ETSI TS 132 373 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):
Common Object Request Broker
Architecture (CORBA) Solution
(3GPP TS 32.373 version 7.0.0 Release 7)**

Reference
DTS/TSGS-0532373v700

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 (TS) 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 Service for Integration Reference Point (IRP): Information Service (IS)".

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

32.375 "Security Service for Integration Reference Point (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 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.

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

The present document introduces security mechanisms in CORBA context to address IRP security requirements defined in 3GPP TS 32.371 [4].

1 Scope

The present document specifies the CORBA Solution for the IRP whose semantics is specified in 3GPP TS 32.372 [5] Security Service for IRP Information Service.

This Solution Set specification is related to 3GPP TS 32.372 [5].

Note that within the present document there are several alternate solutions. Specific choices will to be made to counter identified security threats , and to consider performance and cost criteria, i.e. an implementation is not expected to have to support every option for every deployment.

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 32.301: "Telecommunication management; Configuration Management (CM); Notification Integration Reference Point (IRP): Requirements".

[4] 3GPP TS 32.371 "Telecommunication management; Security Management concept and requirements".

[5] 3GPP TS 32.372: "Telecommunication management; Security Management Integration Reference Point (IRP): Information Service (IS)".

[6] 3GPP TS 32.311: "Telecommunication management; Generic Integration Reference Point (IRP) management: Requirements".

[7] OMG CORBA Specification 02-12-06

[8] OMG CORBA Security Service Specification 02-03-11
http://www.omg.org/technology/documents/corbaservices_spec_catalog.htm

[9] SECP Security Service Protocol
http://www.omg.org/technology/documents/formal/omg_security.htm#SECP

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 32.301 [3] and the following apply:

IRP document version number string (or "IRPVersion"): See 3GPP TS 32.311 [6].

3.2 Abbreviations

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

CM	Configuration Management
CORBA	Common Object Request Broker Architecture (OMG)
EM	Element Manager
IDL	Interface Definition Language (OMG)
IOR	Interoperable Object Reference
IS	Information Service
NC	Notification Channel (OMG)
NE	Network Element
NV	Name and Value pair
OMG	Object Management Group
ORB	Object Request Broker (OMG)
RI	Request Interceptor
QoS	Quality of Service
SAS	Security Attributes Service (OMG)
SECP	Security Protocol
SS	Solution Set
UML	Unified Modelling Language (OMG)
TII	Time-Independent Invocation
CSS	Client Security Service
TSS	Target Security Service
CA	Certificate Authority

4 Architectural features

The overall architectural feature of Security Services is specified in 3GPP TS 32.372 [5]. This clause specifies features that are specific to the CORBA Solution.

4.1 Principles of IRP Security Services

As shown in figure 4.1, the Security Services are between IRP Application layer and Transport layer. Security Attributes which are attached to network management information are transferred between IRPManager and IRPAgent to address Authentication, Authorization, Activity Log and file integrity requirements.

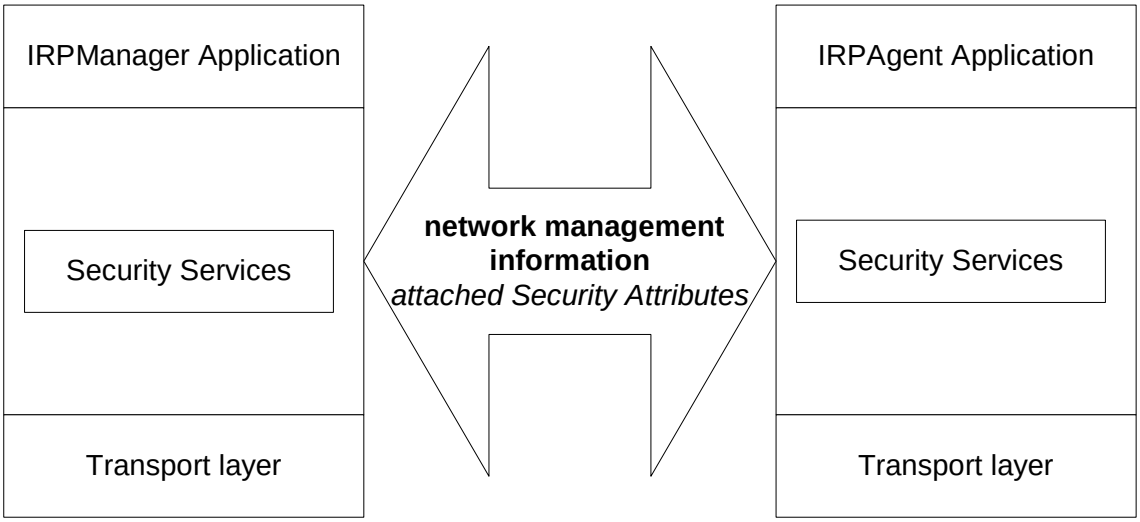

Figure 4.1: Principles of IRP Security Services

The basic idea of these Security Services is as follows:

Security Services on IRPManager side and Security Services on IRPAgent side cooperate to secure the Itf-N.

