3GPP TSG SA WG3 Security ó SA3#35 **S3-040829**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG-SA5 (Telecom Management) **S5-046988**
Meeting #39bis, Sophia Antipolis, FRANCE, 27 Sept ñ 1 Oct 2004

Title:	**LS response to SA3 regarding Security of the Management Plane**
Response to:	**SA3 TD S3-040382 / S5-046680**
Release:	**Release 6**
Work Item:	**OAM-NIM, WT01 Security Management**
Source:	**SA5**
To:	**SA3**
Cc:	**-**

Contact Person:

Name:	**Thomas Tovinger (Chair SA5 SWG-C)**
Tel. Number:	**+46 31 747 3010**
E-mail Address:	**thomas.tovinger@ericsson.com**

Attachments:

3GPP TS 32.371 V6.0.0, Security Management Concept and Requirements (Release 6).

3GPP TS 32.150, V6.1.0, Integration Reference Point (IRP) Concept and Definitions (Release 6).

1. Overall Description:

SA5 would like to thank SA3 for the LS response Re: Security of the Management Plane in TD S3-040382 (from SA3#33). In particular, SA5 appreciated to be informed of the collected comments on ITU-T Security of the Management Plane.

SA5, as you may know, currently has a related work task (WT01) to address security aspects of the Itf-N (standardised NM/EM/NE OAM&P interface) within the Release 6 work plan. SA5 would like to invite SA3 to provide any comments on the first approved document produced by WT01: Security Management Concepts and Requirement, 3GPP TS 32.371 V6.0.0 (attached).

For an understanding of the SA5 IRP concept, please see 3GPP TS 32.150, Integration Reference Point (IRP) Concept and Definitions V6.1.0 (attached).

2. Actions:

To SA3

SA5 asks SA3 to provide any comments to SA5 regarding TS 32.371.

3. Date of Next SA5 Meetings:

SA5#40	15-19 Nov 2004	Sanya, Hainan	CN
SA5#41	24-28 Jan 2005	Lisbon, Portugal	EU

3GPP TS 32.150 V6.1.0 (2004-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Telecommunication management;
Integration Reference Point (IRP) Concept and definitions
(Release 6)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, 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.

1 Scope

The present document provides the overall concept for all Integration Reference Point (IRP) specifications produced by 3GPP. Relevant IRP overview and high-level definitions are already provided in 3GPP TS 32.101 [1] and 3GPP TS 32.102 [2].

The present document is a member of a TS-family consisting of:

3GPP TS 32.150: "Telecommunication management; Integration Reference Point (IRP) Concept and definitions".

3GPP TS 32.151: "Telecommunication management; Integration Reference Point (IRP) Information Service (IS) template".

3GPP TS 32.152: "Telecommunication management; Integration Reference Point (IRP) Information Service (IS) Unified Modelling Language (UML) repertoire".

2 References

The following documents contain provisions which, 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] 3GPP TS 32.151: "Telecommunication management; Integration Reference Point (IRP) Information Service (IS) template".

[4] 3GPP TS 32.152: "Telecommunication management; Integration Reference Point (IRP) Information Service (IS) Unified Modelling Language (UML) repertoire".

[5] ITU-T Recommendation M.3020: "TMN Interface Specification Methodology".

[6] OMG IDL Style Guide, ab/98-06-03, June 17, 1998

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 32.101 [1], 3GPP TS 32.102 [2], 3GPP TS 32.151 [3] and the following apply:

IRPAgent: See 3GPP TS 32.102 [2].

IRPManager: See 3GPP TS 32.102 [2].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TS 32.101 [1], 3GPP TS 32.102 [2], 3GPP TS 32.151 [3] and the following apply:

CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
EM	Element Manager
GDMO	Guidelines for the Definition of Managed Objects
GUI	Graphical User Interface
IDL	Interface Definition Language
IOC	Information Object Class
IRP	Integration Reference Point
IS	Information Service
NE	Network Element
NM	Network Manager
OMG	Object Management Group
ORB	Object Request Broker
PSA	Product Specific Application
SMP	System Management Processes
SNM	Sub-Network Manager
SS	Solution Set
TMF	TeleManagement Forum
TOM	Telecom Operations Map
UML	Unified Modelling Language

4 Integration Reference Points (IRPs)

4.1 Introduction

For the purpose of management interface development 3GPP has developed an interface concept known as Integration Reference Point (IRP) to promote the wider adoption of standardized management interfaces in telecommunication networks. The IRP concept and associated methodology employs protocol and technology neutral modelling methods as well as protocol specific solution sets to achieve its goals.

4.1.2 General

The three cornerstones of the IRP concept are:

- **Top-down, process-driven modelling approach:** The purpose of each IRP is automation of one specific task, related to TMF TOM. This allows taking a "one step at a time" approach with a focus on the most important tasks.

- **Technology-independent modelling:** To create from the requirements an interface technology independent model. This is specified in the IRP Information Service.

- **Standards-based technology-dependent modelling:** To create one or more interface technology dependent models from the technology independent model. This is specified in the IRP Solution Set(s).

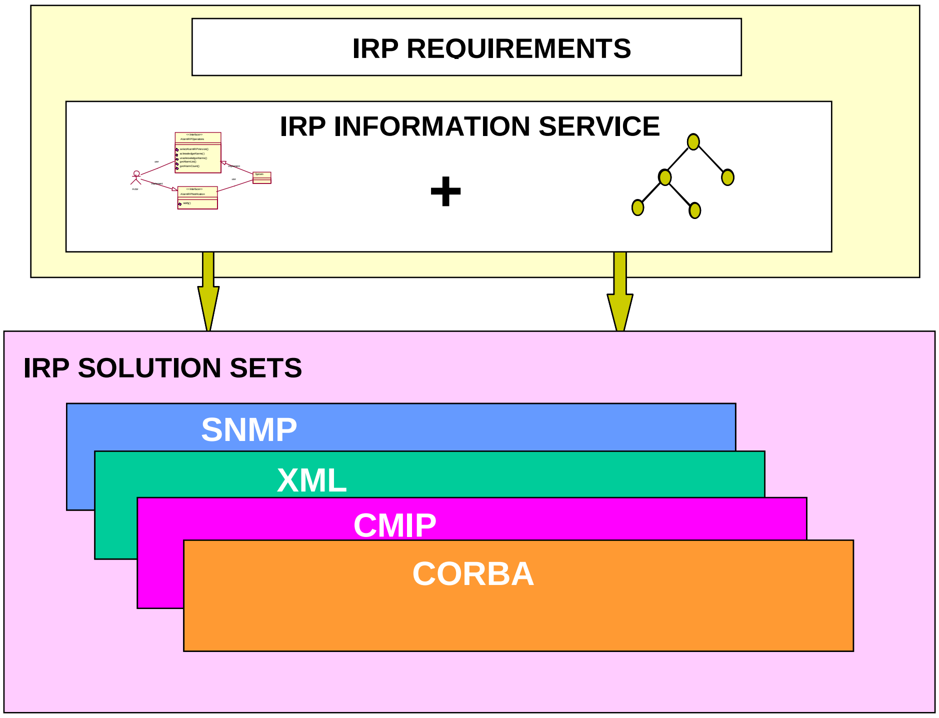

Figure 4.1: IRP components (with example Solution Sets)

4.1.2 IRP Specifications Approach

As highlighted in the previous subclause, IRP interfaces are specified using a 3-level approach: Requirements, IS-level specifications and SS-level.

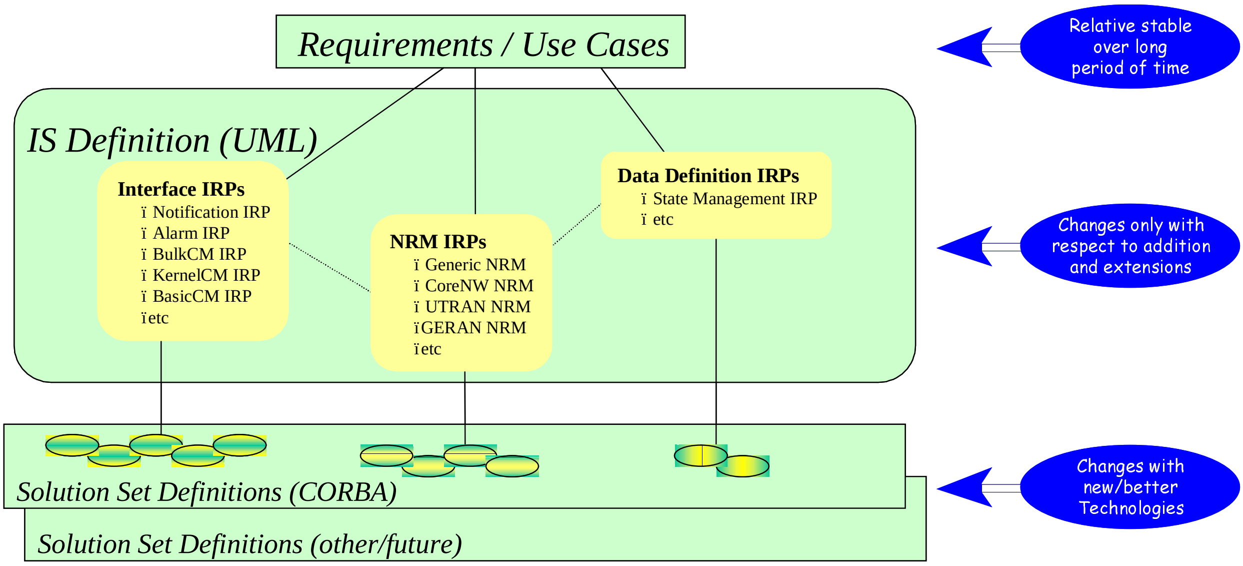

Figure 4.2: The IRP 3-Level Specifications Approach

Level 1:

The "Requirements-level" intends to provide conceptual and use cases definitions for a specific management interface aspect as well as defining subsequent requirements for this IRP.

Level 2:

The "IS-level" provides the technology independent specification of an IRP. From an IS-level perspective there are three types of IRP IS specifications:

- Interface IRPs - providing the definitions for IRP operations and notifications in a network agnostic manner.
- NRM IRPs - providing the definitions for the Network Resources to be managed through the Itf-N (commonly named "Network Resources IRPs").
- Data Definition IRPs - providing data definitions applicable to specific management aspects to be managed via reusing available Interface IRPs and being applied to NRM IRPs as applicable.

Level 3:

The "SS-level" finally provides the mapping of IS definitions into one or more technology-specific Solution Sets. This concept provides support for multiple interface technologies as applicable on a vendor and/or network type basis and also enables accommodation of future interface technologies - without the need to redefine requirements and IS-level definitions.

