3GPP TSG SA WG3 Security — S3#15 **S3-000581**

12-14 September, 2000

Washington DC

3GPP TSG SA WG3 Security — S3#14 **S3-000437**

2-4 August, 2000

Oslo, Norway

ITU-Telecommunication Standardization Sector
WORKING PARTY ¾

Geneva, 24 January – 2 February 2000

QUESTIONS:	Q24/4
SOURCE:	Studygroup 4
	LIASON TO ITU-T SG7 (lead Studygroup for Security), WP3/11(lead for IMT-2000), ETSI,FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, AND TR45-AHG ON IMT2000 SECURITY MANAGEMENT

APPROVAL:	Not yet Approved by Working Party 5/4
FOR:	Information and Response
DEADLINE for REPLY:	2 October 2000
CONTACT:	G. Caryer BT The Chestnuts Rose Hill Grundisburgh Suffolk IP13 6TD, UK Tel: +44 1473 738108 Fax: +44 1473 227884 Email: geoff.caryer@btinternet.com

---

ITU-T Study Group 4 is currently developing a series of Recommendations for the X interface between IMT2000 operators belonging to different 3rd generation families. We are also considering a broader work programme for the future, on the application of TMN to 3rd generation mobile systems.

We attach a new draft recommendations which address the requirements and analysis (Stage 1 and Stage 2) for the management information to be exchanged between Visited and Home Service Providers for the management of the prevention of fraud.

Q24/4 are seeking comments from ITU-T SG7, as the lead Studygroup for Security, and comments and the support and of the 3rd generation families for the proposed approach.

We would appreciate your comments for discussion at our next Q24/4 experts meeting which will be held during October/November 2000

(Attach Draft Recommendations M.3210.imtsec)

Contact: Dia Helmy Tel: +1 972 751 7210
NEC America, Inc. email: helmyd@rss.dl.nec.com

ITU - Telecommunication Standardization Sector DAL02 r1

Dallas 26th – 30th June 2000

Question(s): Q24/4 (JQG6)

SOURCE*: EDITOR OF M.3210.imtsec
TITLE: DRAFT NEW REC. M.3210.IMTSEC – TMN MANAGEMENT SERVICE FOR IMT2000: SECURITY MANAGEMENT; FRAUD INFORMATION GATHERING

EDITOR'S NOTES:
1- This draft is the result of editing decisions made during the JQG6 interim meeting held in Dallas, US during June26, 2000.

2- Add FIGS monitoring levels
3- Add FIGS TAP (Accelerated – Hot Billing) records

TABLE OF CONTENTS

3GPP TSG SA WG3 Security — S3#15 **S3-000581**

12-14 September, 2000

Washington DC

DRAFT NEW RECOMMENDATION M.3210.imtsec

TMN MANAGEMENT SERVICES FOR IMT2000 SECURITY MANAGEMENT

Abstract

This recommendation is one of the series of M.3200 TMN Management Service recommendations that provide description of management services, goals and context for management aspects of IMT2000 networks. This recommendation provides a profile for fraud management in a IMT2000 mobile network. This is done by existing and defining new function sets, functions and parameters and adding additional semantics and restrictions.

Keywords

- Telecommunications Management Network (TMN)
- TMN Management Service
- International Mobile Telecommunications (IMT) 2000
- Security Management
- Fraud Detection and Containment

Contact: Dia Helmy Tel: +1 972 751 7210

NEC America, Inc. email: helmyd@rss.dl.nec.com

1 Introduction

1.1 Recommendation M.3210.imtsec provides Requirements and Analysis of the Security management (Administration) of IMT2000. 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 document is based on ITU-T Recommendation M.3020.Scope

This recommendation describes a subset of Security Management services, identified in Recommendation M.3200 as a TMN managed area, for IMT2000 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 Service Provider and the Visited Service Provider is beyond the scope of this management service.

1.2 Related Recommendations

1. ITU-T Recommendation Q.1701 “Framework of IMT2000 Networks”
2. ITU-T Recommendation Q.1711 “Network Functional Model for IMT2000 ”
3. ITU-T Recommendation Q.1721 “Information Flows for IMT-2000”
4. ITU-T Recommendation M.3010 “Principles for a Telecommunications Management Network”
5. ITU-T Recommendation M.3020 “TMN Interface Specification Methodology”
6. ITU-T Recommendation M.3200 “TMN Management Services”
7. ITU-T Recommendation M.3400 “TMN Management Functions”

1.3 Abbreviations

GDMI	Guidelines for the Definition of TMN Management Interface
IMT2000	International Mobile Telecommunications 2000
ITU	International Telecommunications Union
MS	Management Services
NML	Network Management Layer
SML	Service Management Layer
TMN	Telecommunications Management Network

1.4 Definitions

The following terms are used in this Recommendation:

Visited Service Provider (VSP)	The service provider of the foreign or visited network in providing global roaming.
Home Service Provider (HSP)	The service provider of the home network to which the wireless subscriber subscribes contracts service.
Service Provider (SP)	A general reference to an entity who provides telecommunications services to Customers and other users either on a tariff or contract basis. A SP may or may not operate a network.
Network Operator	An organisation that operates a telecommunications network. A network operator may be a Service Provider and vice versa. A network operator may or may not provide particular telecommunications services
Subscriber Profile	A subscriber profile is the set of characteristics that describe a particular subscriber's usage patterns. This may include limits on usage patterns like duration, cost etc.
Security Event Report	A security event 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 .)

