3GPP TSG SA WG3 Security — S3#32 **S3-040007**
09 - 13 February 2004
Edinburgh, Scotland, UK

3GPP TSG-SA5 (Telecom Management) **S5-037280**
Meeting #36, Shanghai, CHINA, 17 - 21 Nov 2003

Title: LS to SA3 about SA5 Security Requirements
Response to: ---
Release: Release 6
Work Item: SA5 SWGC WT01 - Security

Source: SA5
To: SA3
Cc:

Contact Person:
Name: John ISLIP (Lucent Technologies)
Tel. Number: +44 1793 883931
E-mail Address: islip@lucent.com

Attachments: S5-036785 Draft TS 32.371 V0.0.1 (2003-07)
WT01 Security Management Concepts and Requirements
(*This draft TS is undergoing review and as such is work in progress*)

S5-037227 Security Matrices
(*This document would replace clauses 6 &7 of the "Security Management Concepts and Requirements TS draft*)

---

1. Overall Description:

SA5 wishes to inform SA3 of work being done with respect to the security requirements for IRPs (Integration Reference Points) used on the Itf-N.

As part of the Security Management work task SA5 OAM-NIM WT01, SA5 have produced a draft TS on "Security management concepts and requirements" which is referenced in the in the attachments section of this LS.

2. Work Task Description:

Justification

The 3G Mobile Network is a system that is sensitive to fraud behaviour and contain high sensitive data that is fundamental to the correct operation of the Mobile Network, including sensitive information about subscribers. In the context of managing a 3G Mobile Network, the Management will inter-exchange sensitive data between the management system and the mobile network.

Despite the possibilities for fraudulent attacks on the operation of Mobile Networks, the current 3G Management System of the 3G Mobile Network does not specify the security features. These Security features are required to allow secure access and protect sensitive data in the interaction between the 3G Management System and the 3G Mobile Network. Some basic capabilities such as Authentication, Authorization and/or Encryption are currently missing.

Objective

The objective of this work item is to enhance the 3GPP specified 3G Management System to ensure secure access and data protection throughout the OAM network. The following security features shall be applied:

- **Authentication**
  A capability that allows the IRP Agent to determine if the IRP Manager is the user it claims to be.
- **Authorization**
  A capability that allows the IRP Agent to determine if the authenticated IRP Manager has the right to manage (e.g., read/write Managed Objects attributes, obtain network alarm information) part or all of the managed network.
- **Integrity**
  IRP Managers and IRP Agents exchange network management (NM) messages. The Integrity is a capability that allows the NM message receiving entity to validate (a) if the received NM messages have not been unauthorized modified and (b) the originator of the received NM message.
- **Confidentiality**
  A capability that ensures only the intended NM message recipient (e.g., IRP Manager, IRP Agent) can read the message. In other words, non-intended recipient of a NM message will not be able to read/decode the intercepted NM message.

3. Actions:

To SA3.

ACTION:

1. SA5 asks SA3 to review and provide comments on the attached documents.
2. Is there a possibility that SA5 can re-use any of the work done by SA3 ?
3. Does SA3 think that the SA5 WT is an overlap of any of the SA3 WTs ?

4. Date of Next SA5 Meetings:

3GPPSA5#36-Bis	WG	12 - 16 Jan 2004	Vancouver	Canada
3GPPSA5#37	WG	23 - 27 Feb 2004	Malaga	ES
3GPPSA5#37-Bis	WG	29 Mar - 2 Apr 2004	Sophia Antipolis	FR
3GPPSA5#38	WG	10 - 14 May 2004	Beijing	CN
3GPPSA5#38-bis	WG	28 Jun - 2 Jul 2004	Sophia Antipolis	FR

3GPP TS 32.xx1 V0.0.1 (2003-07)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication Management; Security Management: Security Management: Concepts and Requirements; (Release 6)

Keywords
Security Management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

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

The present document is part 1 of a multi-part TS covering the 3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Telecommunication Management; Security Management, as identified below:

TS 32.xx1: "Security Management **Integration Reference Point: Requirements**";

TS 32.xx2 "Security Management Integration Reference Point: Information Service";

TS 32.xx3: "Security Management Integration Reference Point: CORBA Solution Set";

TS 32.xx4: "Security Management Integration Reference Point: CMIP Solution Set".

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

In 3GPP SA5 context, IRPs are introduced to address process interfaces at the Itf-N interface. The Itf-N interface is built up by a number of Integration Reference Points (IRPs) and a related Name Convention, which realise the functional capabilities over this interface. The basic structure of the IRPs is defined in 3GPP TS 32.101 [1] and 3GPP TS 32.102 [2]. IRP consists of IRPManager and IRPAgent. Usually there are three types of transaction between IRPManager and IRPAgent, which are operation invocation, notification, and file transfer.

However, there are different types of intentional threats against the transaction between IRPManagers and IRPAgents. All the threats are potential risks of damage or degradation of telecommunication services, which operators should take measures to reduce or eliminate to secure the telecommunication service, network, and data.

By introducing Security Management, this document describes security requirements to relieve the threats between IRPManagers and IRPAgents.

As described in 3GPP TS 32.101 "3G Telecom Management principles and high level requirements" [1], the architecture of Security Management is divided into two layers:

Layer A - Application Layer

Layer B - OAM IP Network

The threats and Security Management requirements of different layers are different, which should be taken into account respectively.

3GPP defines three types of IRP specifications, (see 3GPP TS 32.102 [2]). One type relates to the definitions of the interface deployed across the Itf-N. These definitions need to be agreed between the IRPManagers and IRPAgents so that meaningful communication can occur between them. An example of this type is the Alarm IRP.

The other two types (NRM IRP and Data Definition IRP) relate to the network resource model (schema) of the managed network. This network schema needs to be agreed between the IRPManagers and IRPAgents so that network management services can be provided to the IRPManager(s) by the IRPAgent(s). An example of this type is the UTRAN NRM IRP.

This Requirement specification is applicable to the Interface IRP specifications. That is to say, it is concerned only with the security aspects of operations/notifications/file deployed across the Itf-N.

1 Scope

The present document defines, in addition to the requirements defined in [1] and [2], the requirements for Security Management IRP.

The purpose of this document is to specify the necessary security features, services and functions to protect the network management data, including Requests, Responses, Notifications and Files, exchanged across the Itf-N.

Telecommunication network security can be breached by weaknesses in operational procedures, physical installations, communication links, computational processes and data storage. Of concern here in this document is the security problems resulting from the weaknesses inherent in the communication technologies (i.e., the 3GPP-defined Interface IRPs and their supporting protocol stacks) deployed across the Itf-N.