4.2 Integration levels

Virtually all types of telecom/datacom networks comprise many different technologies purchased from several different vendors. This implies that the corresponding management solution need to be built by integrating product-specific applications from different vendors with a number of generic applications that each provide some aspect of multi-vendor and/or multi-technology support. A complete management solution is thus composed of several independent applications.

The following levels of integration are defined:

- **Screen Integration:** Each application provides its own specific Graphical User Interface (GUI) that need to be accessible from a single, unified screen (a common desktop). A seamless integration between the various GUIs is then required. Screen Integration is not specified in the present document.
- **Application Integration:** Applications need to interwork, on a machine-machine basis, in order to automate various end-to-end processes of a communication provider.

4.2.1 Application integration

Interfaces related to application integration can be divided in the following three categories:

1) **High-level generic interfaces:** between generic applications on the network and service management layers. The same approach and concepts apply for these as the next category.

2) **High-level (technology-independent to the extent possible) interfaces:** between product-specific and generic applications are needed in order to automate and streamline frequently occurring tasks applicable to several types of network elements. A top-down approach shall be taken when defining these interfaces, where the main input is:

    a) business processes of a communication provider; and

    b) the types of generic applications that are used to implement the process support.

    The interfaces need to be stable, open and (preferably) standardized. These IRPs are discussed below under the heading Network Infrastructure IRPs.

3) **Detailed (product-specific) interfaces:** between product-specific applications and the corresponding network elements are of course also needed. These interfaces are defined using the traditional bottom-up approach, where the actual network infrastructure is modelled. This is the traditional TMN approach to element management. The management information in these interfaces is not further discussed in the present document, as it is internal to a specific development organization and does not need to be open. In fact, by publishing the management information in these interfaces, too much of the internal design may be revealed and it may become impossible to later enhance the systems that are using the interfaces. The management services (operations and notifications) and protocol shall however be open and standardized as long as they are independent of the NRM describing the managed NEs/NRs.

4.3 Network infrastructure IRPs

When providing integrated management solutions for multi-vendor networks, there is a strong requirement that the NEs and the management solutions that go together with them are systems integratable.

It should be noted that these IRPs could be provided by either the NE, or the Element Manager (EM) or Sub-Network Manager (SNM) that goes together with the type of NE. There is actually not a clear distinction any more between NE and Element Management applications, mainly due to the increased processing capacity of the equipment platforms. Embedded Element Managers providing a web user interface is a common example of that.

These IRPs are introduced to ensure interoperability between Product-Specific Applications (PSA) and the Network and System Management Processes (SMP) of the Network Manager (NM) (3GPP TS 32.101 [1]) shown in figure 4.3. These IRPs are considered to cover the most basic needs of task automation.

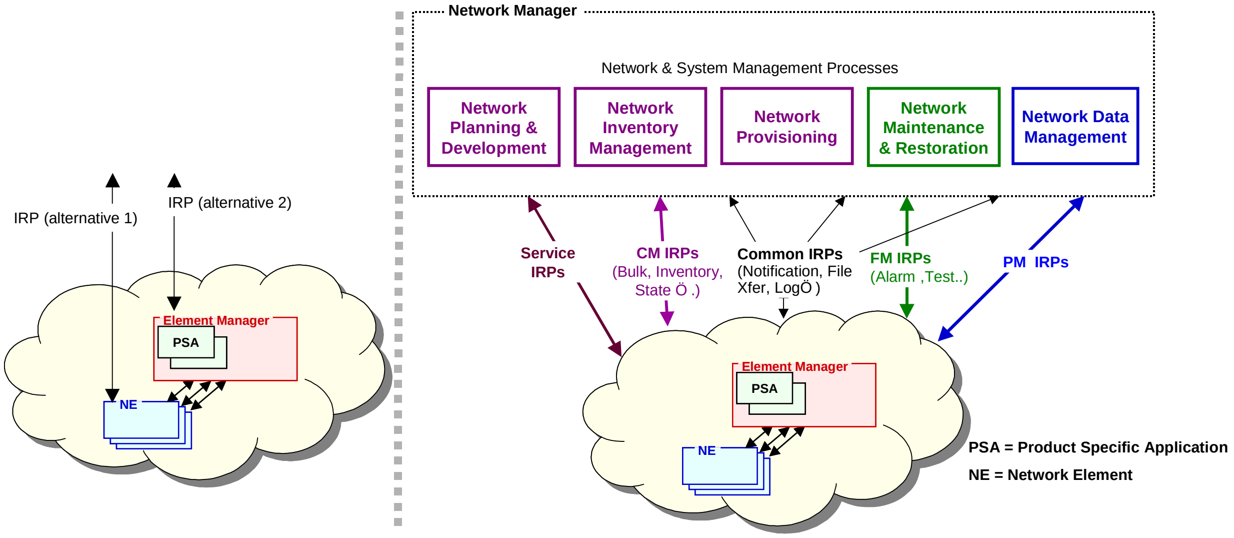
IRP (alternative 1)
IRP (alternative 2)
Element Manager
PSA
NE
Network Manager
Network & System Management Processes
Network Planning & Development
Network Inventory Management
Network Provisioning
Network Maintenance & Restoration
Network Data Management
Service IRPs
CM IRPs (Bulk, Inventory, State Ö .)
Common IRPs (Notification, File Xfer, LogÖ)
FM IRPs (Alarm ,Test..)
PM IRPs
Element Manager
PSA
NE
PSA = Product Specific Application
NE = Network Element

Figure 4.3: IRPs for application integration

The IRPs presented in figure 4.3 are just an example and do not reflect the exact set of IRPs defined by 3GPP.

Taking one of the Common IRPs as an example, the Network and System Management Processes have similar need to receive notifications from various PSAs. The corresponding service is formalized as a *Notification IRP*.
It specifies: firstly, an interface through which subscriptions to different types of notifications can be set-up (or cancelled), and secondly, common attributes for all notifications.

Further, applying a common *Name Convention for Managed Objects* is useful for co-operating applications that require identical interpretation of names assigned to network resources under management.

4.4 Defining the IRPs

It is important to accommodate more than one specific technology, as the technologies will change over time. Applications need to be future-proof. One fundamental principle for achieving this is to clearly separate the semantics of information definition from the protocols definitions (accessing the information) for the external interfaces.

The framework being used to define IRPs allows the implementation of user requirements for each management capability (e.g. configuration management), by modelling the information related to the resources to be managed and the way that the information may be accessed and manipulated. Such modelling is done in a way that is independent of the technology and distribution used in the implementation of a management system.

An IRP for a management capability is composed of three levels of specifications.

Level 1:

The first level of IRP specification captures the **requirements**.

Level 2:

The second level of IRP specifications known as "**IRP Information Service"**, specifies the **information** observable and controlled by management systemís client, related to the network resources under management, in a technology-independent way. It also specifies the semantics of the interactions used to carry applicable information.

Level 3:

The third level of IRP specification, known as **IRP Solution Set**, contains specification of the system in terms of interface technology choice (e.g. CMIP/GDMO, CORBA/IDL). In this type of specification, the syntax, rather than the semantics, is specified. At least one instance of a Solution Set is produced per interface technology supported.

The IRP methodology uses the following steps:

a) Capture the management requirements.

b) Specify the semantics of the information to describe the system. Trace back to item (a).

c) Specify the semantics of the interactions between the management system and its clients. Trace back to item (a).

d) Specify the syntaxes of the information and interactions identified in (b) and (c). The specification is technology dependent. Trace back to items (b) and (c).

As described above, the Information Service (IS) specification may contain two parts, the information related to the resources to be managed and the way that the information may be manipulated.

Part 1:

The first part defines the information types within a distributed system. It is in line with the Analysis phase of ITU-T Recommendation M.3020 [5]. From the point of view of the Network Level modelling work it reflects the information aspects (including states and significant transitions) of the managed resources and the management services. It defines information object classes, the relationships between these object types, their attributes and states along with their permitted state transitions. It may also define the allowable state changes of one or more information objects. As recommended in ITU-T Recommendation M.3020 [5], UML diagrams (class diagram, state diagram) are used to represent information when appropriate. This rest of the specification is described using an information description specified in natural language with appropriate label keywords (e.g. DEFINITION, ATTRIBUTE, CONSTRAINTS, etc.). A definition of the IS information template is provided in annex C.

Management service specific information objects may be created by subclassing from the objects in the basic network model, and extending them for that application. In this case, the new management service specific subclass may include other attributes, in addition to those defined in its superclass. Additional relationships and attributes may also be created as needed for that management service. Completely new objects can also be added.

Part 2:

The second part defines interfaces. Each interface contains one or more operations or one or more notifications that are made visible to management service users. An interface encapsulates information exchanged that is atomic in the sense that either all the information exchanged are visible (to management service users) or none. In addition, the specification of the information exchanged is in semantics only. No syntax or encoding can be implied. The operations or notifications are defined with their name, input and output parameters, pre and post conditions, raised exceptions and operation behaviour. These operation and notification specifications refer, through the utilization of parameter matching, to the information objects. A definition of the IS operations / notifications template is provided in annex C.

The Solution Set (SS) contains the mapping of the information objects and interactions (if applicable) specified in the IS-level specification, into their corresponding syntaxes of a particular chosen technology. The mapping is interface technology specific and satisfies scenarios where interfaces have been selected, according to mapping choices (driven for example by system performance, development cost, time-to-market). The mapping is not always one-to-one. General rules valid for all IRP SSs are defined in annex A. Rules for specific SSs, such as CORBA, are defined in an Annex to the present document as well as within each of the SS technologies used by 3GPP (as applicable).

Managed Object Classes as defined in a CMIP or CORBA Solution Set specifications represent a mapping into GDMO or IDL of Information Object Classes and other additional objects classes that can be introduced to support interfaces defined in the Information Service. Whether instances of Managed Object Classes are directly accessible or not may not be specified by IRP specifications.

Figure 4.4 shows an example of how an IRP can be structured (the Alarm IRP).

