FINAL DRAFT

EUROPEAN TELECOMMUNICATION STANDARD

pr ETS 300 614

March 1996

Source: ETSI TC-SMG

Reference: DE/SMG-061203P

ICS: 33.060.50

Key words: Digital cellular telecommunications system, Global System for Mobile communications (GSM)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Digital cellular telecommunications system (Phase 2); Security management (GSM 12.03)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

*

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1996. All rights reserved.

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Foreword 7

Introduction 7

1 Scope 9

2 Normative references 9

3 Abbreviations 11

4 Management of security features 12
4.1 Subscriber Identity (IMSI) confidentiality management 12
4.2 Subscriber Identity (IMSI) authentication management 12
4.3 Data confidentiality over the air interface 12
4.3.1 Encryption and algorithm management 12
4.3.2 Key management 13
4.4 Management of Mobile Equipment security 13

5 Security management mechanisms 13
5.1 System control mechanisms 14
5.2 Information gathering mechanisms 14
5.2.1 Use of scanners 14
5.2.2 Audit trail mechanisms 14
5.3 Alarm reporting mechanisms 14

6 Security procedures 14
6.1 Subscriber Identity confidentiality management procedures (TMSI) 15
6.1.1 Timer for Periodic Location Update 15
6.1.2 Selector when TMSI reallocation shall be done 15
6.2 Subscriber Identity authentication management procedures 16
6.2.1 Selector when authentication shall be performed 16
6.2.2 Open Identification of MS (authentication retried) 16
6.2.3 Parameters for generation and use of authentication vector 17
6.3 Encryption and algorithm management procedures 17
6.3.1 Encryption Management Procedures 17
6.3.2 Algorithm management procedures 17
6.4 IMEI management procedures 18
6.4.1 Selector when IMEI check shall be performed 18
6.5 Use of counters for security purposes 18
6.5.1 Open transfer of IMSI 18
6.5.2 IMEI related counters 18
6.5.3 Authentication failure 18
6.5.4 Additional security counters 19
6.5.5 Security-related scan reporting 19
6.6 Security reporting 20
6.6.1 Security alarm reports 20
6.6.1.1 Authentication failure in VLR 20
6.6.1.2 IMEI check violation in VLR 20
6.6.1.3 IMEI request failure in VLR 20
6.6.1.4 IMSI request failure in VLR 21
6.6.1.5 Unknown subscriber in HLR (VLR) 21
6.6.1.6 Unknown subscriber in HLR 21
6.6.1.7 Unknown subscriber in AuC(HLR) 21
6.6.1.8 IMSI confidentiality failure In MSC 21
6.6.2 Security audit trail reports 21

7 Security management object model 22
7.1 Security object classes 23
7.1.1 vlr1203AuthenticationFunction 23
7.1.2 vlr1203SubscriberIdFunction 23
7.1.3 vlr1203EquipmentIdFunction 23
7.1.4 msc1203EncryptionFunction 24
7.1.5 msc1203IMSIConfidentialityFunction 25
7.1.6 hlr1203SubscriberIdFunction 25
7.1.7 bts1203EncryptionFunction 25
7.2 Security attributes definitions 26
7.2.1 authenticationNecessaryWhen 26
7.2.2 authenticationRetriedAllowed 26
7.2.3 numberOfAuthenticationVectorsKept 26
7.2.4 authenticationVectorReuseAllowed 26
7.2.5 allocateNewTMSIWhen 26
7.2.6 checkIMEIWhen 26
7.2.7 encryptionControl 27
7.2.8 algorithmListMSC 27
7.2.9 algorithmListBTS 27
7.2.10 threshold 27
7.2.11 vlr1203AuthenticationFunctionId 27
7.2.12 vlr1203SubscriberIdFunctionId 27
7.2.13 vlr1203EquipmentIdFunctionId 28
7.2.14 msc1203EncryptionFunctionId 28
7.2.15 msc1203IMSIConfidentialityFunctionId 28
7.2.16 hlr1203SubscriberIdFunctionId 28
7.2.17 bts1203EncryptionFunctionId 28
7.3 Notifications 28
7.4 Name bindings 29
7.4.1 vlr1203AuthenticationFunction 29
7.4.2 vlr1203SubscriberIdFunction 29
7.4.3 vlr1203EquipmentIdFunction 29
7.4.4 msc1203EncryptionFunction 29
7.4.5 msc1203IMSIConfidentialityFunction 30
7.4.6 hlr1203SubscriberIdFunction 30
7.4.7 bts1203EncryptionFunction 30
7.5 Parameters 30
7.5.1 authenticationFailureInVLRParameter 30
7.5.2 imsiRequestFailureInVLRParameter 30
7.5.3 imsiRequestFailureInVLRParameter 30
7.5.4 imeiCheckViolationInVLRParameter 30
7.5.5 imeiRequestFailureInVLRParameter 30
7.5.6 imsiConfidentialityFailureInMSCParameter 31
7.5.7 imsiConfidentialityFailureInHLRParameter 31
7.6 Abstract syntax definitions 31
7.7 Application contexts 38

Annex A (normative): Relation between the authentication and encryption attributes 39

Annex B (normative): Additional security counters 42

B.1 MSC security measurement function 42
B.1.1 Encrypted connection used 42
B.1.2 Unencrypted connection used 42
B.1.3 Connection to be Cleared Due to Incompatible Encryption 43

B.2 VLR Security Function 43
B.2.1 Authentication Vectors Unavailable 43
B.2.2 Subscriber unknown in HLR(VLR) 43

B.3 HLR Security Function 43
B.3.1 Subscriber Unknown in HLR 43
B.3.2 Subscriber Unknown in AuC(HLR) 44

Annex C (normative): Security measurement Object Model 45

C.1 Model structure and content 45

C.2 Security measurement managed object classes 46
C.2.1 mscSecurityMeasurementFunction 46
C.2.2 vlrSecurityMeasurementFunction 46
C.2.3 hlrSecurityMeasurementFunction 46

C.3 Security measurement package definitions 46
C.3.1 General Security Measurement Function Packages 46
C.3.1.1 basicSecurityMeasurementFunctionPackage 46
C.3.2 MSC Security Measurement Function Packages 47
C.3.2.1 encryptedConnectionPackage 47
C.3.2.2 incompatibleEncryptionPackage 47
C.3.3 VLR Security Measurement Function Packages 47
C.3.3.1 authenticationVectorsUnavailablePackage 47
C.3.3.2 unknownSubscriberInHlrFromVlrPackage 47
C.3.4 HLR Security Measurement Function Packages 47
C.3.4.1 unknownSubscriberInHlrPackage 47
C.3.4.2 unknownSubscriberInAucPackage 47

C.4 Security measurement attribute definitions 48
C.4.1 General Security Measurement Function Related Attributes 48
C.4.1.1 securityMeasurementFunctionId 48
C.4.2 MSC Security Measurement Function Related Attributes 48
C.4.2.1 encryptedConnectionUsed 48
C.4.2.2 unencryptedConnectionUsed 48
C.4.2.3 callClearedIncompatibleEncryption 48
C.4.3 VLR Security Measurement Function Related Attributes 48
C.4.3.1 authVectorsUnavailable 48
C.4.3.2 subsUnknownInHlrFromVlr 49
C.4.4 HLR Security Measurement Function Related Attributes 49
C.4.4.1 subsUnknownInHlr 49
C.4.4.2 subsUnknownInAuc 49

C.5 Security measurement name bindings 50
C.5.1 MSC Name Binding 50
C.5.1.1 mscSecurityMeasurementFunction-"gsm1200:1993":mscFunction 50
C.5.2 VLR Name Binding 50
C.5.2.1 vlrSecurityMeasurementFunction-"gsm1200:1993":vlrFunction 50
C.5.3 HLR Name Binding 50
C.5.3.1 hlrSecurityMeasurementFunction-"gsm1200:1993":hlrFunction 50

C.6 Security measurement behaviour definitions 51
C.6.1 general security measurement function behaviour 51
C.6.2 general security measurement package behaviour 51
C.6.3 general security measurement attribute behaviour 51

C.7 Security measurement abstract syntax definitions 51

Annex D (informative): Index 52

History 54

Blank page

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Special Mobile Group (SMG) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

This final draft ETS describes the management of the security related aspects in the GSM/DCS PLMN within the Digital cellular telecommunications system. This ETS corresponds to GSM technical specification, GSM 12.03, version 4.2.0.

NOTE: TC-SMG has produced documents which give technical specifications for the implementation of the Digital cellular telecommunications system. Historically, these documents have been identified as GSM Technical Specifications (GSM-TSs). These specifications may subsequently become I-ETSs (Phase 1), or European Telecommunication Standards (ETSs)(Phase 2), whilst others may become ETSI Technical Reports (ETRs). These ETSI-GSM Technical Specifications are, for editorial reasons, still referred to in this ETS.

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

The radio communications aspect of the GSM system makes it particularly sensitive to unauthorized use. For this reason, security mechanisms are defined for the GSM system:

- Subscriber identity (IMSI) confidentiality.
- Subscriber identity (IMSI) authentication.
- Data confidentiality over the air interface.
- Mobile equipment security.

The use of these security features, is at the discretion of operators for non-roaming subscribers. For roaming subscribers however, the use of these security features is mandatory, unless otherwise agreed by all the affected PLMN operators (GSM 02.09 [1]).

A number of security parameters have been defined in the core specifications to support these security features. The IMSI is used to uniquely identify subscribers and the TMSI to provide subscriber identity confidentiality. The authentication vectors (Kc,RAND,SRES) are used in the authentication process and the ciphering key (Kc) is used to encrypt signaling and user data over the air interface. Finally the IMEI can be used to establish whether a piece of mobile equipment is suitable to be used on the network, i.e., approved and neither stolen nor faulty.

Formal definitions of these security mechanisms and their technical realization can be found in recommendations GSM 02.09 [2] and GSM 03.20 [3] respectively. The relevant messaging and procedures can be found in recommendations GSM 04.08 [4], GSM 08.08 [22], GSM 08.58 [23], and GSM 09.02 [5].

It is the objective of this ETS to provide a standard mechanism for the management of the aforementioned security features and parameters.

Blank page

1 Scope

This final draft European Telecommunication Standard (ETS) describes the management of the security related aspects in the GSM/DCS PLMN. The management of the relevant security services is addressed with respect to the following aspects:

— Overview of the security features;
— Description of the relevant management procedures;
— Modelling using the object oriented paradigm.

The definitions and descriptions of the security features and mechanisms are contained in the specifications of the underlying procedures and are not defined in this ETS. References to appropriate GSM/DCS specifications have been made throughout the ETS, where necessary. Issues relating to the security of management (e.g. file transfer security, database security, inter-operator security, etc.) are not covered in this ETS.

2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] GSM 02.09 (ETS 300 506): "Digital cellular telecommunication system (Phase 2); Security aspects".

[2] GSM 03.03 (ETS 300 523): "Digital cellular telecommunication system (Phase 2); Numbering, addressing and identification".

[3] GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions".

[4] GSM 04.08 (ETS 300 557): "Digital cellular telecommunication system (Phase 2); Mobile radio interface layer 3 specification".

[5] GSM 09.02 (ETS 300 599): "Digital cellular telecommunication system (Phase 2); Mobile Application Part (MAP) specification".

[6] GSM 12.00 (ETS 300 612-1): "Digital cellular telecommunication system (Phase 2); Objectives and structure of Network Management (NM)".

[7] GSM 12.02 (ETS 300 613): "Digital cellular telecommunication system (Phase 2); Subscriber, Mobile Equipment (ME) and services data administration".

[8] CCITT M.3010: "Principles for a Telecommunication Management Network"

[9] GSM 02.16 (ETS 300 508): "Digital cellular telecommunication system (Phase 2); International Mobile station Equipment Identities (IMEI)".

[10] GSM 12.04 (ETS 300 615): "Digital cellular telecommunication system (Phase 2); Performance data measurements".

[11] CCITT Recommendation X.720 (1992) (ISO/IEC 10165-1 (1992)): “Information technology - Open Systems Interconnection - Structure of management information : Management information model”.

[12] CCITT Recommendation X.721 (1992) (ISO/IEC10165-2 (1992)): “Information technology - Open Systems Interconnection - Structure of Management Information : Definition of Management Information”.

[13] CCITT Recommendation X.722 (1992) (ISO/IEC10165-2 (1992)): “Information technology - Open Systems Interconnection - Structure of Management Information: Guidelines for the Definition of Managed Objects”.

[14] CCITT Recommendation X.731 (1992) (ISO/IEC10164-2 (1992)): “Information technology - Open Systems Interconnection - Systems Management :Part 2: State management function”.

[15] CCITT Recommendation X.733 (1992) (ISO/IEC10164-4 (1992): “Information technology - Open Systems Interconnection - Systems Management :Part 2: Alarm Reporting Function”.

