ETSI TS 132 372 V7.0.0 (2007-03)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Telecommunication management;
Security services for Integration Reference Point (IRP):
Information Service (IS)
(3GPP TS 32.372 version 7.0.0 Release 7)

Reference
DTS/TSGS-0532372v700

Keywords
GSM, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

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 part of a TS-family covering the 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; as identified below:

32.371: "Security Management concept and requirements".

32.372: "Security Services for Integration Reference Points (IRP): Information Service (IS)".

32.373: "Security Services for Integration Reference Points (IRP): Common Object Request Broker Architecture (CORBA) solution".

32.375 "Security Services for Integration Reference Points (IRP): File integrity solution".

In 3GPP SA5 context, IRPs are introduced to address process interfaces at the Itf-N interface. The Itf-N interface is built up by a number of Integration Reference Points (IRPs) and a related Name Convention, which realise the functional capabilities over this interface. The basic structure of the IRPs is defined in 3GPP TS 32.101 [1] and 3GPP TS 32.102 [2]. An 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 mechanisms 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 - O&M IP Network.

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

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

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

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

1 Scope

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.

The present document specifies the Security Service for IRP Information Service.

This Security Service for IRP IS defines the semantics of management information visible across the Itf-N in a protocol and technology neutral way. It does not define the syntax or encoding of the operations and their parameters.

This Information Service specification is related to 3GPP TS 32.371 [6].

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 OSI for CCITT Applications".

[6] 3GPP TS 32.371: "Telecommunication management; Security Management concept and requirements".

[7] 3GPP TS 32.150: "Telecommunication management; Integration Reference Point (IRP) Concept and definitions".

[8] 3GPP TS 32.373: "Telecommunication management; Security Service for Integration Reference Point (IRP):Common Object Request Broker Architecture (CORBA) Solution".

3 Definitions and abbreviations

3.1 Definitions

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

IRP: See 3GPP TS 32.101 [1].

IRPAgent: See 3GPP TS 32.102 [2].

IRPManager: See 3GPP TS 32.102 [2].

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

The present document makes use of the following terms and definitions from 3GPP TS 32.371 [6]:

access control: prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

authentication: See data origin authentication and peer element authentication in 3GPP TS 32.371 [6].

authorization: granting of rights, which includes the granting of access based on access rights

credential: Authentication and Authorization data that can be used to authenticate the claimer is what it claims to be and authorize the claimer's access rights

signature: cryptographic information appended to the transferred management information that allows a receiver to verify integrity of the transferred management information.

3.2 Abbreviations

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

CM	Configuration Management
EM	Element Manager
IOC	Information Object Class
IRP	Integration Reference Point
IS	Information Service (see 3GPP TS 32.101 [1])
Itf-N	Interface N
NDS	Network Domain Security
NE	Network Element
NM	Network Manager
NRM	Network Resource Model
OS	Operations System
PM	Performance Management
SAS	Security Attribute Service
TMN	Telecom Management Network
UML	Unified Modelling Language (OMG)
UMTS	Universal Mobile Telecommunications System

4 System overview

4.1 System context

The general definition of the System Context for the present IRP is found in 3GPP TS 32.150 [7], clause 4.7.

In addition, the set of related IRP(s) relevant to the present IRP is shown in the two diagrams below.