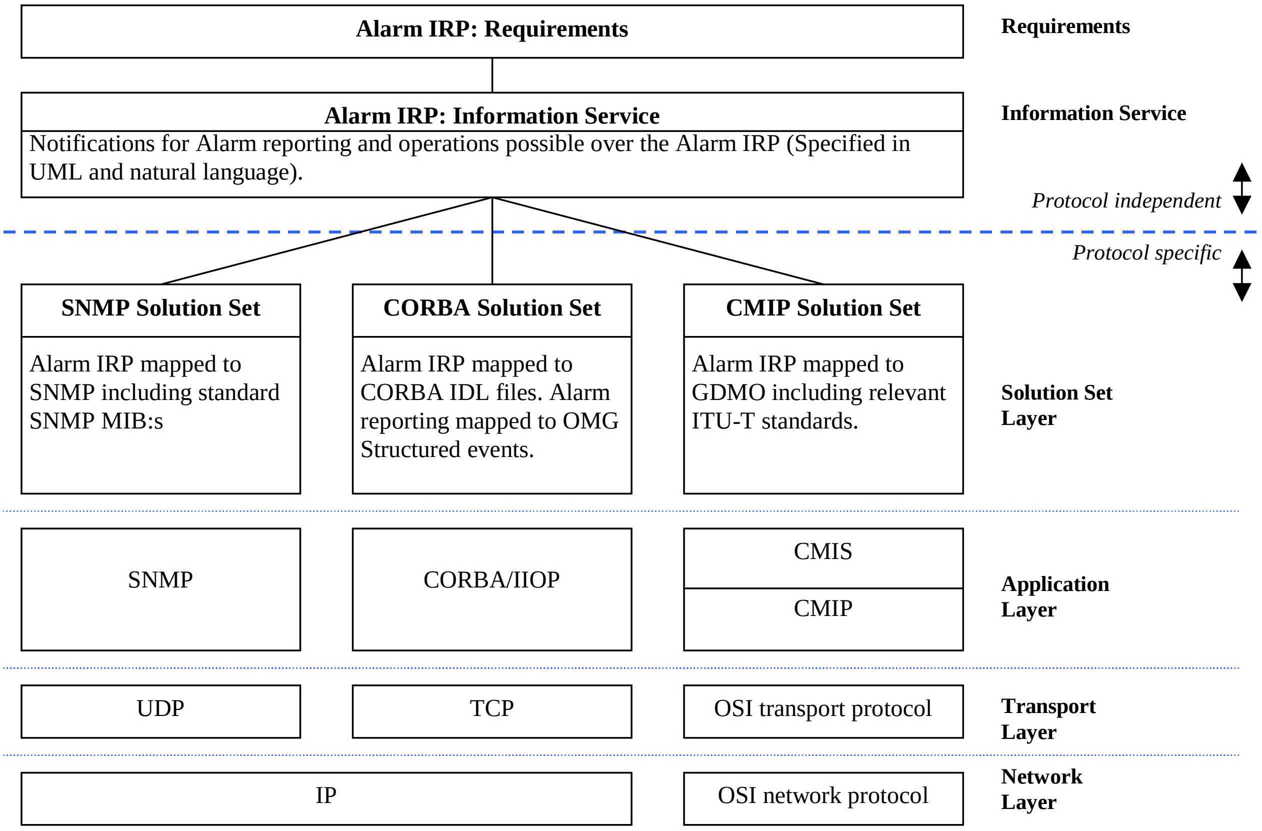
Alarm IRP: Requirements
Requirements
Alarm IRP: Information Service
Notifications for Alarm reporting and operations possible over the Alarm IRP (Specified in UML and natural language).
Information Service
Protocol independent
Protocol specific
SNMP Solution Set
Alarm IRP mapped to SNMP including standard SNMP MIB:s
CORBA Solution Set
Alarm IRP mapped to CORBA IDL files. Alarm reporting mapped to OMG Structured events.
CMIP Solution Set
Alarm IRP mapped to GDMO including relevant ITU-T standards.
Solution Set Layer
SNMP
CORBA/IIOP
CMIS
CMIP
Application Layer
UDP
TCP
OSI transport protocol
Transport Layer
IP
OSI network protocol
Network Layer

Figure 4.4: Example of an IRP (Alarm IRP)

4.5 Relationships among IS-level specifications

This subclause presents the target architecture of the SA5 IRP Information Models. This architecture is based on the concepts of level and partition of information. To achieve this, Information Object Classes (IOCs) and interfaces are defined and grouped into packages that can be related to each other through the *import* relationship.

Level means that the information models are structured in a way that enables re-utilization between levels, either through inheritance or through a traditional relationship between classes. Four levels are identified, namely:

1) A **Generic Network Resource Model**, also called "Generic NRM", which defines the information object classes that are independent of any:

    1. protocol (e.g. CORBA / IDL, CMIP / GDMO, etc.); and

    2. "domain specific network" (e.g. UTRAN, GERAN, CN).

    This Network Resource Model contains definitions of the largest subset of information object classes that are common to all the Network Resources Models to be defined in SA5. This Network Resources Model is part of Level 1. For this Information Service, a number of solution sets may be provided.

2) A number of **Domain-specific Network Resource Models**. Examples of these are: the CN Model, the UTRAN Model and the GERAN Model. They are part of Level 2. These Network Resource Models are specified in corresponding packages and import information object classes from the Generic Network Resources Model defined in Level 1. For each of these Information Services, a number of solution sets may be provided.

3) A number of **function-specific ISs**. Such information services as the Basic CM IRP IS, the Notification IRP IS and the Alarm IRP IS are part of this level. They are part of Level 3. These Information Services are specified in corresponding packages and may import information object classes and interfaces defined in Level 1 and 2. For each of these Information Services, a number of solution sets may be provided.

4) A number of (interface technology-independent) **Information Models**. Up to now, none of them have been defined. They will be part of Level 4. These Information Models are specified in corresponding packages and may import information object classes and interfaces defined both in Level 1, 2 and 3. An example of such Information Model could be a "UTRAN Alarm IM" (see figure 4.5). For each of these Information Models, a number of solution sets may be provided.

These levels provide a means for separation of concerns and re-utilization.

ISs shall be kept as simple as possible. To achieve this, Information Object Classes and interfaces shall be grouped into packages. The grouping shall be based on semantics, i.e. information object classes and interfaces that participate in the definition of a given IRP should be gathered into a dedicated package. See further example(s) on this in annex C.

Re-utilization of information specification contained in an IS previously specified shall be possible through the *import* relationship. The import relationship is a means for re-utilization: once a piece of information (i.e. an information object class, an attribute, a relationship or an interface) defined in an IS is imported in another IS, it is added to the name space of the importing IS. Then, the whole information available in a IS is made up of the information which is owned by the IS itself (i.e. defined in the present document) plus the information which is imported from other IS(s). This imported information can then be utilized in the importing IS, for instance, through:

- inheritance (e.g. any information object class defined at Levels 2 to 4 inherits from the information object class Top defined in the generic NRM at Level 1), either directly or indirectly;

- relationship (e.g. any information object class defined at Levels 2 to 4 may have a containment relationship with the information object class IRPAgent defined in the generic NRM at Level 1).

An illustration of this architecture is provided in figure 4.5; it uses the UML diagrammatic conventions.

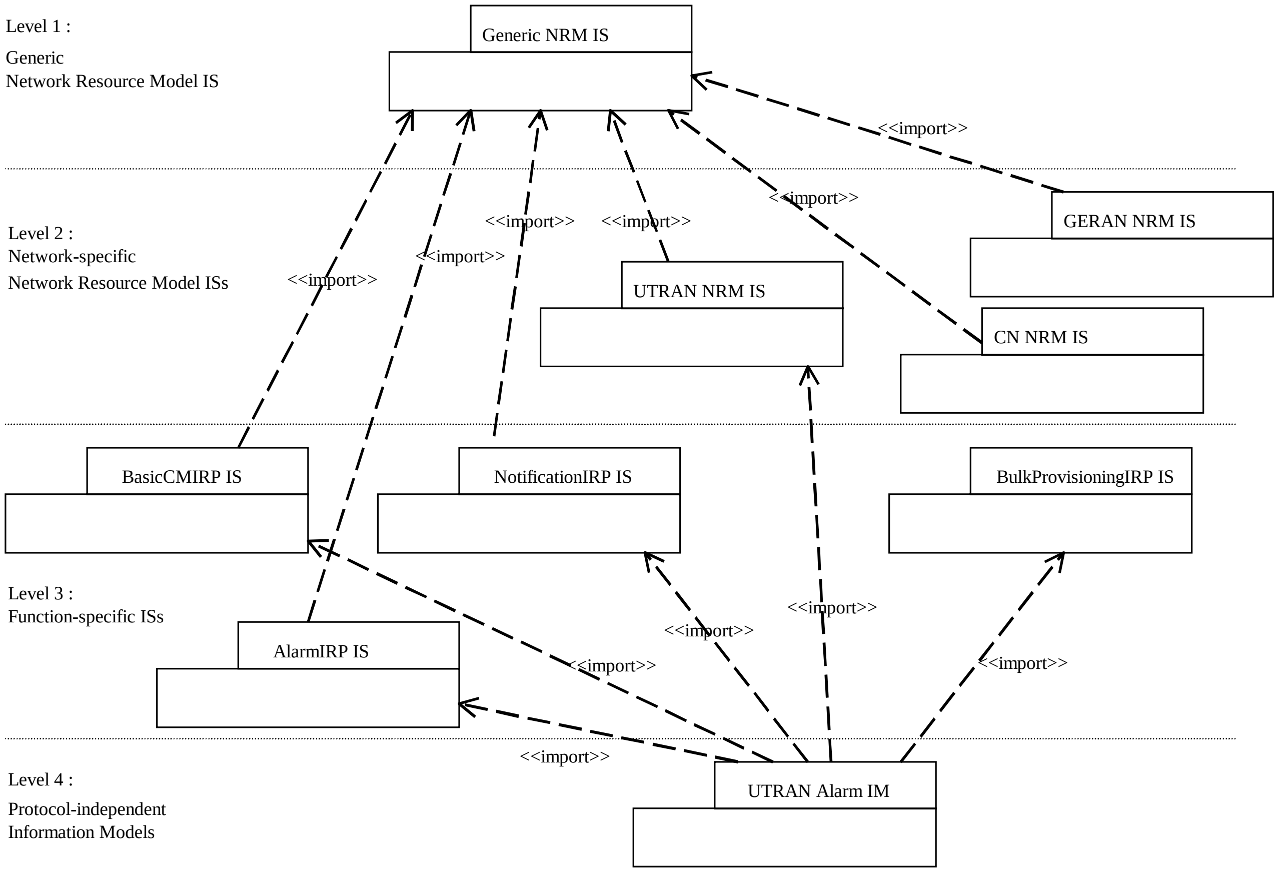

Figure 4.5: Specification architecture (not complete)

In order not to mix up the concept of "Information Object Class" and "interface" with other concepts such as "Managed Object Class" and "manager / agent interface", the former are labelled according to the UML notation capability (cf. stereotype). "Information Object Class" is defined as a stereotype of "Class" in the UML meta-model. As a consequence, information object classes defined in Information Models are labelled <<InformationObjectClass>>. Similarly, interfaces are labelled <<Interface>>. In annex C you can find an example of the inheritance between some ISs.

The following piece of information regarding the Semantics of the relationship "import" can be imported from other standard documents:

1. An Information Object Class. The definition of the IOC, the attributes and the roles that the IOC plays in some relationships are imported. The import clause shall specify the TS number from which the IOC is imported and the name of the IOC.

