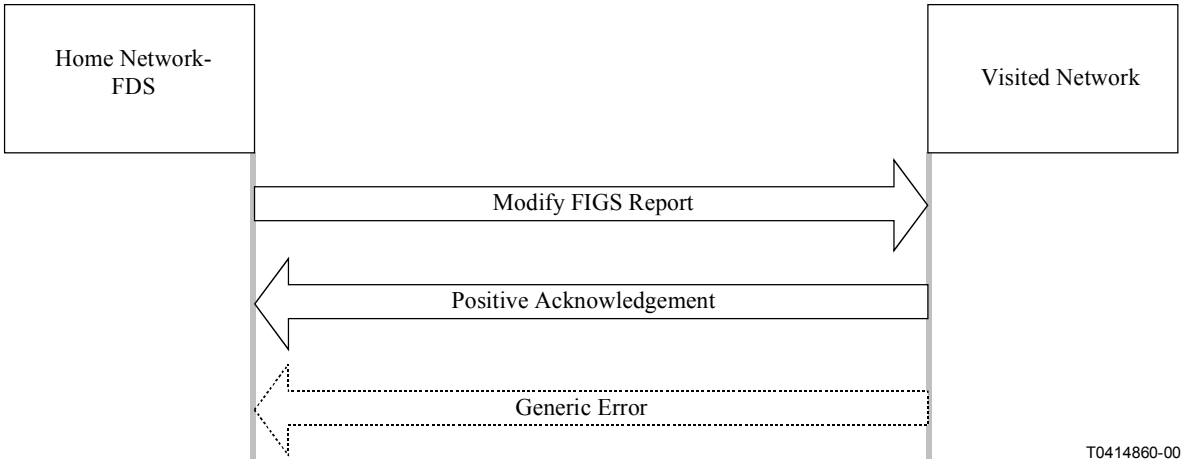

Figure 9/M.3210.1 – Message flow to change reporting schedule

7.3.5.1 Information flow

The Modify FIGS Reporting exchanged information is detailed in Table 7.

Table 7/M.3210.1 – Modify FIGS Reporting exchanged information

	Home Network FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards
New Schedule	c		If the modification request is for a change of schedule, this element is mandatory Choice of: – Time Interval; – Absolute times.
New Monitoring Level	c		If the modification request is for a change of monitoring level, this element is mandatory. Choice of: – Level 1; – Level 2; – Level 3.
Confirmation		m	Result code: R0: other; R1: success; R2: unknown subscriber(s).

7.3.6 Advise Suspend FIGS Monitoring function

The Visited Network monitoring resources may suffer from shortage. This may result in the increased activities of a large number of roamers being monitored, for example, as in Figure 10:

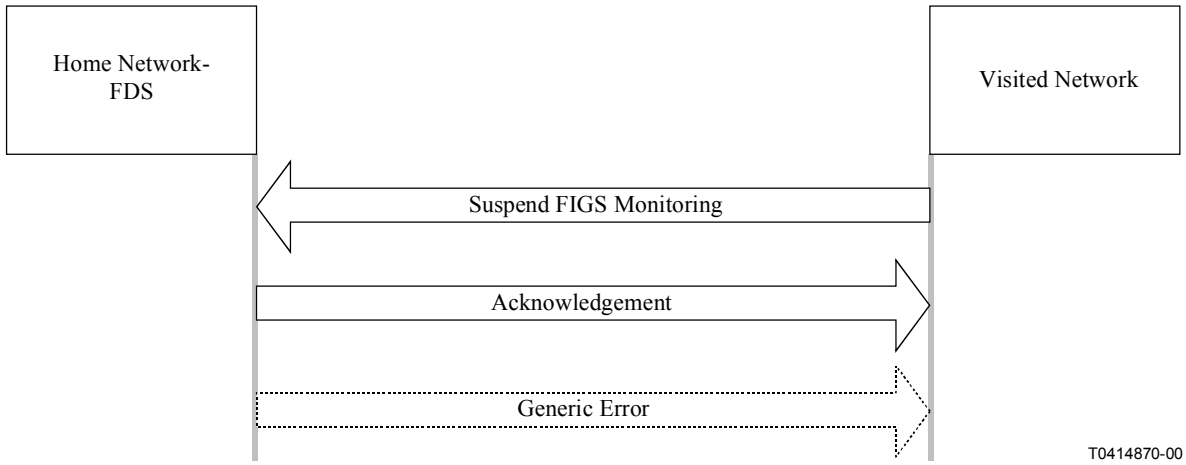

Figure 10/M.3210.1 – Message flow to suspend FIGS

Consequently, as shown in Figure 10, selected subscribers' monitoring may be suspended and the Home Network-FDS is informed. In this scenario, the Home Network-FDS informs the Visited Network of its decision to suspend the monitoring of particular roaming subscriber information.

7.3.6.1 Information flow

The information exchanged between the Home Network-FDS and the Visited Network to suspend the monitoring of a roaming subscriber is detailed in Table 8.

Table 8/M.3210.1 – Advise Suspend FIGS exchanged information

	Home Network FDS	Visited Network	Notes
3G User Identification List	m	m=	List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number).
Electronic Serial Number	m	m=	The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Suspend service code	m		Reason code: – System Problems; – Other.
Confirmation		m	Confirmation code: R0: other; R1: success; R2: unknown subscriber.