When IRPManager and IRPAgent exchange network management information in a secured manner, the sender Security Service attaches Security Attributes to the network management information. The receiver analyses the received Security Attributes to determine if the received network management information is authentic and authorized.

The present document specifies two alternative CORBA solutions for attaching Security Attributes over Itf-N.
They use different CORBA mechanisms to transfer the Security Attributes. One uses The CORBA Request Interceptor while the other uses the CORBA Security Attributes Service (SAS) protocol. Both solutions need to define their respective Security Attributes.

The Security Attributes used by the Interceptor mechanism and the mechanism itself are defined by the present document.
The ones used by the CORBA SAS protocol are defined in CORBA SAS [7].

In addition to the above two alternate mechanisms, the present document also specify a third alternative called Virtual Private Network (VPN) to secure the network management information exchanged between IRPManager and IRPAgent.
Such mechanism is defined in annex A of 3GPP TS 32.371 [4].

Table 4.1 identifies the use of the three alternatives to realize the Security Service such as Authentication Security Service, Authorization Security Service, Activity Log Security Service and File Integrity Security Service.

Table 4.1: Alternate solutions and Security Service relationship

	Authentication Security Service	Authorization Security Service	Activity Log Security Service	File Integrity Security Service
Request Interceptor solution	X	X	X	
SAS solution	X	X	X	
VPN	X	X	X	X
NOTE: "X" means that "The Security Service identified by the column name is realised by the use of Security Attributes in the solution identified by the row name.				

IRPManager and IRPAgent should decide to use one of the two alternative solutions to provide Authentication, Authorization and Activity Log Security Service at configuration/deployment time, and it is not changeable at run time.

IRP Manager and IRP Agents should both support VPN.

In case CORBA-based security services are used to provide Authentication, Authorization and Activity Log Security Service, IRP Managers shall support SAS Solution and Request Interceptor Solution, while IRP Agents may support either SAS Solution or Request Interceptor Solution (it shall be noted that usage is determined at configuration/deployment time, and it is not changeable at run time).

4.2 Request Interceptor

This clause introduces concept of Request Interceptor, definitions and details are addressed in clause 21.3 of OMG CORBA Specification [7]. This CORBA mechanism can be used to transfer Credential over Itf-N.

Request Interceptor (RI) is designed to intercept the flow of a request/reply sequence through the ORB at specific points so that services can query the request information and manipulate the service contexts that are propagated between clients and servers.

In Itf-N scenario, the service context includes Credential as Security Attributes to be exchanged between IRPManager side Security Service and IRPAgent side Security Service to address Authentication, Authorization, and Activity Log requirements. There are two types of Request Interceptors: Client-side and Server-side Interceptor. Both Client-side and Server-side request Interceptors are registered with an ORB (see section 21.7, "Registering Interceptors" in [7]). Each request Interceptor is called at a number of interception points.

As shown in figure 4.2, Client-side Request Interceptor is between Client Application layer and CORBA ORB layer; it comprises 5 kinds of Interception Points described in clause 4.2.1. Server-side Request Interceptor is between Server Application layer and CORBA ORB layer; it comprises 5 kinds of Interception Points described in clause 4.2.2. Information related to request and corresponding result exchanged between Client and Server can be intercepted at these Interception points by Client-side Request Interceptor and/or Server-side Request Interceptor.