2. An attribute. Two cases are valid:

   2.1 An attribute definition. In this case, the attribute definition is imported. The import clause shall specify the TS number from which the attribute is imported and the name of the attribute.

   2.2 An attribute reference within an IOC definition. In this case, the attribute definition is imported together with its qualifier within the specified IOC. The import clause shall specify the TS number from which the attribute is imported, the name of the IOC and the name of the attribute.

3. A relationship. The definition of the relationship is imported. The import clause shall specify the TS number from which the relationship is imported and the name of the relationship.

4. An interface. The definitions of the interface and all its operations or notifications are imported. The import clause shall specify the TS number from which the interface is imported and the name of the interface.

5. An operation or a notification. The definition of the operation / notification is imported. The import clause shall specify the TS number from which the operation / notification is imported, the name of the interface in which the operation / notification is defined and the name of the operation / notification.

A piece of information **must** always be imported from the TS where it is initially defined. It cannot be imported from any other.

4.6 Mandatory, Optional and Conditional qualifiers

This subclause defines a number of terms used to qualify the relationship between the "Information Service", the "Solution Sets" and their impact on the IRP implementations. The qualifiers defined in this clause are used to qualify IRPAgent behaviour only. This is considered sufficient for the specification of the IRPs.

Table 4.1 defines the meaning of the three terms Mandatory, Conditional and Optional when they are used to qualify the relations between operations, notifications and parameters specified in "Information Service" documents and their equivalents in Solution Set (SS) specifications.

Table 4.1: Definitions of Mandatory, Optional and Conditional Used in Information Service specifications

	Mandatory (M)	Conditional (C)	Optional (O)
Operation and Notification	Each Operation and Notification shall be mapped to its equivalents in all SSs. Mapped equivalent shall be M.	Each Operation and Notification shall be mapped to its equivalents in at least one SS. Mapped equivalent can be M or O.	Each Operation and Notification shall be mapped to its equivalents in all SSs. Mapped equivalent shall be O.
Input and output parameter	Each parameter shall be mapped to one or more information elements of all SSs. Mapped information elements shall be M.	Each parameter shall be mapped to its equivalent in at least one SS. Mapped equivalent can be M or O.	Each parameter shall be mapped to its equivalent in all SSs. Mapped equivalent shall be O.
Information relationship	Each relationship shall be supported in all SS's.	Each relationship shall be supported in at least one SS.	Each relationship shall be supported in all SS's.
Information attribute	Each attribute shall be supported in all SS's.	Each attribute shall be supported in at least one SS.	Each attribute shall be supported in all SS's.

Table 4.2 defines the meaning of the two terms Mandatory and Optional when they are used to qualify the operations, parameters of operations, notifications and parameters of notifications in Solution Sets.

Table 4.2: Definitions of Mandatory and Optional Used in Solution Set Documents

Mapped SS Equivalent	Mandatory	Optional
Mapped notification equivalent	IRPAgent shall generate it.	IRPAgent may or may not generate it.
Mapped operation equivalent	IRPAgent shall support it.	IRPAgent may or may not support this operation. If the IRPAgent does not support this operation, the IRPAgent shall reject the operation invocation with a reason indicating that the IRPAgent does not support this operation. The rejection, together with a reason, shall be returned to the IRPManager.
input parameter of the mapped operation equivalent	IRPAgent shall accept and behave according to its value.	IRPAgent may or may not support this input parameter. If the IRPAgent does not support this input parameter and if it carries meaning (i.e. it does not carry no-information semantics), the IRPAgent shall reject the invocation with a reason (that it does not support the parameter). The rejection, together with the reason, shall be returned to the IRPManager.
Input parameter of mapped notify equivalent AND output parameter of mapped operation equivalent	IRPAgent shall generate it.	IRPAgent may generate it.

Annex A (informative): General rules for Solution Sets

A.1 Introduction

The intent of this annex is twofold. The first intent is for 3GPP-internal use to document how a 3GPP Solution Set is produced and what it shall contain. The second intent with the annex is to give the reader of an Information Service (IS) or a Solution Set (SS) a better understanding on how to interpret the IS or SS specifications.

A.2 Solution Set (SS) versioning

For further study.

A.3 Referenced Information Service (IS) specification

A sentence shall be included in the clause "Scope" of all Solution Set specifications. The sentence shall read as follows:

> "This Solution Set specification is related to Z".

where Z is the 3GPP Information Service (IS) specification number including the version, such as "TS 32.111-2 V4.1.X" for the case of Alarm Integration Reference Point (IRP): Information Service.

NOTE: that "X", rather than the actual digit, is actually used in the sentence. This is because the value of X is not relevant for the reference purpose since different values of X identify different 3GPP published specifications that reflect only minor editorial changes.

Annex B (normative): Rules for CORBA Solution Sets

B.1 Introduction

The intent of this annex is threefold.

1) The first intent is for 3GPP internal use to document how a 3GPP CORBA SS is produced and how it is structured.

2) The second intent with the annex is to give the reader or implementer of a CORBA SS a better understanding on how to interpret the CORBA SS specification.

3) The third and maybe most important intent is to put requirement on an implementer of a CORBA SS.

It is expected that this annex is to be extended in later versions of the present document.

B.2 Rules for specification of CORBA Solution Sets

B.2.1 Introduction

This subclause identifies rules for specification of CORBA SSs. This subclause is mainly for 3GPP-internal use. It is only for information for the implementer of a CORBA SS.

B.2.2 Pragma prefix

All IDL-code shall define the pragma prefix using the following statement:

#pragma prefix "3gppsa5.org"

See clause D.1.4.3 for information of this `#pragma` statement in relation to other IDL statements.

B.3 Implementation aspects of CORBA Solution Sets

B.3.1 Introduction

This subclause identifies rules for the implementation of CORBA SSs. This subclause is normative for the implementer of a CORBA SS.

B.3.2 IRPAgent behaviour on incoming optional method

The IRPAgent, claiming compliance to a particular SS version of a particular IRP such as the Alarm IRP, shall implement all Mandatory and all Optional methods. Each method implementation shall have a signature specifying all Mandatory and all Optional parameters.

- If the IRPAgent does not support a particular optional method, it shall throw the `OperationNotSupported` exception when the IRPManager invokes that method.

- If the IRPAgent have not implemented a particular method (because it is compiled with an IDL version that does not define the method), the CORBA ORB of the IRPAgent shall throw a system exception if the IRPManager invokes that method.

In all the above cases when an exception is thrown, the IRPAgent shall restore its state before the method invocation.

B.3.3 IRPAgent Behaviour on incoming optional parameter of operation

An IRPAgent must implement all optional parameters, as well as mandatory parameters, in all methods.

If the IRPAgent supports the implemented method but does not support its (one or more) optional input parameters, upon method invocation, the IRPAgent shall check if those parameters carry "no information" or absence semantics (defined later in subclause B.3.5). If the check is negative, the IRPAgent shall throw the `ParameterNotSupported` exception with a string carrying the name of the unsupported optional parameter.

B.3.4 IRPAgent Behaviour on outgoing attributes of Notification

CORBA SS uses OMG defined structured event to carry notification. The structured event is partitioned into header and body.

The absence semantics of attribute in the header is realized by a string of zero length.

The body consists of one or more name-value pair attributes. The absence semantics of these attributes is realized by their absence.

For optional sub-attributes of an attribute carried by the name-value pair, their absence semantics is realized by the encoding rule of "absence semantics". See subclause B.3.5.

B.3.5 Encoding rule of absence semantics

The operation parameters are mapped to method parameters of CORBA SS. The absence semantics for an operation (input and output) parameter is method parameter type dependent.

- For a string type, if the parameter is specified as a string type, the absence semantics is a string of zero length. If the parameter is specified as a union structure (preferred), the absence semantics is conveyed via a FALSE Boolean value switch.

- For an integer type, if the parameter is specified as a signed, unsigned, long, etc type, the absence semantics is the highest possible positive number. If the parameter is specified as a union structure (preferred), the absence semantics is conveyed via a FALSE Boolean value switch.

- For a boxed valueType (supported by CORBA 2.3), it is the null value.

The notification parameters are mapped to attributes of the CORBA Structured Events. The absence semantics for a notification parameter is attribute position (within the Structured Event) dependent.

- For the fixed header of the Structured Event header, the absence semantics is realized by a string of zero length.

- For the filterable body fields of the Structured Event body, the absence semantics is realized by the absence of the corresponding attribute.

B.4 Void

Annex C (informative): Example of inheritance between ISs

Figure C.1 illustrates the architecture defined in clause 4.6 with a simplified example. This figure is for illustration only.

