ETSI TS 124 423 V7.0.0 (2008-04)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
TISPAN;
PSTN/ISDN simulation services;
Extensible Markup Language (XML) Configuration Access
Protocol (XCAP) over the Ut interface for Manipulating NGN
PSTN/ISDN Simulation Services
(3GPP TS 24.423 version 7.0.0 Release 7)**

**GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS**

Reference
DTS/TSGC-0124423v700

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

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) was been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) and originally published as ETSI TS 183 023 [13]. It was transferred to the 3rd Generation Partnership Project (3GPP) in in January 2008.

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 defines a protocol used for manipulating data related to PSTN/ISDN Simulation services. The protocol is based on the eXtensible Markup Language (XML) Configuration Access Protocol (XCAP) [8]. A new XCAP application usage is defined for the purpose of manipulating PSTN/ISDN Simulation services data. The common XCAP related aspects that are applicable to PSTN/ISDN services are specified in the present document. The protocol allows authorized users to manipulate service-related data either when they are connected to IMS or when they are connected to non-IMS networks (e.g. the public Internet).

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*.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1]   IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[2]   W3C REC-xmlschema-1-20010502: "XML Schema Part 1: Structures".

[3]   IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[4]   IETF RFC 2246: "The TLS Protocol Version 1.0".

[5]   ETSI TS 124 109: "Universal Mobile Telecommunications System (UMTS); Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details (3GPP TS 24.109)".

[6]   ETSI TS 133 222: "Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222)".

[7]   Void.

[8]   draft-ietf-simple-xcap-08.txt: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[9]   ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[10]   draft-ietf-simple-xcap-diff-03.txt: "An Extensible Markup Language (XML) Document Format for Indicating A Change in XML Configuration Access Protocol (XCAP) Resources".

[11]   draft-ietf-sipping-config-framework-08.txt: "A Framework for Session Initiation Protocol User Agent Profile Delivery".

[12]   ETSI TS 183 038: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Simulation Services; Extensible Markup Language (XML) Document Management; Protocol Specification (Endorsement of OMA-TS-XDM-Core-V1-0-20051103-C and OMA-TS-XDM-Shared-V1-0-20051006-C)".

[13]   ETSI TS 183 023 V1.4.0: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating NGN PSTN/ISDN Simulation Services".

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in draft-ietf-simple-xcap-08.txt [8] apply.

3.2   Abbreviations

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

AP	Authentication Proxy
AS	Application Server
AUID	Application Unique ID
HTTP	HyperText Transfer Protocol
ISDN	Integrated Services Digital Network
MIME	Multipurpose Internet Mail Extensions
NAF	Network Application Function
NGN	Next Generation Network
PSTN	Public Switched Telephone Network
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XML	eXtended Markup Language

4   Architecture for manipulating NGN PSTN/ISDN simulation services settings

The protocol described in the present document allows to manipulate settings and variables related that influence the execution of one or more PSTN/ISDN simulation services. Manipulation of supplementary services take place over the Ut interface (UE to AS), as shown in figure 1.
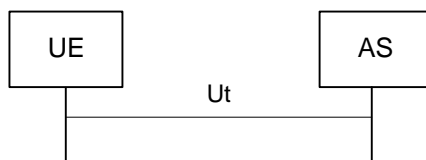

Figure 1: Ut interface

Manipulation of services does not usually take place during real-time operation. Typically users manipulate their services configuration data prior to the invocation and execution of the service.

Authentication of the user with HTTP may take place directly at the AS, such as in figure 1, or with the support of an Authentication Proxy, such as in figure 2. The architecture for authentication is provided in TS 187 003 [9] with the remark that the Network Application Function (NAF) is effectively an AS providing an NGN PSTN/ISDN simulation service in an NGN.
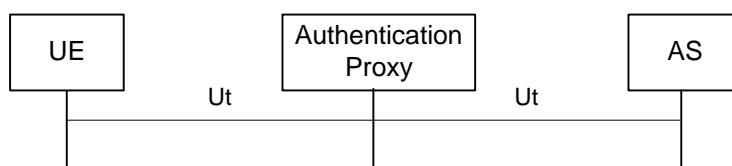

Figure 2: Authentication proxy in the Ut interface path

5   The eXtensible Markup Language (XML) Configuration Access Protocol (XCAP)

5.1   Introduction

For the purpose of manipulating data stored in an application server the XML Configuration Access Protocol (XCAP) [8] is used. XCAP allows a client to read, write and modify application configuration data, stored in XML format on a server. XCAP maps XML document sub-trees and element attributes to HTTP URIs, so that these components can be directly accessed by HTTP [1]. XCAP uses the HTTP methods PUT, GET, and DELETE to operating on XML documents stored in the server.

In the case of PSTN/ISDN simulation services, the data stored in a server is related to the execution of that given service. The present document defines a new XCAP Application Usage for the purpose of allowing a client to manipulate data related to PSTN/ISDN simulation services.