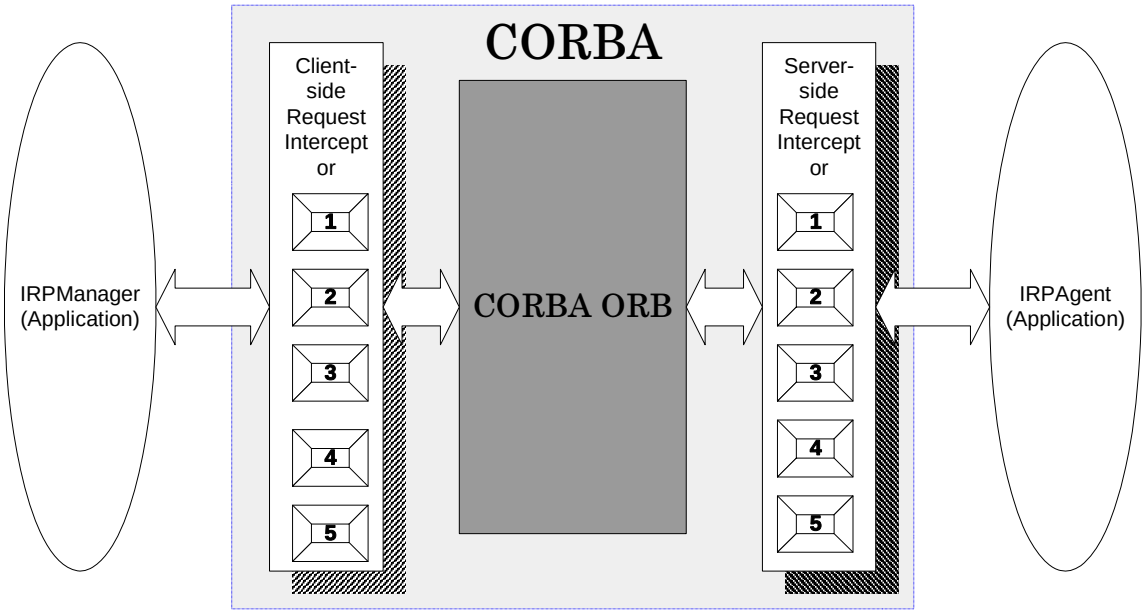

Figure 4.2: Interception points of Request Interceptor

4.2.1 Client-side Interceptor

After Client-side Interceptor is registered with ORB, Client-side Interceptor can be called at the following 5 Interception Points.

1. send_request Interception point:
   - When request is sent to the server, this interception point can be invoked by ORB to query request information and modify the service context.
2. send_poll Interception point:
   - This interception point allows an Interceptor to query information during a Time-Independent Invocation (TII) polling get reply sequence.
3. receive_reply Interception point:
   - When a reply is returned from the server and before control is returned to the client, this interception point can be invoked by ORB to query the information on the reply.
4. receive_exception Interception point:
   - When an exception occurs and before control is returned to the client, this interception point can be called by ORB to query the exception's information before it is raised to the client.
5. receive_other Interception point:
   - This interception point allows an Interceptor to query the information available when a request results in something other than a normal reply or an exception.

4.2.2 Server-side Interceptor

After Server-side Interceptor is registered with ORB, Server-side Interceptor can be called at the following 5 Interception Points.

1. receive_request_service_contexts Interception point:

   - After all the information regarding the request are available and before the request has been invoked by the server, this interception point can be invoked by ORB to query request information.

2. receive_request Interception point:

   - After the target operation has been invoked and before the reply is returned to the client, this interception point can be invoked by ORB to query reply information and modify the reply service context.

3. send_reply Interception point:

   - After the target operation has been invoked and before the reply is returned to the client, this interception point can be invoked by ORB to query reply information and modify the reply service context.

4. send_exception Interception point:

   - When an exception occurs, this interception point can be called by ORB.

5. send_other Interception point:

   - This interception point allows an Interceptor to query the information available when a request results in something other than a normal reply or an exception.

4.2.3 Request Interceptor Security Attributes

ServiceContext is defined in CORBA specification [7], it is composed of context_id and context_data.

Credential which is contained in SecurityContext as context data is used for IRPAgent to extract authentication token and authorization token.

4.3 Security Attributes Service Protocol

This clause introduces concept of Security Attributes Service Protocol, definitions and details are addressed in clause 24.3 of OMG CORBA Specification [6]. This CORBA mechanism can be used to transfer Credential over Itf-N.

The SAS protocol is designed to exchange its protocol elements in the service context of General Inter-ORB Protocol (GIOP) request and reply messages that are communicated over a connection-based transport. The protocol is intended to be used in environments where transport layer security exists.

Two security interceptors are used by ORB to exchange Security Attribute, but neither is available on application layer:

1. Secure Invocation Interceptor. This is a message-level interceptor, which is able to check and protect messages (requests and replies) for both integrity and confidentiality.

2. Access Control Interceptor. This is a request-level interceptor, which determines whether an invocation should be permitted.

The protocol provides client authentication, delegation, and privilege functionality that may be applied to overcome corresponding deficiencies in an underlying transport.

The SAS protocol is divided into two layers:

1. The authentication layer is used to perform client authentication where sufficient authentication could not be accomplished in the transport.

2. The attribute layer may be used by a client to push (that is, deliver) security attributes (identity and privilege) to a target where they may be applied in access control decisions.

4.3.1 Security Attribute Service context element

The Security Attribute Service (SAS) context element is used to associate security related service contexts with GIOP request and reply messages.

Four message types comprise the security attribute service context management protocol. Each security attribute service context element contains a context id and a message data that carries one of the following message body types:

1. EstablishContext: Sent by a Client Security Service (CSS) to establish a security attribute service context.
2. ContextError: Sent by a Target Security Service (TSS) to indicate errors that were encountered in context creation, in the message protocol, or in use of a context.
3. CompleteEstablishContext: Sent by a Target Security Service (TSS) to indicate the outcome of a successful request to establish a security attribute service context.
4. MessageInContext: Sent by a Client Security Service (CSS) to associate request messages with an existing stateful security attribute service context. This message may also be used to indicate that the context should be discarded after processing the request. Stateful contexts, also known as reusable contexts, endure until they are discarded, and can be referenced for use with subsequent requests.