Appropriate level of security for a telecommunication network is essential. Secured access to the network management applications, and network management data, is essential. The 3GPP-defined Interface IRPs (and their supporting protocol stacks), deployed across the Itf-N, are used for such access, and therefore, their security is considered essential.

Many network management security standards exist. However, there is no recommendation on how to apply them in the Itf-N context. Their deployment across the Itf-N is left to operators. This document and the corresponding solutions identify and recommend security standards in the Itf-N context.

The business case for secured Itf-N is complex as it does not relate to the functions of the Interface IRPs (the functions are constant) but rather, it relates to variants such as the cost of recovering from security breaks, the probability of security incidents and the cost of implementing Security Management, all of which differs depending on specific deployment scenarios.

This document describes the security functions for a 3G network in terms of Security Domains (clause 4.1). Clause 5 defines the Itf-N Security Management scope in terms of its context (5.1) and the possible threats that can occur there are defined in clause 6. Clause 7 specifies the Itf-N security Requirements.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 32.101: "3G Telecom Management principles and high level requirements".

[2] 3GPP TS 32.102: "3G Telecom Management architecture".

[3] ITU-T Recommendation M.3016 (1998): "TMN security overview".

[4] 3GPP TS 33.102 “3G Security; Security Architecture”

[5] ITU-T Recommendation X.800: “Security Architecture for OSI for CCITT Applications

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

IRP: See 3GPP TS 32.101 [1].

IRPAgent: See 3GPP TS 32.102 [2].

IRPManager: See 3GPP TS 32.102 [2].

Operations System (OS): indicates a generic management system, independent of its location level within the management hierarchy.

Principal: Access entity to IRPAgent over Itf-N. In the scope of Itf-N, only the identity of principal is visible to IRPAgent, and the role played by the principal is out of the scope of Itf-N. However, principal must meet the following conditions: (a) Identifiable -an entity should have one or more distinguishing identifiers, and each identifier is unique among all entities’ identifiers. (b) Accountable -the actions of an entity may be traced uniquely to the entity.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

IRP	Integration Reference Point
IS	Information Service (see [1])
ITU-T	International Telecommunication Union, Telecommunication Standardisation Sector
OAM	
OS	Operations System
TMN	Telecom Management Network
UML	Unified Modelling Language (OMG)
UMTS	Universal Mobile Telecommunications System

4 Security Management Background

The objective of this clause is to provide the foundations for the development of security within the management domain and scope of a third generation mobile telecommunications network. This will be accomplished through the establishment of the boundaries of security from the perspective of the management subsystem of a 3G mobile telecommunications network. The definition of the concepts of security objectives, security threats, and finally security mechanisms and services are identified.

This clause gives an overall view of Security Management in general, before entering clause 5 Security Management context and architecture discussion. The general security mechanisms and services used by the management subsystem will depend on the requirements defined in clause 7. How they are used is out side the scope of these requirements. Such aspects may be further specified in corresponding IS specifications.

4.1 Security Domains

Security within a telecommunications network is a vast functional area covering most aspects and all components of a 3G system. To devise a solution more manageable and easier to evolve, the total network security scope is split into different and separate parts. For this document purpose, the security scope is partitioned into four different domains.

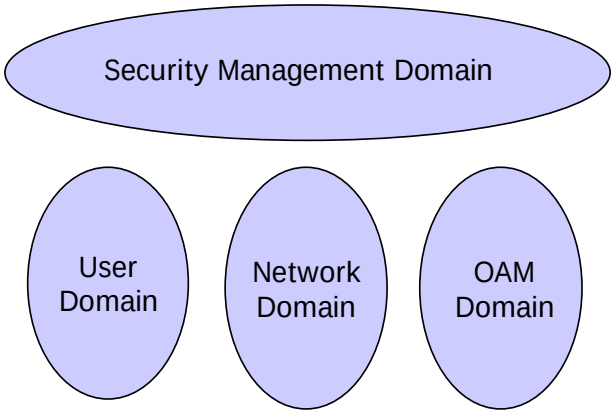

Figure 1 Security Model/Architecture

The **User domain** contains a set of security features that protects User Equipment against attacks on radio interface and provides users with secure access to subscribed services and applications. Examples of security features in this user domain are:

- the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link
- the set of security features that secure access to mobile stations
- the set of security features that enable applications in the user and in the provider domain to securely exchange messages

The **Network domain** provides the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;. This domain covers protection of the network, network elements and all internal (control and signalling) traffic against security threats. The network elements can belong to a single operator (intra-operator) or to different operators (inter-operator).

The **OAM domain** accommodates management tools to supervise all nodes of a cellular network. The OAM domain security provides the protection of all the operation and maintenance traffic, authentication of users, applications and access control to the nodes. It protects the resources of network elements and management applications from intentional and unintentional destructive manipulation.

The **Security Management domain** comprises all activities to establish, maintain and terminate the security aspects of a system. Examples of the features covered by the Security Management domain are:

– management of security services;
– installation of security mechanisms;
– key management (management part);
– establishment of identities, keys, access control information, etc.;
– management of security audit trail and security alarms.

Using the above partitioned view, the scope of this document is focused on security requirements of the OAM domain and is not focused on requirements of other domains. Furthermore, since the Itf-N operates within the OAM domain,

the scope of this document is further “narrowed” towards a component, namely the Itf-N component of the OAM domain.

For further explanation of the semantics of the general security terms referred to in following sub-clauses 4.2, 4.3 and 4.4, refer to reference [5]. It is not intended to repeat them here.

4.2 Security Objectives

Security objectives are necessary in order to define the intended purpose of security within a network. [3] defines the following objectives for security.

- confidentiality
- data integrity
- accountability
- availability

4.3 Security Threats

A security threat is defined by [3] as a potential violation of security that can be directed at one of the four basic security objectives [see subclause 4.1.1]. [5] defines the following security threats

- Masquerade
- Eavesdropping
- Unauthorized access
- Loss or corruption of information
- Repudiation
- Forgery
- Denial of service

[editor’s note: In contemporary network security jargon, “denial of service” is most often used to describe a class of attacks that are intended to subvert the delivery of service. In this context the “denial of service” threat can be best described as “denial of service delivery”. Further study is required to better understand how this can be presented in a manner that is clear and non-ambiguous]

4.4 Security Mechanisms and services

[5] defines a set of security mechanisms that can be used to implement security objectives within a network Security mechanisms are manifested within and/or by security services. The fundamental security services are identified by [5] as being:

- Peer entity authentication
- Data origin authentication
- Access control service
- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic flow confidentiality
- Connection Integrity with recovery
- Connection integrity without recovery
- Selective field connection integrity
- Connectionless integrity
- Selective field connectionless integrity
- Non-repudiation Origin
- Non-repudiation. Delivery

4.5 Security Functional Requirement Area and Security Threats

The table below shows how Security mechanisms are used to counter Security Threats.

