Technical Specification Group Services and System Aspects **TSGS#23(04)0126**
Meeting #23, Phoenix, USA, 15 - 18 March 2004

Source: **SA5 (Telecom Management)**

Title: New Rel-6 TS 32.371-100 "Telecommunication management; Security Management Concept and Requirements" - **For SA Information**

Document for: **Information**

Agenda Item: **7.5.3**

SP-040126 New Rel-6 TS 32.371-100 "Telecommunication management; Security Management Concept and Requirements" - **For SA Information**

3GPP TSG-SA5 (Telecom Management) **S5-046214**
Meeting #37, Málaga, España, 23 – 27 February 2004

Presentation of Technical Specification to TSG SA

Presentation to:	**TSG SA Meeting #23**
Document for presentation:	**TS 32.371, Version 1.0.0** **Security Management Concept and Requirements**
Presented for:	**Information**

Abstract of document:
This TS defines the concept and requirements for the Security Management IRP.

Work done against the WID contained in SP-020754 (Work Item ID: OAM-NIM).

Purpose of This Specification:

This TS is intended for Release 6 and is part of the Security Management IRP, which consists of:

Number	Title
32.371	**Security Management Concept and Requirements**
32.372	Security Management Integration Reference Point (IRP): Information service
32.373	Security Management Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS)
32.374	Security Management Integration Reference Point (IRP): Common Management Information Protocol (CMIP) Solution Set (SS)

The purpose of this set of specifications is to provide a Security Management mechanism over Itf-N to secure the interaction between the network manager and the managed systems over Itf-N for Release 6.

Changes since last presentation to TSG-SA:
New

Outstanding Issues:
None

Contentious Issues:
None

3GPP TS 32.371 V1.0.0 (2004-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Telecommunication Management;
Security Management Concept 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 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

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

TS 32.371: "Concept and Requirements";

TS 32.372: "Integration Reference Point (IRP): Information Service (IS)";

TS 32.373: "Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS)";

TS 32.374: "Integration Reference Point (IRP): Common Management Information Protocol (CMIP) Solution Set (SS)".

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 realize 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, the present document describes security requirements to relieve the threats between IRPManagers and IRPAgents.

As described in 3GPP TS 32.101 [1], the architecture of Security Management is divided into two layers:

Layer A - Application Layer

Layer B - OAM&P transport 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 3GPP TS 32.101 [1] and 3GPP TS 32.102 [2], the requirements for Security Management IRP.

The purpose of the present 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 the present 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. The present 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.

The present document describes the security functions for a 3G network in terms of Security Domains (subclause 4.1). Clause 5 defines the Itf-N Security Management scope in terms of its context (subclause 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: "Telecommunication management; Principles and high level requirements".

[2] 3GPP TS 32.102: "Telecommunication 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 Open Systems Interconnection for CCITT applications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ITU-T Recommendation X.800 [5], ITU-T Recommendation M.3016 [3] and the following apply:

access control: prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner, see ITU-T Recommendation X.800 [5]

accountability: property that ensures that the actions of an entity may be traced uniquely to the entity, see ITU-T Recommendation X.800 [5]

audit: See Security Audit

authentication: See data origin authentication and peer element authentication, see ITU-T Recommendation X.800 [5]

authorization: granting of rights, which includes the granting of access based on access rights, see ITU-T Recommendation X.800 [5]

availability: property of being accessible and useable upon demand by an authorized entity, see ITU-T Recommendation X.800 [5]

confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes, see ITU-T Recommendation X.800 [5]

credentials: data that is transferred to establish the claimed identity of an entity, see ITU-T Recommendation X.800 [5]y

cryptography: discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized us, see ITU-T Recommendation X.800 [5]e

data integrity: property that data has not been altered or destroyed in an unauthorized manner, see ITU-T Recommendation X.800 [5]

data origin authentication: corroboration that the source of data received is as claimed, see ITU-T Recommendation X.800 [5]

denial of service: prevention of authorized access to resources or the delaying of time-critical operations, see ITU-T Recommendation X.800 [5]

digital signature: data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient, see ITU-T Recommendation X.800 [5]

eavesdropping: breach of confidentiality by monitoring communication, see ITU-T Recommendation M.3016 [3]

forgery: entity fabricates information and claims that such information was received from another entity or sent to another entity, see ITU-T Recommendation M.3016 [3]

IRP: See 3GPP TS 32.101 [1].