[16] CCITT Recommendation X.734 (1993) (ISO/IEC10164-5 (1993): “Information technology - Open Systems Interconnection - Systems Management :Event Report Management Function”.

[17] CCITT Recommendation X.735 (1992) (ISO/IEC10164-6 (1992): Information technology - Open Systems Interconnection - Systems Management: Log Control Function”.

[18] CCITT Recommendation X.736 (1992) (ISO/IEC10164-7 (1992): “Information technology - Open Systems Interconnection - Systems Management :Part 2: Security Alarm Reporting Function”.

[19] CCITT Recommendation X.740 (1992) (ISO/IEC10164-8 (1992): “Information technology - Open Systems Interconnection - Systems Management :Security Audit Trail Function”.

[20] GSM 12.20 (ETS 300 622): "Digital cellular telecommunication system (Phase 2); Base Station System (BSS) Management Information".

[21] GSM 12.08 (ETS 300 627): "Digital cellular telecommunication system (Phase 2); “Subscriber and Equipment Trace”.

[22] GSM 08.08 (ETS 300 590): "Digital cellular telecommunication system (Phase 2); Mobile Switching Centre - Base Station System (MSC - BSS) interface Layer 3 specification".

[23] GSM 08.58 (ETS 300 596): "Digital cellular telecommunication system (Phase 2); Base Station Controller - Base Transceiver Station (BSC - BTS) interface Layer 3 specification".

[24] CCITT M.3100: "Generic Network Information Model"

[25] GSM 12.30 (ETR 128): "ETSI object identifier tree; Common domain Mobile domain; O&M managed Object registration definition"

3 Abbreviations

For the purposes of this ETS, the following abbreviations apply.

A3	Authentication Algorithm
A5	Ciphering Algorithm
A8	Ciphering Key Computation Algorithm
AuC	Authentication Centre
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BSS	Base Station Sub-system
BTS	Base Transceiver Station
CKSN	Ciphering Key Sequence Number
CM	Call Management
EIR	Equipment Identity Register
GDMO	Guidelines for the Definition of Managed Objects
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
Kc	Ciphering Key
Ki	Individual Subscriber Authentication Key
LU	Location Update
MAP	Mobile Application Part
ME	Mobile Equipment
MM	Mobility Management
MO	Mobile Originating, Managed Object
MOC	Managed Object Class
MS	Mobile Station
MSC	Mobile Switching Centre
MT	Mobile Terminating
NE	Network Element
OS	Operations System
PLMN	Public Land Mobile Network
RAND	Random Number
Rec.	Recommendation
SIM	Subscriber Identity Module
SMS	Short message service
SRES	Signed Response to RAND
SS	Supplementary Service
TMN	Telecommunications Management Network
TMSI	Temporary Mobile Subscriber Identity
TS	Technical Specification
VLR	Visitor Location Register

4 Management of security features

Clause 4 identifies the manageable aspects of the security features in the previous clause. The security management mechanisms which can be used are listed in clause 5. Clause 6 defines the procedures introduced in clause 4, and clause 7 provides the object model for the management these parameters.

4.1 Subscriber Identity (IMSI) confidentiality management

Subscriber confidentiality in the GSM PLMN is provided by the use of the Temporary Mobile Subscriber Identity (TMSI on the air interface. Avoiding the use of the International Mobile Subscriber Identity (IMSI) over the air interface by substituting the TMSI, provides both a high level of confidentiality for user data and signalling, and protection against the tracing of a user's location. This mechanism is described in GSM 03.20 [3] and the structure of the TMSI is described in GSM 03.03 [2].

As the frequency of reallocation of the TMSI has an effect on the subscriber confidentiality, a parameter is defined to provide control over it.

If the (old) TMSI is unknown to the Visitor Location Register (VLR) or wrong, the mobile subscriber can only be identified by using the IMSI . As encryption is not possible during that stage, the IMSI has to be sent unencrypted over the air interface. The occurrence of such an event (or similar) affects the quality of the subscriber confidentiality service. Counters are defined to provide information about this service.

4.2 Subscriber Identity (IMSI) authentication management

The GSM PLMN offers a mechanism for the authentication of subscriber identity. The purpose of this feature, is to protect the network against unauthorized use. It also enables the protection of the GSM PLMN subscribers, by making it practically impossible for intruders to impersonate authorized users.

Subscriber authentication may be included in the Mobile Application Part (MAP) procedures for access request and location update. The use of authentication should be under the control of the operator and a parameter is defined for this purpose.

Authentication may be retried to recover from failure due to incorrect TMSI by requesting open transfer of the IMSI over the air interface. This should be under the control of the operator and a parameter to this effect is defined.

To support authentication, vectors are generated in the AuC. The VLR requests these authentication vectors for use in the authentication procedures. Under exceptional conditions, these vectors may need to be reused. This may have an effect on the security of the network, and should be under the control of the operator.

4.3 Data confidentiality over the air interface

4.3.1 Encryption and algorithm management

In a GSM PLMN, encryption may be used to protect the confidentiality of data and signalling on the air interface .Two algorithms are essentially involved in the encryption process; the ciphering algorithm (A5) and the cipher key generation algorithm (A8). In general, the authentication algorithm (A3) and the A8 algorithm, are implemented as one in the AuC and the SIM, and may be operator-specific. The A5 algorithm is implemented in the ME and at the BTS.

The negotiation (between the MS and the MSC) of up to seven versions of the ciphering algorithm (A5/1, A5/2...,A5/7), is catered for in signalling. The MSC will then identify which of these versions are allowed by the network for this call (perhaps based on the user identity) and will pass the list of acceptable versions to the BSS. The BSS must then select a version from this list. If any versions in this list are supported by the BTS, then encryption must be used. For the case where multiple choices are available, the order of preference for this BSS selection should be set by the operator. A BTS related attribute specifying a priority ordered list of version choices is defined in this ETS. If no version match is available, the MSC must decide whether or not to complete the call in unencrypted mode. An MSC related attribute to allow/prohibit unencrypted communications is defined in this ETS.

4.3.2 Key management

Two types of keys are defined in GSM; the authentication key (Ki) and the cipher key (Kc).

The Ki is unique to the subscriber. It is stored in the SIM during pre-personalization and in the authentication centre

The Kc is normally generated at the same time as the authentication parameters. The same random number (RAND) that is passed through the A3 algorithm with the Ki during authentication, is passed through a different algorithm, the A8, again with the Ki to generate the Kc. The key Kc may be stored and used by the mobile station, until it is updated at the next authentication. Attention is necessary to achieve key consistency during all these operations and after (re)synchronization of nodes. This consistency is provided for by the use of the Ciphering Key Sequence Number (CKSN) and authentication retry.

The administration of the (IMSI,Ki) pair is described in recommendation GSM12.02 [7]. The generation of the Kc is described in recommendation GSM 03.20 [3].

4.4 Management of Mobile Equipment security

For equipment security, the international mobile equipment identity (IMEI) has been defined. The IMEI is physically secure in the ME, as defined in GSM 02.09 [1].

Equipment identification is achieved by requesting the IMEI from the ME. To control this identification, a parameter is defined in subclause 6.4.1 of this ETS. It is used to select which MAP procedures shall include the request of the IMEI.

The Equipment Identity Register (EIR) is used to store IMEIs in the network. An IMEI is classified as white, gray or black.

The IMEI management functions related to the EIR are described in GSM 12.02 [7].

IMEI tracing can be used for the detection and elimination of security breaches. This process is also described in GSM 12.08 [21].

5 Security management mechanisms

In line with the requirements for GSM management (as defined in GSM 12.00 [6]), management of security features will be modelled according to the TMN principles defined in CCITT M.3010 [8] and X.722 [13]. Various standardized mechanisms, described in CCITT Recommendations [11] up to [19], are employed to derive the PLMN security management model.

Security management functions are modelled using:

— Security dedicated managed object classes, characterized by various attributes whose behaviour is completely described.

— General objects defined in GSM 12-series and CCITT.

This approach enables the control of security features and allows for the use of various standardized managed objects.

The object model developed in this ETS is based on the principle that the use of modelled objects should be minimized, in order to avoid unnecessary overheads. Security features are modelled through the definition of attributes and notifications, collected in related packages.

This clause of the ETS identifies the specific mechanisms to be used for managing the features identified in clause 4.

The mechanisms are grouped into:

— mechanisms used for the control of security features
— mechanisms for obtaining information such as possible attempts at breaching security

— mechanisms which allow the analysis of security problems.

5.1 System control mechanisms

Control of security features is provided by the object classes and the attributes defined therein. Instantiation of a security managed object class within a managed element, provides access to the attributes that control the features within that element. Attributes are provided to represent various aspects of the security features. Values for these attributes can be set to change the behaviour of the system. Where necessary, specific values or ranges of values are specified to determine permissible settings of these attributes.

5.2 Information gathering mechanisms

It is desirable to record the occurrence of various security events. Depending on the type of information, frequency of occurrence and the importance of the event, one of several mechanisms may be employed to record the occurrence :

— The use of scanners to collect and periodically report measurement information on high frequency or low importance events.
— The use of a counter associated with a metric object, allowing for the definition of threshold crossing and notification severity. Metric objects are not used however in this ETS.
— The use of security alarms for high importance and/or infrequent events.

5.2.1 Use of scanners

Scanners are managed object classes which collect and report the values of the counters which are defined as attributes in other object classes. Some of the counters defined in GSM 12.04 [10] are used to count security-related events. Their complete definition and the definition of their collection process can be found in GSM 12.04 [10]. The list of the relevant counters is provided in subclause 6.5 of this ETS.

5.2.2 Audit trail mechanisms

Some security events that occur during the life of a system may need to be reviewed immediately and immediate actions may need to be taken. For other events it may be useful to review the history in order to identify patterns of failures or abuse. It is recommended that this data is maintained in a log instance which holds security audit records. This log conforms to the general format of logs (defined in GSM 12.00 [6]), and may be kept either at the agent or at the manager side. The general usage conditions of this log is the same as that defined in GSM 12.00 [6]. The security audit trail mechanism, notification and record are defined in X.740 [19].

5.3 Alarm reporting mechanisms

The manager needs to be alerted whenever an event indicating a potential breach in the security of the PLMN is detected. This detection may be reported by an alarm notification.

The format of these alarm notifications is defined in CCITT X.736 [18]. The security alarm record is defined in X.721 [12].

The security alarm report shall identify the cause of the security alarm, its perceived severity and the event that caused it.

6 Security procedures

This clause describes the procedures and covers the technical details of the concepts discussed in clause 4.

Some security procedures (e.g. authentication, TMSI reallocation, IMEI checking) are activated conditionally. The activation of these procedures is controlled by administrable security triggers. Security triggers are defined for the various type of subscribers (home, visiting, ...). Each subscriber is assigned one of these subscriber types.

For each security procedure, security triggers can be assigned per subscriber type. For each subscriber type, the security triggers describe the condition on which the applicable security procedure is to be performed. The condition is defined in terms of predefined triggering events, e.g. the establishment of a mobile originating call, a periodic location update, ... The predefined triggering events may be assigned to groups based on how often the operator wants the security procedure to be activated: never, always or after a frequency N that can be administered by the operator.

One or more events can be grouped so that the security procedure can be triggered when a certain threshold has been exceeded. The grouping of the events is left to the operator.

For each of these groups, a counter is to be maintained per subscriber. This initial value of this counter is 0, and it is increased by one each time a triggering event from this set occurs. On the Nth occurrence, the counter is reset and the appropriate security procedure is executed for this subscriber.

NOTE: It is administered on a per VLR basis when a security function is invoked. The execution of the security procedure will be applicable to the VLR area where the security function is administered. The associated counter when to invoke a procedure is defined in the VLR per subscriber and per event group.

6.1 Subscriber Identity confidentiality management procedures (TMSI)

As discussed in clause 4, the frequency of TMSIreallocation has an effect on subscriber confidentiality. The following management capabilities are necessary to control the reallocation frequency:

— The specification of the frequency of TMSI reallocation via the frequency of periodic location update.
— The selection of MAP procedures that should include TMSI reallocation.

6.1.1 Timer for Periodic Location Update

A parameter (Timer T3212) is conveyed to the MS via the BCCH (ref. GSM 04.08 [4]). It is used in the MS for performing periodic LUs. This is security-relevant because during each LU, TMSI reallocation is performed, i.e. the frequency of LU determines the frequency of TMSI reallocation.

The attribute timerPeriodicUpdateMS is defined in GSM 12.20 [20] to contain the time values in tenths of an hour.

Reducing the value of this timerPeriodicUpdateMS will therefore improve the degree of IMSI confidentiality, but has the net effect of increasing the signalling load on the network, in particular when LU is used with Authentication.

6.1.2 Selector when TMSI reallocation shall be done

The frequency of TMSI reallocation depends also on how many MAP procedures require TMSI reallocation.