1.5 Conventions Used in this Document

Symbol	Explanation
m	Mandatory
m (=)	The recipient must provide the same value in the response asprovided 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.

1.6 Security Management Service

1.6.1 Security Issues

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 (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 effect 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 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.

1.6.2 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 service provider and the home service provider.)

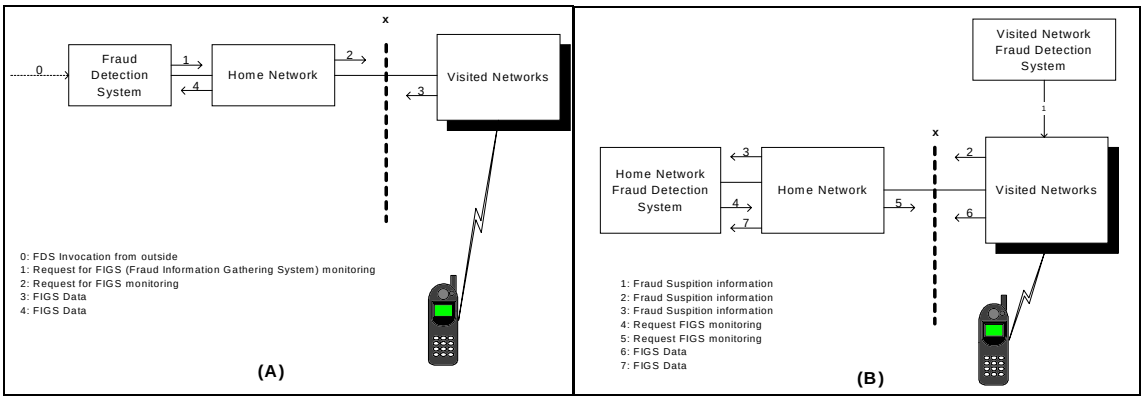

Figure 1**: IMT2000 Security Management Service: Fraud Information Gathering collaboration diagrams.**

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.
In Figure 1-A, The home network 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 de-registration from the visited network. The information received by the home network shall be passed to the home network fraud detection system. 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.

2 Management High Level Requirements

The home service provider or the visited service provider can take preventive actions to control and prevent fraudulent activities, according to the security policies. The security management services described here are applicable, across different service providers operating different or similar wireless networks. This management service provides the Visited Service Provider and the Home Service Provider with the capability to exchange and to control the exchange of information related to potential fraudulent activities in the visited network.

In most cases, the visited service provider obtains requests from the home service provider for monitoring suspicious subscriber activities. In some cases, it is conceivable that the Home Service Provider receives unsolicited subscriber alerts from the Visited Service Provider, especially if the roaming subscriber continues to obtain service from the visited service provider for extended periods of time.

The following minimum capabilities are required:

1. Fraud information gathering is controlled by the home network and can be activated and deactivated by the home network only.

2. This network 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.

3. The Home network shall be able to specify whether it would like call information on Mobile Originated sessions, Mobile Terminated sessions, or both.

4. The following service conditions shall apply:

   - FIGS should not modify the Visited network service,

   - FIGS should not alter any standard 3G Wireless functionality seen by the customer or affect the service quality;

   - If the Visited network does not have the resources to support a FIGS request, it should respond accordingly to the Home network.

5. Information should be transferred from the Visited network to the Home network 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; the sooner fraud can be stopped.

6. The information should be transferred from the Visited to the Home network over existing communication links (e.g., TMN X Interface, SS7 signaling links).

7. FIGS system 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 be able to support the associated data transfer. The setting of this limit is outside the scope of this recommendation.

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

9. A mechanism should be required whereby a Visited network can charge an Home network for the bulk data transfer made to that Home network.

Within the Home Network:

10. to mark a subscriber as being under FIGS monitoring,

11. to receive from the Visited Network FIGS Data,

12. to cease monitoring of a subscriber's activities,

Within the Visited Network:

13. based on roaming agreements, to transmit FIGS Data to the Home network based on:

    - Frequency requested by Home network,

    - Events specified by Home network, and/or

    - On demand.

14. based on roaming agreements, to advise the Home network of information that suggests fraudulent activities.