IRPAgent: See 3GPP TS 32.102 [2].

IRPManager: See 3GPP TS 32.102 [2].

loss or corruption of information: integrity of data transferred is compromised by unauthorized deletion, insertion, modification, re-ordering, replay or delay, see ITU-T Recommendation M.3016 [3]

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

masquerade: pretence by an entity to be a different entity, see ITU-T Recommendation X.800 [5].

password: confidential authentication information, usually composed of a string of characters, see ITU-T Recommendation X.800 [5]

Peer Entity Authentication: The corroboration that a peer entity in an association is the one claimed, see ITU-T Recommendation X.800 [5]

repudiation: denial by one of the entities involved in a communication of having participated in all or part of the communication, see ITU-T Recommendation X.800 [5]

security audit: independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures, see ITU-T Recommendation X.800 [5]

threat: potential violation of security, see ITU-T Recommendation X.800 [5]

unauthorized access: entity attempts to access data in violation of the security policy in force, see ITU-T Recommendation M.3016 [3]

3.2 Abbreviations

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

CM	Configuration Management
CS	Communication Surveillance
DCN	Data Communication Network
EM	Element Manager
EP	Entry Point
FT	File Transfer
IRP	Integration Reference Point
IS	Information Service (see 3GPP TS 32.101 [1])
ITU-T	International Telecommunication Union - Telecommunication standardization sector
NE	Network Element
NL	Notification Log
NM	Network Manager
NRM	Network Resource Model
OAM&P	Operations, Administration, Maintenance and Provisioning
OS	Operations System
PM	Performance Management
TM	Test Management
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 the present document purpose, the security scope is partitioned into four different domains.

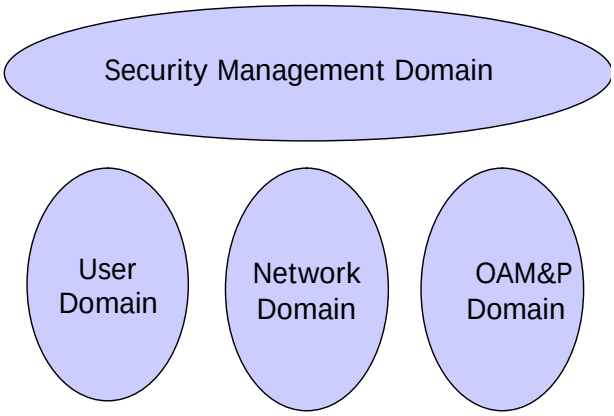

Figure 1: Security model/architecture

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&P domain** accommodates management tools to supervise all nodes of a cellular network. The OAM&P 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 the present document is focused on security requirements of the OAM&P domain and is not focused on requirements of other domains. Furthermore, since the Itf-N operates within the OAM&P domain, the scope of the present document is further "narrowed" towards a component, namely the Itf-N component of the OAM&P domain.

For further explanation of the semantics of the general security terms referred to in following subclauses 4.2, 4.3 and 4.4, refer to ITU-T Recommendation X.800 [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. ITU-T Recommendation M.3016 [3] defines the following objectives for security.

- Confidentiality;
- Data integrity;
- Accountability;
- Availability;

4.3 Security threats

A security threat is defined by ITU-T Recommendation M.3016 [3] as a potential violation of security that can be directed at one of the four basic security objectives (see subclause 4.2). ITU-T Recommendation X.800 [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

ITU-T Recommendation X.800 [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 ITU-T Recommendation X.800 [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 TMN perspective regarding security threats

Table 1 is taken from ITU-T Recommendation M.3016 [3]. It shows TMN perspective on which security functions are required to counter the Security Threats identified in subclause 4.3.

The security mechanisms identified in subclause 4.4 may be used to achieve the security requirements.