TMSI reallocation in the MAP process access request procedure can be enabled/disabled, based on the following CM service type values:

— MO call
— Emergency call establishment
— SMS
— SS activation
— MO call re-establishment
— MT call

TMSI reallocation in the MAP location update procedure can be enabled/disabled, based on the following types of LU:

— Normal Location Update
— Periodic Location Update

— IMSI attach

The distinction between the various types of location updates is lost in the MAP-procedures. Additional information needs to be supplied to allow the management of TMSI reallocation. This TS assumes that the MSC-VLR interface is manufacturer-dependent, and therefore the addition of such information is left open.

The attribute allocateNewTMSIWhen of object class vlr1203SubscriberIdFunction is available to select one or several of the cases listed above to include TMSI reallocation.

6.2 Subscriber Identity authentication management procedures

As discussed in clause 4, authentication security can be managed based on when authentication is done, when authentication is retried and when authentication vectors are reused. The following management capabilities are necessary to control these aspects:

— The selection of which MAP procedures shall include subscriber identity authentication
— The selection of which conditions subscriber authentication shall be retried by the network
— The control of the reuse of authentication vectors.

6.2.1 Selector when authentication shall be performed

Subscriber authentication may be initiated by the MAP (vlr1203AuthenticationFunction) procedure for the access request and by the MAP location update procedure. The same selection criteria used in TMSI reallocation are applicable.

Including subscriber authentication in more than one procedure will improve the overall protection of the PLMN against unauthorized use.

If encryption is not used, authentication should be included in every service access procedure, otherwise there will be no protection against unauthorized use of services. If encryption is to be used, it is not necessary to perform authentication for every call, as it is possible to refer to a previously used encryption key, by using the ciphering key sequence number. This number is sent to the MS by the network during authentication procedure (reference GSM 04.08 [4], subclause 4.3.2).

In subsequent calls, this number is sent to the network by the MS (PAGING RESPONSE and in several MM messages, reference GSM 04.08 [4]). The network may check this number against the CKSN sent during some previous authentication procedure and skip the authentication procedure for the current call if the two numbers are equal and use that previously-used key again for encryption.

The attribute authenticationNecessaryWhen of object class vlr1203AuthenticationFunction contains the selection when the authentication procedure shall be mandatory.

If the abovementioned ciphering key sequence number check (which is done at the beginning of a call) does not allow to perform encryption, but encryption itself is not disabled (reference subclause 6.3.1), then authentication shall be included in the call, irrespective of the setting of the attribute.

6.2.2 Open Identification of MS (authentication retried)

Authentication could fail due to the following reasons:

— The TMSI of an MS is not known in the VLR
— The TMSI is allocated with a different IMSI (due to TMSI reallocation with TMSI reuse).

In order to obtain the identity of an MS in these cases, the network has to retry authentication with open transfer of the IMSI (reference to GSM 09.02 [5], macro Process_Access_Request_VLR). The attribute authenticationRetriedAllowed of object class vlr1203AuthenticationFunction will allow/disallow this.

Open identification of IMSI will make the subscriber traceable for one call or until the next handover. Additionally, if encryption is not used, the IMSI will be traceable until the next IMSI detach.

6.2.3 Parameters for generation and use of authentication vector

The following parameters influence the generation and use of the authentication vector:

— number of authentication vectors per subscriber to be kept in VLR. If for a subscriber the number of authentication vectors in the VLR is less than this number, new authentication vectors will be requested from the HLR/AuC for this subscriber (reference GSM 09.02 [5]: MAP-SEND-AUTHENTICATION-INFO service) until a manufacturer-dependent (maximal) number of authentication vectors in VLR is reached.

This parameter only affects the computing and signalling load caused by the subscriber authentication and encryption security service.

— Authentication vector reuse allowed.

By reuse of RAND and SRES, the level of data confidentiality and authentication can be degraded as it potentially makes it easier to guess or compute Kc or even Ki. If no encryption is used, SRES should not be reused, as it would make possible a security attack by masquerade. If no unused authentication vectors are available in the VLR and authentication vector reuse is not allowed, then calls shall be cleared.

The attributes numberOfAuthenticationVectorsKept and authenticationVectorReuseAllowed of object class vlr1203AuthenticationFunction control the various authentication vector reuse options.

6.3 Encryption and algorithm management procedures

The use of encryption is a network option subject to the restrictions of GSM 02.09 [1]. The service and procedures to be managed are described in GSM 09.02 [5] (MAP-SET-CIPHERING-MODE service). The various versions of the ciphering algorithm supported by the ME are signalled to the network over the air interface and an appropriate encryption algorithm or not encryption has to be selected by the network (reference GSM 04.08 [4], subclause 3.4.7, ciphering mode setting procedure).

6.3.1 Encryption Management Procedures

For the management of the existing encryption options, an attribute, encryptionControl, with the following values is defined.

— noEncryption;
— encryptionSupported (i.e. to be used where possible);
— encryptionNecessary (i.e. call shall either continue in encrypted mode or shall be cleared if encryption is not possible).

The value of this attribute shall be tested at the beginning of the call (the exact implementation is left to the manufacturer).

If the attribute value is noEncryption**,** no encryption will be used for the call. If it is one of the other two values, the network will negotiate a feasible algorithm with the BSC. The result of this negotiation will be either an encryption algorithm which is supported by both the network and the MS or no encryption.

If the attribute value is encryptionNecessary, and no encryption has been negotiated, the call shall be cleared by the network. Otherwise the call shall proceed as negotiated.

6.3.2 Algorithm management procedures

For the management of the ciphering algorithm two, possibly single element lists, must be defined. The MSC must select from the list of ciphering algorithms indicated by the ME. This selection would be based on a managed list of algorithms permitted in the network. The intersection between this list and the list from the ME is passed in signalling to the BSS. The BSC must then select from this list based on an administered priority and based on the capabilities of the relevant BTS to support the various ciphering algorithms.

For the MSC, the attribute algorithmListMSC will be provided to allow the OS to set the list of ciphering algorithms allowed in the network.

For the BSS, the attribute algorithmListBTS will be provided, per BTS, to allow the OS to set the list of ciphering algorithms supported by the BTS and to indicate the priority order of their use.

6.4 IMEI management procedures

Equipment identification is done by requesting the IMEI from the ME (reference GSM 04.08, [4] CIPHERING MODE COMMAND MESSAGE and GSM 09.02 [5] MAP_PROCESS_ACCESS_REQUEST).

To control this identification, the attribute checkIMEIWhen has been defined in this ETS. It is used to select which MAP procedures shall include the request of the IMEI .

6.4.1 Selector when IMEI check shall be performed

The attribute checkIMEIWhen is provided to select whether the network will issue an identity request and perform the IMEI check. IMEI check may be initiated by the MAP (VLR-) procedures for access requests and location updates. The same selection criteria used in TMSI reallocation are applicable.

The identity of a ME is required for identifying (white-, grey- or black-listed-) equipment and tracing black- or grey-listed equipment.

The security of this mechanism against attacks (e.g. masquerade) is not influenced by the network; it depends entirely on the implementation of the IMEI and related reporting functions in the ME.

The attribute checkIMEIWhen of object class vlr203EquipmentIdFunction contains the selection when IMEI check shall be performed.

6.5 Use of counters for security purposes

6.5.1 Open transfer of IMSI

Counters on the occurrence of the open transfer of the IMSI, provide information about the quality of the subscriber confidentiality service. The following such counters have been defined in GSM 12.04 [10]:

— "Successful transactions on the MM-Layer where subscriber was identified with TMSI"; and
— "Successful transactions on the MM-Layer where subscriber was identified with IMSI".

6.5.2 IMEI related counters

Several counters provide information on the number of IMEI-related transactions. These counters, (listed below) have been defined in GSM 12.04 [10]:

— "Number of transmitted IMEI check request" in MSC;
— "Number of white answers" in MSC;
— "Number of grey answers" in MSC;
— "Number of black answers" in MSC;
— "Number of unknown IMEI answers" in MSC;
— "Number of received IMEI check request" in EIR;
— "Number of white answers" in EIR;
— "Number of grey answers" in EIR;
— "Number of black answers in EIR;
— "Number of unknown IMEI answers" in EIR.

6.5.3 Authentication failure

Authentication failure may occur in the following situations:

— different SRES values, reference GSM 04.08 [4], AUTHENTICATION REJECT message;
— timeout (SRES not received in time), reference GSM 04.08 [4], timer T3260;
— The TMSI of an MS is not known in the VLR;
— The TMSI is allocated with a different IMSI (due to TMSI reallocation with TMSI reuse).

Counters to measure these events are specified in GSM 12.04 [10]:

— "attempted authentication procedures in the VLR";
— "successful authentication procedures in the VLR".

6.5.4 Additional security counters

The following counters for security purposes are currently defined in this recommendation (Annex B), but they will eventually need to be integrated in GSM 12.04 [10], along with other counter objects in the future.

Three counters are defined in the MSC to provide information on the use of encryption:

- “Encrypted connection used” in MSC;
- “Unencrypted connection used” in MSC;
- “Connection cleared due to incompatible encryption” in MSC.

The following counter is defined to measure the unsuccessful authentication due to the loss or the unavailability of authentication vectors from the AuC:

- “Authentication vectors unavailable” in VLR.

Counters are defined in several network elements to measure the level of possible unauthorized intrusions in the network:

- “Subscriber unknown in HLR” in VLR;
- “Subscriber unknown in HLR” in HLR;
- “Subscriber unknown in AuC(HLR)” in HLR.

6.5.5 Security-related scan reporting

The following tables list all recommended security related counters, available to scan reports relevant to specific GSM Network Elements.

Operators shall also be able to generate these scan reports on demand or at regular scheduled intervals.

MSC

— Subscriber identified with IMSI on radio path;
— Subscriber identified with TMSI on radio path;
— Encrypted connection used;
— Unencrypted connection used;
— Connection cleared due to incompatible encryption;
— Number of transmitted IMEI check requests;
— Number of white answers;
— Number of grey answers;
— Number of black answers;
— Number of unknown IMEI answers.

VLR

— Attempted authentication procedures in the VLR;
— Successful authentication procedures in the VLR;
— Subscriber unknown in HLR;
— Authentication vectors unavailable.

HLR

— Subscriber unknown in HLR;
— Subscriber unknown in AuC(HLR).

EIR

— Number of received IMEI check requests;
— Number of white answers;
— Number of grey answers;
— Number of black answers;
— Number of unknown IMEI answers.

6.6 Security reporting

6.6.1 Security alarm reports

The following security related alarms shall be generated and presented to operating personnel of a GSM network, immediately after the cause which triggered them is identified.

The generated alarms can be stored in a log in the NE and/or forwarded to an OS. The storage of alarms in the NE is modelled through the managed object class “log” as specified in CCITT X.735 [17]. The forwarding of alarms is modelled via ‘Event Forwarding Discriminator (EFD)’ objects, defined in CCITT X.734 [16]. Additional information can be found in GSM 12.00 [6].

6.6.1.1 Authentication failure in VLR

An authentication failure (mismatched or missing SRES) is reported by the VLR as a security alarm. The following information should be available (in addition to VLR id and time stamp etc.):

— IMSI;
— IMEI (optional, only if available);
— type of failure (missing or mismatched SRES);
— location information.

The security alarm notification type shall be the “Security service or mechanism violation”, as defined in X.736 [18]. authenticationFailureInVLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition AuthenticationFailureInVLRSecurityAlarmInfo.

6.6.1.2 IMEI check violation in VLR

An alarm shall be reported when the VLR receives a “non-white-listed” response from the EIR. The following information should be reported in this case:

— IMSI;
— IMEI;
— type of failure (black-listed, grey-listed, unknown, no response from EIR);
— location information.

The security alarm notification type shall be the “Security service or mechanism violation”, as defined in X.736 [18]. imeiCheckViolationInVLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition ImeiCheckViolationInVLRSecurityAlarmInfo.

6.6.1.3 IMEI request failure in VLR

The MS does not send its IMEI to network when requested. The alarm shall contain:

— IMSI;
— TMSI if available;
— location information.

The security alarm notification type shall be the “Security service or mechanism violation”, as defined in X.736 [18]. imeiRequestFailureInVLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition ImeiRequestFailureInVLRSecurityAlarmInfo.

6.6.1.4 IMSI request failure in VLR

The MS does not reveal its identity (IMSI) when requested after the identification with TMSI failed. The alarms contain only the TMSI and location information. The security alarm notification type shall be the “Security service or mechanism violation”, as defined in X.736 [18]. imsiRequestFailureInVLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition ImsiRequestFailureInVLRSecurityAlarmInfo.

6.6.1.5 Unknown subscriber in HLR (VLR*)*

The VLR receives a request from an MS that is not identified in the HLR. The only available information is the IMSI, the identity of the HLR and the location of the attempt. The security alarm notification type shall be the “Integrity violation”, as defined in X.736 [18]. unknownSubscriberInVLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition UnknownSubscriberInVLRSecurityAlarmInfo.

