ETSI TS 132 375 V8.0.0 (2009-01)

Technical Specification

Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Security services for Integration Reference Point (IRP): File integrity solution (3GPP TS 32.375 version 8.0.0 Release 8)

Reference

RTS/TSGS-0532375v800

Keywords

GSM, LTE, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 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 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].
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.

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 XML Signature mechanism to address File Integrity security requirement defined in 3GPP TS 32.371 [4].

1 Scope

The present document contains the Security Services for IRP: File integrity solution whose semantics are specified in 3GPP TS 32.372 [5].

This solution specification is related to 3GPP TS 32.372 V 8.0.X [5].

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 Service for 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

[9] XML-Signature Syntax and Processing
http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

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:

CORBA	Common Object Request Broker Architecture (OMG)
EM	Element Manager
IS	Information Service
OMG	Object Management Group
ORB	Object Request Broker (OMG)

4 Architectural features

The overall architectural feature of Security Service is specified in 3GPP TS 32.372 [5]. This clause specifies features that are specific to the File integrity solution.

4.1 Principles of IRP Security Services

Figure 4.1 shows that 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.

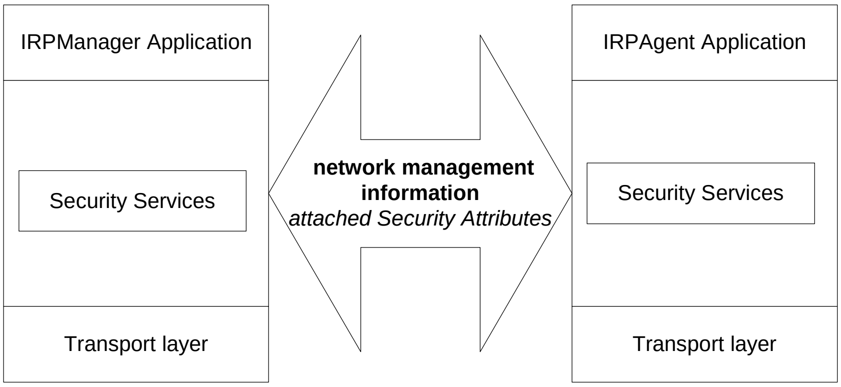

Figure 4.1 : Principles of IRP Security Service

The basic idea of these Security Services is as follows:

- IRP Security Services on IRPManager side and IRP Security Services on IRPAgent side co-operate to provide Security Services for IRP.
  This avoids modifying IRPManager and IRPAgent much.

- When the IRPManager and/or IRPAgent send network management information to each other, the IRP Security Service (on IRPManager and/or IRPAgent side) attaches Security Attributes to the network management information. The receiver works with the attached Security Attributes to implement the IRP security requirement.

The present document addresses File integrity solution by using the XML Signature Mechanism defined by [9].

Table 4.1 identifies the use of File Integrity solution to realize File Integrity Security Service.

Table 4.1 : File Integrity solution and Security Service relationship

	Authentication Security Service	Authorization Security Service	Activity Log Security Service	File Integrity Security Service
File Integrity solution				X
NOTE: "X" indicates which CORBA solution exchanges Security Attributes are relevant to which Security Service.				

4.2 XML Signature Recommendation

This clause introduces the concept of XML Signature detailed in [9]. It is used to transfer XML Signature over Itf-N to provide the File Integrity Security Service.

Based on [9], data to be signed is canonicalized by using a specific method, i.e. using a unique form to represent XML files with the same semantic content but different text. The canonicalized data may be transformed before it is digested by using a specific method. The digest value is encrypted by using a specific signature method. The key information used to verify the signed value of signed data may be included in the XML Signature.

As shown in [9], XML digital signatures are represented by the Signature element which has the following structure (where "?" denotes zero or one occurrence; "+" denotes one or more occurrences; and "*" denotes zero or more occurrences):

```
<Signature ID?>
   <SignedInfo>
     <CanonicalizationMethod/>
     <SignatureMethod/>
     (<Reference URI? >
       (<Transforms>)?
       <DigestMethod>
       <DigestValue>
     </Reference>)+
   </SignedInfo>
   <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
 </Signature>
```

5 Mapping

5.1 File Integrity Solution Mapping

5.1.1 Security Attribute Mapping

In File Integrity Solution scenario, XML Signature as Security Attributes is exchanged over Itf-N accompanying the file(s) to be transferred.

Table 5.1: Mapping from IS Security Attribute to File Integrity Solution Equivalents

IS IOC in 3GPP TS 32.372 [5]	XML Signature Solution IOC	Qualifier
Signature	element Signature (defined in [9])	M

5.1.2 Operation Mapping

Editor's note: FFS.

6 Itf-N Security Service Behaviour

This clause describes some behaviour of IRPManager and IRPAgent not captured by XML Schema in File Integrity Solution.

6.1 File Integrity Solution

This clause addresses how to use XML Signature to provide File Integrity Security Service.

To Enable IRPManager and IRPAgent to use XML Signature, these two sides should agree with Canonicalization Method, Transform Method, Digest Method, and Signature Method before they start communication.
Mandatory methods defined in [9] should be supported by IRPManager and IRPAgent.

When an XML document instance is to be exchanged over Itf-N, the sender should make sure the whole XML document instance should be signed. The corresponding XML Signature should be held in the XML document instance.

When an XML document instance is received, the receiver should verify the XML document instance by using the process defined in [9].

If the verification is successful, receiver works with the XML document instance as normal; otherwise receiver should raise a security alarm if it is IRPAgent or process the failure in a vendor specific way if it is IRPManager.

Annex A (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Cat**	**Old**	**New**
Jun 2006	SA_32	SP-060253	--	--	Submitted to TSG SA#32 for Information	--	1.0.0	
Dec 2006	SA_34	SP-060736	--	--	Submitted to TSG SA #34 for Approval	--	2.0.0	7.0.0
Dec 2008	SA_42	--	--	--	Upgrade to Release 8	--	7.0.0	8.0.0

History

Document history		
V8.0.0	January 2009	Publication