2.1 Telecommunications Resources

2.1.1 Fraud Information Gathering System

The Home network Fraud detection system is provided with data on the activities of subscribers in a Visited network by the way of using the Fraud Information Gathering System. 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. Two operations maybe invoked in the FIGS:

1. Activate information gathering: This operation starts up the process of monitoring a particular subscriber activities,
2. Deactivate information gathering: This operation concludes the process of monitoring the subscriber's activities,
3. Modify reporting schedule: This operation alters the schedule of delivering subscriber activities,

2.2 Fraud Information Gathering Use Cases

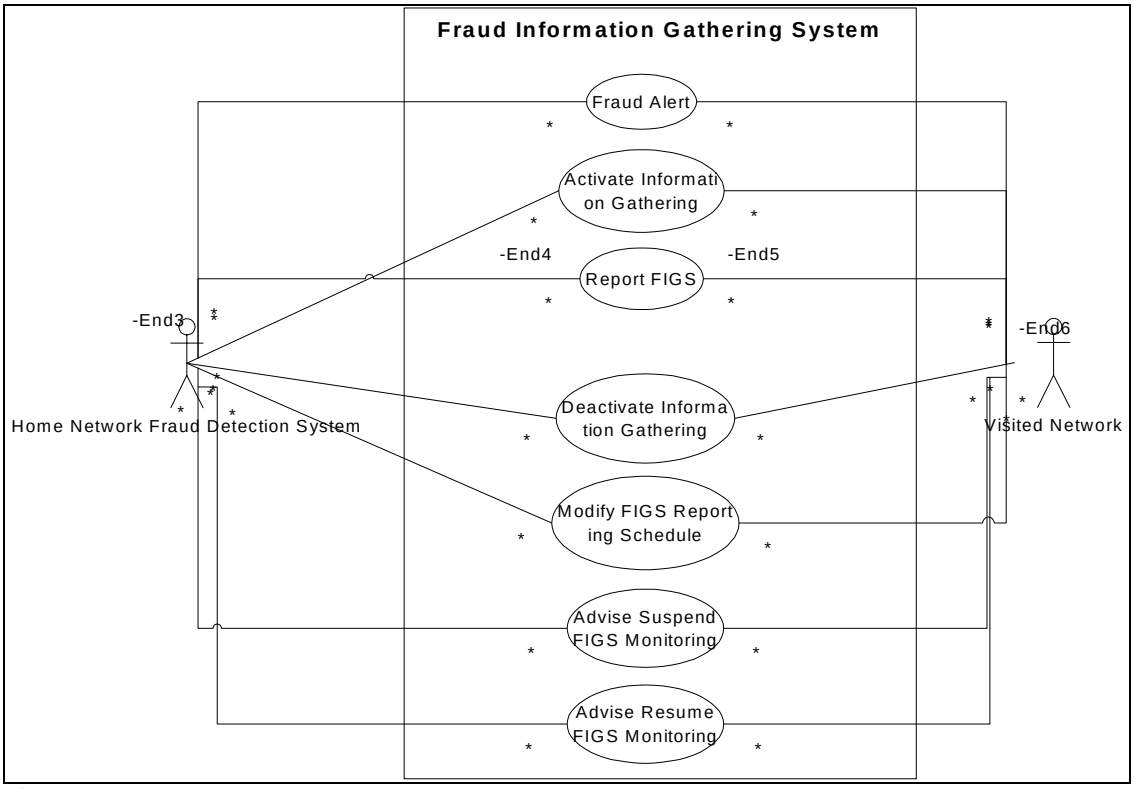

Figure 2: FIGS Use cases

2.2.1 Activate Fraud Information Gathering Use Case

Name	Activate Fraud Information Gathering
Summary	
Actor(s)	1. Home Network Fraud Detection System 2. Visited Network
Pre-Conditions	Subscriber Fraud suspected
Begins When	Receive request from either: • Home network Fraud detection system • Visited Network request
Description	Request is accepted and passed to the Visited service provider
Ends When	Home network Fraud detection system 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 fulfills the following requirements: 1, 2, 3, 4, 7, 8 and 14

2.2.2 Deactivate Fraud Information Gathering Use Case

Name	Deactivate Fraud Information Gathering
Summary	
Actor(s)	3. Home Network Fraud Detection System

	4. Visited Network
Pre-Conditions	Either case is reached: • Subscriber Fraud not suspected • Subscriber finished roaming
Begins When	Receive request from the Home network Fraud detection system
Description	Request is accepted and passed to the Visited service provider
Ends When	
Exceptions	
Post-Conditions	Fraud no longer suspected Subscriber device deactivated
Traceability	This use case fulfills the following requirements: 1, 4, 7, 8, 10 and 12

2.2.3 Modify schedule for delivering Fraud Information Use Case

Name	Modify schedule for delivering Fraud Information
Summary	
Actor(s)	5. Home Network Fraud Detection System 6. Visited Network
Pre-Conditions	• FIGS monitoring is in progress for a Subscriber • Home FDS requires subscriber activities on a different schedule than identified in the roaming agreement.
Begins When	Receive request from the Home network Fraud detection system
Description	Request is accepted and passed to the Visited service provider
Ends When	
Exceptions	Visited System cannot process request
Post-Conditions	New delivery schedule is established
Traceability	This use case fulfills the following requirements: 1, 2, 4, 5, 6, 10 and 13

2.2.4 Visited Service Provider (VSP)

A Visited Service Provider (Visited Service Provider) can receive detection requests. A VSP can then perform some of the following actions:

- Inquire about HSP's needed measurements. The Home Service Provider is then notified of security events as a result of the measurements activities.