XCAP [8] defines two logical roles: XCAP client and XCAP servers. An XCAP client is an HTTP/1.1 compliant client. Similarly an XCAP server is an HTTP/1.1 compliant server. The XCAP server acts as a repository of XML documents that customize and modify the execution of NGN PSTN/ISDN simulation services. Figure 3 depicts the XCAP architecture where an XCAP client sends an HTTP/1.1 request to an XCAP server. The server replies with an HTTP/1.1 response.
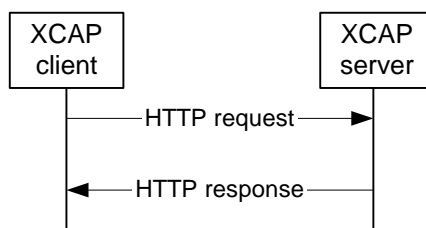
Figure 3: XCAP architecture

According to XCAP [8], each application that makes use of XCAP defines its own XCAP application usage. The present document defines an NGN PSTN/ISDN simulation services XCAP application usage in clause 6. This application usage defines the XML schema [2] for the data used by the application, along with other key pieces of information.

XCAP focuses on the definition of XML documents that are compliant with the XML schema and constrains defined for a particular XCAP application usage. XCAP allows application to provide XML documents that are common for all users or XML documents that affect the service of a given user.

Central to XCAP is the construction of the HTTP URI that points to particular XML document or certain components of it. A component in an XML document can be an XML element, attribute, or the value of it.

5.2 Functional entities

5.2.1 User Equipment (UE)

5.2.1.1 General

The UE implements the role of an XCAP client, as described in clause 5.3.1.

The UE shall implement access authentication as specified in RFC 2617 [3].

The UE shall implement Transport Layer Security (TLS) (see RFC 2246 [4]).

On sending an HTTP request, the UE may indicate the user's identity intended to be used with the AS by adding a HTTP X-3GPP-Intended-Identity header (TS 124 109 [5]) to the outgoing HTTP request.

5.2.1.2 Subscription for notification of state changes in XML document

In order to keep the simulation services state synchronized with the network elements and other terminals that the user might be using, the UE should subscribe to changes in the XCAP simserv documents by generating a SUBSCRIBE request in accordance with draft-ietf-simple-xcap-diff-03.txt [10] and draft-ietf-sipping-config-framework-08.txt [11].

5.2.2 Authentication Proxy (AP)

5.2.2.1 Introduction

An Authentication Proxy is an HTTP/1.1 [1] compliant server whose main purpose is to authenticate the user requests. The Authentication Proxy is used to separate the authentication procedure and the Application Server (AS) specific application logic to different logical entities.

The AP is configured as a HTTP reverse proxy, i.e. the FQDN of the AS is configured to the AP such a way that the IP traffic intended to the AS is directed to the AP by the network. The AP performs the authentication of the UE. After the authentication procedure has been successfully completed, the AP assumes the typical role of a reverse proxy, i.e. the AP forwards HTTP requests originating from the UE to the correct AS, and returns the corresponding HTTP responses from the AS to the originating UE.

The AP allows authorized users to manipulate services when they are connected to an IMS network or when they are connected to a non-IMS network (e.g. the public Internet). Authentication details can differ in both situations.

Provisioning of credentials to authenticate the user is outside the scope of the present document. TS 187 003 [9] provides further architectural authentication details.

5.2.2.2 Authentication

On receiving an HTTP request, the AP shall first determine the mechanism used to authenticate the user. The XDM specification [12] provides guidelines for the Authentication Proxy to take such decision. If the Generic Authentication Architecture [6] is used, the AP shall attempt to authenticate the user via the mechanisms specified in TS 133 222 [6] and the AP shall follow the procedures indicated in clause 5.2.2.2.1. If the Generic Authentication Architecture [6] is not used, the AP shall attempt to authenticate the user according to RFC 2617 [3].

5.2.2.2.1 Authentication based on the generic authentication architecture

On receiving an HTTP request that contains the Authorization header field, the AP shall:

   a)   use the value of that username parameter of the Authorization header field to authenticate the user;

   b)   apply the procedures specified in RFC 2617 [3] for authentication;

   c)   if the HTTP request contains an X-3GPP-Intended-Identity header field (TS 124 109 [5]), then the AP may verify that the user identity belongs to the subscriber. This verification of the user identity shall be performed dependant on the subscriber's application specific or AP specific user security settings;

   d)   if authentication is successful, remove the Authorization header field from the HTTP request;

   e)   insert an HTTP X-3GPP-Asserted-Identity header field (TS 124 109 [5]) that contains the asserted identity or a list of identities; and

   f)   forward the HTTP request to the appropriate AS.

On receiving an HTTP response for the previous request, the AP shall:

   a)   add an Authentication-Info header field in accordance to the procedures described in TS 133 222 [6]; and

   b)   forward the response to the XCAP client.

On receiving an HTTP request that does not contain the Authorization header field, the AP shall:

   a)   challenge the user by generating a 401 Unauthorized response according to the procedures specified in TS 133 222 [6] and RFC 2617 [3]; and

   b)   forward the 401 Unauthorized response to the sender of the HTTP request.

