



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3210.1

(01/2001)

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.

© ITU 2001

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from ITU.

CONTENTS

Page

1	Introduction.....	1
1.1	Purpose and scope.....	1
2	References.....	1
3	Definitions	1
3.5	Role-related definitions.....	2
4	Abbreviations and acronyms	2
4.1	Conventions	2
5	Security Management Service	3
5.1	Security issues.....	3
5.2	Management Service description.....	3
6	Management high-level requirements	4
6.1	Management Service overview.....	6
6.2	Telecommunication resources	6
6.2.1	Fraud Information Gathering System (FIGS).....	6
6.2.2	Visited Network.....	7
6.2.3	Home Network Fraud Detection System (HN-FDS).....	7
6.3	Fraud Information Gathering use cases	7
6.3.1	Fraud Alert use case	8
6.3.2	Activate Information Gathering use case	8
6.3.3	Report FIGS use case	9
6.3.4	Deactivate Information Gathering use case.....	9
6.3.5	Modify FIGS Report use case	10
6.3.6	Advise Suspend FIGS Monitoring use case	10
6.3.7	Advise Resume FIGS Monitoring use case.....	11
7	Management Functions analysis.....	11
7.1	Fraud Information Gathering Function set	11
7.2	Object Classes and State Chart	11
7.3	Fraud Information Gathering functions and sequence diagrams	13
7.3.1	Fraud Alert function	13
7.3.2	Activate Information Gathering function	13
7.3.3	Report FIGS function	14
7.3.4	Deactivate Information Gathering function.....	15
7.3.5	Modify FIGS Report function	16
7.3.6	Advise Suspend FIGS Monitoring function	18
7.3.7	Advise Resume FIGS Monitoring function.....	19

	Page
Annex A – Fraud Management criteria.....	20
Annex B – Information transferred by the Visited Network	21

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.

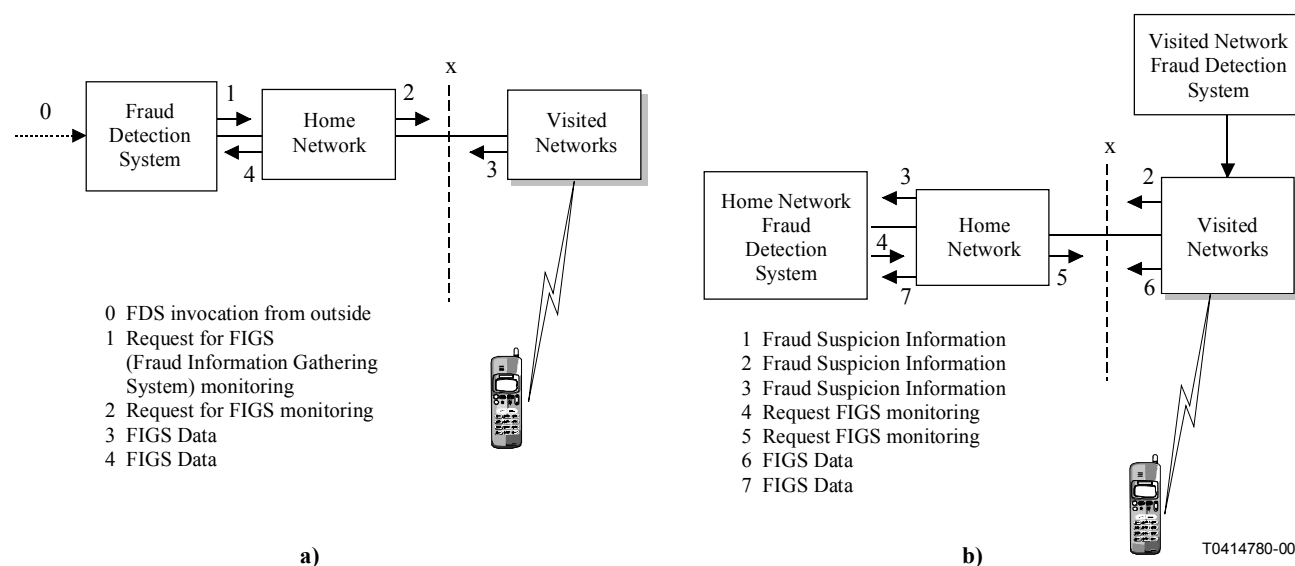


Figure 1/M.3210.1 – IMT-2000 Security Management Service: Fraud Information Gathering collaboration diagrams