- The VSP may also send security event reports of visiting subscribers to the home network at the discretion of the visited service provider and/or what is negotiated in the roaming agreement.

2.2.5 Home Network Fraud Detection System

The Home network Fraud detection system invokes FIGS to request the Visited network to start collecting data about subscriber activities.

identifies needed subscriber measurements to the Visited Service Provider for the initiating fraud management procedures. The Home Service provider then schedules receipt of security event reports, as specified in an agreed upon time interval. Alternativley, the Home Service Provider requests security event reports at any time from the Visited Service Provider. In either case, security information should be delivered in as close to real time as possible.

2.3 Management Service Overview

Security Management includes the following function set groups according to M.3400

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

Among the function set groups of 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:

1. Determination of security related events,
2. Recording of security related events
3. Reporting of security related events.

Several sources of detecting security violations in a wireless network exist. The processes in place in home service provider and the visited service provider 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 & date stamp, Deviation usage data, Usage data records, Alarm event reports, Subscriber Information.

3 Management Functions Analysis

This section 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.

3.1 Fraud Information Gathering function set

3.1.1.1 Summary

This set supports the request and reporting of usage data from other service provider
This function set consists of the following functions with the originator and recipient as follows:

1.	Fraud Alert function	Visited Service Provider	Home Service Provider
2.	Activate Information Gathering function	Home Service Provider	Visited Service Provider
3.	Modify FIGS reporting schedule function	Home Service Provider	Visited Service Provider
4.	Report FIGS function	Visited Service Provider	Home Service Provider
5.	Advise Suspend FIGS Monitoring function	Visited Service Provider	Home Service Provider
6.	Advise Resume FIGS Monitoring	Visited Service Provider	Home Service Provider
7.	Deactivate Information Gathering function	Home Service Provider	Visited Service Provider