7.3.7 Advise Resume FIGS Monitoring function

When the Visited Network monitoring resources are restored after shortage, monitoring of suspended roaming subscribers is resumed. The Home Network-FDS is informed.

In this scenario, as shown in Figure 11, the Visited Network informs the Home Network-FDS of its decision to resume monitoring of the previously suspended roaming subscriber.

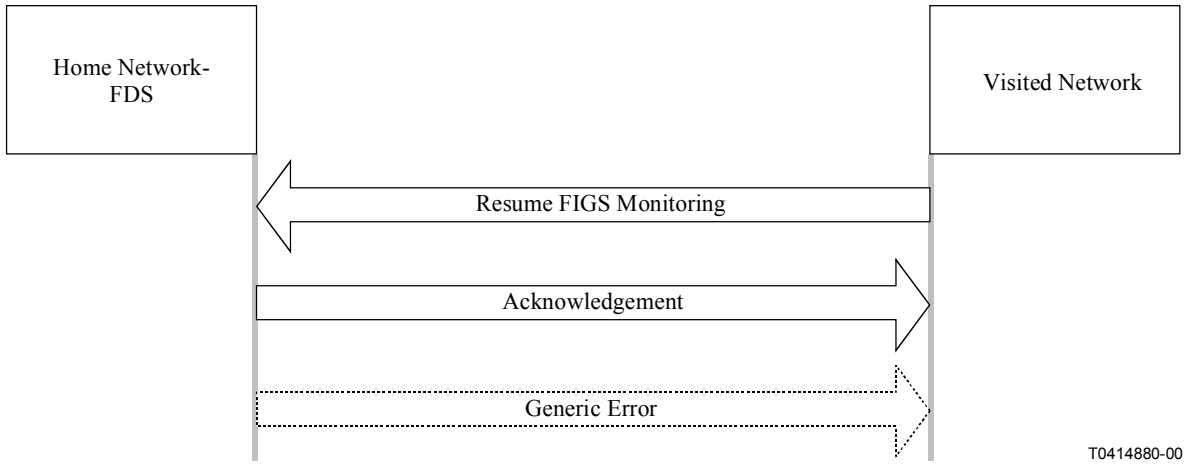

Figure 11/M.3210.1 – Message flow to resume FIGS

7.3.7.1 Information flow

The Advise Resume FIGS exchanged information is detailed in Table 9.

Table 9/M.3210.1 – Advise Resume FIGS exchanged information

	Home Network FDS	Visited Network	Notes
3G User Identification List	m	m=	List of unique identification of the wireless subscriber, e.g. (International Mobile Subscriber Identity (IMSI) or Universal Personal Telecommunications Number).
Electronic Serial Number	m	m=	The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Resume service code	m		Reason code: – System restored; – Other.
Confirmation		m	Confirmation code: R0: other; R1: success; R2: unknown subscriber.

ANNEX A

Fraud Management criteria

Telecommunications Management Networks need to provide the management means to detect and analyse security violations and include security aspects that evolve from the mobility of customers. Examples of detecting fraudulent use may be the result of:

- analysis of collected subscriber information on a customer suspected of security violations such as simple MIN/ESN cloning;
- analysis of collected network information on the network to detect a suspected security violation;
- customer usage pattern analysis indicating a significant variation from normal usage patterns;
- internal traffic and activity pattern analysis that results in the detection of a customer or user (external or internal) security violation.

Fraudulent use may or may not be a consequence of the following detected failures:

- network failure to decrypt customer-encrypted messages;
- customer failure to produce correct responses to authentication challenges;
- mismatches in the customer-reported value of the "call-count" parameter;
- failure reports indicating difficulty in updating users, Shared Secret Data (SSD).

ANNEX B

Information transferred by the Visited Network

Information	Description
Dialled digits	The **Dialled digits** are required as these are an important indicator in deciding if a call is fraudulent or not – certain call destinations are more likely to be called fraudulently than others.
A subscriber	**A subscriber** can be used to identify the subscriber.
B, C subscriber	**B, C subscribers** are relevant as some call destinations are more subject to fraud than others.
CGI	**Cell Global Identifier (CGI)** is relevant as some cells in a PLMN are more subject to fraud than others.
IMSI	The **IMSI** is used to reference the subscriber.
IMEI	The **IMEI** can be used to check if a stolen handset has been used.
Call Start Time/Date	The **Call Start Time/Date** is required so that the call duration can be calculated (if the call end time and not call duration is given at call conclusion) and because the call start time can also be an important indicator of fraudulency.
Call Duration	The **Call Duration** gives the duration of the call at the sending of the partial call information – call duration can be an important indicator of fraudulency. If call end is sent instead, the duration can be calculated using the call start and end times.
Call Reference	The **Call Reference** is used to reference a particular call.
MO/MT indicator	The **MO/MT indicator** is required because call charging is different for MO and MT calls.
Visited MSC address	The **Visited MSC address** gives the PLMN on which the call was made.
Type of SS event	The **Type of SS event** record is sent if the "call" start is actually the invocation of a supplementary service, e.g. ECT. The **Type of SS event** is required as this can help to indicate if the mobile is being fraudulently used or not.
Type of Basic Service	The **Type of Basic Service** indicates whether a teleservice or bearer service is being used and which sort of teleservice or bearer service is being used and is sent if the event is a call and not a supplementary service. The **Type of Basic Service** is required as this can help to indicate if the mobile station is being fraudulently used or not.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2001