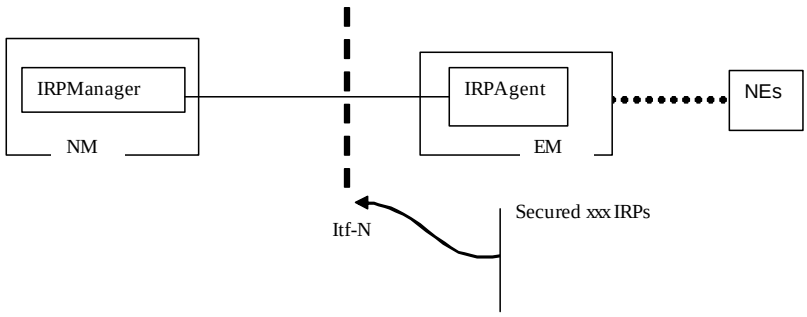

Figure 4.1.1: System Context A

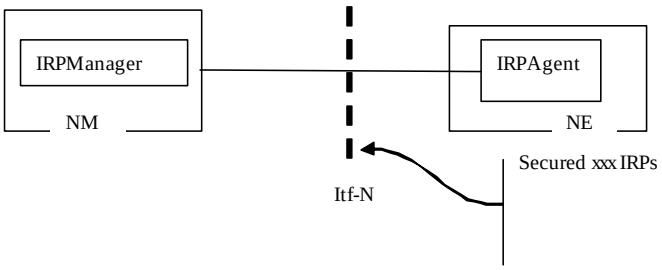

Figure 4.1.2: System Context B

4.2 Security Architecture

Figure 4.2.1 shows a view of the architecture of the IRPAgent and IRPManager in the context of a Secured IRP.

Secured communication between IRPManager and IRPAgent is realised by using one or more Security Services to address the specific identified threats.. Note that there is no mandatory need to support all of the security services, these services may be used on an as needed basis in order to counter identified threat(s). The agreements regarding which security services are necessary are subject to network operator and equipment vendor negotiation and are not the subject of standardization.

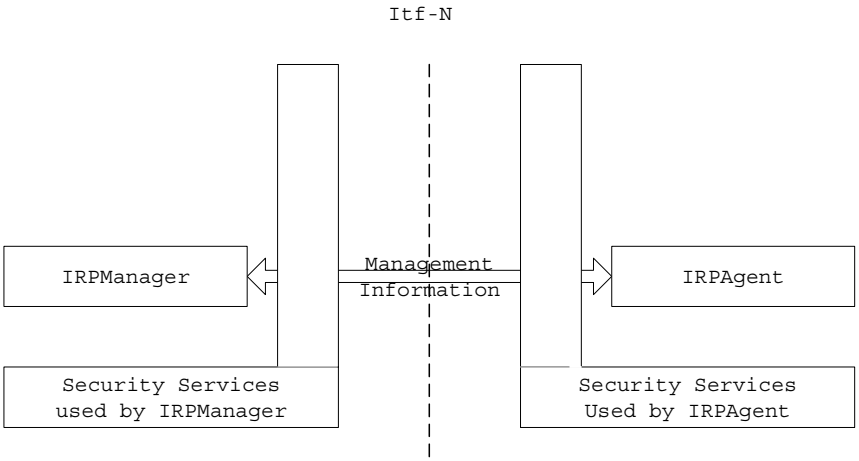

Figure 4.2.1: Security Architecture for a secured IRP

The environment in which the IRPManager and IRPAgent operate has a big impact on identifying set of potential threats and appropriate security services to be deployed. If the Itf-N used is within the operator's closed network, which has no possibility of connection to external pubic networks there may not be a need for using any security services. However if the Itf-N used can be accessed via a public network, then if Security Services are not used for the communication between yyyIRP and IRPManager then the IRP can be considered as being non-secured IRP. To enable Secured communication between a particular IRPManager and its corresponding yyyIRP, both have to use their respective IRPManager, and IRPAgent side Security Services appropriate to the identified threats.

Some security services are expensive both in terms of license costs, and machine CPU cycles, it is not advised to make use of all the security services unless they are indeed necessary as the resulting solution will be impacted both by costs such as larger processing machines (to cope with the additional protocols and authorization checking algorithms) with possibly degraded performance when compared with an unsecured implementation.

4.2.1 Security Features offered by IP Transport Network (IPsec or NDS)

The IP transport network may be protected by using IPSec, or NDS (Network Domain Security.

It is assumed throughout this IS that some of the Security Services are provided by a transport network which may be secured as per informative annexes A and B of 3GPP TS 32.371 [6] to provide the following Security capabilities:

1. Confidentiality of authentication information.
2. Confidentiality of session identification information.
3. Data integrity.