3.2 Object Classes and State Chart

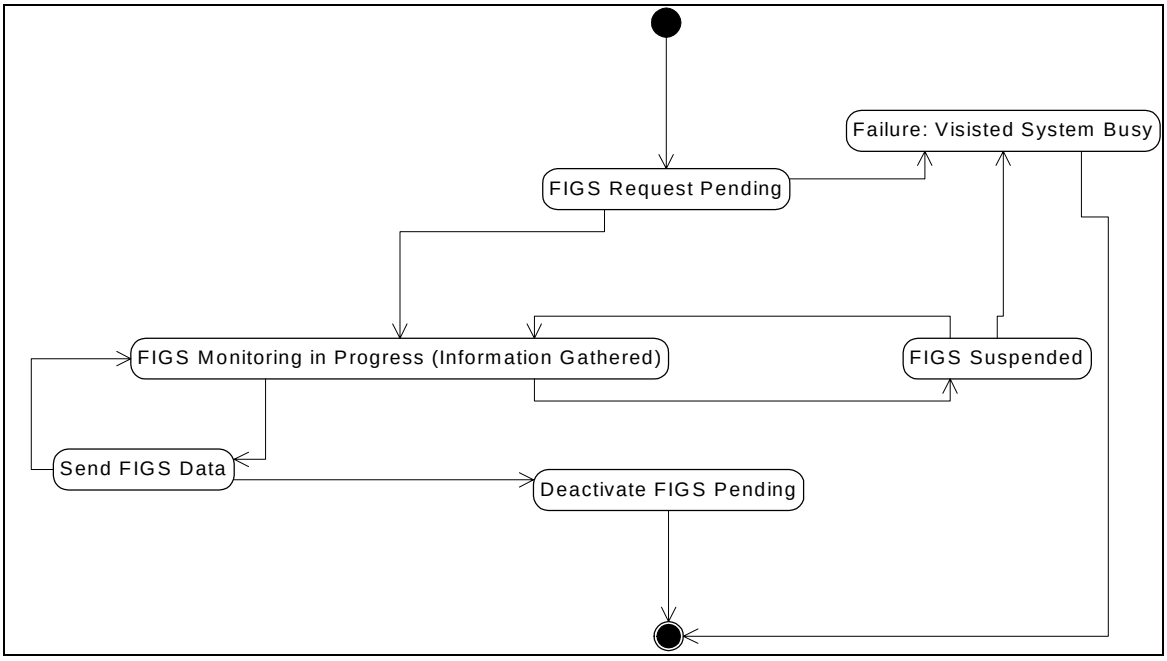

Figure 3: FIGS State Diagram

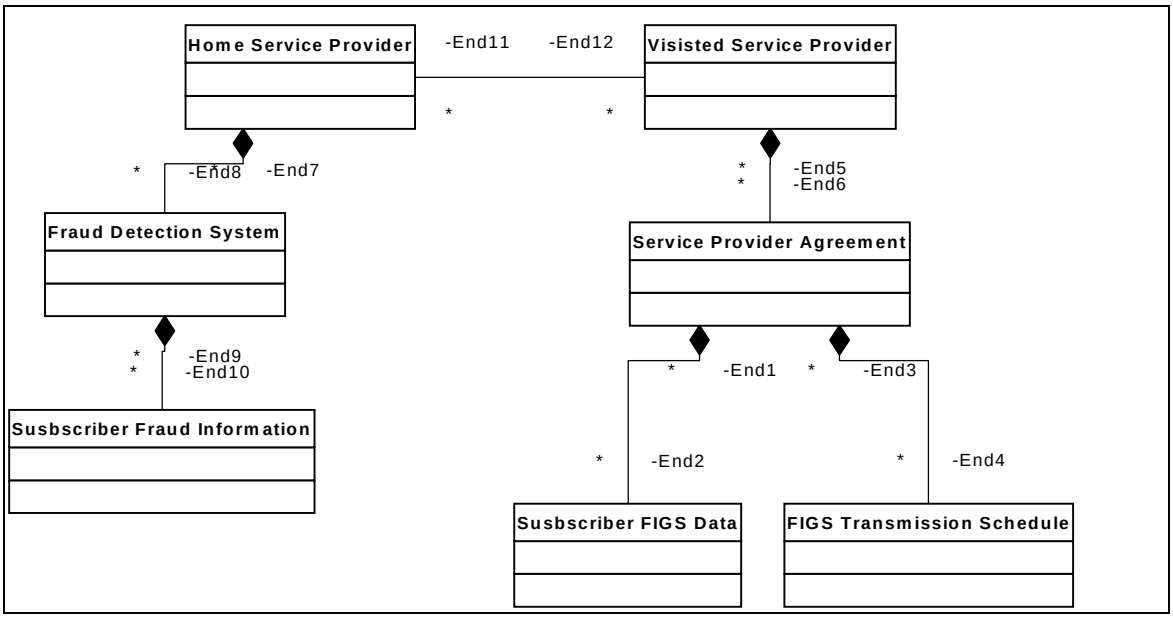

Figure 4: FIGS Class Diagram

3.2.1.1 Activate Information Gathering Function

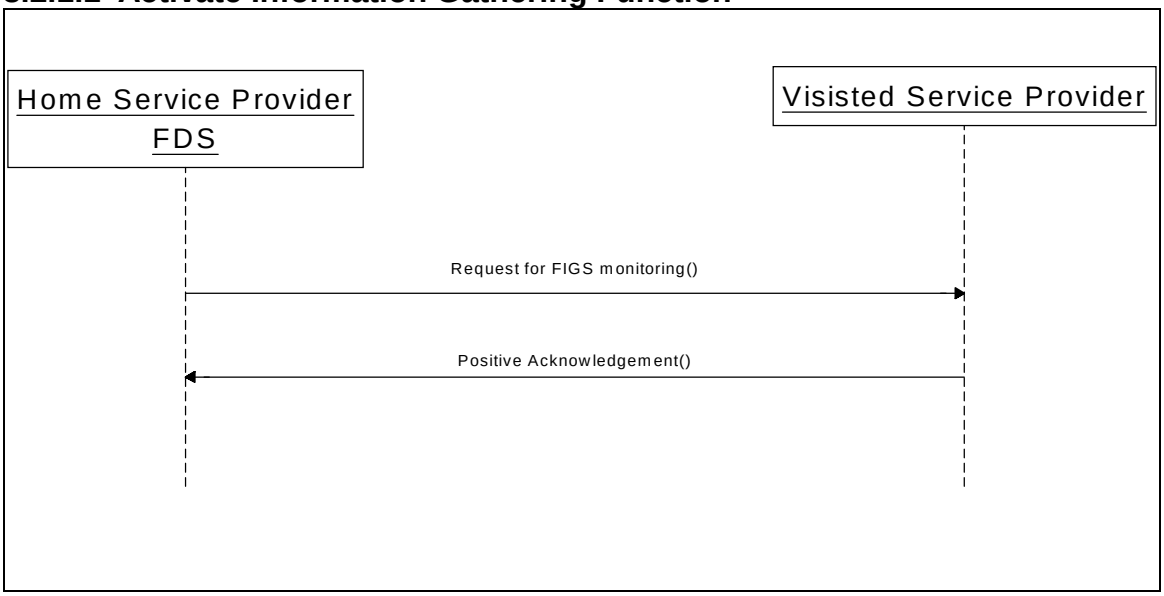

Figure 5: Message flow to activate FIGS

The request to activate information gathering is initiated by the Home service provider FDS and transmitted to the visited service provider as shown in Figure 5.