6.6.1.6 Unknown subscriber in HLR

The HLR receives a request from a VLR with an IMSI that is unknown in the HLR. The information available is the IMSI and the identity of the VLR. The security alarm notification type shall be the “Integrity violation”, as defined in X.736 [18]. unknownSubscriberInHLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition UnknownSubscriberInHLRSecurityAlarmInfo.

NOTE: This reports the same event as in subclause 6.6.1.5, but is kept separate to account for the case of the event occurs in a different network.

6.6.1.7 Unknown subscriber in AuC(HLR)

The Auc(HLR) receives a vector request for an IMSI that is unknown in the AuC(HLR). The only information available is the IMSI. The security alarm notification type shall be the “Integrity violation”, as defined in X.736 [18]. unknownSubscriberInAuCHLR is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition UnknownSubscriberInAuCHLRSecurityAlarmInfo.

6.6.1.8 IMSI confidentiality failure In MSC

If the number of IMSIs used for subscriber identification on a radio path increases over a threshold during the reporting period, this alarm should be generated.

The security alarm notification type shall be the “Security service or mechanism violation”, as defined in X.736 [18]. subscriberIdentityConfidentialityFailureInMSC is defined as a new security alarm cause for this alarm notification with its own object identifier. The alarm info parameter in the alarm notification has as ASN.1 syntax definition ImsiConfidentialityFailureInMSCSecurityAlarmInfo.

6.6.2 Security audit trail reports

No security audit trail reports are defined in this ETS.

7 Security management object model

This clause of the ETS contains the full definition of the management information model. To aid understanding this model, a containment tree is presented below. This containment tree contains a graphical representation of the naming hierarchy of the managed objects defined in this model.

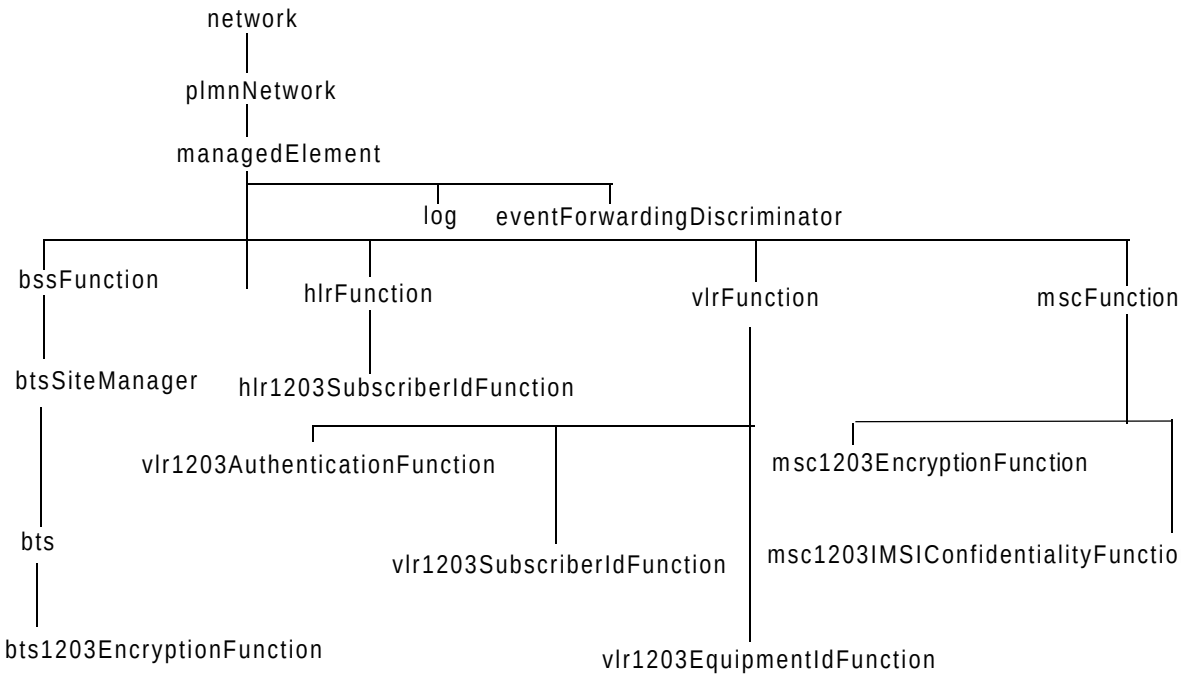

Figure 1

7.1 Security object classes

7.1.1 vlr1203AuthenticationFunction

vlr1203AuthenticationFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Rec.X.721:1992":top;
CHARACTERIZED BY
"Rec. M.3100:1992":createDeleteNotificationsPackage**,**
vlr1203authenticationPackage **PACKAGE**
BEHAVIOUR
vlr1203authenticationBehaviour
BEHAVIOUR DEFINED AS "Refer to subclause 6.2. The securityServiceOrMechanismViolation notification is sent based on an authentication failure in the VLR;the reported security alarm cause is authenticationFailureInVLR. Refer to subclause 6.6.1.1 for further details" ;
;
ATTRIBUTES
vlr1203AuthenticationFunctionId **GET,**
authenticationNecessaryWhen **GET-REPLACE ADD-REMOVE,**
authenticationRetriedAllowed **GET-REPLACE,**
numberOfAuthenticationVectorsKept **GET-REPLACE,**
authenticationVectorReuseAllowed **GET-REPLACE;**

NOTIFICATIONS
"Rec.X.721:1992".securityServiceOrMechanismViolation
authenticationFailureInVLRParameter ;;;
REGISTERED AS {gsm1203managedObjectClass 1};

7.1.2 vlr1203SubscriberIdFunction

vlr1203SubscriberIdFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Rec.X.721:1992":top;
CHARACTERIZED BY
"Rec. M.3100:1992":createDeleteNotificationsPackage,
vlr1203subscriberIdPackage **PACKAGE**
BEHAVIOUR
vlr1203subscriberIdBehaviour
BEHAVIOUR DEFINED AS "Refer to subclause 6.1.2. The securityServiceOrMechanismViolation notification is sent as an imsi request failure in the VLR ; the reported security alarm cause is imsiRequestFailureInVLR. The integrityViolation notification is sent based on the unknownSubscriberInVLRevent and the unknownSubscriberInVLR will be reported as the security alarm cause. Refer to subclauses 6.6.1.4 and 6.6.1.5 for further details" ;
;
ATTRIBUTES
vlr1203SubscriberIdFunctionId **GET,**
allocateNewTMSIWhen **GET-REPLACE ADD-REMOVE**;
NOTIFICATIONS
"Rec.X.721:1992".securityServiceOrMechanismViolation
imsiRequestFailureInVLRParameter ,
"Rec.X.721:1992".integrityViolation
unknownSubscriberInVLRParameter ;;;
REGISTERED AS {gsm1203managedObjectClass 2};

7.1.3 vlr1203EquipmentIdFunction

vlr1203EquipmentIdFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Rec.X.721:1992":top;
CHARACTERIZED BY
"Rec. M.3100:1992":createDeleteNotificationsPackage,

vlr1203equipmentIdPackage **PACKAGE**
BEHAVIOUR
vlr1203equipmentIdBehaviour
BEHAVIOUR DEFINED AS “Refer to subclause 6.4.1. The securityServiceOrMechanismViolation notification is sent as an imei check violation in VLR or an imei request failure in VLR . The imeiCheckViolationInVLR and imeiRequestFailureInVLR will be reported as the security alarm causes respectively. Refer to subclauses 6.6.1.2 and 6.6.1.3 for further details“ ;
;
ATTRIBUTES
vlr1203EquipmentIdFunctionId **GET,**
checkIMEIWhen **GET-REPLACE ADD-REMOVE**;
NOTIFICATIONS
“Rec.X.721:1992”.securityServiceOrMechanismViolation
imeiCheckViolationInVLRParameter ,
“Rec.X.721:1992”.securityServiceOrMechanismViolation
imeiRequestFailureInVLRParameter ;;;
REGISTERED AS {gsm1203managedObjectClass 3};

7.1.4 msc1203EncryptionFunction

msc1203EncryptionFunction **MANAGED OBJECT CLASS**
DERIVED FROM
“Rec.X.721:1992”:top;
CHARACTERIZED BY
“Rec. M.3100:1992”:createDeleteNotificationsPackage,
msc1203EncryptionPackage **PACKAGE**
BEHAVIOUR
msc1203EncryptionBehaviour
BEHAVIOUR DEFINED AS “Refer to subclause 6.3“;
;
ATTRIBUTES
msc1203EncryptionFunctionId **GET,**
encryptionControl **GET-REPLACE**,
algorithmListMSC **GET-REPLACE**;;;
REGISTERED AS {gsm1203managedObjectClass 4};

7.1.5 msc1203IMSIConfidentialityFunction

msc1203IMSIConfidentialityFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Rec.X.721:1992":top;
CHARACTERIZED BY
"Rec. M.3100:1992":createDeleteNotificationsPackage,
msc1203IMSIConfidentialityPackage **PACKAGE**
BEHAVIOUR
msc1203IMSIConfidentialityBehaviour
BEHAVIOUR DEFINED AS "The securityServiceOrMechanismViolation notification is sent as an imsi confidentiality failure in MSC ; the imsiConfidentialityFailureInMSC will be reported as the security alarm cause. Refer to subclause 6.6.1.8 for further details";
;
ATTRIBUTES
msc1203IMSIConfidentialityFunctionId**GET,**
threshold **GET-REPLACE;**
NOTIFICATIONS
"Rec.X.721:1992".securityServiceOrMechanismViolation
imsiConfidentialityFailureInMSCParameter ;;;
REGISTERED AS {gsm1203managedObjectClass 5};

7.1.6 hlr1203SubscriberIdFunction

hlr1203SubscriberIdFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Rec.X.721:1992":top;
CHARACTERIZED BY
"Rec. M.3100:1992":createDeleteNotificationsPackage,
hlr1203subscriberIdPackage **PACKAGE**
BEHAVIOUR
hlr1203subscriberIdBehaviour
BEHAVIOUR DEFINED AS "The integrityViolation notification is sent as an unkown subscriber in HLR event and the unkownSubscriberInHLR will be reported as the security alarm cause. Refer to subclause 6.6.1.6 for further details";
;
ATTRIBUTES
hlr1203SubscriberIdFunctionId **GET;**
NOTIFICATIONS
"Rec.X.721:1992".integrityViolation
unknownSubscriberInHLRParameter ;;;
REGISTERED AS {gsm1203managedObjectClass 6};

7.1.7 bts1203EncryptionFunction

bts1203EncryptionFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Rec.X.721:1992":top;
CHARACTERIZED BY
"Rec. M.3100:1992":createDeleteNotificationsPackage,
bts1203EncryptionPackage **PACKAGE**
BEHAVIOUR
bts1203EncryptionBehaviour
BEHAVIOUR DEFINED AS "Refer to subclause 6.3.2";
;
ATTRIBUTES
bts1203EncryptionFunctionId **GET,**
algorithmListBTS **GET-REPLACE;;;**
REGISTERED AS {gsm1203managedObjectClass 7};

7.2 Security attributes definitions

7.2.1 authenticationNecessaryWhen

authenticationNecessaryWhen **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.SecurityTriggers;
BEHAVIOUR authenticationNecessaryWhenBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines which MAP procedures shall include authentication. Refer to subclause 6.2.1";;
REGISTERED AS {gsm1203attribute 1};

7.2.2 authenticationRetriedAllowed

authenticationRetriedAllowed **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.AuthenticationRetriedAllowed;
BEHAVIOUR authenticationRetriedAllowedWhenBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines whether the network can retry authentication in case of a TMSI authentication failure. Refer to subclause 6.2.2";;
REGISTERED AS {gsm1203attribute 2};

7.2.3 numberOfAuthenticationVectorsKept

numberOfAuthenticationVectorsKept **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.NumberOfAuthenticationVectorsKept;
BEHAVIOUR numberOfAuthenticationVectorsKeptBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines the number of authentication vectors to be kept in the VLR. Refer to subclause 6.2.3";;
REGISTERED AS {gsm1203attribute 3};

7.2.4 authenticationVectorReuseAllowed

authenticationVectorReuseAllowed **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.AuthenticationVectorReuseAllowed;
BEHAVIOUR authenticationVectorReuseAllowedBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines whether the VLR can reuse authentication vectors. Refer to subclause 6.2.3";;
REGISTERED AS {gsm1203attribute 4};

7.2.5 allocateNewTMSIWhen

allocateNewTMSIWhen **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.SecurityTriggers;
BEHAVIOUR allocateNewTMSIWhenBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines which MAP procedures should include TMSI reallocation. Refer to subclause 6.1.2";;
REGISTERED AS {gsm1203attribute 5};