Table 1: Correlation of Security Management Functional Area with Threats, M.3016

Functional Requirement Area / Security Management	Masquerade	Eavesdropping	Unauthorized access	Loss/corruption of information	Repudiation	Forgery	Denial of Service
Verification of identities	x		x				
Controlled access and authorization			x				x
Protection of confidentiality		x	x				
Protection of data integrity				x			
Accountability							
Activity logging	x		x		x	x	x
Alarm reporting	x		x	x			x
Audit	x		x		x	x	x

Editor note: correlation between ITU and requirements in clauses 6 and 7 is pending.

5 Security Management context and architecture

This section puts the security issues identified in clause 4 into the context of 3G OAM domain. It also identifies the architectural framework within which security is required in 3G OAM domain.

5.1 Context

This clause defines the Itf-N Security Management (SM) Context. The Itf-N is one of many interfaces defined within the OAM domain (see clause 4.1.). Therefore, this Itf-N Security Management Context is within that OAM Domain.

The following diagram highlights the types of communication links that are realised across the Itf-N. All 3GPP Interface IRPs operate across the Itf-N using these links.

The link-a-1 and link-a-2 represent the two-way links carrying Request from NM (playing the role of IRPManager) and Response from Managed System (playing the role of IRPAgent). The link-b represents a one-way link carrying Notification from the Managed System (playing the role of IRPAgent). The link-c represents the two-way link for File download and upload.

Figure 2: Security Management Context

The Requirements are related to these communication links. They are also related to the end-points (communicating entities) of the communication links. These end-points are the NM when playing the role of IRPManager and the Managed System when playing the role of IRPAgent.

Securing the end-points means to protect them from unauthorized use (see sub-clause 5.3).

The Requirements are not related to other kinds of links nor entities that exist in the OAM Domain. Examples of link and entity types to be excluded are:

- Non-IRP links reaching NM (e.g., the customer-service-oriented application accessing the applications in NM space, a user to logon to NM).
- Non-IRP links reaching IRPAgents (e.g., a user to log on to a Element Manager, a remote network management application access the IRPAgent functions).
- Non-IRP links reaching Network Elements (e.g., a subnetwork management application communicating with the MSC using vendor-specific means, a user to logon to a radio base station).
- All applications running in the NM space and Managed System space that are not playing the roles of IRPManager and IRPAgent.

5.2 Architecture

Within the context defined in clause 4.1 this section defines:

- the architecture of security within the OAM domain

.The security architecture for 3G networks is defined within [4] based on the concept of stratums and feature groups. This specification extend the security architecture defined within [4] to support security in the management system of a 3G network. The following figure depicts the extension of the 3G security architecture to cover 3G OAM&P Security.

Editors note: potential relation 3GPP security stratum is still under study. The figure below shows relation to 32.101 architecture.

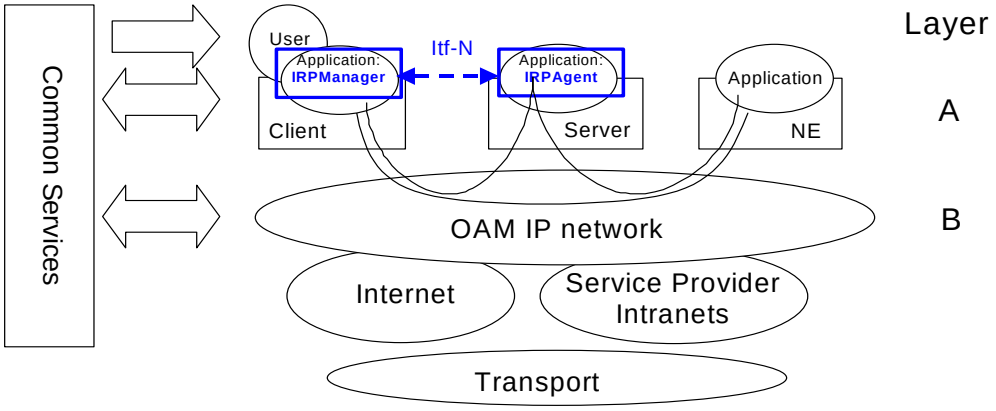

Figure 3: The Management Layers of the 3G Security Architecture (32.101 [1])

Within the Management layer there are defined two additional security feature groups. These feature groups are

- **OAM Domain Security (VI-for further study):** the set of security features that provides protection to all OAM communication related to all applications, actors, and communications traffic related to the operations and management of a 3G network over Itf-N

6 Security Threats in IRP context

This clause describes security threats in IRP context.

If no security mechanisms are in place, the affects on the IRPs are analysed below.

In the IRP context, principal (access entity to IRPAgent via Itf-N) and IRPAgent are not identified to each other. This results in:

1. One principal and/or IRPAgent can masquerade as another easily.

In the IRP context, usage of operations of IRP is not under any security control, each principal is permitted to perform any operation arbitrarily, and this results in:

2. Unauthorized access by a principal to IRPAgent, causing unexpected disclosure of information from IRPAgent, and even damage to IRPAgent and Network Elements under its control.

In the IRP context, there is bulk data and intermittent sequential data to be transferred across Itf-N. Additionally, some sensitive information related to Security Management may also be transferred across Itf-N. However, no measures have been taken to protect them against unauthorized deletion, insertion, modification, re-ordering, replay or delay. This results in:

3. Loss or corruption of information including bulk data, sequenced data.

In the IRP context, there is no mechanism to protect the confidentiality of sensitive information. For example, Security Management always involves such sensitive information as authentication information. Therefore, there is currently a security threat:

4. Eavesdropping on sensitive information.

In the IRP context, no record is kept of requests made by principal and actions performed by IRPAgent. Therefore, there is a security threat:

5. Repudiation, principal and/or IRPAgent can deny the fact that it has sent or received some management information.

In the IRP context, Threat 1, 2, 3 and 4 imply that any principal may flood IRPManager and/or IRPAgent through arbitrarily performing functions, sending bulk data and/or sequential data without restriction. This may be partly responsible for (To flood IRPManager and/or IRPAgent is only one method to cause Denial of Service. To reduce extra traffic across Itf-N cannot completely prevent Denial of Service):

6. Denial of service, as flooded IRPManager and/or IRPAgent has to deal with this extra traffic and has no spare capacity to deal with normal management operations.

The table below shows which Security Threat(s) each IRP faces.