4.3.2 CORBA Security Service

Note that the OMG security service [8] has a status indicating it is being replaced by a security protocol (SECP) specification.. SECP is a work in progress.

Should an operator and vendor agree to deploy the OMG security service they should be aware of the following cautions.

- The status of the OMG security service indicates that changes are deemed necessary due to the development of a replacement specification in SECP [9].
- The OMG security service is known to require more processing power. This may impact the processing platform and memory requirements, leading to higher cost solutions.

IRPManager and IRPAgent access Security Attributes via CORBA Security Service.

Editor Note: OMG is defining a new OMG CORBA Security Service to replace [8].

IRPManager side CORBA Security Service authenticates IRPManager explicitly or implicitly, and returns a credential as a warrant to the IRPManager. Since then, when the authenticated IRPManager sends a request to a IRPAgent, IRPManager side CORBA Security Service will transfer the IRPManager's credential to the target IRPAgent.
The target IRPAgent side CORBA Security Service validates the transferred Credential to accomplish IRPManager authentication. Similarly, IRPManager side CORBA Security Service may authenticate IRPAgent if required.

CORBA Security Service provides authentication service on transport layer and maybe also on application layer.

5 Mapping

5.1 RI Solution Mapping

RI Solution can be alternatively used to provide Authentication, Authorization and Activity Log Security Service for Itf-N.

5.1.1 Security Attribute Mapping

In Request Interceptor Solution scenario, Security Attributes are attached to operation request transferred between IRPManager and IRPAgent within CORBA ORB layer.

Table 5.1.1: Mapping from IS Security Attribute to RI Solution Equivalents

IS IOC in 3GPP TS 32.372 [5]	RI Solution IOC	Qualifier
Credential	interface Credential (see note)	M
NOTE: interface Credential contains auth_data of CORBA Any type, detailed content is authentication mechanism specific. A list of authentication mechanisms are recommended in Annex B.		

Table 5.1.2: Mapping from IS Security Exception to RI Solution Equivalents

IS IOC in 3GPP TS 32.372 [5]	RI Solution IOC	Qualifier
There is no corresponding IS parameter	exception AuthenticationException (see note 1)	M
There is no corresponding IS parameter	exception AuthorizationException (see note 2)	M
NOTE 1: See details in clause 6.1.1. NOTE 2: See details in clause 6.1.2.		

5.2 SAS Solution Mapping

SAS Solution can be alternatively used to provide Authentication, Authorization and Activity Log Security Service for Itf-N.

5.2.1 Security Attribute Mapping

In Security Attribute Service protocol Solution scenario, Security Attributes are attached to operation request transferred between IRPManager and IRPAgent within CORBA ORB layer.

Table 5.2.1: Mapping from IS Security Attribute to SAS Solution Equivalents

IS IOC in 3GPP TS 32.372 [5]	SAS Solution IOC	Qualifier
Credential	SAS ServiceContext (see note)	M
NOTE: SAS Service Context are defined in clause 24.3 of OMG CORBA Specification [6].		

6 Itf-N Security Service Behaviour

This clause describes some behaviours of IRPManager and IRPAgent not captured by IDL in RI Solution and SAS Solution respectively. IRPManager and IRPAgent should apply RI Solution or SAS Solution to provide Authentication, Authorization and Activity Log Security Service.

6.1 Request Interceptor Solution

At configuration/deployment time, Request Interceptor on IRPManager and IRPAgent side should be configured to run respectively before IRPManager and IRPAgent start to run.

6.1.1 Authentication

This clause addresses how to use Request Interceptor to provide IRPManager Authentication and IRPAgent Authentication as well if required.

When IRPManager sends request to IRPAgent, Client-side Request Interceptor request credential from local Security Service, then inserts it into service context and attaches the service context to the request; when IRPAgent receives the request, Server-side Request Interceptor extracts the service contexts attached to the request and performs authentication method to check the validity of the credential inserted. If the check succeeds, Server-side Request Interceptor performs authorization for the request and works with the request as normal after successful authorization, otherwise an authenticationException is raised and sent to IRPManager by Server-side Request Interceptor.

When IRPAgent has processed the request from IRPManager and is going to sends result, Server-side Request Interceptor may insert IRPAgent's credential into a service context and attach the service context to the result; when IRPManager receives the result, Client-side Request Interceptor may extract the service contexts including the IRPAgent's credential and check its validity. If the check succeeds, IRPManager works with the result as normal, otherwise an authenticationException is raised and sent to IRPManager by Client-side Request Interceptor.

Implementation may or may not support IRPAgent authentication; if implementation supports IRPAgent authentication, it shall be configured at configuration/ deployment time; this configuration is not changeable at running time.

How IRPManager side local authentication mechanism and IRPAgent side local authentication mechanism cooperate to complete authentication is not standardized in this release.

6.1.2 Authorization

This clause addresses how to resolve Authorization requirement by using Request Interceptor.

IRPAgent is able to extract accessor Identifier from the credential attached to the request.