7.2.6 checkIMEIWhen

checkIMEIWhen **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.SecurityTriggers;
BEHAVIOUR checkIMEIWhenBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines which MAP procedures should include the request of the IMEI. Refer to subclause 6.4.1";;

REGISTERED AS {gsm1203attribute 6};

7.2.7 encryptionControl

encryptionControl **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.EncryptionControl;
BEHAVIOUR encryptionControlBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines whether encryption is not necessary, desirable or mandatory . Refer to subclause 6.3.1";;
REGISTERED AS {gsm1203attribute 7};

7.2.8 algorithmListMSC

algorithmListMSC **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.CipheringAlgorithmList;
BEHAVIOUR algorithmListMSCBehaviour
BEHAVIOUR DEFINED AS
" This attribute defines the list of ciphering algorithms supported by the MSC. Refer to subclause 6.3.2";;
REGISTERED AS {gsm1203attribute 8};

7.2.9 algorithmListBTS

algorithmListBTS **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.CipheringAlgorithmList;
BEHAVIOUR algorithmListBTSBehaviour
BEHAVIOUR DEFINED AS
"This attribute defines the list of ciphering algorithms supported by the BTS. Refer to subclause 6.3.2 ";;
REGISTERED AS {gsm1203attribute 9};

7.2.10 threshold

threshold **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Threshold;
BEHAVIOUR thresholdBehaviour
BEHAVIOUR DEFINED AS
"This attribute controls the generation of alarms. Refer to subclause 6.6.1.8";;
REGISTERED AS {gsm1203attribute 10};

7.2.11 vlr1203AuthenticationFunctionId

vlr1203AuthenticationFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR vlr1203AuthenticationFunctionBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class vlr1203authenticationFunction";;
REGISTERED AS {gsm1203attribute 11};

7.2.12 vlr1203SubscriberIdFunctionId

vlr1203SubscriberIdFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR vlr1203SubscriberIdFunctionIdBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class vlr1203subscriberIdFunction";;
REGISTERED AS {gsm1203attribute 12};

7.2.13 vlr1203EquipmentIdFunctionId

vlr1203EquipmentIdFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR vlr1203EquipmentFunctionIdBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class vlr1203EquipmentIdFunction";;
REGISTERED AS {gsm1203attribute 13};

7.2.14 msc1203EncryptionFunctionId

msc1203EncryptionFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR msc1203EncryptionFunctionIdBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class msc1203EncryptionFunctionId";;
REGISTERED AS {gsm1203attribute 14};

7.2.15 msc1203IMSIConfidentialityFunctionId

msc1203IMSIConfidentialityFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR msc1203IMSIConfidentialityFunctionIdBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class msc1203IMSIConfidentialityFunction";;
REGISTERED AS {gsm1203attribute 15};

7.2.16 hlr1203SubscriberIdFunctionId

hlr1203SubscriberIdFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR hlr1203SubscriberFunctionIdBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class hlr1203subscriberIdFunction";;
REGISTERED AS {gsm1203attribute 16};

7.2.17 bts1203EncryptionFunctionId

bts1203EncryptionFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX GSM1203TypeModule.Identifier;
BEHAVIOUR bts1203EncryptionFunctionIdBehaviour
BEHAVIOUR DEFINED AS
"This ATTRIBUTE is the unique identifier for an instance of the object class bts1203EncryptionFunction";;
REGISTERED AS {gsm1203attribute 17};

7.3 Notifications

The notifications identified for security management are specified by CCITT. They are listed below:

"Recommendation X.721:1992".securityServiceOrMechanismViolation
"Recommendation X.721:1992".integrityViolation
"Recommendation X721:1992".objectCreation
"Recommendation X721:1992".objectDeletion

The latter 2 notifications are contained in the createDeleteNotificationsPackage package defined in CCITT recommendation M.3100 [24].

7.4 Name bindings

7.4.1 vlr1203AuthenticationFunction

vlr1203AuthenticationFunction-vlrFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS vlr1203AuthenticationFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.00 : 1994". vlrFunction;
WITH ATTRIBUTE vlr1203AuthenticationFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 1};

7.4.2 vlr1203SubscriberIdFunction

vlr1203SubscriberIdFunction -vlrFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS vlr1203SubscriberIdFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.00 : 1994". vlrFunction;
WITH ATTRIBUTE vlr1203SubscriberIdFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 2};

7.4.3 vlr1203EquipmentIdFunction

vlr1203EquipmentIdFunction -vlrFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS vlr1203EquipmentIdFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.00 : 1994". vlrFunction;
WITH ATTRIBUTE vlr1203EquipmentIdFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 3};

7.4.4 msc1203EncryptionFunction

msc1203EncryptionFunction mscFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS msc1203EncryptionFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.00 : 1994". mscFunction;
WITH ATTRIBUTE msc1203EncryptionFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 4};

7.4.5 msc1203IMSIConfidentialityFunction

msc1203IMSIConfidentialityFunction -mscFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS msc1203IMSIConfidentialityFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.00 : 1994". mscFunction;
WITH ATTRIBUTE msc1203IMSIConfidentialityFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 5};

7.4.6 hlr1203SubscriberIdFunction

hlr1203SubscriberIdFunction -hlrFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS hlr1203SubscriberIdFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.00 : 1994". hlrFunction;
WITH ATTRIBUTE hlr1203SubscriberIdFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 6};

7.4.7 bts1203EncryptionFunction

bts1203EncryptionFunction -bts **NAME BINDING**
SUBORDINATE OBJECT CLASS bts1203EncryptionFunction;
NAMED BY SUPERIOR OBJECT CLASS "GSM 12.20 : 1994".bts;
WITH ATTRIBUTE bts1203EncryptionFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 7};

7.5 Parameters

7.5.1 authenticationFailureInVLRParameter

authenticationFailureInVLRParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo
WITH SYNTAX GSM1203TypeModule.AuthenticationFailureInVLRSecurityAlarmInfo ; ;

7.5.2 imsiRequestFailureInVLRParameter

imsiRequestFailureInVLRParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo
WITH SYNTAX GSM1203TypeModule.imsiRequestFailureInVLRSecurityAlarmInfo ; ;

7.5.3 imsiRequestFailureInVLRParameter

unknownSuscriberInVLRParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo
WITH SYNTAX GSM1203TypeModule.unknownSubscriberInVLRSecurityAlarmInfo ; ;

7.5.4 imeiCheckViolationInVLRParameter

imeiCheckViolationInVLRParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo
WITH SYNTAX GSM1203TypeModule.imeiCheckViolationInVLRSecurityAlarmInfo ; ;

7.5.5 imeiRequestFailureInVLRParameter

imeiRequestFailureInVLRParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo

WITH SYNTAX GSM1203TypeModule.imeiRequestFailureInVLRSecurityAlarmInfo ; ;

7.5.6 imsiConfidentialityFailureInMSCParameter

imsiConfidentialityFailureInMSCParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo
WITH SYNTAX GSM1203TypeModule. imsiConfidentialityFailureInMSCSecurityAlarmInfo ; ;

7.5.7 imsiConfidentialityFailureInHLRParameter

imsiConfidentialityFailureInHLRParameter **PARAMETER**
CONTEXT Attribute-ASN1Module.SecurityAlarmInfo
WITH SYNTAX GSM1203TypeModule. imsiConfidentialityFailureInHLRSecurityAlarmInfo ; ;

7.6 Abstract syntax definitions

This subclause contains the ASN.1 module defining the attributes syntax referenced by the managed object classes in subclause 7.1.

```
GSM1203TypeModule
        {ccitt (0) identified-organisation (4) etsi (0)
        mobileDomain(0) gsm-Operation-Maintenance(3)
        gsm-12-03(3) informationModel(0) asn1Module(2)
        asn1TypeModule(0) version1(1)}

    DEFINITIONS IMPLICIT TAGS ::=

BEGIN
IMPORTS
IMSI,TMSI,IMEI FROM MAP-CommonDataTypes
        {ccitt (0) identified-organisation (4) etsi (0)
        mobileDomainId(0) gsm-NetworkId(1) moduleId(3)
        map-CommonDataTypes(18) version2(2)}


VlrId FROM GSM1200ATypeModule
        {ccitt (0) identified-organisation (4) etsi (0)
        mobileDomain(0) gsm-Operation-Maintenance(3)
        gsm-12-00(0) annexA(0)informationModel(0) asn1Module(2)
        version1(1)}


gsm-12-03 FROM GSM-DomainDefinitions
        {ccitt(0) identified-organisation (4) etsi(0)
        mobileDomain(0) gsm-Operation-Maintenance(3)
        gsm-12-30(30) informationModel(0) asn1Module(2)
        gsm-OM-DomainDefinitions(0) version1(1)}

SecurityAlarmCause, ManagementExtension, SecurityAlarmInfo FROM Attribute-ASN1Module
        {joint-iso-ccitt ms(9) smi(3) part2(2) asn1Module(2) 1}

-- Object Identifiers


-- Information Model Related Object Identifiers

gsm1203informationModel    OBJECT IDENTIFIER ::=    { gsm-12-03 informationModel(0) }

gsm1203managedObjectClass  OBJECT IDENTIFIER ::=
                                    { gsm1203informationModel managedObjectClass(3) }
gsm1203package             OBJECT IDENTIFIER ::=
```

```
                                { gsm1203informationModel package(4) }
gsm1203nameBinding      OBJECT IDENTIFIER ::=
                                { gsm1203informationModel nameBinding(6) }
gsm1203attribute        OBJECT IDENTIFIER ::=
                                { gsm1203informationModel attribute(7) }
gsm1203notification     OBJECT IDENTIFIER ::=
                                { gsm1203informationModel notification(10) }
```

-- Application Context Related Object Identifiers

```
gsm1203applicationContext       OBJECT IDENTIFIER ::=
        {gsm-12-03 protocolSupport(1) applicationContext(0) gsm-Management(0)}
```

-- 1203 Specific Alarm-related object Identifiers

```
gsm1203standardSpecificExtension        OBJECT IDENTIFIER ::=
        {gsm1203informationModel standardSpecificExtension(0)}

gsm1203securityAlarmCause               OBJECT IDENTIFIER ::=
        {gsm1203standardSpecificExtension gsm1203securityAlarmCause(1) }

gsm1203extendedInformation              OBJECT IDENTIFIER ::=
        {gsm1203standardSpecificExtension gsm1203extendedInformation(2)}

authenticationFailureInVLRSecurityAlarmInformation          OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 1}
imeiCheckViolationInVLRsecurityAlarmInformation             OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 2}
imeiRequestFailureInVLRSecurityAlarmInformation             OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 3}
imsiRequestFailureInVLRSecurityAlarmInformation             OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 4}
unknownSubscriberInVLRSecurityAlarmInformation              OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 5}
unknownSubscriberInHLRSecurityAlarmInformation              OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 6}
unknownSubscriberInAuCHLRSecurityAlarmInformation           OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 7}
imsiConfidentialityFailureInMSCSecurityAlarmInformation     OBJECT IDENTIFIER::=
                                                                {gsm1203extendedInformation 8}
```

-- 12.03 Specific alarm cause related object identifiers

```
authenticationFailureInVLR          SecurityAlarmCause ::=      { gsm1203securityAlarmCause 1}
imeiCheckViolationInVLR             SecurityAlarmCause ::=      { gsm1203securityAlarmCause 2}
imeiRequestFailureInVLR             SecurityAlarmCause ::=      { gsm1203SecurityAlarmCause 3}
imsiRequestFailureInVLR             SecurityAlarmCause ::=      { gsm1203SecurityAlarmCause 4}
unknownSubscriberInVLR              SecurityAlarmCause ::=      { gsm1203securityAlarmCause 5}
unknownSubscriberInHLR              SecurityAlarmCause ::=      { gsm1203securityAlarmCause 6}
unknownSubscriberInAuCHLR           SecurityAlarmCause ::=      { gsm1203securityAlarmCause 7}
imsiConfidentialityFailureInMSC     SecurityAlarmCause ::=      { gsm1203SecurityAlarmCause 8}
```