Table 2: Interface IRPs' Security Threats

Threats / IRPs	Masquerade1	Masquerade2	Unauthorized access	Loss or corruption of Sequential data	Loss or corruption of Bulk data	Eavesdropping	Repudiation	Forgery	Denial of service
Basic CM	x		x				x		x
Bulk CM	x	x	x	x	x		x		x
Kernel CM	x	x	x	x			x		x
Alarm	x	x	x	x			x		x
Notification	x		x				x		x
Test Management	x	x	x	x	x		x		x
File Transfer	x	x	x	x			x		x
Entry Point	x	x	x	x			x		x
Security Management	x	x	x	x	x	x	x	x	x
Performance Management	x	x	x	x	x	x	x		x
Communication Surveillance	x	x	x	x			x		x
Log Management	x	x	x	x	x		x		x

Note: Masquerade1 is where a principal masquerades as another principal

Masquerade2 is where an entity masquerades as an IRPAgent

Unauthorised Access is where entity gains unauthorised access to IRPAgent

[Motorola comment: this section needs a more detailed vulnerability/

6.1 Mapping of Security requirements and Threats in IRP Context

It is necessary to take measures to prevent the threats described in this section in IRP context.

The table below shows how the threats identified in this section are countered by security mechanisms.

Table 3: Mapping of Security requirements and Threats

Security Requirements \ Security Threats	Masquerade 1	Masquerade 2	Unauthorized access	Loss or corruption of information	Eavesdropping	Repudiation	Forgery	Denial of service
Authentication1	x		x					
Authentication2		x						
Controlled access and Authorization			x					x
integrity protection				x				
confidentiality protection			x		x			
security alarm	x			x				x
activity log	x					x	x	x

Note1:Authentication1 represents that IRPAgent authenticates principal

Note2:Authentication2 represents that IRPManager authenticates the origin of data received from IRPAgent.

Note 3: Controlled access and authorisation1 represents that IRPAgent controls the access of principal

The security mechanisms identified in the table above are

- Authentication1: In the context of the IRP, IRPAgent authenticates principal
- Authentication2: In the context of the IRP, IRPManager authenticates the origin of data received from IRPAgent.
- Controlled access and authorisation: In the context of the IRPs, the agent may authorise and control the principal access to functions and data of the IRPAgent.

- Integrity protection: In the context of IRP this is the protection of data transferred from the IRPAgent to the IRPManager or from the IRPManager to the IRPAgent.
- Confidentiality Protection: In the context of IRP this is the protection of confidentiality of data transferred from the IRPAgent to the IRPManager or from the IRPManager to the IRPAgent
- Security Alarm: In the context of the IRP this is the issuance of a security alarm by the IRPAgent.
- Activity Log: In the context of the IRP this is the maintenance of a activity log by the IRPAgent.

7 Security requirement of Itf-N

Editors note: The requirements are still subject to discussion following agreement on clauses 4 – 6.

This clause specifies the Security Management requirements for the present release.

A capability should be standardized that allows

1. IRPAgent to authenticate principal. It implies that the principal should be identified so as to be authenticated.
2. IRPAgent to authorize the principal, i.e. IRPAgent checks if the principal has been authorized to perform the operations on receiving operation request.
3. IRPManager to ensure that notifications are received from an authenticated IRPAgent.
4. Receiver (IRPManager or IRPAgent) of bulk data, sequential data to check the integrity of the management information
5. The confidentiality of sensitive management information to be protected.
6. IRPAgent to report security alarm to IRPManager when breach of security is detected, e.g. request for unauthorized operation, damage of file transferred, etc.
7. IRPManager to find out who (i.e., identities of principal or IRPAgents) did what (i.e., names of operations and notifications) and when. This capability is called the activity log. It includes information about requested operations, operations performed, emitted notifications/alarms, and transferred files. In the context of Itf-N, IRPAgent maintains activity log(s) and the activity log(s) of IRPManager are out of scope of this specification.

Interface IRPs' Security Management requirement table shows which Security Management requirements specific IRPs shall meet.

Table 4: Interface IRPs' Security Management requirement

IRPs / Requirements	Authentication1	Authentication2	Controlled access and authorization1	Controlled access and authorization2	integrity protection	confidentiality protection	security alarm	activity log
Approved IRP								
Basic CM IRP								
Bulk CM IRP								
Kernel CM IRP								
Alarm IRP								
Notification IRP								
Test Management IRP								
IRP under discussion								
File Transfer IRP								
Entry Point IRP								
Security Management IRP								
Performance management IRP								
Communication Surveillance IRP								
Log Management IRP								

Note1: Integrity of alarm sequence is protected, not individual alarms

Note2: Integrity of notification sequence is protected, not individual notifications.

Note3: Integrity of files includes integrity of file sequences as well as integrity of individual files.

Note4: Loss of Performance Management data must be detected

1. Those IRPs where IRPManager requests actions of IRPAgent should meet Authentication1 and Controlled access and authorization requirement.
2. Those IRPs that transfer management information from IRPAgent to IRPManager should meet Authentication2 requirement.
3. Those IRPs that may transfer bulk data or sequential data across Itf-N should meet integrity protection requirement.
4. Security Management IRP should meet Confidentiality protection requirement to protect sensitive information from being disclosed.
5. Any IRP that meets one of Authentication1, Controlled access and Authorization, Authentication2, integrity protection, confidentiality protection requirements should meet Security Alarm and Activity Log requirement.

Annex A (informative):

Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
Nov 2003	--	--	--	--	First Draft	0.0.1	

3GPP TSG-SA5 (Telecom Management) **S5-037227**
Meeting #36, Shanghai, CHINA, 17 - 21 Nov 2003

Source: **Huawei**

Title: **Rel-6 Security Matrices**

Agenda Item:

Document for:

Late submission	

Decision	X
Discussion	X
Information	

Work Item: **OAM-NIM**

WT addressed **SWGC WT01**

Specs involved: **32.371**

---

1 Decision/action requested

This contribution is expected to be approved by SA5.

2 References

None.

3 Rationale

This contribution has been agreed by SA5 SWGC.

4 Consequences and implications

5 Issues of discussion

Matrix of Security threats

This table identifies the security threats in IRP context.
The definitions of the column headings of the table follow:

1. Manager Masquerade: One entity can masquerade as an IRPManager.
2. Unauthorized Access: Unauthorized access by an IRPManager to IRPAgent, causing unexpected disclosure of information from IRPAgent, and even damage to IRPAgent and Network Elements under its control.
3. Agent Masquerade: One entity can masquerade as an IRPAgent.
4. Loss or Corruption: Loss or corruption of information including bulk data.
5. Eavesdropping (Note 7): Eavesdropping on sensitive management information.
6. Repudiation: IRPManager and/or IRPAgent denies the fact that it has sent or received some management information.

“File transfer” in the row headings of the table refers to the file transfer mechanism used by the corresponding IRPs. Because the IRPs use the file transfer mechanisms provided by the File Transfer IRP the threats relating to file transfer mechanisms are shown in rows associated with the FT IRP.
“File content” in the row name of the table refers to the file content of files used by the corresponding IRPs. The threats to file content are dependant on the IRP to which the file belongs, and these are therefore shown against the IRP that created or uses the files.