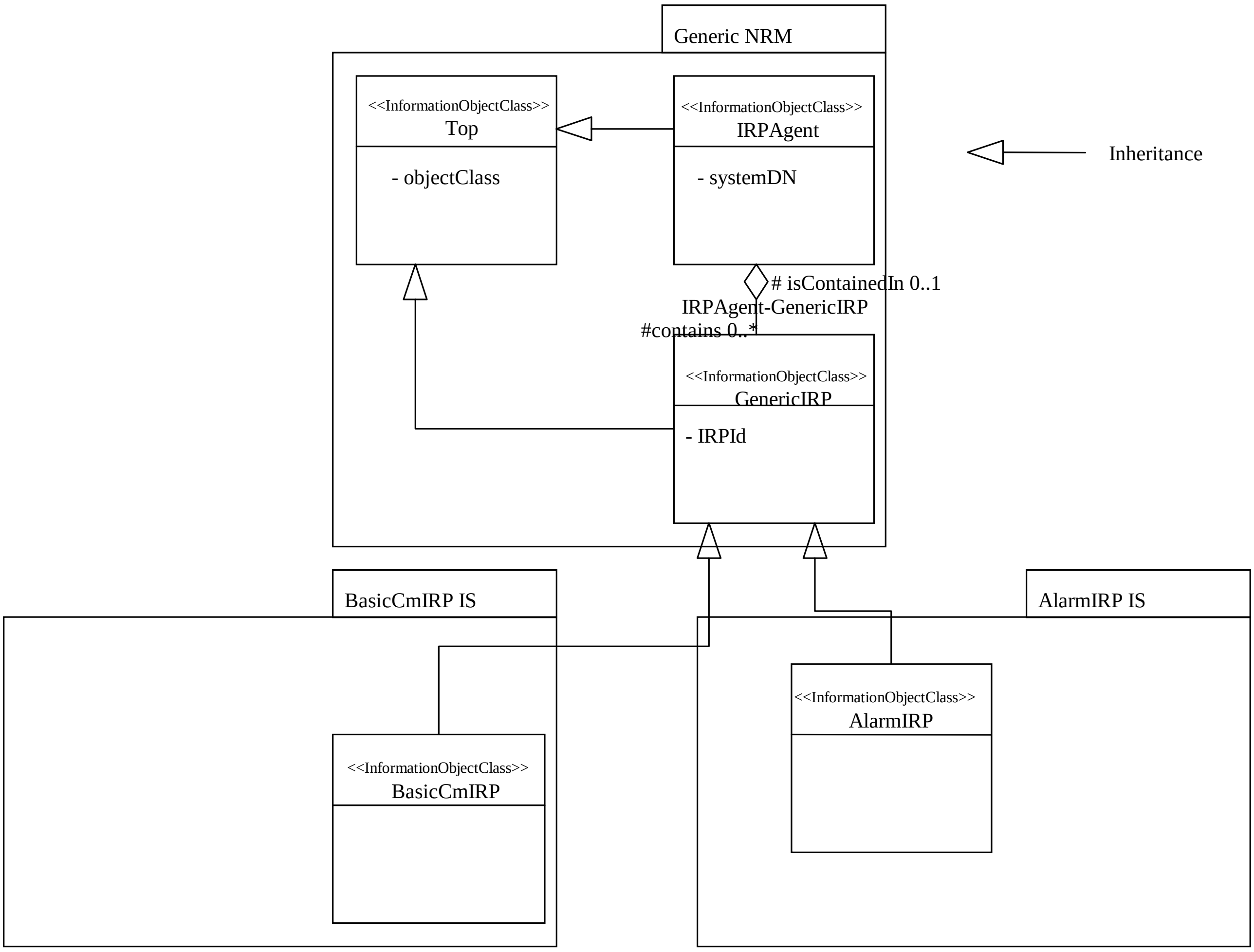

Figure C.1: Example of possible packages together with Information Object Classes (IOCs) and their inter-relationships

The following aspects are illustrated in figure C.1:

1) IOCs that are common to all Network Resources Models / some Information Services are captured in the GenericNRM package: Top, IRPAgent, GenericIRP, together with their attributes and relationships.

2) The IOC BasicCmIRP is defined in the BasicCmIRP IS package. As illustrated in the previous figure, this package imports the GenericNRM package.

3) The IOC AlarmIRP is defined in the AlarmIRP IS package. As illustrated in the previous figure, this package imports the GenericNRM package.

4) As a consequence, every IOC can inherit from the class Top, either directly or indirectly.

5) The IRPAgent class is defined in the GenericNRM.

6) A GenericIRP IOC is defined in the Generic NRM. It represents an abstraction of all the IRPs such as, e.g. BasicCmIRP or AlarmIRP. A containment relationship between IRPAgent and GenericIRP is defined.

7) Both the IOCs BasicCmIRP and AlarmIRP (defined in different ISs) inherit from GenericIRP. As a first consequence, they inherit the attributes IRPId and IRPVersion (from GenericIRP) and objectClass (from Top). As a second consequence, both BasicCmIRP and AlarmIRP are contained in IRPAgent.

Annex D (informative):
Style Guide for CORBA SS IDL

This annex is the style guide for writing IDL statements for Interface IRP and NRM IRP. The guidelines are largely based on the OMG IDL Style Guide (OMG document: ab/98-06-03) [6] with extensions for 3GPP IRP use.

The guide sets out consistent naming, structural conventions and usage of SS interface for the IDL in 3GPP IRP CORBA SS specifications.

D.1 Modules and File

D.1.1 Use of Modules

All declarations of IDL shall be contained in modules. No declarations of interfaces and definitions shall appear in the global scope.

Nesting modules is a useful technique when dealing with large namespaces to avoid name clashes and clarify relationships. A module nested within another module shall not have the same name as a top-level module in any other IRP CORBA SS specification.

D.1.2 File Names

CORBA SS specifications contain IDL statements.

The rule defined below specifies:

a) How to partition/extract these IDL statements to be placed in a file; and

b) How to name the file.

Note that IDL uses `"#include "X""` statement where `X` is a name of a file containing IDL statements.

Rule:

> In the annex where IDL statements are defined, use a special marker to indicate that a set of IDL statements shall be contained in one file. The name of the file shall be the name of the first IDL module, concatenated with four characters ì`.idl`î. Within a CORBA SS, multiple markers (implying multiple files), can be used.

It is not allowed to have an IDL module split into multiple files.

D.1.3 Include Conventions

All included IDL files shall be specified using the `"…"` form of `#include`. For example:

```
#include "ManagedGenericIRPConstDefs.idl"
```

D.1.4 File Structure

D.1.4.1 File Internal Identification

The first line of the IDL file shall contain ì//File:î followed by a single space followed by the name of the file. For example,

```
   //File: ExampleIRPConstDefs.idl
```

D.1.4.2 File Guard

An IDL file shall use a *guard* (consisting of three preprocessor lines) to avoid multiple definition errors. An example of a guard for the file called TestManagementIRPConstDefs.idl is:

```
#ifndef _TESTMANAGEMENTIRPCONSTDEFS_IDL_

#define _TESTMANAGEMENTIRPCONSTDEFS_IDL_


...remainder of the IDL


#endif // _TESTMANAGEMENTIRPCONSTDEFS_IDL_
```

D.1.4.3 Required Contents

If any other files are to be included, the #include statements come after the guard.

After #include lines, if any, and immediately before the module statement, the following line shall appear:

```
   #pragma prefix "3gppsa5.org"
```

D.1.4.4 Example illustrating a File Structure

```
   //File: ExampleIRPConstDefs.idl

   #ifndef _EXAMPLE_IRP_CONST_DEFS_IDL_

   #define _EXAMPLE_IRP_CONST_DEFS_IDL_


   // This module describes/is part of…

   #include "ExampleIncludeOne.idl"

   #include "ExampleIncludeTwo.idl"


   #pragma prefix "3gppsa5.org"
```

```
module ExampleIRPConstDefs {


// IDL Definitions here


};
#endif // _EXAMPLE_IRP_CONST_DEFS_IDL_
```

D.2 Identifiers

D.2.1 Mixed Case, Beginning Upper, No Underscores

The following categories of identifiers follow the *Mixed Case, Beginning Upper, No Underscores* rules:

- `module`
- `interface`
- `typedef`
- Constructed types (`struct, union, enum`)
- `exception`

The ìNo underscoresî rule is also applicable to all words that begin with an upper case letter with the remaining letters being lower case.

As a further note on naming, it is not necessary to append the value ì*Type*î to an identifier. The fact that it is a type is obvious from the consistent application of this naming convention.

Examples:

```
module PMIRPConstDefs(…);
interface AttributeNameValue(…);
```

D.2.2 Lower Case with Underscores

The following categories of identifiers follow the *Lower Case with Underscores* rules. All letters are lower case and words (if more than one) are separated with underscores.

- Operation name and notification name
- Attribute name
- Parameter name
- Structure member name

Examples:

```
get_notification_categories(…);
string comment_text;
void get_alarm_count (…, out unsigned long critical_count,..);
struct Comment {…; string user_id; string system_id;..};
```

D.2.3 Upper Case with Underscores

The following categories of identifiers follow *Upper Case with Underscores* rules. All letters are in upper case and words have an underscore separating them.

- Enum value
- Constant

Examples:

```
enum SubscriptionState {ACTIVE, SUSPENDED, INVALID};
const string JOB_ID = "JOB_ID";
```

D.2.4 Naming IDL Sequence Types

Typically a new type declared as an IDL sequence of another type will have the text ìListî appended to the name of the base type. Another convention is to declare such types as unordered sequences or ordered sets for consistency with ASN.1 notation. In this case they should have the ìSeqî or ìSetî (instead of ìListî) appended respectively.

Example of an ìordered setî:

```
typedef sequence <SubscriptionId> SubscriptionIdSet;
```

D.3 Interface IRP

Every Interface IRP should have 3 IDL modules (each specified in a separate IDL file):

```
module YyyIRPConstDefs {…};  // no change from Rel-5 practice.
module YyyIRPSystem {…}; // no change from Rel-5 practice.
module YyyIRPNotifications {…}; // new compared to Rel-5 practice
```

The first module defines all necessary IDL constructs, such as constant strings and type definitions, for the methods and notifications. The second module defines the methods. The third module defines the notifications.

D.3.1. Constant String and Type Definitions

This first module defines all necessary IDL constructs used by the methods (defined in the second module) and notifications (defined in the third module). The name of this module is YyyIRPConstDefs where Xxx is the name of the subject Interface IRP. An example is ìPMIRPConstDefsî.

Within this module, define data types used in the methods.

Also, define the data types of the attribute values used in the notifications.

CORBA SS authors should always check the generic types defined in ìManagedGenericIRPConstDefsî before creating a new type.

For the attribute names of the structured notifications, define an interface AttributeNameValue that captures the string definitions. Make sure these definitions do not clash with those defined for the notification header, i.e. notification id, event time, system DN, managed object class and managed object instance (see NotificationIRPNotification::Notify).

An example from PMIRPConstDefs:

```
/**
 * This block identifies attributes which are included as part of the
 * PMIRP. These attribute values should not
 * clash with those defined for the attributes of notification
 * header (see IDL of Notification IRP).
 */

interface AttributeNameValue
{
    const string JOB_ID = "JOB_ID";
    const string JOB_STATUS = "JOB_STATUS";
    const string REASON = "REASON";
    const string MONITOR_ID = "MONITOR_ID";
    const string MONITOR_STATUS = "MONITOR_STATUS";
};
```

D.3.2 Operations

The second module defines the methods. The name of the module is YyyIRPSystem where Yyy is the name of the subject Interface IRP. An example is AlarmIRPSystem.

At the beginning of this module, define all required exceptions. Naming conventions for exception are covered in D.2.1 above. CORBA SS authors should always check if the generic exceptions defined in the ManagedGenericIRPSystem can be reused before declaring new exception types.

Then define one interface called YyyIRP encapsulating all methods of the subject Yyy Interface IRP. If the subject Interface IRP IS specifies that its YyyIRP inherits from XxxIRP, then reflect the inheritance relation in the interface definition. The following is an example of AlarmIRP that inherits from ManagedGenericIRP.

```
module AlarmIRPSystem

{

…

…

interface AlarmIRP : ManagedGenericIRPSystem:: ManagedGenericIRP {…};

…

};
```

Naming conventions for operations are covered in D.2.2 above.

D.3.3 Notifications

Use a separate module to define the notifications. The name the module is YyyIRPNotifications where Yyy is the name of the subject Interface IRP. Examples are KernelCMIRPNotifications and PMIRPNotifications.