-- 1203 Specific Type Definitions

--Authentication failure in VLR group begin

```
AuthenticationFailureInVLRAdditionalInformation ::=
        SET OF AuthenticationFailureInVLRManagementExtension

AuthenticationFailureInVLRInformation ::= SEQUENCE    {
```

```
        iMSI                        IMSI,
        iMEI                        IMEI OPTIONAL,
        authenticationFailureType   AuthenticationFailureType,
        locationInfo                LocationInfo}

AuthenticationFailureInVLRManagementExtension ::= ManagementExtension
    ( WITH COMPONENTS
        { identifier (authenticationFailureInVLRSecurityAlarmInformation),
          significance (TRUE),
          information (INCLUDES AuthenticationFailureInVLRInformation)
        }
    )

AuthenticationFailureInVLRSecurityAlarmInfo ::= SecurityAlarmInfo
    ( WITH COMPONENTS
        { securityAlarmCause (authenticationFailureInVLR),
          securityAlarmSeverity,
          securityAlarmDetector,
          serviceUser,
          serviceProvider,
          notificationIdentifier        ABSENT,
          correlatedNotifications   ABSENT,
          additionalText                ABSENT,
          additionalInformation (INCLUDES AuthenticationFailureInVLRAdditionalInformation)
        }
    )
--Authentication failure in VLR group end

AuthenticationRetriedAllowed ::= ENUMERATED {
    disallow    (0),
    allow  (1)  }

AuthenticationFailureType ::= ENUMERATED {
    mismatchedSRES (1),
    missingSRES             (2) }

AuthenticationVectorReuseAllowed ::= ENUMERATED {
    disallow    (0),
    allow  (1)  }

CounterTrigger ::= INTEGER

CipheringAlgorithm ::= ENUMERATED {
    a5_1(1),
    a5_2(2),
    a5_3(3),
    a5_4(4),
    a5_5(5),
    a5_6(6),
    a5_7(7)     }

CipheringAlgorithmList ::= SEQUENCE OF CipheringAlgorithm
-- The reason for this is that at the BTS, one needs an ordered list of algorithms

EncryptionControl ::= ENUMERATED {
    noEncryption                (1),
    encryptionSupported     (2),
    encryptionNecessary     (3)  }

Frequency ::= INTEGER(1..255)
-- 1.. 255 reduced

HlrId ::= GraphicString
```

```
Identifier ::= INTEGER


IMEICheckFailureType ::= ENUMERATED {
        black-listed            (1),
        grey-listed             (2),
        unknown                         (3),
        noResponseFromVLR       (4) }


--Imei check violation in VLR group begin

ImeiCheckViolationInVLRAdditionalInformation ::=
                SET OF ImeiCheckViolationInVLRManagementExtension

ImeiCheckViolationInVLRInformation ::= SEQUENCE {
          iMSI                  IMSI,
          iMEI                  IMEI OPTIONAL,
          iMEICheckFailureType  IMEICheckFailureType,
          locationInfo          LocationInfo }

ImeiCheckViolationInVLRManagementExtension ::= ManagementExtension
        (WITH COMPONENTS
                { identifier (imeiCheckViolationInVLRSecurityAlarmInformation),
                  significance (TRUE),
                  information (INCLUDES ImeiCheckViolationInVLRInformation)
                }
        )

ImeiCheckViolationInVLRSecurityAlarmInfo ::= SecurityAlarmInfo
        ( WITH COMPONENTS
                { securityAlarmCause (imeiCheckViolationInVLR),
                  securityAlarmSeverity,
                  securityAlarmDetector,
                  serviceUser,
                  serviceProvider,
                  notificationIdentifier        ABSENT,
                  correlatedNotifications   ABSENT,
                  additionalText                ABSENT,
                  additionalInformation (INCLUDES ImeiCheckViolationInVLRAdditionalInformation)
                }
        )

--Imei check violation in VLR group end


--Imei request failure in VLR group begin

ImeiRequestFailureInVLRAdditionalInformation ::=
                SET OF ImeiRequestFailureInVLRManagementExtension

ImeiRequestFailureInVLRInformation ::= SEQUENCE {
          iMSI                  IMSI,
          tMSI                  TMSI OPTIONAL,
          locationInfo          LocationInfo }

ImeiRequestFailureInVLRManagementExtension ::= ManagementExtension
        (WITH COMPONENTS
                { identifier (imeiRequestFailureInVLRSecurityAlarmInformation),
                  significance (TRUE),
                  information (INCLUDES ImeiRequestFailureInVLRInformation)
                }
```

```
        )

ImeiRequestFailureInVLRSecurityAlarmInfo ::= SecurityAlarmInfo
        ( WITH COMPONENTS
                { securityAlarmCause (imeiRequestFailureInVLR),
                  securityAlarmSeverity,
                  securityAlarmDetector,
                  serviceUser,
                  serviceProvider,
                  notificationIdentifier          ABSENT,
                  correlatedNotifications   ABSENT,
                  additionalText                  ABSENT,
                  additionalInformation (INCLUDES ImeiRequestFailureInVLRAdditionalInformation)
                }
        )
```

--Imei request failure in VLR group end

--Imsi confidentiality failure in MSC group begin

```
ImsiConfidentialityFailureInMSCAdditionalInformation ::=
                SET OF ImsiConfidentialityFailureInMSCManagementExtension

ImsiConfidentialityFailureInMSCInformation ::= SEQUENCE { }
--If no useful information can be supplied, this attribute will be deleted

ImsiConfidentialityFailureInMSCManagementExtension ::= ManagementExtension
        ( WITH COMPONENTS
                { identifier (imsiConfidentialityFailureInMSCSecurityAlarmInformation),
                  significance (FALSE),
                  information ABSENT
                }
        )

ImsiConfidentialityFailureInMSCSecurityAlarmInfo ::= SecurityAlarmInfo
        ( WITH COMPONENTS
                { securityAlarmCause (ImsiConfidentialityFailureInMSC),
                  securityAlarmSeverity,
                  securityAlarmDetector,
                  serviceUser,
                  serviceProvider,
                  notificationIdentifier          ABSENT,
                  correlatedNotifications   ABSENT,
                  additionalText                  ABSENT,
                  additionalInformation (INCLUDES ImsiConfidentialityFailureInMSCAdditionalInformation)
                }
        )
```

-Imsi confidentiality failure in MSC group end

--Imsi request failure in VLR group begin

```
ImsiRequestFailureInVLRAdditionalInformation ::=
                SET OF ImsiRequestFailureInVLRManagementExtension

ImsiRequestFailureInVLRInformation ::= SEQUENCE {
          tMSI                  TMSI OPTIONAL,
          locationInfo          LocationInfo }

ImsiRequestFailureInVLRManagementExtension ::= ManagementExtension
        (WITH COMPONENTS
```

```
                { identifier (imsiRequestFailureInVLRSecurityAlarmInformation),
                  significance (TRUE),
                  information (INCLUDES ImsiRequestFailureInVLRInformation)
                }
        )

ImsiRequestFailureInVLRSecurityAlarmInfo ::= SecurityAlarmInfo
        ( WITH COMPONENTS
                { securityAlarmCause (imsiRequestFailureInVLR),
                  securityAlarmSeverity,
                  securityAlarmDetector,
                  serviceUser,
                  serviceProvider,
                  notificationIdentifier          ABSENT,
                  correlatedNotifications   ABSENT,
                  additionalText                  ABSENT,
                  additionalInformation (INCLUDES ImsiRequestFailureInVLRAdditionalInformation)
                }
        )

--Imsi request failure in VLR group end


LocationInfo ::= OCTET STRING (SIZE(2..5))

NumberOfAuthenticationVectorsKept ::= INTEGER(0..65535)

ResetInterval ::= INTEGER(0..65535)
-- time interval in minutes
-- 0 means “infinite”

SecurityTriggers ::= ResetInterval

SubscriberType ::= INTEGER(1..16)
-- homePlmnSubscriber   ::=1
-- visitingSubscriber        ::=2

SubscriberTypeSecurityTriggers ::= SEQUENCE {
                subscriberType          SubscriberType,
                triggerCondition        TriggerCondition }
--each TriggerEvent is , per subscriber type, occuring at most once in the triggerCondition

Threshold ::= SEQUENCE {
                thresholdFrequency      Frequency,
                thresholdCounter        CounterTrigger,
                resetInterval           ResetInterval}
                resetInterval           GeneralizedTime }

TriggerCondition ::= SEQUENCE {
                triggerEvents       TriggerEvents,
                frequency    Frequency }

TriggerEvent ::= INTEGER {
                locationUpdateNewVlr                    (1),
                locationUpdateSameVlr           (2),
                periodicLocationUpdate          (3),
                mobileOriginatingCall                   (4),
                mobileOriginatingCallReestablishment(5),
                mobileTerminatingCall                   (6),
                supplementaryServiceUsage       (7),
                shortMessageServiceMobileOriginating    (8),
                shortMessageServiceMobileTerminating    (9),
                accessViaIMSI                           (10),
```

```
        imsiAttach                                  (11),
        emergencyCall                               (12)    }

TriggerEvents ::= SET OF TriggerEvent


--Unknown subscriber in AuC(HLR) group begin

UnknownSubscriberInAuCHLRAdditionalInformation ::=
        SET OF UnknownSubscriberInAuCHLRManagementExtension

UnknownSubscriberInAuCHLRInformation ::= SEQUENCE {
    iMSI        IMSI }

UnknownSubscriberInAuCHLRManagementExtension ::= ManagementExtension
    (WITH COMPONENTS
        { identifier (unknownSubscriberInAuCHLRSecurityAlarmInformation),
          significance (TRUE),
          information (INCLUDES UnknownSubscriberInAuCHLRInformation)
        }
    )

UnknownSubscriberInAUCSecurityAlarmInfo ::= SecurityAlarmInfo
    ( WITH COMPONENTS
        { securityAlarmCause (unknownSubscriberInAuCHLR),
          securityAlarmSeverity,
          securityAlarmDetector,
          serviceUser,
          serviceProvider,
          notificationIdentifier        ABSENT,
          correlatedNotifications   ABSENT,
          additionalText                ABSENT,
          additionalInformation (INCLUDES UnknownSubscriberInAuCHLRAdditionalInformation)
        }
    )

--Unknown subscriber in AuC(HLR) group end


--Unknown subscriber in HLR group begin

UnknownSubscriberInHLRAdditionalInformation ::=
        SET OF UnknownSubscriberInHLRManagementExtension

UnknownSubscriberInHLRInformation ::= SEQUENCE {
    iMSI            IMSI,
    vLRIdentity   VlrId }

UnknownSubscriberInHLRManagementExtension ::= ManagementExtension
    ( WITH COMPONENTS
        { identifier (unknownSubscriberInHLRSecurityAlarmInformation),
          significance (TRUE),
          information (INCLUDES UnknownSubscriberInHLRInformation)
        }
    )

UnknownSubscriberInHLRSecurityAlarmInfo ::= SecurityAlarmInfo
    ( WITH COMPONENTS
        { securityAlarmCause (unknownSubscriberInHLR),
          securityAlarmSeverity,
          securityAlarmDetector,
          serviceUser,
          serviceProvider,
```

```
                notificationIdentifier          ABSENT,
                correlatedNotifications   ABSENT,
                additionalText                  ABSENT,
                additionalInformation (INCLUDES UnknownSubscriberInHLRAdditionalInformation)
              }
        )
```

--Unknown subscriber in HLR group end

--Unknown subscriber in VLR group begin

```
UnknownSubscriberInVLRAdditionalInformation ::=
              SET OF UnknownSubscriberInVLRManagementExtension

UnknownSubscriberInVLRInformation ::= SEQUENCE {
        iMSI                    IMSI,
        hLRIdentity   HlrId,
        locationInfo  LocationInfo }

UnknownSubscriberInVLRManagementExtension ::= ManagementExtension
        (WITH COMPONENTS
              { identifier (unknownSubscriberInVLRSecurityAlarmInformation),
                significance (TRUE),
                information (INCLUDES UnknownSubscriberInVLRInformation)
              }
        )

UnknownSubscriberInVLRSecurityAlarmInfo ::= SecurityAlarmInfo
        ( WITH COMPONENTS
              { securityAlarmCause (unknownSubscriberInVLR),
                securityAlarmSeverity,
                securityAlarmDetector,
                serviceUser,
                serviceProvider,
                notificationIdentifier          ABSENT,
                correlatedNotifications   ABSENT,
                additionalText                  ABSENT,
                additionalInformation (INCLUDES UnknownSubscriberInVLRAdditionalInformation)
              }
        )
```

--Unknown subscriber in VLR group end

-- Security measurement related types

```
GSMSecurityMeasurementFunctionId ::= INTEGER
GSMMeasurementType1 ::= INTEGER

END -- End of GSM1203TypeModule module --
```

7.7 Application contexts

The application context name of the GSM 12.03 application context shall have the following object identifier value:

{gsm-OM-DomainId gsm-12-03(3) protocolSupport(1) applicationContext(0) gsm-Management(0) }

and the following object descriptor value:

“gsm 12.03 management application context”

The object identifier gsm-OM-DomainId is defined in the ETR GSM 12.30 [25]

Annex A (normative): Relation between the authentication and encryption attributes

Due to the fact that authentication and encryption are correlated, and that several caching and reuse mechanisms (CKSN, authentication set reuse) exist, care should be taken when setting the attributes used in the management of authentication and encryption.

This annex describes the relation between the attributes encryptionControl and authenticationNecessaryWhen, used in the management of authentication and encryption respectively.

The management of authentication comprises for every CM service type and LU type the following options:

- off (i.e. authentication not necessary);
- on (i.e. authentication mandatory).