Table 1 Matrix of Security threats

	Manager Masquerade	**Unauthorized Access**	**Agent Masquerade**	**Loss or Corruption**	**Eavesdropping** (Note 7)	**Repudiation**
Basic CM IRP						
operation	X	X	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
Bulk CM IRP						
operation	X	X	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
file content (Active) (Note 4)	N/A	N/A	N/A	X	-	X
file content (Passive)	N/A	N/A	-	-	-	-
Alarm IRP						
operation	X	-	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
file content	N/A	N/A	N/A	N/A	N/A	N/A
Notification IRP						
operation	X	X (Note 5)	N/A	N/A	-	X
notification (n/a)	N/A	N/A	N/A	N/A	N/A	N/A
TM IRP						
operation	X	X (Note 5)	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
file content	N/A	N/A	-	-	-	-
FT IRP						
operation	X	X	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
file transfer	X	X	N/A	N/A	-	X
EP IRP						
operation	X	**(TBD)**	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
PM IRP						
operation	X	-(Note 5)	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
file content	N/A	N/A	N/A	-	-	-
CS IRP						
operation	X	-	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
NL IRP						
operation	X	-	N/A	N/A	-	X
notification	N/A	N/A	-	-	-	-
file content	N/A	N/A	N/A	-	-	-

N/A: Not applicable
TBD: To Be Decided
-: Not a Threat
X: A Threat

Note 4: The IRPAgent shall check that a downloaded file has not been changed during a session before performing a pre-activation or activation.
Note 5: relationship between operations is for further study.

Note 7: Assume security of DCN between IRPManager and IRPAgent is not described in this document.

Matrix of Security Requirements

This table identifies the security requirements in IRP context.
The definitions of the column headings of the table follow:

1. Manager Authentication: IRPAgent authenticates IRPManager. It implies that the IRPManager shall be identified so as to be authenticated.

2. Authorization: IRPAgent authorizes the IRPManager, i.e. IRPAgent checks if the IRPManager has been authorized to perform the operations on receiving operation request.

3. Agent Authentication: IRPManager authenticates IRPAgent. It implies that the IRPAgent shall be identified so as to be authenticated.

4. Integrity Protection: Receiver (IRPManager or IRPAgent) of bulk data checks the integrity of the management information

5. Confidentiality Protection: The confidentiality of sensitive management information is protected.

6. Non-Repudiation: Means are provided to prove that exchange of data between IRPAgent and IRPManager actually took place.

7. Security Alarm: IRPAgent issues security alarm to IRPManager when breach of security is detected, e.g. request for unauthorized operation, damage of file transferred, etc.

8. Activity Log: It helps to find out who (i.e., identities of IRPManager) did what (i.e., names of operations and notifications) and when. This capability is called the activity log. It includes information like requested operations, operations performed, emitted notifications/alarms, and transferred files. In the context of Itf-N, IRPAgent maintains activity log(s) and the activity log(s) of IRPManager are out of scope of this specification.

“ File transfer” in row name of the table refers to the file transfer mechanism used by corresponding IRP. Because the IRPs use the file transfer mechanisms provided by the File Transfer IRP the threats relating to file transfer mechanisms are shown in rows associated with the FT IRP.

“ File content” in row name of the table refers to the file content of corresponding IRP.

Table 2 Matrix of Security Requirements

	Manager Authentication	**Authorization**	**Agent Authentication**	**Integrity Protection**	**Confidentiality Protection**	**Non-Repudiation**	**Security Alarm**	**Activity Log**
Basic CM IRP								
operation	X	X	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
Bulk CM IRP								
operation	X	X	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content (Active)	N/A	N/A	N/A	X	-	-	X	X(Note 12)
file content (Passive)	N/A	N/A	-	-	-	-	N/A (Note 11)	N/A
Alarm IRP								
operation	X	-	N/A	N/A	-	-	X	X

notification	N/A	N/A	-	-	-	-	N/A	-
file content (Note 10)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Notification IRP								
operation	X	X	N/A	N/A	-	-	X	X
notification (n/a)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TM IRP								
operation	X	X	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content	N/A	N/A	-	-	-	-	N/A	-
FT IRP								
operation	X	X	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file transfer	X	X	N/A	X(Note 13)	-	-	X	X
EP IRP								
operation	X	TBD	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
PM IRP								
operation	X	X(Note5)	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content	N/A	N/A	-	-	-	-	N/A	-
CS IRP								
operation	X	-	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
NL IRP								
operation	X	-	N/A	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content	N/A	N/A	N/A	-	-	-	N/A	-

Note 9: A security Alarm is issued if the integrity check of the file fails.
Note 10: N/A because no file transfer operations for this IRP have yet been defined.
Note 11 – This field is N/A because no integrity check is performed on the file contents and therefore no security alarm can be issued as a result. If file contents are checked and no requirement for issuing an alarm identified this field would be "-".
Note 12: Activity log of Bulk CM IRP constains suboperations of active files.
Note 13: FT IRP is reponsible for checking the integrity of the files transferred, but not the file content semantics.
Note: this matrix is a Working draft

3GPP TS 32.xx1 V0.0.1 (2003-07)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication Management; Security Management: Security Management: Concepts and Requirements; (Release 6)

Keywords
Security Management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

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

The present document is part 1 of a multi-part TS covering the 3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Telecommunication Management; Security Management, as identified below:

TS 32.xx1: "Security Management **Integration Reference Point: Requirements**";

TS 32.xx2 "Security Management Integration Reference Point: Information Service";

TS 32.xx3: "Security Management Integration Reference Point: CORBA Solution Set";

TS 32.xx4: "Security Management Integration Reference Point: CMIP Solution Set".

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

In 3GPP SA5 context, IRPs are introduced to address process interfaces at the Itf-N interface. The Itf-N interface is built up by a number of Integration Reference Points (IRPs) and a related Name Convention, which realise the functional capabilities over this interface. The basic structure of the IRPs is defined in 3GPP TS 32.101 [1] and 3GPP TS 32.102 [2]. IRP consists of IRPManager and IRPAgent. Usually there are three types of transaction between IRPManager and IRPAgent, which are operation invocation, notification, and file transfer.

However, there are different types of intentional threats against the transaction between IRPManagers and IRPAgents. All the threats are potential risks of damage or degradation of telecommunication services, which operators should take measures to reduce or eliminate to secure the telecommunication service, network, and data.

By introducing Security Management, this document describes security requirements to relieve the threats between IRPManagers and IRPAgents.