For NotificationIRPNotifications, do:

- Define one IDL interface Notify. Capture the four constant strings that are the names of the four NV (name value) pairs of filterable_body_field of the CORBA structured event. These four CORBA NV pairs are mapped from the five notification header attributes (defined by the Notification IRP IS), i.e. the objectClass, objectInstance, notificationId, eventTime and systemDN.

For YyyIRPNotifications where Yyy is not Notification, do:

- At the beginning of this module, define the const strings for the notification types that correspond to the set of notifications specified by (and not inherited by and not imported by) the subject Interface IRP.
- Then define a number of IDL interfaces corresponding to notifications specified in the subject Interface IRP. These interfaces should inherit from NotificationIRPNotifications::Notify. Within each interface, the first IDL statement defines the notification type (that is used as the second field of the fixed header of the structured notification). The second and subsequent IDL statements define the attribute names of this notification type, excepting those already defined by NotificationIRPNotifications::Notify. The data type of the attribute value, which is defined in YyyIRPConstDefs, should be mentioned in the comment block of this IDL statement.
- Then define a number of IDL interfaces corresponding to notifications imported, if any. These interfaces should inherit from the imported interface. An example is interface NotifyObjectCreation : KernelCMIRPNotifications:: NotifyObjectCreation. Within this interface, define all necessary IDL constructs, if any, which are not defined in the imported interface. This interface may contain no IDL statement if the IDL constructs defined in the imported interface are sufficient. For each interface imported, insert a comment ìThe first field of this notification carries the IRPVersion of this CORBA SS.î
- There is no need to re-define interfaces for notifications that are already specified in other Interface IRP, and from which the subject IRP inherits.

The following is an extract from PMIRPNotifications.

```
  module PMIRPNotifications
  {

     const string ET_MEASUREMENT_JOB_STATUS_CHANGED = "notifyMeasurementJobStatusChanged";
     const string ET_THRESHOLD_MONITOR_STATUS_CHANGED = "notifyThresholdMonitorStatusChanged";

     interface NotifyMeasurementJobStatusChanged: NotificationIRPNotifications::Notify
     {
       const string EVENT_TYPE = ET_MEASUREMENT_JOB_STATUS_CHANGED;

       /**
       * This constant defines the name of the jobId property,
       * which is transported in the filterable_body fields.
       * The data type for the value of this property
       * is PMIRPConstDefs::JobIdType.
       */
       const string JOB_ID = PMIRPConstDefs::AttributeNameValue::JOB_ID;

       …
       …
     };


     interface NotifyXXX : NotificationIRPNotifications::Notify
     {
         …
     };

     …
  };
```

D.4 NRM IRP

Use one module to define the IDL constructs for the managed object classes. The name of this module is `XxxNRIRPConstDefs` where `Xxx` is the name of the subject NRM IRP.

An example is `UtranNRIRPConstDefs`.

Within the module, define a set of IDL interfaces each of which corresponds to a managed object class specified. The interface definition respects the inheritance relation specified. An example of managed object class `RncFunction,` which inherits from `GenericNRIRPConstDefs::ManagedFunction`, is shown below.

```
module UtranNRIRPConstDefs
{
      Ö


      /**
       *  Definitions for MO class RncFunction
       */
      interface RncFunction : GenericNRIRPConstDefs::ManagedFunction
      {
         const string CLASS = "RncFunction";

         // Attribute Names
         //
         const string rncFunctionId = "rncFunctionId";

         const string mcc= "mcc";
         const string mnc= "mnc";
         const string rncId= "rncId";
      };
…
};
```

Annex E (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Dec 2003	S_22	SP-030613	--	--	Submitted to TSG SA#22 for Information	1.0.0	
Mar 2004	S_23	SP-040113	--	--	Submitted to TSG SA#23 for Approval	2.0.0	6.0.0
Sep 2004	S_25	SP-040559	001	--	Add Style Guide for CORBA SS IDL	6.0.0	6.1.0

3GPP TS 32.371 V6.0.0 (2004-09)

Technical Specification

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

Keywords

UMTS, Management, Security

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; as identified below:

TS 32.371: "Security Management Concept and Requirements";

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

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

TS 32.374: "Security Management 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].

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].

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.

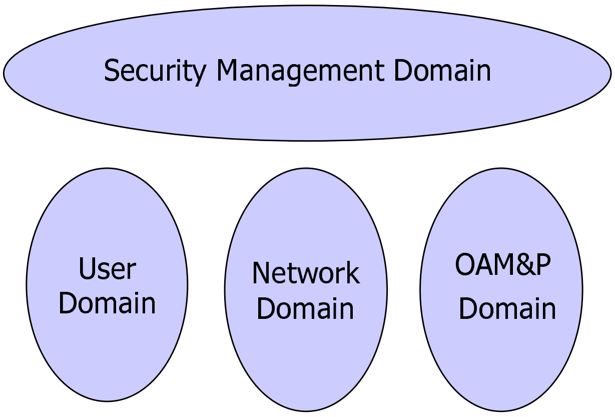

Figure 1: Security model/architecture

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.

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".

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.

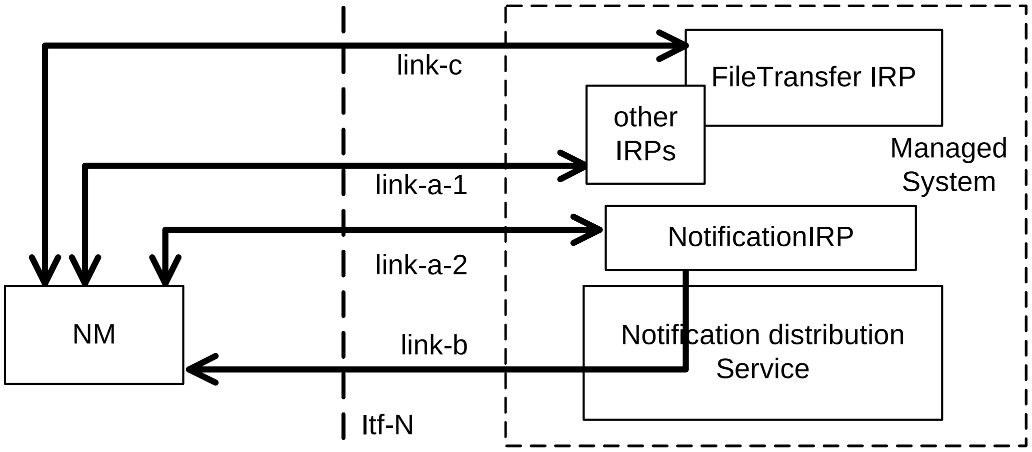

Figure 2: Security management context

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.

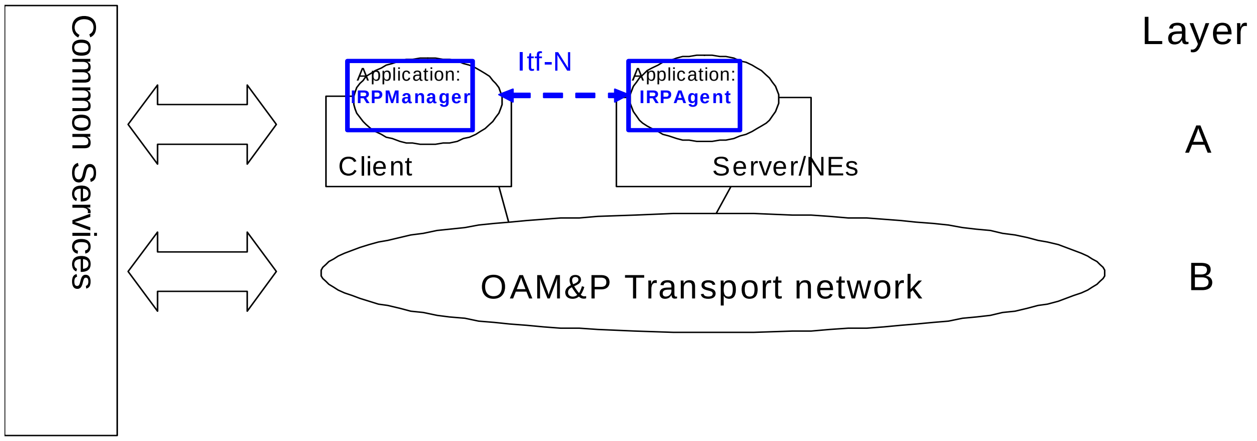

Figure 3: The Management layers of the 3G security architecture (based on 3GPP TS 32.101 [1])

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 is 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 Threats **Security Requirements**	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 is used in isolation.

Annex A (informative): Protocols for IP Network Security to Support Itf-N

Many security threats exist to the management plane of the telecommunications networks. In addition, new security threats to the management plane are being introduced as the network evolves. The purpose of this document is to provide security guidelines for using IP Network security protocols such as Internet Protocol Security (IPsec), SSL/TLS (Secure Socket Layer/Transport Layer Security) and Secure Shell(SSH) to help mitigate security risks to the management network. The security provided by IP Network security protocols may be obtained by implementing these protocols within network equipment or through the use of external mechanisms such as IPsec VPN devices.

In some telecommunications networks, management traffic is transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the management plane are isolated from malicious activity on the end-user plane. With evolving telecommunications networks however, management traffic is often combined on a single network with end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, new security challenges are introduced. Threats in the end-user plane now become threats to the management plane since the management plane becomes accessible to the multitude of end-users. Thus security, which was very important before, becomes even more critical with the evolving network.

Scope

This document provides recommendations and guidelines for using IP Network security protocols such as Internet Protocol Security (IPsec), SSL/TLS (Secure Socket Layer/Transport Layer Security) and Secure Shell (SSH) to help mitigate security risks for management traffic. The use of IP Network security protocols can be used to provide a basic level of network security for the 3GPP Itf-N interface and underlying network used to transport management traffic. In addition to the use of IP Network security protocols, other aspects of security including operator authentication/authorization, operating system hardening and security event logging must also be considered to provide an overall secure solution, however these aspects are beyond the scope of this document.

Framework Model

The framework model used by this document is from Figure 1, clause 5.1.1 of TS 32.101 [TS 32.101]. This diagram, reproduced below in Figure 1, identifies a set of interfaces used by 3GPP. The recommendations of this document apply specifically to management interfaces of Type 2 [EM-NM; also known as Interface N], including the underlying IP transport network used to support this interface.

The recommendations and guidelines in this document may also be considered in future to provide security for other interfaces such as the Type 1 [NE-EM] interface.