Each time IRPAgent receives request, Server-side Request Interceptor extracts accessor identifier from the credential attached to the request.

Server-side Request Interceptor is also able to retrieve request related information.

Server-side Request Interceptor then checks the accessor identifier, request related information against Access Control Policy predefined in IRPAgent to decide to accept the request or not. If the check succeeds, IRPAgent works with the request as normal, otherwise an authorizationException is raised and sent to IRPManager by Server-side Request Interceptor.

6.1.3 Activity Log

This clause addresses how to log activity of IRPAgent by means of Request Interceptor.

Server-side Request Interceptor logs activity of IRPAgent in the following way:

1. After receiving operation request, Server-side Request Interceptor logs the received operation request and corresponding parameters, sender identifier, and timestamp.

2. After finishing IRPManager Authentication, Server-side Request Interceptor logs authentication result.
3. After finishing Authorization, Server-side Request Interceptor logs authorization result.
4. After sending operation result, Server-side Request Interceptor logs operation result, i.e. normal reply or system/user exception.

6.2 Security Attributes Service Solution

This clause addresses how to provide IRPManager Authentication, IRPAgent Authentication, Authorization, and Activity Log Security Service by using Security Attributes Service.

At configuration/deployment time, IRPManager and IRPAgent should be configured to run over CORBA Security Service providing authentication service, authorization service and security audit service.

6.2.1 Authentication

IRPManager invokes operation authenticate (defined in CORBA Security Service specification [8]) to get a credential as a warrant.

Optionally, IRPManager may continue to invoke operation continue_authentication (defined in CORBA Security Service specification [8]) to carry out mutual authentication.

6.2.2 Authorization

When operation request reaches IRPAgent, IRPAgent side CORBA Security Service extracts accessor identifier from the credential attached to the request and invokes operation access_allowed (defined in CORBA Security Service specification [8]) to accomplish authorization due to the accessor identifier and predefined Access Control policy.

6.2.3 Activity Log

CORBA Security Service provides Security Audit Service. IRPAgent invokes operation audit_needed (defined in CORBA Security Service specification [8]) to decide which security activity/event to be logged; corresponding activity/event are logged by CORBA Security Service automatically when happens. OMG CORBA Security Service [8] defines the following activities/events that can be logged:

AuditAll
AuditPrincipalAuth
AuditSessionAuth
AuditAuthorization
AuditInvocation
AuditSecEnvChange
AuditPolicyChange
AuditObjectCreation
AuditObjectDestruction
AuditNonRepudiation

Annex A (normative): IDL specifications

NOTE: All the IDL files below are only applicable to RI Solution. SAS Solution related IDL definition is defined in CORBA Security Service specification [8].

A.1 IDL specification (file name "SecurityServiceConstDefs.idl")

```
//File: SecurityServiceConstDefs.idl

#ifndef _SECURITYSERVICECONSTDEFS_IDL_
#define _SECURITYSERVICECONSTDEFS_IDL_

// This statement must appear after all include statements
#pragma prefix "3gppsa5.org"


/* ## Module: SecurityServiceConstDefs
This module contains definitions specific for Security Service Request Interceptor Solution.
================================================================
*/
module SecurityServiceConstDefs
{

   typedef Any Auth_Data;
   /*
   Define the credential in Request Interceptor Solution specified in
   the Security Service: IS.
   */
   interface Credential
   {
      Auth_Data authenticationData;
   };

};

#endif  // _SECURITYSERVICECONSTDEFS_IDL_
```

A.2 IDL specification (file name "SecurityServiceSystem.idl")

```
//File: SecurityServiceSystem.idl

#ifndef _SECURITYSERVICESYSTEM_IDL_
#define _SECURITYSERVICESYSTEM_IDL_

#include "SecurityServiceConstDefs.idl"

// This statement must appear after all include statements
#pragma prefix "3gppsa5.org"

/* ## Module: SecurityServiceSystem
This module implements capabilities of IRP Security Service.
================================================================
*/
module SecurityServiceSystem
{
   /*
   System fails to complete the operation.  System can provide reason
   to qualify the exception.  The semantics carried in reason
   is outside the scope of this IRP.
   */
   exception AuthenticationException { string reason; };
   exception AuthorizationException { string reason; };
}
#endif  // _SECURITYSERVICESYSTEM_IDL_
```

Annex B (informative): Authentication mechanism

In this release, IRP Security Service credential is not specified at syntax level. This annex recommends the following Industrial Authentication services that IRP Security Service can adopt. They are of different kinds of Credentials, security strength, performance cost, and implementation cost.

B.1 Basic authentication

Client sends credential comprising username and password encoded in base64 to server, server check the validity of the credential to complete authentication.

E.g. HTTP v1.0 employs basic authentication service.

B.2 Digest authentication

Digest authentication offers the same features as basic authentication but involves a different way of transmitting the authentication credential. The authentication credential passes through MD5 hashing process per [RFC-1321].
The result is not feasible to decrypt it.