As described in 3GPP TS 32.101 "3G Telecom Management principles and high level requirements" [1], the architecture of Security Management is divided into two layers:

Layer A - Application Layer

Layer B - OAM IP Network

The threats and Security Management requirements of different layers are different, which should be taken into account respectively.

3GPP defines three types of IRP specifications, (see 3GPP TS 32.102 [2]). One type relates to the definitions of the interface deployed across the Itf-N. These definitions need to be agreed between the IRPManagers and IRPAgents so that meaningful communication can occur between them. An example of this type is the Alarm IRP.

The other two types (NRM IRP and Data Definition IRP) relate to the network resource model (schema) of the managed network. This network schema needs to be agreed between the IRPManagers and IRPAgents so that network management services can be provided to the IRPManager(s) by the IRPAgent(s). An example of this type is the UTRAN NRM IRP.

This Requirement specification is applicable to the Interface IRP specifications. That is to say, it is concerned only with the security aspects of operations/notifications/file deployed across the Itf-N.

1 Scope

The present document defines, in addition to the requirements defined in [1] and [2], the requirements for Security Management IRP.

The purpose of this document is to specify the necessary security features, services and functions to protect the network management data, including Requests, Responses, Notifications and Files, exchanged across the Itf-N.

Telecommunication network security can be breached by weaknesses in operational procedures, physical installations, communication links, computational processes and data storage. Of concern here in this document is the security problems resulting from the weaknesses inherent in the communication technologies (i.e., the 3GPP-defined Interface IRPs and their supporting protocol stacks) deployed across the Itf-N.

Appropriate level of security for a telecommunication network is essential. Secured access to the network management applications, and network management data, is essential. The 3GPP-defined Interface IRPs (and their supporting protocol stacks), deployed across the Itf-N, are used for such access, and therefore, their security is considered essential.

Many network management security standards exist. However, there is no recommendation on how to apply them in the Itf-N context. Their deployment across the Itf-N is left to operators. This document and the corresponding solutions identify and recommend security standards in the Itf-N context.

The business case for secured Itf-N is complex as it does not relate to the functions of the Interface IRPs (the functions are constant) but rather, it relates to variants such as the cost of recovering from security breaks, the probability of security incidents and the cost of implementing Security Management, all of which differs depending on specific deployment scenarios.

This document describes the security functions for a 3G network in terms of Security Domains (clause 4.1). Clause 5 defines the Itf-N Security Management scope in terms of its context (5.1) and the possible threats that can occur there are defined in clause 6. Clause 7 specifies the Itf-N security Requirements.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 32.101: "3G Telecom Management principles and high level requirements".

[2] 3GPP TS 32.102: "3G Telecom Management architecture".

[3] ITU-T Recommendation M.3016 (1998): "TMN security overview".

[4] 3GPP TS 33.102 “3G Security; Security Architecture”

[5] ITU-T Recommendation X.800: “Security Architecture for OSI for CCITT Applications

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

IRP: See 3GPP TS 32.101 [1].

IRPAgent: See 3GPP TS 32.102 [2].

IRPManager: See 3GPP TS 32.102 [2].

Operations System (OS): indicates a generic management system, independent of its location level within the management hierarchy.

Principal: Access entity to IRPAgent over Itf-N. In the scope of Itf-N, only the identity of principal is visible to IRPAgent, and the role played by the principal is out of the scope of Itf-N. However, principal must meet the following conditions: (a) Identifiable -an entity should have one or more distinguishing identifiers, and each identifier is unique among all entities’ identifiers. (b) Accountable -the actions of an entity may be traced uniquely to the entity.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

IRP	Integration Reference Point
IS	Information Service (see [1])
ITU-T	International Telecommunication Union, Telecommunication Standardisation Sector
OAM	
OS	Operations System
TMN	Telecom Management Network
UML	Unified Modelling Language (OMG)
UMTS	Universal Mobile Telecommunications System

4 Security Management Background

The objective of this clause is to provide the foundations for the development of security within the management domain and scope of a third generation mobile telecommunications network. This will be accomplished through the establishment of the boundaries of security from the perspective of the management subsystem of a 3G mobile telecommunications network. The definition of the concepts of security objectives, security threats, and finally security mechanisms and services are identified.

This clause gives an overall view of Security Management in general, before entering clause 5 Security Management context and architecture discussion. The general security mechanisms and services used by the management subsystem will depend on the requirements defined in clause 7. How they are used is out side the scope of these requirements. Such aspects may be further specified in corresponding IS specifications.

4.1 Security Domains

Security within a telecommunications network is a vast functional area covering most aspects and all components of a 3G system. To devise a solution more manageable and easier to evolve, the total network security scope is split into different and separate parts. For this document purpose, the security scope is partitioned into four different domains.

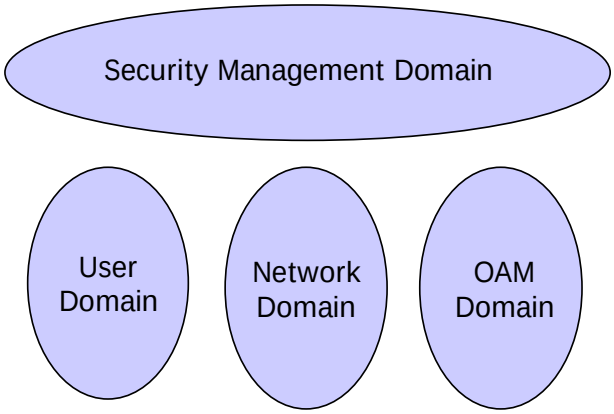

Figure 1 Security Model/Architecture

The **User domain** contains a set of security features that protects User Equipment against attacks on radio interface and provides users with secure access to subscribed services and applications. Examples of security features in this user domain are:

- the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link
- the set of security features that secure access to mobile stations
- the set of security features that enable applications in the user and in the provider domain to securely exchange messages

The **Network domain** provides the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;. This domain covers protection of the network, network elements and all internal (control and signalling) traffic against security threats. The network elements can belong to a single operator (intra-operator) or to different operators (inter-operator).

The **OAM domain** accommodates management tools to supervise all nodes of a cellular network. The OAM domain security provides the protection of all the operation and maintenance traffic, authentication of users, applications and access control to the nodes. It protects the resources of network elements and management applications from intentional and unintentional destructive manipulation.

The **Security Management domain** comprises all activities to establish, maintain and terminate the security aspects of a system. Examples of the features covered by the Security Management domain are:

- management of security services;
- installation of security mechanisms;
- key management (management part);
- establishment of identities, keys, access control information, etc.;
- management of security audit trail and security alarms.

Using the above partitioned view, the scope of this document is focused on security requirements of the OAM domain and is not focused on requirements of other domains. Furthermore, since the Itf-N operates within the OAM domain,

the scope of this document is further “narrowed” towards a component, namely the Itf-N component of the OAM domain.