4.2.2 Limitations of IP transport layer security

Figure 4.2.2 shows several inter connected ORBs which can communicate with each other. IPSec provides a protected point to point transport connection. However should any unprotected transport allow an alien ORB onto the CORBA bus, the "protected " communications links will guard against an alien ORB, as it will share any inter-ORB communications via the IIOP protocol from any ORB which somehow gains access to the CORBA bus. Once access to the CORBA bus has been obtained, normal inter ORB communications will permit access to any connected ORB, even if there is a point to point IPSec connection to the "protected" ORB.

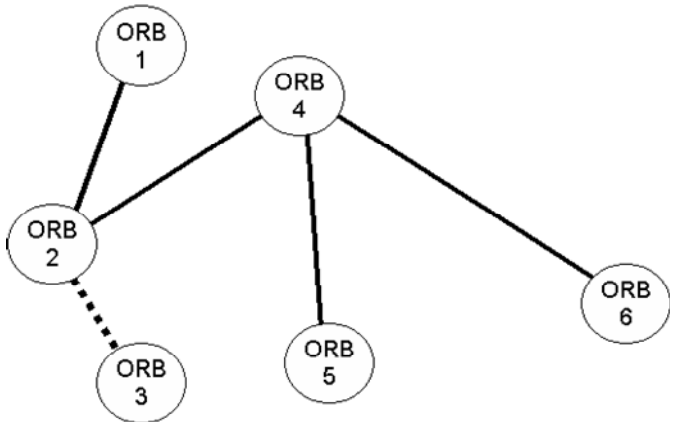

Figure 4.2.2: TLS and ORB to ORB communication Risks

For example ORB 3 uses an unprotected IP transport connection. Since ORB 3 can communicate to ORB 2, it can also use any of the "protected" ORBs 1,2, 4, 5 or 6. i.e. TLS needs to be used cautiously.

In Summary, IPSEC is a cheap, and efficient manner of protecting point to point communications links. Care has to be taken in the overall design of the secure system regarding how all systems intercommunicate and the protection offered at each ORB in the network, as point to point security is only as strong as the weakest link.

4.3 Compliance rules

All of the security services described in the present document may be used on an as needed basis, and are all therefore optional. Actual usage is subject to the environment and the related threats which need to be prevented by counter measures. Selection of counter measures is subject to negotiation between an equipment provider and a network operator, and as such is outside the scope of the present document.

For general definitions of compliance rules related to qualifiers (Mandatory/Optional/Conditional) for operations, notifications and parameters (of operations and notifications) please refer to 3GPP TS 32.102 [2].

5 Security Services

This clause addresses Security Services which meet IRP security Requirements addressed in 3GPP TS 32.371 [6].

Table 5.1.1 shows which Security Service meets which Security Requirement.

Table 5.1.1: Security Requirement and Security Service relationship

	Manager Authentication Security Requirement	Agent Authentication Security Requirement	Authorization Security Requirement	Integrity protection Security Requirement	Security alarm Security Requirement	Activity log Security Requirement
Authentication Security Service	X	X				
Authorization Security Service			X			
Activity Log Security Service						X
File Integrity Security Service				X		

NOTE 1: The "X" in the matrix above means the relationship between the Security Service and relevant Security requirement that the Security Service meets.
NOTE 2: It is defined in 3GPP TS 32.371 [6] that:
- Integrity protection Security requirement is applicable to BulkCMIRP active file and files transferred by FTIRP.
- Confidentiality protection Security requirement is not applicable to any IRP.
- Security alarm is supported by AlarmIRP.

For Authentication Security Service, Authorization Security Service, and File Integrity Security Service, each of them is composed of two parts, i.e. Security Service on IRPManager side and Security Service on IRPAgent side. These Security Services meet corresponding Security requirements respectively by exchanging relevant security attributes between the two parts. Table 5.1.2 shows relationship between security attribute and Security Service.

Table 5.1.2: Security Attribute and Security Service relationship

	Authentication Security Service	Authorization Security Service	Activity Log Security Service	File Integrity Security Service
Credential Security Attribute	X	X	X	
Signature Security Attribute				X

NOTE: Activity Log Security Service does not log the Credential Security Attributes.

5.1 Authentication Security Service

The authentication Security Service is provided by exchanging Authentication information as required between the communicating peers. In this present document, the authentication information used to provide the identity of communication peer is defined is the Security Attribute "Credential".