Table 1: Correlation of security management functional area with threats (from ITU-T Recommendation M.3016 [3])

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

5 Security management context and architecture

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

5.1 Context

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

The following diagram highlights the types of communication links that are realized 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.

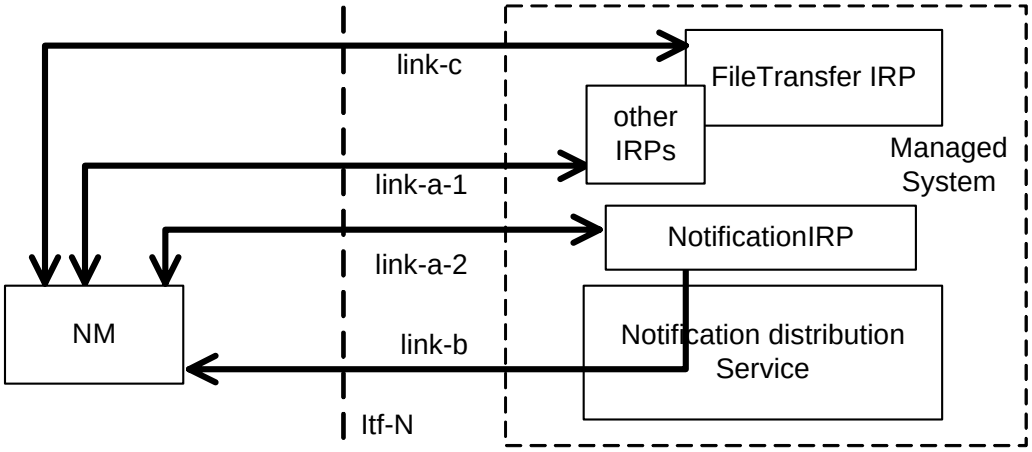

Figure 2: Security management context

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 subclause 5.3).

The Requirements are not related to other kinds of links nor entities that exist in the OAM&P 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 an Element Manager, a remote network management application accessing 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

The security architecture for 3G networks is defined within 3GPP TS 33.102 [4] based on the concept of stratums and feature groups. The present document extends the security architecture defined within 3GPP TS 33.102 [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.

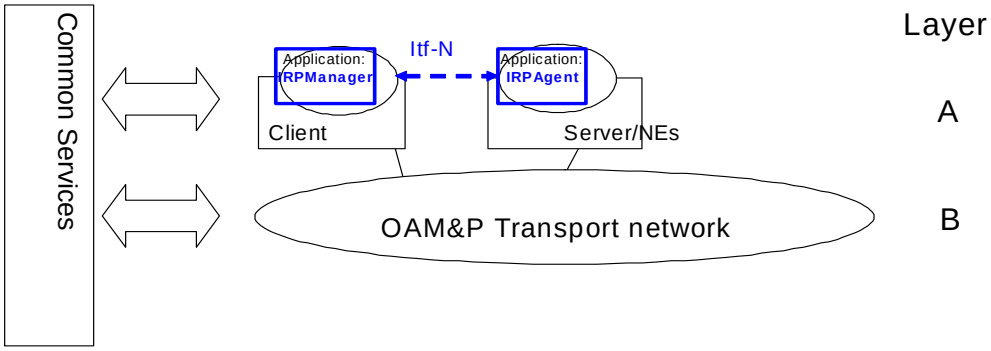

Figure 3: The Management layers of the 3G security architecture (based on 3GPP TS 32.101 [1])

Within the Management layer there is defined an additional security feature group. This feature group is:

OAM&P Domain Security (VI-for further study): the set of security features that provides protection to all OAM&P 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

6.1 Security threats to IRPs

The table below identifies the security threats in IRP context for the present release.