For further explanation of the semantics of the general security terms referred to in following sub-clauses 4.2, 4.3 and 4.4, refer to reference [5]. It is not intended to repeat them here.

4.2 Security Objectives

Security objectives are necessary in order to define the intended purpose of security within a network. [3] defines the following objectives for security.

- confidentiality
- data integrity
- accountability
- availability

4.3 Security Threats

A security threat is defined by [3] as a potential violation of security that can be directed at one of the four basic security objectives [see subclause 4.1.1]. [5] defines the following security threats

- Masquerade
- Eavesdropping
- Unauthorized access
- Loss or corruption of information
- Repudiation
- Forgery
- Denial of service

[editor’s note: In contemporary network security jargon, “denial of service” is most often used to describe a class of attacks that are intended to subvert the delivery of service. In this context the “denial of service” threat can be best described as “denial of service delivery”. Further study is required to better understand how this can be presented in a manner that is clear and non-ambiguous]

4.4 Security Mechanisms and services

[5] defines a set of security mechanisms that can be used to implement security objectives within a network Security mechanisms are manifested within and/or by security services. The fundamental security services are identified by [5] as being:

- Peer entity authentication
- Data origin authentication
- Access control service
- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic flow confidentiality
- Connection Integrity with recovery
- Connection integrity without recovery
- Selective field connection integrity
- Connectionless integrity
- Selective field connectionless integrity
- Non-repudiation Origin
- Non-repudiation. Delivery

4.5 Security Functional Requirement Area and Security Threats

The table below shows how Security mechanisms are used to counter Security Threats.

Table 1: Correlation of Security Management Functional Area with Threats, M.3016

Functional Requirement Area / Security Management	Masquerade	Eavesdropping	Unauthorized access	Loss/corruption of information	Repudiation	Forgery	Denial of Service
Verification of identities	x		x				
Controlled access and authorization			x				x
Protection of confidentiality		x	x				
Protection of data integrity				x			
Accountability							
Activity logging	x		x		x	x	x
Alarm reporting	x		x	x			x
Audit	x		x		x	x	x

Editor note: correlation between ITU and requirements in clauses 6 and 7 is pending.

5 Security Management context and architecture

This section puts the security issues identified in clause 4 into the context of 3G OAM domain. It also identifies the architectural framework within which security is required in 3G OAM domain.

5.1 Context

This clause defines the Itf-N Security Management (SM) Context. The Itf-N is one of many interfaces defined within the OAM domain (see clause 4.1.). Therefore, this Itf-N Security Management Context is within that OAM Domain.

The following diagram highlights the types of communication links that are realised across the Itf-N. All 3GPP Interface IRPs operate across the Itf-N using these links.

The link-a-1 and link-a-2 represent the two-way links carrying Request from NM (playing the role of IRPManager) and Response from Managed System (playing the role of IRPAgent). The link-b represents a one-way link carrying Notification from the Managed System (playing the role of IRPAgent). The link-c represents the two-way link for File download and upload.

Figure 2: Security Management Context

The Requirements are related to these communication links. They are also related to the end-points (communicating entities) of the communication links. These end-points are the NM when playing the role of IRPManager and the Managed System when playing the role of IRPAgent.

Securing the end-points means to protect them from unauthorized use (see sub-clause 5.3).

The Requirements are not related to other kinds of links nor entities that exist in the OAM Domain. Examples of link and entity types to be excluded are:

- Non-IRP links reaching NM (e.g., the customer-service-oriented application accessing the applications in NM space, a user to logon to NM).
- Non-IRP links reaching IRPAgents (e.g., a user to log on to a Element Manager, a remote network management application access the IRPAgent functions).
- Non-IRP links reaching Network Elements (e.g., a subnetwork management application communicating with the MSC using vendor-specific means, a user to logon to a radio base station).
- All applications running in the NM space and Managed System space that are not playing the roles of IRPManager and IRPAgent.

5.2 Architecture

Within the context defined in clause 4.1 this section defines:

- the architecture of security within the OAM domain

.The security architecture for 3G networks is defined within [4] based on the concept of stratums and feature groups. This specification extend the security architecture defined within [4] to support security in the management system of a 3G network. The following figure depicts the extension of the 3G security architecture to cover 3G OAM&P Security.

Editors note: potential relation 3GPP security stratum is still under study. The figure below shows relation to 32.101 architecture.

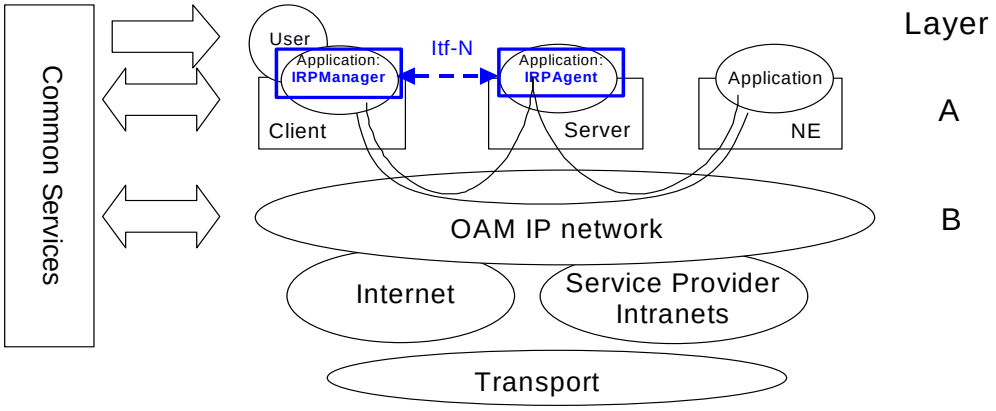

Figure 3: The Management Layers of the 3G Security Architecture (32.101 [1])

Within the Management layer there are defined two additional security feature groups. These feature groups are

- **OAM Domain Security (VI-for further study):** the set of security features that provides protection to all OAM communication related to all applications, actors, and communications traffic related to the operations and management of a 3G network over Itf-N

6 Security Threats in IRP context

This clause describes security threats in IRP context.

If no security mechanisms are in place, the affects on the IRPs are analysed below.

In the IRP context, principal (access entity to IRPAgent via Itf-N) and IRPAgent are not identified to each other. This results in:

1. One principal and/or IRPAgent can masquerade as another easily.

In the IRP context, usage of operations of IRP is not under any security control, each principal is permitted to perform any operation arbitrarily, and this results in:

2. Unauthorized access by a principal to IRPAgent, causing unexpected disclosure of information from IRPAgent, and even damage to IRPAgent and Network Elements under its control.