To authenticate an IRPManager , the IRPManager's Authentication Security Service generates an IRPManager Credential, This credential is sent with each and every request to the IRPAgent.

The IRPAgent's Authentication Security Service receives the IRPManager's Credential, and validates it. If the validation is successful, IRPAgent processes the request and sends requested results back to the IRPManager.

IF the authentication fails an alert mechanism may be used to indicate the attempted security breach and the IRPManagers request is to be rejected. It is not always appropriate to raise an Itf-N security alarm as doing so may provide information to the system attempting unauthorized access - this is left open for negotiation depending upon agreed local policies.

5.1.1 Mutual Authentication

Once the IRPManager has been authenticated by the IRPAgent the IRPManager may perform IRPAgent Authentication if required to achieve mutual Authentication.

To authenticate an IRPAgent the IRPAgent's Authentication Security Service generates the IRPAgent's Credential. The IRPAgent sends it's credential with each request result sent to the IRPManager.

The IRPManager's Authentication Security Service receives the IRPAgent's response plus the IRPAgent's Credential, and validates it.

If the validation is successful, the IRPManager can accept request results from the IRPAgent and may send additional requests to the IRPAgent.

If the authentication fails the IRPManager ceases making any more requests to the IRPAgent or accepting any request result from the IRPAgent.

The Credential should be exchanged over Itf-N in a secured way to avoid eavesdropping or other security risk. This is achieved by applying encryption algorithm to Authentication information that can't be known or held by any entity other than the owner.

The Authentication Mechanism used for the application layer Authentication Security Service is solution specific. Industrial Authentication Mechanisms available for application layer Authentication Security Service is shown in 3GPP TS 32.373 [6], annex A. For transport/network layer Authentication Security Service, Authentication Mechanisms are defined in respective transport/network security protocols addressed in annex A of 3GPP 32.371 [6]. The concrete content of Credential is dependent on the Authentication Mechanism applied.

In secured IRP scenario, IRPManager and IRPAgent shall agree with the use of a specific Authentication Mechanism.

Editor's note: whether the establishment of the agreement is within 3GPP scope or not is FFS.

This TS-family recommends a number of Authentication Mechanisms for use. Out of the scope is:

- to recommend / identify encryption algorithm to be used by Authentication Mechanism;
- to recommend key distribution mechanism.

5.2 Authorization Security Service

Authorization Security Service is provided by controlling access to resource(s) to only those users who are authorized due to an enforced access control policy. Usually an access control policy is a necessary component of Authorization Security Service, it contains access identity indicating authorized user, identity indicating access rights, their relationship of ownership, and maybe other context information as well.

In Itf-N scenario, IRPManager side Authorization Service provides IRPManager's accessor identity to IRPAgent side Authorization Security Service when IRPManager sends request to IRPAgent, IRPAgent side Authorization Security Service validates if the IRPManager is authorized to make the desired request by checking IRPManager's accessor identity against the access control policy on behalf of IRPAgent.

The accessor identity of IRPManager is a part of Credential stated above, which will be transferred over Itf-N, it is:

a) either the same as its Authentication identity, that is authorized certain access rights according to the access control policy; or

b) an identity of role/group, that is authorized certain access rights according to the access control policy.

Access control policy may be specified in one of the following access right granularities:

1. Authorization to use particular IRPs.
2. Authorization to perform particular operations within an IRP.
3. Authorization to perform a particular operation on particular IOCs or IOC instances.
4. Authorization to perform within specific contexts such as time schedule, workstation, and such things.
5. Authorization to access or use a specific non-persistent logical IOC, e.g. Bulk CM session, notification registration.

In secured IRP scenario, IRPManager and IRPAgent shall agree with the access control policy before starting communication, i.e. IRPAgent should assign IRPManager an accessor identity and authorize IRPManager certain access rights before IRPManager is able to make request to the IRPAgent.

The present document does not specify access control policy or access right granularity in IRPAgent side Authorization Security Service.

5.3 Activity Log Security Service

Activity Log Security Service is provided by logging request-related information transferred between communication entities.

In secured IRP scenario, IRPAgent side Activity Log Security Service logs request-related information made by IRPManager.