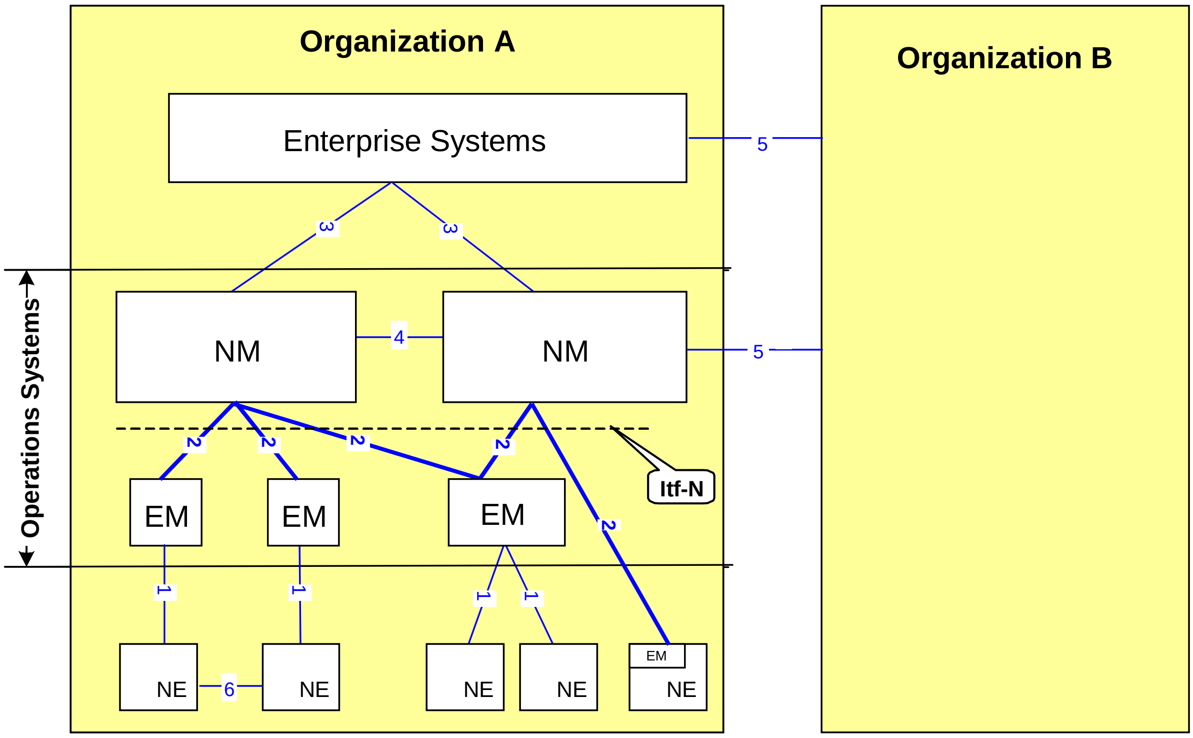

Figure A.1: 3GPP Management System Interactions

Security Threats

A number of serious security threats are commonly associated with the OAM&P management network infrastructure. Security threats include Masquerade, Eavesdropping, Unauthorized Access, Loss/Corruption of Information, Repudiation, Forgery and Denial of Service.

Attacks may be launched from inside the network by insiders such as disgruntled employees and also from external sources such as hackers. IP Network security protocols such as IPsec, SSL/TLS and SSH can be effective in mitigating many of these security threats. In addition, other security services may be able to make use of security provided by the IP Network security protocols. For example passwords used for application level authentication will be protected against eavesdropping when transmitted over a network infrastructure secured by IP Network security protocols.

Table 1, taken from ITU-T Recommendation M.3016, illustrates a mapping of security functions required to mitigate identified security threats [M.3016]. In Table 2, the general capabilities of IP Network security protocols (IPsec, SSL/TLS and SSH) is mapped against required security functions. This illustrates how IP Network security protocols can help mitigate security vulnerabilities.

Table A.1: Correlation of Security Management Functional Area with Threats (from ITU-T Recommendation M.3016 [2])

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			
Activity logging		x		x		x	x	x
Alarm reporting		x		x	x			x
Audit		x		x		x	x	x

Table A.2: Correlation of Security Functional Area with Security Services Provided by IP Network Security Protocols

Functional Requirement Area	Threat Mitigation Measures Provided by IP Network Security Protocols.
Verification of identities	Machine-to-machine (server-to-server) authentication services can be provided based on password or X.509 certificates. Application layer authentication is not provided.
Controlled access and authorization	Network/transport layer packet filtering service can reject non-authorized packets.
Protection of confidentiality	Confidentiality service is provided by underlying encryption technology within the Network Security protocol. The strength of the encryption service can vary to extremely strong dependent on underlying encryption algorithm and key length chosen.
Protection of data integrity	Strong data integrity service is provided by underlying cryptographic service within the Network Security protocol. (E.g. Keyed Hashed Message Authentication Code with Secure Hash Algorithm-1).
Activity logging	Not provided.
Alarm reporting	Not provided.
Audit	Not provided.

Security Solutions

Application Layer Security

Application layer security provides a security solution targeted specifically to a particular application, which must be implemented in the end hosts. Application layer security has the advantage of easy access to user credentials because it operates in the context of the user, which makes user AAA services easier to implement. Also, an application can be extended for security without having to depend on the operating system to provide these services.

The disadvantage of application level security is that security mechanisms must be designed independently for every application that needs to be secured. Thus, it is very difficult to create seamless and scalable security architectures using only application layer security.

Transport Layer Security

Transport layer security provides security services at the Transport layer (Layer 4). SSL, which has been revised and standardized by the Internet Engineering Task Force (IETF) as TLS, is the security protocol that provides security at the transport layer.

A single SSL/TLS instance can be used to create multiple SSL/TLS sessions through an Internet protocol (IP) network to provide security for various applications. Modifications are required to each application to allow that application to request SSL/TLS security services. SSL/TLS is the de-facto standard for Web-based HTTP traffic, and all standard Web browsers include built-in SSL/TLS technology.

Because SSL/TLS technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services. SSL/TLS is applicable only to TCP traffic and cannot be used to protect UDP traffic.

Network Layer Security

Network layer security provides security services at the Network layer (Layer 3). The IETF IPsec Suite is the security protocol that provides security at the network layer. IPsec is optional for IPv4 and a mandatory component of IPv6. IPsec can be used to protect data from any different application or transport protocols. No modifications are required to the applications, and the security services appear transparent to the applications. IPsec is the de-facto standard used for creating network layer virtual private networks. (IPsec VPN).

Because IPsec technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services.

Recommendations

Service providers are increasingly using in-band network management and thus logical separation of management traffic through the use of IP network security protocols is a beneficial security practice. Also, security statistics show that up to 70% of all compromises of resources are caused by ìinsidersî. Use of IP network security protocols for management traffic provides a good degree of protection against insiders with the exception of the small group of insiders that have legitimate access to the encryption keys.

It is recommended to provide baseline infrastructure security between machines communicating across the Itf-N through the use of IP network security protocols such as IPsec, SSL/TLS and SSH. These IP network security protocols employ security services through the use of cryptographic mechanisms and provide services including data confidentiality, data integrity, machine-to-machine authentication, and others. The recommended IP network security protocols are IPSec (Internet Protocol security suite), Secure Shell (SSH), and Secure Socket Layer/Transport Layer Security (SSL/TLS), and the choice and use of a particular IP network security protocol is based on particular service provider requirements.

External IPsec VPN devices may also be used to meet these recommendations for protection of management traffic. Using an external IPSec VPN instead of embedded IPsec solutions however introduces extra complexity and does not provide end-to-end protection between management servers. Thus the preferred longer-term solution is to incorporate the capability directly into the management platforms.

All of the IP network security protocols rely on underlying cryptographic algorithms such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), TDEA (Triple Data Encryption Algorithm), HMAC-MD5 (Hashed Message Authentication Code with Message Digest 5), HMAC-SHA-1 (Hashed Message Authentication Code with Secure Hash Algorithm-1), RSA (Rivest, Shamir, Adleman) and other cryptographic algorithms to provide the security services. Please note that the choice of particular cryptographic algorithms and key lengths for use with IP network security protocols is based on particular service provider and market requirements, and no specific recommendations are made in this document. {References [FIPS-46-3], [FIPS-197], [RFC 2403], [RFC 2404], [RFC 2437]}.

IPsec Security Services:

Overview and Capabilities

IPsec addresses security at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms. IPSec protocol runs between the Network layer (Layer 3) and the Transport layer (Layer 4) and can be used to protect any type of data traffic (TCP or UDP) and is independent of applications. IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered by IPsec includes:

a) Data integrity

b) Data origin authentication based on IP address

c) Machine-to-machine authentication

d) Anti-Replay Protection

e) Data confidentiality

f) Cryptographic key exchange

These objectives are met through the use of two traffic security services, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. AH service provides data origin authentication, machine-to-machine authentication and data integrity for IP packets. ESP service provides data confidentiality service in addition to data origin authentication, machine-to-machine authentication and data integrity for IP packets. IPsec mechanisms also designed to be cryptographic algorithm-independent to permits selection of different sets of algorithms without affecting the other parts of the implementation.

Key Management is provided by the Internet Key Exchange (IKE) protocol. Both manual and automatic mechanisms for key negotiation between endpoints are provided. Automatic key negotiation can be based on pre-shared keys (e.g. passwords) or X.509 certificates.

Recommendations for use of IPsec for Itf-N Security

This section provides basic recommendation for the use of IPsec for protection of network management traffic crossing the Itf-N interface, and is not intended to be exhaustive.

a) The Itf-N servers operate in a client-server (host to host) environment and therefore the use IPsec transport mode versus IPsec tunnel mode is recommended.

b) ESP service is recommended versus AH service since it can provide encryption service and/or authentication services. AH service can only provide authentication service.

c) It is recommended to use always use the optional ESP authentication service when using ESP encryption service.

d) If only authentication services are needed, it is recommended to use ESP service with null encryption to accomplish this.

e) It is recommended to choose underlying cryptographic algorithms depending on service provider and market requirements. (For North American applications 128 bit AES should be strongly considered).

f) References [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197].

SSL/TLS Security Services:

Overview and Capabilities

The Secure Sockets Layer (SSL) security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection at the transport layer (layer 4). SSL is currently at revision 3.0. Transport Layer Security (TLS) is the IETF standardized version of SSL which includes security enhancements over SSL including:

- Required Diffie-Hellman and DSA digital signatures algorithm (DSA) support, with optional RSA support.
- Use of stronger hashed message authentication algorithm (HMAC) instead of a non-standard SSL defined MAC algorithm.
- Modified key generation algorithm which uses MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) with the HMAC.

The SSL/TLS protocol runs above the Network Layer (Layer 4) and works with Transport Control Protocol (TCP) protocol only and cannot work with User Datagram Protocol (UDP). The application layer protocols that commonly run on top of SSL/TLS include, but are not limited to, Hypertext Transport Protocol (HTTP), the Lightweight Directory Access Protocol (LDAP), and the Internet Messaging Access Protocol. Higher application-level protocol can work above SSL/TLS without any regard for SSL/TLS; however the application level must be linked to SSL/TLS through the use of I/O callbacks.