If abstracted from the differentiation according to CM service/LU type and user classes, the following options exist for the management of authentication and encryption:

encryption:

- off (encryptionControl = noEncryption(1))
- on where possible (encryptionControl = encryptionSupported(2))
- necessary (encryptionControl = encryptionNecessary(3))

authentication:

- off (authenticationNecessaryWhen = 0.
  This is a relevant factor since securityTrigger in the attribute authenticationNecessaryWhen is not present).
- on (authenticationNecessaryWhen = 1.
  This is the relevant factor since securityTrigger in the attribute authenticationNecessaryWhen is present).

These parameters allow 6 combinations, the effects of which are discussed in table A.1

Table A.1

	authentication on	**authentication off**
encryption off	authentication set reuse is not recommended (security breach by masquerade)	no protection mechanism is active
encryption on where possible	if possible (note 2) :maximum security level; else: same as encryption off	if possible: same as encryption necessary; else: same as encryption off
encryption necessary	maximum security level; however calls, including emergency calls will be rejected in case of incompatible encryption algorithms (note 3) .	(nearly (note 4)) maximum security level; however the call will fail in case of problems with the CKSN (notes 5, 6, and 7)

NOTE 1: (omitted in the table above) a change in the value of encryptionManagement affects all MAP procedures and has to be checked against all the (possibly different) settings of the authenticationNecessaryWhen attribute for all CM service/LU types procedures. The interaction between the various attributes is illustrated in the flowchart below (Ommitting the distinction between service type, subscriber class and type):

NOTE 2: “Not possible” means:

- incompatible encryption algorithms, or
- HANDOVER FAILURE with error cause “Ciphering Algorithm not supported” from BSS to MSC (in this case, the MSC may decide, depending on other considerations to continue in unencrypted mode or to clear the call, reference GSM 08.08 [22]), or
- CIPHER MODE REJECT with error cause “Ciphering algorithm not supported” from BSS to MSC (reference GSM 08.08 [22]).

In all those cases, the MSC may decide to clear the call or not.

The case where the CKSN is undefined (value “no key available” for CKSN in PAGING RESPONSE and various MM messages, reference GSM 04.08 [4]) or has a value different from that stored in the MSC/VLR is not(!) considered as “not possible”, as is would allow an intruder to disable encryption by simply setting this value to “no key available”. In this case, authentication shall always be performed if encryption is wanted (reference Subclause 6.3.1).

NOTE 3: A5/1 only mobile (e.g. Phase 1) in A5/2 network.

NOTE 4: In this case, an intruder may use an SRES obtained by scanning the air interface. However this will to put him in a position to decrypt the data exchanged subsequently over the air interface as he still will not know the Ki or the encryption key. This means that he still is not able to get any reasonable service, nor will he be able to get any protected information.

NOTE 5: “problems with CKSN” means:

The CKSN in the network and in the mobile have the same value but refer to different RAND values respectively so that encryption starts with different keys in the network and the mobile

NOTE 6: In this case, authentication depends on the availability of a valid CKSN in the mobile. If no valid CKSN is available in the mobile, then authentication shall be performed (reference Subclause 6.2.1).

NOTE 7: It should be kept in mind that a change in the value of encryptionControl affects all MAP procedures whereas authenticationNecessaryWhen has individual settings for every CM service/LU type procedure.

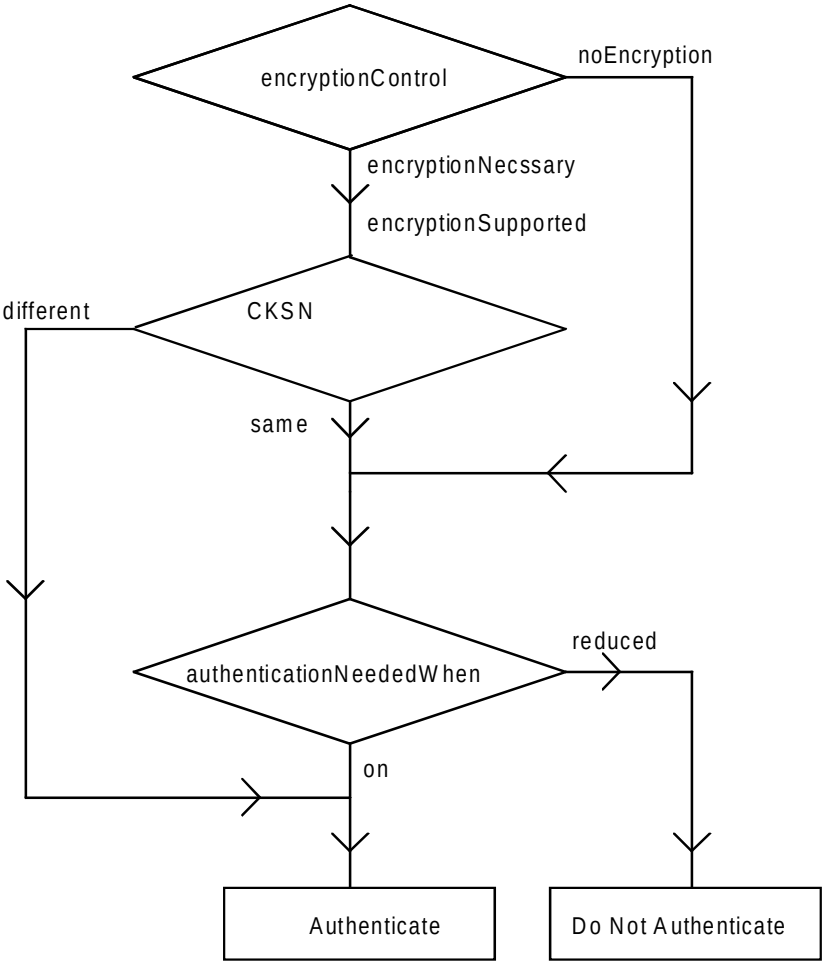
encryptionControl
noEncryption
encryptionNecssary
encryptionSupported
different
CKSN
same
authenticationNeededWhen
reduced
on
Authenticate
Do Not Authenticate

Figure A.1

Annex B (normative): Additional security counters

Following is the template used to describe the security measurements contained in this annex. It is the same template as used in GSM TS 12.04 [10] annex B.

A. Description
A short explanation of the measurement operation.

B. Collection Method
The form in which this measurement data is obtained:
- CC (Cumulative Counter)

C. Condition
The GSM condition which causes this measurement to be updated. Where it is not possible to give a precise GSM condition, then the conditional circumstances leading to the update are stated.

D. Measurement Attribute Name
The Measurement Attribute Name which will be referenced by the Object Model

E. Measurement Result
A short description of expected result value (e.g. a single integer value)

F. Measurement Function Name
Measurement Function Name for which this measurement is defined

B.1 MSC security measurement function

B.1.1 Encrypted connection used

A. This measurement counts the number of times that encryption has been used on the air interface.

NOTE: This may be multiple times per connection.

B. CC

C. Receipt of “MAP_SET_CIPHERING_MODE” service indication from VLR with parameter “Ciphering mode” set to any other value than “no encryption” (09.02)

D. encryptedConnectionUsed

E. A single integer value

F. MSC Security Measurement Function

B.1.2 Unencrypted connection used

A. This measurement counts the number of times that no encryption has been used on the air interface

NOTE: This may be multiple times per connection.

B. CC

C. Receipt of “MAP_SET_CIPHERING_MODE” service indication from VLR with parameter “Ciphering mode” set to “no encryption” (09.02)

D. unencryptedConnectionUsed

E. A single integer value

F. MSC Security Measurement Function

B.1.3 Connection to be Cleared Due to Incompatible Encryption

A. This measurement provides the number of connections released due to incompatible encryption algorithms

B. CC

C. Receipt of 'Cipher Mode Reject' message with cause 'ciphering algorithm not supported' from the BSS when encryption is required

D. callClearedIncompatibleEncryption

E. A single integer value

F. MSC Security Measurement Function

B.2 VLR Security Function

B.2.1 Authentication Vectors Unavailable

A. This counter counts the unsuccessful authentications due to no authentication vectors available at the VLR (neither locally nor from the AuC).

B. CC

C. Internal function of the VLR: inability to perform authentication because no authentication vectors are available (neither locally nor from the AuC) and thus authentication is not possible

D. authVectorsUnavailable

E. A single integer value

F. VLR Security Measurement Function

B.2.2 Subscriber unknown in HLR(VLR)

A. This measurement counts the number of times a request for subscriber data from the HLR is unsuccessful because the subscriber is unknown in the HLR.

B. CC

C. Receipt of a MAP_UPDATE_LOCATION service confirmation with a "user error " parameter equal to "Unknown Subscriber"

D. subsUnknownInHLRFromVlr

E. A single integer value

F. VLR Security Measurement FunctionLR Security Measurement Function

B.3 HLR Security Function

B.3.1 Subscriber Unknown in HLR

A. Request for subscriber data from HLR is unsuccessful because the subscriber is unknown in the HLR.

B. CC

C. Transmission of a MAP_UPDATE_LOCATION service response with a “user error “ parameter equal to “Unknown Subscriber”

D. subsUnknownInHlr

E. A single integer value

F. HLR Security Measurement Function

B.3.2 Subscriber Unknown in AuC(HLR)

A. Request for subscriber data from HLR is unsuccessful because the subscriber is unknown in the AuC(HLR).

B. CC

C. Transmission of a MAP_SEND_AUTHENTICATION_INFO service confirmation with a “user error” parameter equal to “Unknown Subscriber”

D. subsUnknownInAuC

E. A single integer value

F. HLR Security Measurement Function

Annex C (normative): Security measurement Object Model

This Annex to GSM 12.03 comprises the Object Model for Security Measurements to complement the high level Object Model in GSM 12.00 [6]. The Object Model is similar as the Object Model for Performance Measurement as provided in GSM 12.04 [10].

The whole management approach defined in GSM 12.00 [6]defines all entities of GSM network as managed functions These are BSS, BSS, MSC, HLR etc. and one or more of these can be contained in a managed element and each of these functions can obtain its own security measurement function.

C.1 Model structure and content

The following security measurement function model takes its basis from the proposed GSM 12.00 [6] high level object model and the performance measurement object model in GSM 12.04 [10].

Figure C.1 shows the containment tree of all the measurement Object Classes. The formal GDMO definitions of the 12.03 specific Managed Object Classes concerning security measurement functions are described in this clause. For the Object Classes log, efd and simpleScanner, see GSM 12.04 [10] annex C.

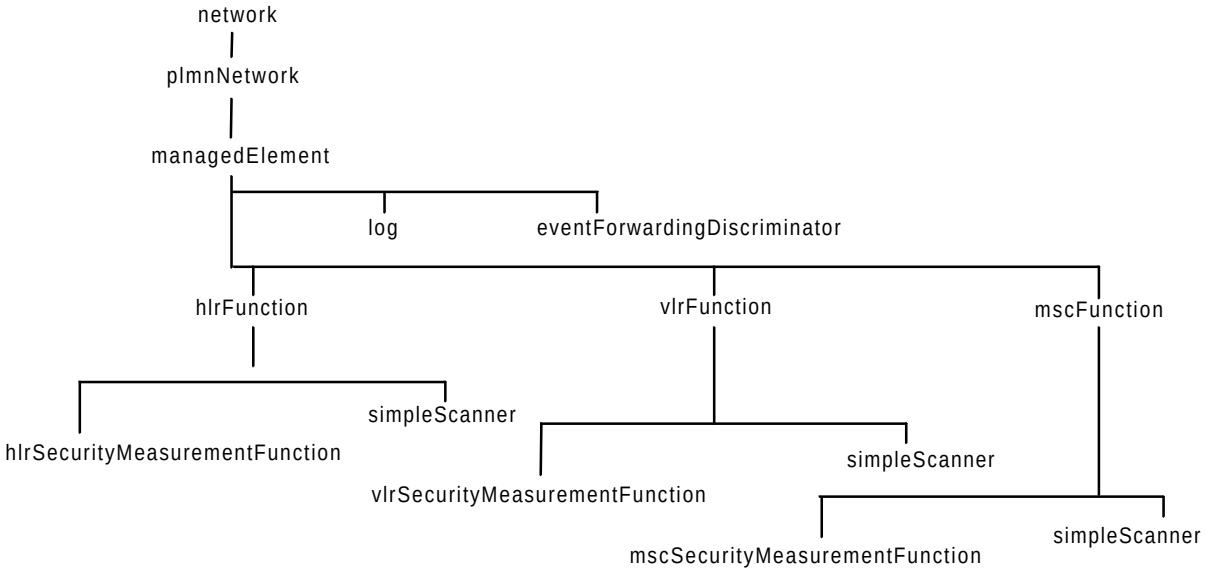

Figure C.1: GSM 12.03 Security Measurement Object Class Containment

C.2 Security measurement managed object classes

C.2.1 mscSecurityMeasurementFunction

mscSecurityMeasurementFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Recommendation X.721:1992":top;
CHARACTERIZED BY
basicSecurityMeasurementFunctionPackage;
CONDITIONAL PACKAGES
encryptedConnectionPackage **PRESENT IF** "an instance supports it" ,
incompatibleEncryptionPackage **PRESENT IF** "an instance supports it" ;
REGISTERED AS {gsm1203managedObjectClass 110};

C.2.2 vlrSecurityMeasurementFunction

vlrSecurityMeasurementFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Recommendation X.721:1992":top;
CHARACTERIZED BY
basicSecurityMeasurementFunctionPackage;
CONDITIONAL PACKAGES
authenticationVectorsUnavailablePackage **PRESENT IF** "an instance supports it" ,
unknownSubscriberInHlrFromVlrPackage **PRESENT IF** "an instance supports it" ;
REGISTERED AS {gsm1203managedObjectClass 120};

C.2.3 hlrSecurityMeasurementFunction

hlrSecurityMeasurementFunction **MANAGED OBJECT CLASS**
DERIVED FROM
"Recommendation X.721:1992":top;
CHARACTERIZED BY
basicSecurityMeasurementFunctionPackage;
CONDITIONAL PACKAGES
unknownSubscriberInHlrPackage **PRESENT IF** "an instance supports it" ,
unknownSubscriberInAucPackage **PRESENT IF** "an instance supports it" ;
REGISTERED AS {gsm1203managedObjectClass 130};

C.3 Security measurement package definitions

The following describes the individual security measurements defined GSM 12.03, Annex B, as packages of attributes to be referenced by the appropriate managed object class.