Each Activity Log Record is associated with a single operation and corresponding response. An activity log record contains the following information:

- IRPManager Authentication identity, timestamp and Authentication result.
- Authorization result.
- The IRPManager's request (operation name and parameters including parameter values) and a time stamp of its reception at the IRPAgent.
- The corresponding response (return status or exception, only in case a response was sent) and a time stamp of its despatch at the IRPAgent.

It should be possible to audit Activity after a long period of time has elapsed since the activity happened. How to audit Activity Log is not specified in the present document.

5.4 File Integrity Security Service

File Integrity Security Service is provided by applying Signature mechanism.

In Itf-N scenario, both IRPManager and IRPAgent can transfer data file to each other. File Integrity Security Service on both IRPManager and IRPAgent side should be able to sign data file to be transferred, to send the result signature as a Security Attribute to the receiver, to receive the result signature, and to verify the signed file received. The result signature can be transferred in a detached file.

In case that IRPAgent acting as file receiver finds integrity of its received file is broken, IRPAgent should refuse the received file and raise a security alarm reflecting this error; in case that IRPManager acting as file receiver finds integrity of its received file is broken, IRPManager should refuse the received file and may request IRPAgent to re-transfer the file.

In secured IRP scenario, IRPManager and IRPAgent should agree with the digest algorithm, encryption algorithm and key distribution method if necessary before they exchange file(s).

6 Information Object Classes

6.1 Class diagram

This clause introduces the set of Information Object Classes (IOCs) that encapsulate information available over Itf-N. This clause provides the overview of all support object classes in UML. Subsequent clauses provide more detailed specifications of various aspects of these support object classes.

6.1.1 Attributes and Relationships

6.1.1.1 Class Diagram

6.2 Information Object Class Definitions

6.2.1 Credential

6.2.1.1 Definition

This IOC represents authentication and authorization information of its owner.

However, its attributes and behaviours are mechanism specific.

6.2.1.2 Attributes

Attribute name	Visibility	Support Qualifier	Read Qualifier	Write Qualifier
authData	%	M	-	-

6.2.2 Signature

6.2.2.1 Definition

This IOC represents cryptographic information appended to the transferred management information that allows a receiver to verify integrity of the transferred management information.

However, its attributes are mechanism specific.

6.2.2.2 Attributes

Attribute name	Visibility	Support Qualifier	Read Qualifier	Write Qualifier
sigData	%	M	-	-

6.4 Information attribute definition

6.4.1 Definition and legal values

Attribute Name	Definition	Legal Values
authData	Authentication and Authorization data that can be used to authenticate the claimer is what it claims to be and authorize the claimer's access rights.	Authentication and Authorization mechanism related data.
sigData	Cryptographic information appended to the transferred management information that allows a receiver to verify integrity of the transferred management information.	Signature mechanism related data.

7 Interface definition

This clause addresses interface between IRPManager side Security Service and IRPAgent side Security Service, including IRPManager Authentication, IRPAgent Authentication, Authorization, Activity Log, and File Integrity Security Service.

7.1 Credential transfer interface

As described in clause 5, Credential can contain IRPManager Authentication identity, optional IRPAgent Authentication identity and IRPManager accessor identity.

For each request exchanged between IRPManager and IRPAgent, IRPManager side Security Service and IRPAgent side Security Service should cooperate to exchange Credential accompanying the request and maybe corresponding result as well.

Concrete procedure of Credential transfer mechanism/interface is Security Service Solution specific.

7.2 Signature transfer Interface

As described in clause 5, Signature contains encrypted digest value of the transferred file, whose concrete content is mechanism specific.

XML document instances are secured by transferring the Signature in the document instances.

Annex A(informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Cat	Old	New
Jun 2006	SA_32	SP-060252	--	--	Submitted to TSG SA#32 for Information	--	1.0.0	
Jun 2006	--	--	--	--	History box clean-up	--	1.0.0	1.0.1
Mar 2007	SA_35	SP-070056	--	--	Submitted to TSG SA#35 for Approval	--	2.0.0	7.0.0

History

Document history		
V7.0.0	March 2007	Publication