The SSL/TLS protocol provides three security functions for TCP traffic: data confidentiality, data integrity and authentication.

The SSL/TLS security protocol architecture provides two layers which run over TCP: The SSL/TLS Upper Layer Protocols, and the SSL/TLS Record Protocol.

The SSL/TLS Upper Layer Protocols includes the SSL/TLS Handshake Protocol, SSL/TLS Cipher Change Protocol, and the SSL/TLS Alert Protocol for notifications. SSL/TLS sessions are initially created by the SSL/TLS handshake protocol which provides:

a) Negotiation of authentication and security mechanisms.

b) Authentication of client and server. (Using the server and client public/private keys).

c) Establishment of security keys.

Once the SSL/TLS session is established, the SSL/TLS Record Protocol is used for bulk data transport services. The SSL/TLS Record Protocol provides:

a) Data origin authentication based on the server keys.

b) Data integrity.

c) Confidentiality.

Recommendations for use of SSL/TLS for Itf-N Security

This section provides basic recommendation for the use of SSL/TLS for protection of network management traffic crossing the Itf-N interface, and is not intended to be exhaustive.

a) Where SSL/TLS is required, either SSLv3 or TLS may be used . However, it is noted that TLS has enhanced security over SSL.

b) SSL/TLS allows either unidirectional authentication where the server is authenticated to the client only, or bidirectional authentication where both client and server authenticate to each other. Unidirectional authentication is the usual method used in the public internet, however for network management applications bidirectional authentication is recommended to allow both parties to know they are communicating with the desired endpoint.

c) References [RFC 2246], [RFC 3546], [SSL V3].

SSH Security Services:

Overview and Capabilities

SSH is an Application Layer (Layer 7) security protocol commonly used to directly replace insecure protocols Telnet and File Transfer Protocol (FTP) protocols. Telnet and FTP are insecure protocols which transmit passwords and all other data in the clear. SSH can also be used to protect other protocols through the use of port forwarding, so it can be used as a general network security protocol..

There are two versions of SSH: SSHv1 and SSHv2. SSHv1 was developed in 1998 and is now considered insecure/obsolete.

Secure Shell 2 features are:

- Full replacement for Telnet, Rlogin, Rsh, Rcp, and FTP protocols to provide secure file transfer and file copying.
- Automatic authentication of users. (no passwords sent in clear-text).
- Bi-directional authentication (both the server and the client are authenticated).
- Tunneling of arbitrary TCP/IP-based applications through the use of port forwarding.
- Encryption of data for data confidentiality.
- Multiple authentication options including passwords, public key, and SecureID authentication
- Multiple ciphers suites available.

The SSHv2 architecture is consists of three major components:

- The Transport Layer Protocol [SSH-TRANS] provides server authentication, data confidentiality, and data integrity. It may optionally also provide compression.
- The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server.
- The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels.

The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunneling") arbitrary TCP/IP ports and connections.

Port number 22 has been registered with the IANA as the standard port to use for SSHv2 applications.

Recommendations for use of SSH for Itf-N Security

This section provides basic recommendation for the use of SSH for protection of network management traffic crossing the Itf-N interface, and is not intended to be exhaustive.

a) It is recommended to use SSHv2 where SSH protocol is required because of its widespread acceptance and enhanced security over SSHv1.

b) SSHv1 should be considered insecure/obsolete.

c) Interoperating with an SSHv1 protocol is not recommended and SSHv1 connection attempts should be rejected.

d) References [SSH-ARCH], SSH-TRANS], [SSH-USERAUTH], [SSH-CONNECT].

Conclusions/Recommendations

IP Network Security protocols (IPsec, SSL/TLS or SSH) can be used to provide baseline infrastructure security between machines communicating across the Itf-N. It is recommended to use these IP Network security protocols to provide underlying security for the 3GPP OA&M network, with the choice of protocols and cryptographic dependant on particular service provider and market requirements.

References

[TS 32.101]	3GPP TS 32.101: "Telecommunication management; Principles and high level requirements".
[M.3016]	ITU-T Recommendation M.3016 (1998): "TMN security overview".
[RFC2401]	IETF RFC 2401, "Security Architecture for the Internet Protocol", November 1998, S. Kent, R. Atkinson; http://www.ietf.org/rfc/rfc2401.txt?number=2401
[NDS/IP]	3GPP TS 33.210, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security.
[RFC 2402]	IETF RFC 2402, "Internet Protocol Authentication Header", November 1998, S. Kent, R. Atkinson; http://www.ietf.org/rfc/rfc2402.txt?number=2402
[RFC 2403]	IETF RFC 2403, " The Use of HMAC-MD5-96 within ESP and AH,î http://www.ietf.org/rfc/rfc2403.txt?number=2403
[RFC 2404]	IETF RFC 2404, " The Use of HMAC-SHA-1-96 within ESP and AH,î http://www.ietf.org/rfc/rfc2404.txt?number=2404
[RFC 2405]	IETF RFC 2405, "The ESP DES CBC Cipher Algorithm with Explicit IV,î http://www.ietf.org/rfc/rfc2405.txt?number=2405
[RFC 2406]	IETF RFC 2406, "IP Encapsulating Security Payload (ESP),î http://www.ietf.org/rfc/rfc2406.txt?number=2406
[RFC 2407]	IETF RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP,î http://www.ietf.org/rfc/rfc2407.txt?number=2407
[RFC 2408]	IETF RFC 2408, " Internet Security Association and Key Management Protocol,î http://www.ietf.org/rfc/rfc2408.txt?number=2408
[RFC 2409]	IETF RFC 2409, "Internet Key Exchange,î http://www.ietf.org/rfc/rfc2409.txt?number=2409
[RFC 2410]	IETF RFC 2410, ìThe Null Encryption Algorithm and Its Use with IPsec,î http://www.ietf.org/rfc/rfc2410.txt?number=2410
[RFC 2411]	IETF RFC 2411, ìIP Security Document Roadmap,î http://www.ietf.org/rfc/rfc2411.txt?number=2411
[RFC 2412]	IETF RFC 2412, ìThe OAKLEY Key Determination Protocol,î http://www.ietf.org/rfc/rfc2412.txt?number=2412
[RFC 3602]	IETF RFC 3602, ìThe AES-CBC Cipher Algorithm and Its Use with IPsecî http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt
[RFC 2451]	The ESP CBC-Mode Cipher Algorithms http://www.ietf.org/rfc/rfc2451.txt
[RFC 2246]	IETF RFC 2236, ìThe TLS Protocol, Version 1.0î ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt
[RFC 3546]	IETF RFC 3546, ìTransport Layer Security (TLS) Extensionsî ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt
[SSL V3]	Secure Socket Layer Version 3.0 Specification, Netscape Communications. http://wp.netscape.com/eng/ssl3/
[SSH-ARCH]	Ylonen, T., "SSH Protocol Architecture", I-D draft-ietf-architecture-15.txt, Oct 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt
[SSH-TRANS]	Ylonen, T., "SSH Transport Layer Protocol", I-D draft-ietf-transport-17.txt, Oct 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt
[SSH-USERAUTH]	Ylonen, T., "SSH Authentication Protocol", I-D draft-ietf-userauth-18.txt, Sept 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt
[SSH-CONNECT]	Ylonen, T., "SSH Connection Protocol", I-D draft-ietf-connect-18.txt, Oct 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt
[FIPS-46-3]	Data Encryption Standard. (Describes both DES and 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
[FIPS-197]	Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[FIPS-197]	Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[RFC 2437]	PKCS #1: RSA Cryptography Specifications Version 2.0. B. Kaliski, J. Staddon. October 1998 http://www.ietf.org/rfc/rfc2437.txt?number=2437

Annex B (informative): Firewalls for Network Security to Support Itf-N

A firewall is a fundamental security building block that provides network isolation at boundaries between network segments or between different networks. A firewall performs isolation based on specific traffic filtering rules configured onto the firewall. Firewalls may be used in conjunction with other security mechanisms to provide an additional layer of security for the Itf-N interface. For the Itf-N interface, firewalls may be used to only allow traffic between the IRPManager and IRPAgent host machines to transit the firewall boundaries. The addition of firewalls at the Itf-N interface helps provide ìdefense in depthî security whereby multiple security mechanisms are overlaid to achieve stronger security.

A firewall examines both inbound and outbound traffic, and should be configured to deny all traffic unless specifically allowed by the firewall rules. A firewall may also provide logging of traffic and trigger alarms when unauthorized packets are detected. Firewalls can physically be provided for the Itf-N interface as separate appliances at the IRPManager and IRPAgent host machines or may be provided as software on the host machines themselves. Types of firewalls include static packet filtering, application layer, and state aware packet filtering firewalls. Any of the firewall types may be used to provide protection for the Itf-N interface, and the choice will depend on particular customer needs and preferences.

Static packet filtering firewalls examine incoming and outgoing packets and apply a set of rules to determine whether packets will be allowed to transit the firewall or be dropped. This determination is typically based on the packet source and destination IP addresses, the protocol type, and the TCP source and destination ports. Depending on the packet and the criteria, the firewall will drop or forward the packet, and possibly create a log entry and/or raise an alarm. Some static packet filtering firewalls may also provide deeper inspection of packets, possibly up to the application layer.

Application layer firewalls run applications on behalf of the machines in the network they are protecting, and are often called ìproxyî firewalls. When performing the applications, application layer firewalls will detect any anomalous activity and if found will not pass the data onto the machines they are protecting. Application layer firewalls must be enabled with all necessary application and must run these applications on behalf of all protected machines. Because of this, application layer firewalls have a high impact on network performance.

State aware firewalls perform packet filtering functions similar to static packet filtering firewalls, and in addition maintain information about the state of traffic connections. The state information allows the firewall to make better decisions about whether to allow or deny particular traffic. For example, a state aware firewall may be configured to only allow traffic from machines on one side of the network to initiate communications. This is particularly useful where private networks are connected to public networks since typically only the machines on the private network are trusted to initiate data communications.

When using firewalls as an additional security mechanism for the Itf-N interface, the firewalls should be configured to allow only communication between the IRPManager and the IRPAgent host machines. Any other traffic on the network attempting to access the IRPManager or IRPAgent host machines should be denied. This will isolate the IRPManager to IRPAgent network communications from other network traffic, thereby providing a layer of protection for these machines.

Note that providing firewalls may have system engineering and product impacts, and some applications may have to be made firewall aware. Also note that firewalls will not protect against all security attacks such as an attacker spoofing legitimate IRPManager or IRPAgent packet information.

Annex C (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	
Sep 2004	S_25	SP-040565	--	--	Submitted to TSG SA#25 for Approval	2.0.0	6.0.0