Additional information is added to the password before hashing so that the password hash can not be captured and reused to impersonate the true user.

E.g. HTTP v1.1 employs digest authentication service.

B.3 Kerberos and SPKM

Generic Security Service Application Program Interface (GSS-API) defines an interface to strong authentication and other security services at a generic level which is independent of particular underlying mechanisms, e.g. Kerberos per RFC 1964, and SPKM per RFC 2025.

A GSS-API caller accepts tokens provided by its local GSS-API implementation and transfers the tokens to a peer on a remote system; that peer passes the received tokens to its local GSS-API implementation for processing.

B.4 OMG CORBA CSIv2 Conformance Level 0 of Security

Refer to clause C.5.

Annex C (normative): Use of OMG specified security service

C.1 General

This annex specifies the use of OMG specified security service to secure the IRP. The use of this service is optional in the understanding that a) all 3GPP specified security service are qualified as optional and b) the choice of service depends on the operating context such as, the cost, the risk of security violation, the cost of recovery, etc.

C.2 Authentication

The Secured Interface IRP shall be in conformance to OMG CSIv2 conformance Level 0. See clause C.5.

We recommend 3GPP to standardize two methods: the Transport Layer based method (2.1) and the Supplemental Client Authentication Layer based method (2.2). 3GPP should qualify each of them, in terms of support, in the following sense:

- To support IRPManager authentication, a Secured Interface IRP instance shall support method 1 (2.1) or method 2 (2.2).
- To support IRPAgent-to-IRPManager and IRPManager authentication (mutual authentication), a Secured Interface IRP instance shall support method 1.
- The Secured Interface IRPs from a particular vendor supporting an Itf-N instance shall all have the same supported authentication method(s).

EXAMPLE: A vendor providing a secured IRPAgent including BulkCMIRP, NotificationIRP and AlarmIRP, shall implement the same set of authentication methods in the three IRPs involved.

C.2.1 Transport Layer based method

The IRPManager authentication and IRPAgent-to-IRPManager authentication shall be supported by this method. This method operates at the Transport Layer as shown in the following diagram (extracted, with modification specific for IRP context, from section 24.1.1 of [8].

In this mode, the supporting ORB and its related Transport Layer will implement the authentication method and provide the authentication security service to the IRPManager and IRPAgent applications.

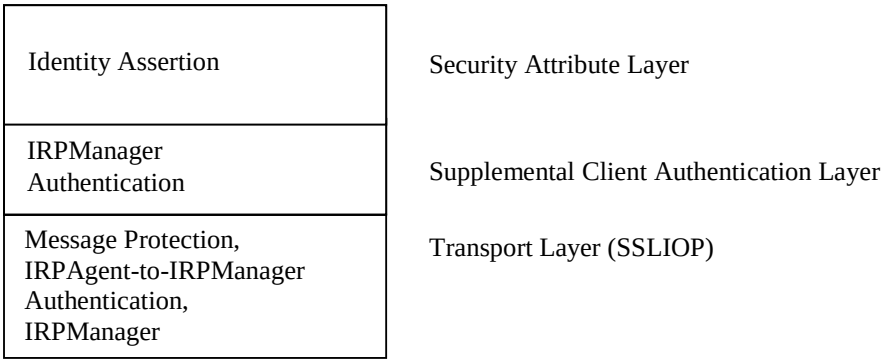

Figure C.1: Protocol stack supporting CORBA secured IRP

Authentication should be accomplished by using the subject (e.g. IRPManager) identity inside a X.509 digital certificate provided to the object (e.g. the secured IRPAgent application) and vice versa.

The IRPManager must first obtain a credential (container for security attributes) containing the subject access identity only (see note 1) for use during future CORBA session in a secured IRP environment. How IRPManager can obtain a credential is outside the 3GPP standard scope.

The IRPAgent application can obtain the IRPManager's credential at runtime by making appropriate authenticate call (non-3GPP standardized) to its local ORB interface.

Likewise, the IRPAgent application must also obtain a credential for use during future CORBA session. How IRPAgent can obtain its credential is outside the 3GPP standard scope.

The IRPManager application can obtain the IRPAgent's credential at runtime by making appropriate authenticate call (non-3GPP standardized) to its local ORB interface.

To allow the IRPManager to authenticate received notifications, our preference is to use the following scheme.

- The Notification IRPAgent should need another key pair (different key than one used for authentication mentioned above) for signing the notifications.
- Notification IRPManager at notification subscription time can ask for secured (i.e. notification carries IRPAgent's signature) or non-secured notifications (i.e. notification does not carry digital signature).
- We would prefer the Notification IRPAgent to include its digital signature in the notifications, rather than to rely on SSL to provide authentication for notifications. This preference is to avoid the 3 or 4 protocol exchanges required at the SSL to achieve authentication for each notification sent. This preference also allows the IRPManager, if it considers the received notification is of no significance from security viewpoint, needs not spend its CPU cycles to authenticate the incoming signature.