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 3): 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 headings 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 2: Matrix of security threats

	Manager Masquerade	Unauthorized Access	Agent Masquerade	Loss or Corruption	Eavesdropping (Note 3)	Repudiation
Basic CM IRP						
operation	H	H	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
Kernel CM IRP						
operation	H	H	L	N/A	L	H
Notification (note 4)	N/A	N/A	L	L	L	L
Bulk CM IRP						
operation	H	H	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
file content (Active) (note 1)	N/A	N/A	N/A	H	L	H
file content (Passive)	N/A	N/A	L	L	L	L
Alarm IRP						
operation	H	L	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
file content	N/A	N/A	N/A	N/A	N/A	N/A
Notification IRP						
operation	H	H (note 2)	L	N/A	L	H
notification (n/a)	N/A	N/A	N/A	N/A	N/A	N/A
TM IRP						
operation	H	H (note 2)	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
file content	N/A	N/A	L	L	L	L
FT IRP						
operation	H	H	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
file transfer	H	H	N/A	N/A	L	H
EP IRP						
operation	H	H	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
PM IRP						
operation	H	L(Note 2)	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
file content	N/A	N/A	N/A	L	L	L
CS IRP						
operation	H	L	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
NL IRP						
operation	H	L	L	N/A	L	H
notification	N/A	N/A	L	L	L	L
file content	N/A	N/A	N/A	L	L	L

Legend:

H: A security threat of a higher level.
L: A security threat of a lower level.
N/A: Not applicable.
TBD: To Be Decided.

NOTE 1: The IRPAgent shall check that a downloaded file has not been changed during a session before performing a pre-activation or activation.
NOTE 2: Relationship between operations is for further study.
NOTE 3: Assume security of DCN between IRPManager and IRPAgent is not described in the present document.
NOTE 4: Applicable when Kernel CM IRP used in isolation.

6.2 Mapping of Security requirements and Threats in IRP Context

It is necessary to take measures to prevent the threats described in subclause 6.1 in IRP context.

Table 3 shows how the threats identified in subclause 6.1 are countered by security mechanisms.

Table 3: Mapping of security requirements and threats

Security Requirements \ Security Threats	Manager Masquerade	Unauthorized Access	Agent Masquerade	Loss or Corruption	Eavesdropping	Repudiation
Manager Authentication	X	X				
Agent Authentication			X			
Authorization		X				
Integrity protection				X		
Confidentiality protection		X			X	
Non-repudiation						X
Security alarm	X	X		X		
Activity log	X	X				X (see note)
NOTE: Activity Log can partly counter the threat of Repudiation.						

7 Security requirement of Itf-N

Table 4 identifies the security requirements in IRP context for the present release.

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 bulk data.

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 the present document.

"File transfer" in row headings 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 headings of the table refers to the file content of file created or used by the corresponding IRP.

"Active" in relation to file content for Bulk CM IRP refers to configuration files downloaded to the IRPAgent from the IRPManager.

"Passive" in relation to file content for Bulk CM IRP refers to configuration files uploaded to the IRPManager from the IRPAgent.

Table 4 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	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
Kernel CM IRP								
operation	X	X	-	N/A	-	-	X	X
Notification (note 6)	N/A	N/A	-	-	-	-	N/A	-
Bulk CM IRP								
operation	X	X	-	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content (Active)	N/A	N/A	N/A	X	-	-	X	X (note 3)
file content (Passive)	N/A	N/A	-	-	-	-	N/A (note 2)	N/A
Alarm IRP								
operation	X	-	-	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content (note 1)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Notification IRP								
operation	X	X (note 5)	-	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 (note 5)	-	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	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file transfer	X	X	N/A	X (note 4)	-	-	X	X
EP IRP								
operation	X	X	-	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
PM IRP								
operation	X	X (note 5)	-	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	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
NL IRP								
operation	X	-	-	N/A	-	-	X	X
notification	N/A	N/A	-	-	-	-	N/A	-
file content	N/A	N/A	-	-	-	-	N/A	-

N/A: Not applicable.
"-": Not a Release 6 requirement.
X: A Release 6 requirement.

NOTE 1: N/A because no file transfer operations for this IRP have yet been defined.
NOTE 2: 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 3: For active files the activity log of Bulk CM IRP contains details of the suboperations.
NOTE 4: FT IRP is responsible for checking the integrity of the files transferred, but not the file content semantics.
NOTE 5: Relationship between operations is for further study.
NOTE 6: Applicable when Kernel CM IRP used in isolation.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Mar 2004	S_23	SP-040126	--	--	Submitted to TSG SA#23 for Information	1.0.0	