3.2.1.2 Stop Monitoring

This is the management function initiated by the home service provider. This is to stop monitoring FIGS by the visited service provider. The actual suspension of the service is done in the home subscriber system (e.g. Home Location Register (HLR of the subscriber). The reason the visited service provider is informed is to assist the visited service provider to detect any duplicate subscribers in their own network. If this is a list of subscribers, submitted by the home service provider to the visited service provider for suspension, the VSP shall provide confirmation of

suspension, only if all subscribers were matched. Otherwise, the VSP shall return a failure code for all the subscribers.

3.2.1.3 Information Flow

Service Provider Request and Service Provider Response	Home Service Provider	Home Service Provider	Notes
IMT2000 User Identification List	m		List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Persona Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscribe terminal as defined in the wireless signaling standards.
Suspend service reason	c		Reason Code : 1. Suspect country called 2. Bad correlations of locations 3. Bad correlations of times. 4. Numerous suspicious fraud patterns
Confirmation		M	Result code: R0: other R1: Success R2: Unknown subscriber(s)

3.2.1.4 Resume Monitoring

This is the management function initiated by the home service provider. This management function is only for the information of the visited service provider, so that the OS of the visited provider can resume the fraud management activities of the subscriber, by requesting profiles etc. from the home service provider. The actual activation of the service is done in the home subscriber system (e.g. Home Location Register (HLR of the subscriber). The visited service provider can now start active fraud management duties on the records of the subscriber. This scenario typically happens, when there is suspicious activity being investigated with the cooperation of the legitimate subscriber and there is resolution or elimination of the fraudulent pattern.

3.2.1.5 Information Flow

Service Provider Request and Service Provider Response	Home Service Provider	Visited Service Provider	Notes
IMT2000 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 signaling standards.
Resume service code	M		Reason code : 1. Incorrect suspension 2. Problem resolved
Confirmation		M	Confirmation code : r0: other r1: Success