NOTE 1: In general, credential can contain, in addition to access identity, the privilege attributes such as security role name. Our recommendation is not to use privilege attributes in credential because we propose the use of the widely supported CSIv2 conformance level 0. Unfortunately, privilege attributes are only supported in CSIv2 conformance level 1.

NOTE 2: The SSL v3.0/TLS 1.0 protocol specified by CSIv2 conformance level 0 provide strong authentication X.509 certificate based public key technology. This certificate-based authentication method operates at the transport (SSLIOP) layer and not at the higher levels of the CSIv2 stack. The PKI infrastructure and support needed for of distribution of public/private keys are limited given the small amount of participating IRPManagers and IRPAgents. One simple way to distribute keys is to store them in file, place them on disk and physically and securely shipped them to appropriate administrators for installing in their systems. Third party authorities or the operator's own Certificate Authority (CA) can be used to certify the keys being distributed.

C.2.2 Client Authentication layer based method

To supplement IRPManager authentication offered by the Transport Layer, we recommend 3GPP to also standardize the use of the Client Authentication Tokens and Identity Tokens as defined in the CSIv2 (i.e. the so-called General Security Services Username Password (GSSUP)-based authentication method). These mechanisms operate at the Supplemental Client Authentication Layer and the Security Attribute Layer (see Figure C.1) There is no need to standardize the use of Authorization Tokens (which also operates at the Security Attribute Layer).

- The Client Authentication Token, if used by IRPManager, is the client authentication token used by the username password (GSSUP) mechanism for client authentication. For 3GPP standard, all secured IRPAgent, supporting IRPManager authentication, shall support this method. IRPManager can choose to use or not to use it.
- The Identity Token, if present, is an identity token used by the IRPAgent's identity assertion functionality. It identifies the client of the request. For 3GPP standard, secured IRPAgent, may choose to use it or ignore it.

In this mode, similar to the other mode of 2.1, the supporting ORB and its related Transport Layer will implement the authentication method and provide the authentication security service to the IRPManager applications.

C.3 Authorization and Access Control

Access control means restricting IRPManager's usage of methods and access to managed resources. In the context of IRP security, we envision various schemes of granularity for access control:

1. Scheme-1: Is this IRPManager allowed to use all methods of this particular xxx IRP and access to all managed resources known by the IRPAgent?

2. Scheme-2: Is this IRPManager allowed to use this method of this particular xxx IRP? If yes, is this IRPManager allowed to access this managed resource?

We recommend that 3GPP to standardize the Scheme-1 access control. Because the number of xxx IRP instances is small and their lifecycles are long (e.g. in years), we propose that there is no need to standardize a mechanism to name these resources. Vendor supplying an instance of the secured xxx IRP shall document the naming/identification of these resources (i.e. instances of xxx IRPs) and provide a secured vendor-specific mechanism for the management of the authorizations that the IRPAgent shall use for access control purposes.

We also recommend that vendor, supplying an instance of the secured xxx IRP, should provide access control to resources at granularity Scheme-2 above. In such case, the vendor shall be required to identify the resources (i.e. methods, managed resources) that can be subject to access control. The vendor shall also be required to describe the semantics of its IRPAgent access control mechanism together with a secured vendor-specific mechanism for the management of the authorizations that the IRPAgent shall use for access control purposes.

We do not recommend 3GPP to standardize the use of Authorization Tokens as a mean to distribute security attributes such as role. As a consequence, conformance to OMG CSIv2 conformance Level 1 is not a requirement for implementations for complying to the 3GPP Secured Interface IRP. From the 3GPP viewpoint, the way an IRPAgent obtains the required security attribute information about an IRPManager is vendor specific.

C.4 (Message) Integrity and Confidentiality Protection

Data integrity is provided by the use of the Secure Sockets Layer (SSL version 3.0) protocol on links between IRPManager and IRPAgent.

There is no confidentiality requirement stated so far. Therefore, solution for confidentiality is not discussed. (Note that CSIv2 conformance Level 0 provides confidentiality.)

Message integrity (and confidentiality) could also be provided by VPN links between IRPManager and IRPAgent.

C.5 Quotation from OMG CORBA CSIv2 3 Conformance Levels of Security

This part is quoted from section 24.6 "Conformance Levels" of [8].

"

24.6.1 Conformance Level 0

Level 0 defines the base level of secure interoperability that all implementations are required to support. Level 0 requires support for SSL/TLS protected connections.

Level 0 implementations are also required to support username/password client authentication and identity assertion by using the service context protocol defined in this specification.

24.6.1.1 Transport-Layer Requirements

Implementations shall support the Security Attribute Service (SAS) protocol within the service context lists of GIOP request and reply messages exchanged over SSL 3.0 and TLS 1.0 protected connections.

Implementations shall also support the SAS protocol within the service context lists of GIOP request and reply messages over unprotected transports defined within IIOP. (SAS protocol elements should only be sent over unprotected transports within trusted environments.)