C.3.1 General Security Measurement Function Packages

C.3.1.1 basicSecurityMeasurementFunctionPackage

basicSecurityMeasurementFunctionPackage **PACKAGE**
BEHAVIOUR
generalSecurityMeasurementFunctionBehaviour;
ATTRIBUTES
securityMeasurementFunctionId **GET;**
NOTIFICATIONS
"Recommendation X.721:1992":objectCreation,
"Recommendation X.721:1992":objectDeletion;
REGISTERED AS {gsm1203package 100};

C.3.2 MSC Security Measurement Function Packages

C.3.2.1 encryptedConnectionPackage

encryptedConnectionPackage **PACKAGE**
BEHAVIOUR
generalSecurityMeasurementPackageBehaviour;
ATTRIBUTES
encryptedConnectionUsed **GET,**
unencryptedConnectionUsed **GET;**
REGISTERED AS {gsm1203package 111};

C.3.2.2 incompatibleEncryptionPackage

incompatibleEncryptionPackage P**ACKAGE**
BEHAVIOUR
generalSecurityMeasurementPackageBehaviour;
ATTRIBUTES
callClearedIncompatibleEncryption **GET;**
REGISTERED AS {gsm1203package 112};

C.3.3 VLR Security Measurement Function Packages

C.3.3.1 authenticationVectorsUnavailablePackage

authenticationVectorsUnavailablePackage **PACKAGE**
BEHAVIOUR
generalSecurityMeasurementPackageBehaviour;
ATTRIBUTES
authVectorsUnavailable **GET;**
REGISTERED AS {gsm1203package 121};

C.3.3.2 unknownSubscriberInHlrFromVlrPackage

unknownSubscriberInHlrFromVlrPackage **PACKAGE**
BEHAVIOUR
generalSecurityMeasurementPackageBehaviour;
ATTRIBUTES
subsUnknownInHlrFromVlr **GET;**
REGISTERED AS {gsm1203package 122};

C.3.4 HLR Security Measurement Function Packages

C.3.4.1 unknownSubscriberInHlrPackage

unknownSubscriberInHlrFromVlrPackage **PACKAGE**
BEHAVIOUR
generalSecurityMeasurementPackageBehaviour;
ATTRIBUTES
subsUnknownInHlr **GET;**
REGISTERED AS {gsm1203package 131};

C.3.4.2 unknownSubscriberInAucPackage

unknownSubscriberInAucPackage **PACKAGE**
BEHAVIOUR
generalSecurityMeasurementPackageBehaviour;
ATTRIBUTES
subsUnknownInAuc **GET;**
REGISTERED AS {gsm1203package 132};

C.4 Security measurement attribute definitions

C.4.1 General Security Measurement Function Related Attributes

C.4.1.1 securityMeasurementFunctionId

securityMeasurementFunctionId **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMSecurityMeasurementFunctionId;
BEHAVIOUR
securityMeasurementFunctionIdBehaviour;
REGISTERED AS {gsm1203attribute 101};

securityMeasurementFunctionIdBehaviour **BEHAVIOUR**
DEFINED AS
"This is the identity of the security measurement function";

C.4.2 MSC Security Measurement Function Related Attributes

C.4.2.1 encryptedConnectionUsed

encryptedConnectionUsed **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 111};

C.4.2.2 unencryptedConnectionUsed

unencryptedConnectionUsed **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 112};

C.4.2.3 callClearedIncompatibleEncryption

callClearedIncompatibleEncryption **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 113};

C.4.3 VLR Security Measurement Function Related Attributes

C.4.3.1 authVectorsUnavailable

authVectorsUnavailable **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 121};

C.4.3.2 subsUnknownInHlrFromVlr

subsUnknownInHlrFromVlr **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 122};

C.4.4 HLR Security Measurement Function Related Attributes

C.4.4.1 subsUnknownInHlr

subsUnknownInHlr **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 131};

C.4.4.2 subsUnknownInAuc

subsUnknownInAuc **ATTRIBUTE**
WITH ATTRIBUTE SYNTAX
GSM1203TypeModule.GSMMeasurementType1;
BEHAVIOUR
generalSecurityMeasurementAttributeBehaviour;
REGISTERED AS {gsm1203attribute 132};

C.5 Security measurement name bindings

C.5.1 MSC Name Binding

C.5.1.1 mscSecurityMeasurementFunction-"gsm1200:1993":mscFunction

mscSecurityMeasurementFunction-"gsm1200:1993":mscFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS mscSecurityMeasurementFunction
NAMED BY SUBORDINATE OBJECT CLASS "gsm1200:1993":mscFunction;
WITH ATTRIBUTE securityMeasurementFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 111};

C.5.2 VLR Name Binding

C.5.2.1 vlrSecurityMeasurementFunction-"gsm1200:1993":vlrFunction

vlrSecurityMeasurementFunction-"gsm1200:1993":vlrFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS vlrSecurityMeasurementFunction
NAMED BY SUBORDINATE OBJECT CLASS "gsm1200:1993":vlrFunction;
WITH ATTRIBUTE securityMeasurementFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 121};

C.5.3 HLR Name Binding

C.5.3.1 hlrSecurityMeasurementFunction-"gsm1200:1993":hlrFunction

hlrSecurityMeasurementFunction-"gsm1200:1993":hlrFunction **NAME BINDING**
SUBORDINATE OBJECT CLASS hlrSecurityMeasurementFunction
NAMED BY SUBORDINATE OBJECT CLASS "gsm1200:1993":hlrFunction;
WITH ATTRIBUTE securityMeasurementFunctionId;
CREATE;
DELETE;
REGISTERED AS {gsm1203nameBinding 131};

C.6 Security measurement behaviour definitions

C.6.1 general security measurement function behaviour

generalSecurityMeasurementFunctionBehaviour **BEHAVIOUR**

DEFINED AS

"This object is defined to contain the various optional security measurement packages, and one or more instances of this class may exist in the scope of the containing object. A scanner may scan the attributes of the object class in various combinations and permutations of packages, and further may scan simultaneously as many times as necessary within the processing limits of the network." ;

C.6.2 general security measurement package behaviour

generalSecurityMeasurementPackageBehaviour **BEHAVIOUR**

DEFINED AS

"This package provides a grouping of related measurement attributes. If it is required to have multiple appearances of these attributes, multiple object instances must be created. The simple scanner has been designed to read the values of the attributes according to a given schedule." ;

C.6.3 general security measurement attribute behaviour

generalSecurityMeasurementAttributeBehaviour **BEHAVIOUR**

DEFINED AS

"The security measurement that corresponds to this attribute, is described in Annex B. The name of this attribute is given in the description part (D) of each security measurement definition contained in Annex B." ;

C.7 Security measurement abstract syntax definitions

All abstract syntax definitions for the security measurement object model are provided in subclause 7.5.

The abstract syntax definitions required for the security measurement object model comprise:

- Object Identifier values for the registered objects
- definition of GSMMeasurementType1 as an INTEGER

Annex D (informative): Index

A3, 11; 12; 13
A5, 11; 12; 41
A8, 11; 12; 13
algorithmListBTS, 18; 25; 27
algorithmListMSC, 18; 24; 27
allocateNewTMSIWhen, 16; 23; 26
AuC, 11; 12; 17; 19; 20; 21; 37; 44; 45
Authentication Failure in VLR, 20
authenticationNecessaryWhen, 16; 23; 26; 40; 41
authenticationRetriedAllowed, 16; 23; 26
authenticationVectorReuseAllowed, 17; 23; 26
authVectorsUnavailable, 44; 48; 49

BCCH, 11; 15
BSC, 11; 17
BSS, 11; 12; 17; 18; 41; 46
BTS, 11; 12; 17; 18; 27; 33
bts1203EncryptionFunction, 25; 28; 30; 31
bts1203EncryptionFunctionId, 25; 28; 30

callClearedIncompatibleEncryption, 44; 48; 49
checkIMEIWhen, 18; 24; 27
CKSN, 11; 13; 16; 40; 41; 42
CM, 11; 15; 40; 41

EIR, 11; 13; 18; 20
encryptedConnectionUsed, 43; 48; 49
encryptionControl, 17; 24; 27; 40; 41; 42

GDMO, 11; 46

HLR, 11; 17; 19; 20; 21; 25; 37; 38; 44; 45; 46; 48; 50; 51
hlr1203SubscriberIdFunction, 25; 30
hlr1203SubscriberIdFunctionId, 25; 28; 30
hlrSecurityMeasurementFunction, 47; 51

IMEI, 7; 11; 13; 14; 18; 19; 20; 27; 31; 33; 34
IMEI Check Violation in VLR, 20
IMEI Request Failure in VLR, 20
IMSI, 7; 11; 12; 13; 15; 16; 18; 19; 20; 21; 31; 33; 34; 37; 38
IMSI Confidentiality Failure In MSC, 21
IMSI Request Failure in VLR, 21

Kc, 7; 11; 13; 17
Ki, 11; 13; 17; 41

LU, 11; 15; 40; 41

MAP, 11; 12; 13; 15; 16; 17; 18; 26; 27; 31; 41; 43; 44; 45
ME, 11; 12; 13; 17; 18
MM, 11; 16; 18; 41
MO, 11; 15
MOC, 11
MS, 11; 12; 15; 16; 17; 19; 20; 21
MSC, 11; 12; 16; 17; 18; 19; 21; 25; 27; 35; 41; 43; 44; 46; 48; 49; 51
msc1203EncryptionFunction, 24; 29
msc1203EncryptionFunctionId, 24; 28; 29
msc1203IMSIConfidentialityFunction, 25; 28; 30
msc1203IMSIConfidentialityFunctionId, 25; 28; 30
mscSecurityMeasurementFunction, 47; 51
MT, 11; 15

NE, 11; 20
numberOfAuthenticationVectorsKept, 17; 23; 26

OS, 11; 18; 20

PLMN, 7; 9; 11; 12; 13; 14; 16

RAND, 7; 11; 13; 17; 41

securityMeasurementFunctionId, 47; 49; 51
SIM, 11; 12; 13
SMS, 11; 15
SRES, 7; 11; 17; 18; 20; 41
SS, 11; 15
subsUnknownInAuc, 48; 50
subsUnknownInHlr, 45; 48; 50
subsUnknownInHlrFromVlr, 48; 50

threshold, 14; 15; 21; 25; 27
TMN, 11; 13
TMSI, 7; 11; 12; 14; 15; 16; 18; 19; 20; 21; 26; 31; 34; 36

unencryptedConnectionUsed, 43; 48; 49
Unknown Subscriber in AuC(HLR), 21
Unknown Subscriber in HLR, 21
Unknown Subscriber in HLR(VLR), 21

VLR, 11; 12; 15; 16; 17; 18; 19; 20; 21; 23; 24;
26; 33; 34; 35; 36; 38; 41; 43; 44; 48; 49; 51
vlr1203AuthenticationFunction, 16; 17; 23; 29
vlr1203AuthenticationFunctionId, 23; 27; 29
vlr1203EquipmentIdFunction, 24; 28; 29
vlr1203EquipmentIdFunctionId, 24; 28; 29
vlr1203SubscriberIdFunction, 16; 23; 29
vlr1203SubscriberIdFunctionId, 23; 28; 29
vlrSecurityMeasurementFunction, 47; 51

History

Document history		
July 1995	Public Enquiry	PE 88: 1995-07-24 to 1995-11-17
March 1996	Vote	V 100: 1996-03-25 to 1996-05-17