In the IRP context, there is bulk data and intermittent sequential data to be transferred across Itf-N. Additionally, some sensitive information related to Security Management may also be transferred across Itf-N. However, no measures have been taken to protect them against unauthorized deletion, insertion, modification, re-ordering, replay or delay. This results in:

3. Loss or corruption of information including bulk data, sequenced data.

In the IRP context, there is no mechanism to protect the confidentiality of sensitive information. For example, Security Management always involves such sensitive information as authentication information. Therefore, there is currently a security threat:

4. Eavesdropping on sensitive information.

In the IRP context, no record is kept of requests made by principal and actions performed by IRPAgent. Therefore, there is a security threat:

5. Repudiation, principal and/or IRPAgent can deny the fact that it has sent or received some management information.

In the IRP context, Threat 1, 2, 3 and 4 imply that any principal may flood IRPManager and/or IRPAgent through arbitrarily performing functions, sending bulk data and/or sequential data without restriction. This may be partly responsible for (To flood IRPManager and/or IRPAgent is only one method to cause Denial of Service. To reduce extra traffic across Itf-N cannot completely prevent Denial of Service):

6. Denial of service, as flooded IRPManager and/or IRPAgent has to deal with this extra traffic and has no spare capacity to deal with normal management operations.

The table below shows which Security Threat(s) each IRP faces.

Table 2: Interface IRPs' Security Threats

Threats / IRPs	Masquerade1	Masquerade2	Unauthorized access	Loss or corruption of Sequential data	Loss or corruption of Bulk data	Eavesdropping	Repudiation	Forgery	Denial of service
Basic CM	x		x				x		x
Bulk CM	x	x	x	x	x		x		x
Kernel CM	x	x	x	x			x		x
Alarm	x	x	x	x			x		x
Notification	x		x				x		x
Test Management	x	x	x	x	x		x		x
File Transfer	x	x	x	x			x		x
Entry Point	x	x	x	x			x		x
Security Management	x	x	x	x	x	x	x	x	x
Performance Management	x	x	x	x	x	x	x		x
Communication Surveillance	x	x	x	x			x		x
Log Management	x	x	x	x	x		x		x

Note: Masquerade1 is where a principal masquerades as another principal

Masquerade2 is where an entity masquerades as an IRPAgent

Unauthorised Access is where entity gains unauthorised access to IRPAgent

[Motorola comment: this section needs a more detailed vulnerability/

6.1 Mapping of Security requirements and Threats in IRP Context

It is necessary to take measures to prevent the threats described in this section in IRP context.

The table below shows how the threats identified in this section are countered by security mechanisms.

Table 3: Mapping of Security requirements and Threats

Security Requirements \ Security Threats	Masquerade 1	Masquerade 2	Unauthorized access	Loss or corruption of information	Eavesdropping	Repudiation	Forgery	Denial of service
Authentication1	x		x					
Authentication2		x						
Controlled access and Authorization			x					x
integrity protection				x				
confidentiality protection			x		x			
security alarm	x			x				x
activity log	x					x	x	x

Note1:Authentication1 represents that IRPAgent authenticates principal

Note2:Authentication2 represents that IRPManager authenticates the origin of data received from IRPAgent.

Note 3: Controlled access and authorisation1 represents that IRPAgent controls the access of principal

The security mechanisms identified in the table above are

- Authentication1: In the context of the IRP, IRPAgent authenticates principal
- Authentication2: In the context of the IRP, IRPManager authenticates the origin of data received from IRPAgent.
- Controlled access and authorisation: In the context of the IRPs, the agent may authorise and control the principal access to functions and data of the IRPAgent.

- Integrity protection: In the context of IRP this is the protection of data transferred from the IRPAgent to the IRPManager or from the IRPManager to the IRPAgent.
- Confidentiality Protection: In the context of IRP this is the protection of confidentiality of data transferred from the IRPAgent to the IRPManager or from the IRPManager to the IRPAgent
- Security Alarm: In the context of the IRP this is the issuance of a security alarm by the IRPAgent.
- Activity Log: In the context of the IRP this is the maintenance of a activity log by the IRPAgent.

7 Security requirement of Itf-N

Editors note: The requirements are still subject to discussion following agreement on clauses 4 – 6.

This clause specifies the Security Management requirements for the present release.

A capability should be standardized that allows

1. IRPAgent to authenticate principal. It implies that the principal should be identified so as to be authenticated.
2. IRPAgent to authorize the principal, i.e. IRPAgent checks if the principal has been authorized to perform the operations on receiving operation request.
3. IRPManager to ensure that notifications are received from an authenticated IRPAgent.
4. Receiver (IRPManager or IRPAgent) of bulk data, sequential data to check the integrity of the management information
5. The confidentiality of sensitive management information to be protected.
6. IRPAgent to report security alarm to IRPManager when breach of security is detected, e.g. request for unauthorized operation, damage of file transferred, etc.
7. IRPManager to find out who (i.e., identities of principal or IRPAgents) did what (i.e., names of operations and notifications) and when. This capability is called the activity log. It includes information about requested operations, operations performed, emitted notifications/alarms, and transferred files. In the context of Itf-N, IRPAgent maintains activity log(s) and the activity log(s) of IRPManager are out of scope of this specification.

Interface IRPs' Security Management requirement table shows which Security Management requirements specific IRPs shall meet.

Table 4: Interface IRPs' Security Management requirement

IRPs / Requirements	Authentication1	Authentication2	Controlled access and authorization1	Controlled access and authorization2	integrity protection	confidentiality protection	security alarm	activity log
Approved IRP								
Basic CM IRP								
Bulk CM IRP								
Kernel CM IRP								
Alarm IRP								
Notification IRP								
Test Management IRP								
IRP under discussion								
File Transfer IRP								
Entry Point IRP								
Security Management IRP								
Performance management IRP								
Communication Surveillance IRP								
Log Management IRP								

Note1: Integrity of alarm sequence is protected, not individual alarms

Note2: Integrity of notification sequence is protected, not individual notifications.

Note3: Integrity of files includes integrity of file sequences as well as integrity of individual files.

Note4: Loss of Performance Management data must be detected

1. Those IRPs where IRPManager requests actions of IRPAgent should meet Authentication1 and Controlled access and authorization requirement.
2. Those IRPs that transfer management information from IRPAgent to IRPManager should meet Authentication2 requirement.
3. Those IRPs that may transfer bulk data or sequential data across Itf-N should meet integrity protection requirement.
4. Security Management IRP should meet Confidentiality protection requirement to protect sensitive information from being disclosed.
5. Any IRP that meets one of Authentication1, Controlled access and Authorization, Authentication2, integrity protection, confidentiality protection requirements should meet Security Alarm and Activity Log requirement.

Annex A (informative):

Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
Nov 2003	--	--	--	--	First Draft	0.0.1	