Required Ciphersuites

Conforming implementations are required to support both SSL 3.0 and TLS 1.0 and the mandatory TLS 1.0 ciphersuites identified in [IETF RFC 2246]. Conforming implementations are also required to support the SSL 3.0 ciphersuites corresponding to the mandatory TLS 1.0 ciphersuites. An additional set of recommended ciphersuites is identified in Section 24.4.2.1, "Recommended SSL/TLS Ciphersuites," on page 24-31.

24.6.1.2 Service Context Protocol Requirements

All implementations shall support the Security Attribute Service (SAS) context element protocol in the manner described in the following sections.

Stateless Mode

All implementations shall support the stateless CSS and stateless TSS modes of operation as defined in Section 24.3.2, "Session Semantics," on page 24-21, and in the protocol message definitions appearing in Section 24.2.2, "SAS context_data Message Body Types," on page 24-5.

Client Authentication Tokens and Mechanisms

All implementations shall support the username password (GSSUP) mechanism for client authentication as defined in Section 24.2.4.1, "Username Password GSS Mechanism (GSSUP)," on page 24-12.

Identity Tokens and Identity Assertion

All implementations shall support the identity assertion functionality defined in Section 24.3.1.1, "Context Validation," on page 24-17 and the identity token formats and functionality defined in Section 24.2.5, "Identity Token Format," on page 24-14.

All implementations shall support GSSUP mechanism specific identity tokens of type **ITTPrincipalName**.

Authorization Tokens (not required)

At this level of conformance, implementations are not required to be capable of including an authorization token in the SAS protocol elements they send or of interpreting such tokens if they are included in received SAS protocol elements.

The format of authorization tokens is defined in Section 24.2.3, "Authorization Token

Format," on page 24-10.

24.6.1.3 Interoperable Object References (IORs)

The security mechanism configuration of CSIv2 target objects, shall be as defined in Section 24.5.1, "Target Security Configuration," on page 24-32, with the exception that Level 0 implementations are not required to support the **DelegationByClient** functionality described in Section 24.5.1.1, "AssociationOptions Type," on page 24-33.

24.6.2 Conformance Level 1

Level 1 adds the following additional requirements to those of Level 0.

24.6.2.1 Authorization Tokens

Level 1 implementations shall support the push model for privilege attributes. Level 1 requires that a CSS provide clients with an ability to include an authorization token, as defined in Section 24.2.3, "Authorization Token Format," on page 24-10, in SAS EstablishContext protocol messages.

Level 1 requires that a TSS be capable of evaluating its support for a received authorization token according to the rules defined in Section 24.2.3.1, "Extensions of the IETF AC Profile for CSIv2," on page 24-11. A Level 1 TSS shall recognize the standard attributes and extensions defined in the attribute certificate profile defined in [IETF ID PKIXAC].

Level 1 requires that a target object that supports pushed privilege attributes include in its IORs the names of the privilege authorities trusted by the target object (as defined in "struct SAS_ContextSec" on page 24-40).

24.6.3 Conformance Level 2

Level 2 adds to Level 1 the following additional requirements.

24.6.3.1 Authorization-Token-Based Delegation

Level 2 adds to Level 1 a requirement that implementations support the authorizationtoken-based delegation mechanism implemented by the SAS protocol. A Level 2 TSS shall be capable of evaluating proxy rules arriving in an authorization token to determine whether an asserting entity has been endorsed (by the authority which vouched for the privilege attributes in the authorization token) to assert the identity to which the privilege attributes pertain. The semantics of the relationship between the identity token and authorization token shall be as defined in Section 24.3.1.1, "Context Validation," on page 24-17.

A Level 2 TSS shall recognize the Section 24.2.3.1, "Extensions of the IETF AC Profile for CSIv2," on page 24-11" (that is, the Proxy Info extension) as defined on that page.

Level 2 requires that a target object that accepts identity assertions based on endorsements in authorization tokens represent this support in its IORs as defined in Table 24-17 on page 24-42.

Level 2 requires that a target object that requires an endorsement to act as proxy for its callers represent this requirement in its IORs as defined in Table 24-17 on page 24-42.

24.6.4 Stateful Conformance

Implementations are differentiated not only by the conformance levels described in the preceding sections but also by whether or not they support stateful security contexts.

For an implementation to claim stateful conformance, it shall implement the stateless and stateful functionality as defined in Section 24.3.2, "Session Semantics," on page 24-21 and in Section 24.2.2, "SAS context_data Message Body Types," on page 24-5.

"

Annex D (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Cat	Old	New
Sep 2006	SA_33	SP-060556	--	--	Submitted to TSG SA#33 for Information	--	1.0.0	
Mar 2007	SA_35	SP-070057	--	--	Submitted to TSG SA#35 for Approval	--	2.0.0	7.0.0

History

Document history		
V7.0.0	March 2007	Publication