			r2: Unknown subscriber

3.2.2 Sequence Diagrams

{Editor’s Note: Subscriber profile exchanges eliminated }

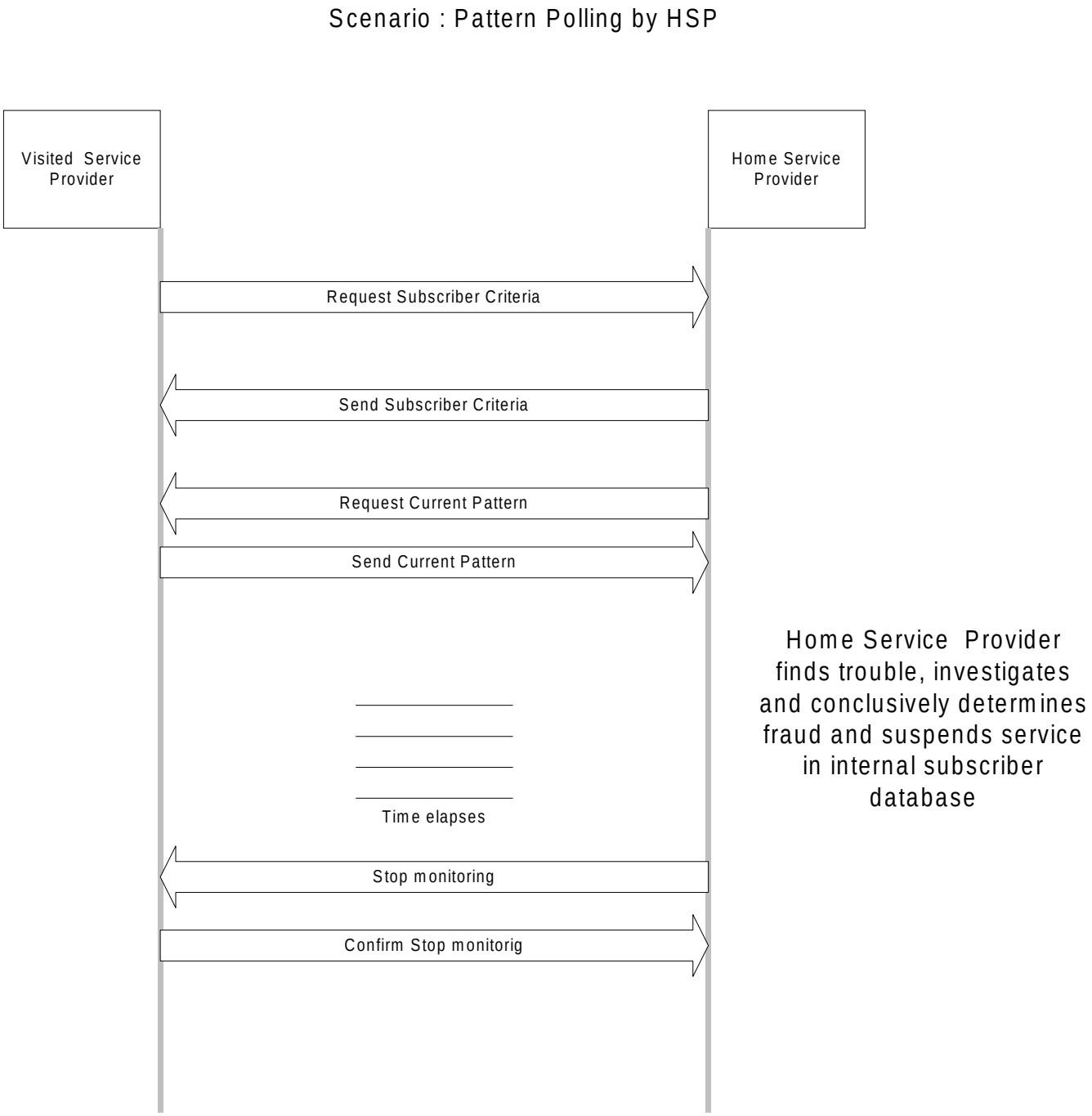

Figure 5: Scenario for Pattern Polling

3.2.2.1 pattern polling

In this scenario, the home service provider requests the most recent pattern from the visited service provider, after supplying the subscriber profiles. Based on the information in the current pattern, the service is suspended in the home database by the home service provider and the visited service provider is informed. This scenario is an example of the home service provider playing an active role in fraud management.

3.2.2.2 criteria-based information exchange

The visited service provider requests the home service provider to supply the criteria required for event reporting. The visited service provider receives the security criteria and when the trigger conditions specified by the home service provider are met the visited service provider generates the security events. This scenario also depicts that the visited service provider generates these security events, periodically.

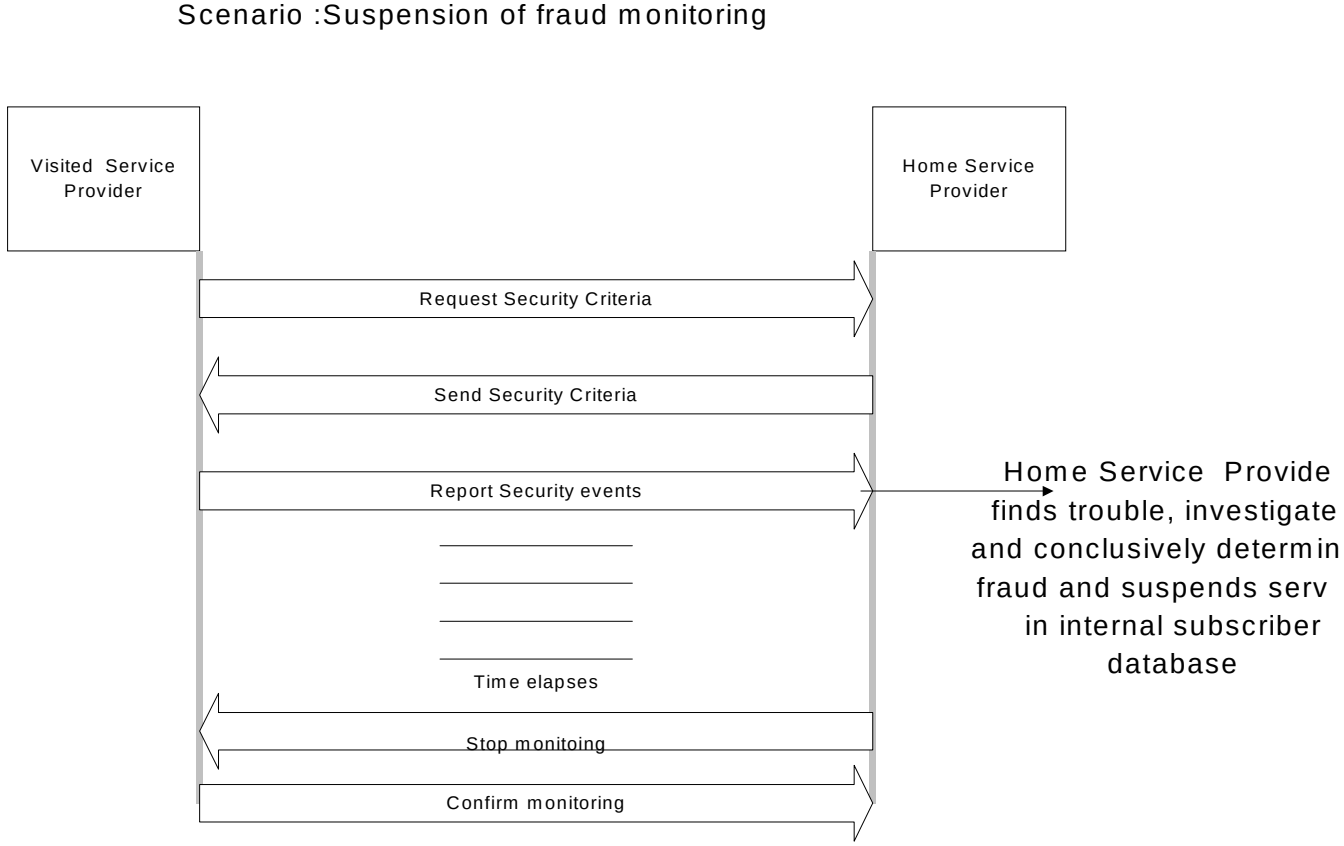

Figure 6: Scenario for criteria exchange and suspension of fraud monitoring

3.2.2.3 Stop monitoring

In the above scenario, the visited service provider after receiving the security criteria, generates security events. The home service provider after investigation finds that fraudulent activity has occurred. The home service provider suspends service in the internal subscriber database and informs the visited service provider that suspension has occurred. It is to be noted that the home service provider does the notification of suspension of service to the visited service provider after the actual suspension of service. The home service provider does the notification to the visited service provider so that the visited service provider now can remove the subscriber from its fraud monitoring database.

3.2.2.4 Resume monitoring

In this scenario, a subscriber's service is restored, after the fraudulent problem is eliminated. The home service provider enables the service in the home system and then informs the visited service provider about activating the fraud monitoring for the subscriber. The visited service provider requests the security criteria, so that new security criterion is obtained for the subscriber. The security events are reported periodically by the visited service provider.

3.2.2.5 Generic Errors

The home service provider in response to any request by the visited service provider can generate a generic error. This error message may be because some of the information contents in the request were not meaningful to the home service provider.

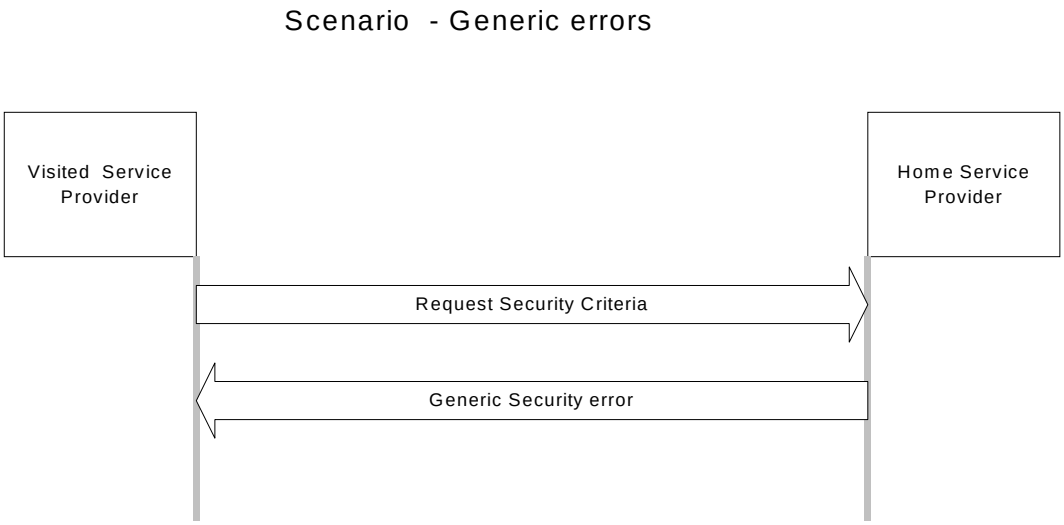

Figure 10: Scenario for Generic errors

3GPP TSG SA WG3 Security — S3#15 **S3-000581**

12-14 September, 2000

Washington DC

Annex: Fraud Management Criteria (Informative)

Telecommunication Management Networks need to provide the management means to detect and analyze 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)

Contact: Dia Helmy Tel: +1 972 751 7210
NEC America, Inc. email: helmyd@rss.dl.nec.com

Annex-XX: Information Transferred by the Visited Network

Information	Description
Dialled digits	The D**ialled 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 subscriber** 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 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.

* Co-Issue Managers:	John Visser	Geoff Caryer
	Nortel Networks, Canada	British Telecom, UK
Phone	+1-613-763-7028	+44-1473-738108
Fax	+1-613-765-5598	+44-1473-227884
Email	jvisser@nortelnetworks.com	geoff.caryer@btinternet.com