5.2.2.2.2 Void

5.2.2.3 Authorization

The AP shall be able to decide whether particular subscriber, i.e. the UE, is authorized to access a particular AS. On doing so, the AP may use the User Security Settings specified in TS 124 109 [5].

The AP may indicate an asserted identity or a list of identities to the AS by adding an HTTP X-3GPP-Asserted-Identity header field to the HTTP requests prior to forwarding the request to the AS. In case of multiple identities, they shall be separated by comma (,) and each identity shall be surrounded by quotation marks ("). Whether the AP supports this handling of an asserted identity or a list of identities then it shall depend on local policy in the AP. In addition the subscriber's application specific or AP specific user security settings may be considered.

The AP may indicate an authorization flag or a list of authorization flags from the application specific user security settings (USS) to the AS by adding a HTTP X-3GPP-Authorization-Flags header field to the HTTP request prior to forward it to the XCAP server. The HTTP X-3GPP-Authorization-Flags header field shall contain a list of authorization flags separated by comma (,) and each authorization flag is surrounded by quotation marks ("). In case the AP supports this handling of authorization flags from USS then it shall depend on local policy in the AP.

5.2.3 Application Server (AS)

5.2.3.1 General

An Application Server implements the role of an XCAP server as described in clause 5.3.2.

The AS shall implement access authentication as specified in RFC 2617 [3].

The AS shall implement Transport Layer Security (TLS) (see RFC 2246 [4]).

5.2.3.2 Authentication and authorization

If an Authentication Proxy (AP) is provided in the path of the HTTP request, then the AS receives an HTTP request from a trusted source (the AP) and contains an HTTP X-3GPP-Asserted-Identity header (TS 124 109 [5]) that includes an asserted identity of the user. In this case the AS does not need to authenticate the user, but just provide authorization to access the requested resource.

If an HTTP X-3GPP-Asserted-Identity header (TS 124 109 [5]) is not present in the HTTP request or if the request is received from a non-trusted source, then the AS needs to authenticate the user prior to providing authorization to the XCAP resource by applying the procedures described in clause 5.2.3.2.1.

5.2.3.2.1 HTTP digest authentication

On receiving an HTTP request that does not contain an Authorization header the AS shall:

a) challenge the user by generating a 401 Unauthorized response that contains the proper Digest authentication parameters (e.g. realm), according to RFC 2617 [3]. Provisioning of credentials to authenticate the user is outside the scope of the present document; and

b) forward the 401 Unauthorized response to the sender of the HTTP request.

On receiving an HTTP request that contains an Authorization header, the AS shall:

a) apply the authentication procedures defined in RFC 2617 [3]; and

b) authorize or deny authorization depending on the authenticated identity.

5.2.3.3 Subscription acceptance and notification of state changes in XML document

When the AS receives a SUBSCRIBE request having the Event header field value set to "ua-profile", the AS shall first authenticate the source of the SUBSCRIBE request and then perform authorization. Afterwards, the AS shall generate a response to the SUBSCRIBE request and notifications in accordance with draft-ietf-simple-xcap-diff-03.txt [10] and draft-ietf-sipping-config-framework-08.txt [11].

5.3 Roles

5.3.1 XCAP client

5.3.1.1 Introduction

The XCAP client is a logical function as defined in draft-ietf-simple-xcap-08.txt [8]. The XCAP client provides the means to manipulate the general data, such as configuration settings related to NGN PSTN/ISDN simulation services.

NOTE: In order to be able to manipulate data stored on the XCAP server, the XCAP client needs to know the XCAP root directory on the XCAP server and the user's directory name. It is assumed that these values are pre-provisioned or the UE uses some means to discover it. Discovery mechanisms are outside the scope of the present document.

5.3.1.2 Manipulating NGN PSTN/ISDN simulation services

When the XCAP client intends to manipulate a resource list, it shall generate an HTTP PUT, HTTP GET or HTTP DELETE request in accordance with draft-ietf-simple-xcap-08.txt [8] and the NGN PSTN/ISDN simulation services application usage specified in clause 6.

5.3.2 XCAP server

5.3.2.1 Introduction

The XCAP server is a logical function as defined in draft-ietf-simple-xcap-08.txt [8]. The XCAP server can store data related to the configuration of NGN PSTN/ISDN simulation services. The XCAP server shall provide or deny authorization to access XCAP resources by authenticated users.

5.3.2.2 Manipulation acceptance

When the XCAP server receives an HTTP PUT, HTTP GET or HTTP DELETE request for manipulating or fetching a resource list, the XCAP server shall first authenticate the request and then perform authorization. Clause 5.2.2 provides more details on the authentication and authorization of HTTP requests.

Afterwards the XCAP server shall perform the requested action and generate a response in accordance with draft-ietf-simple-xcap-08.txt [8] and the NGN PSTN/ISDN simulation services application usage specified in clause 6.

6 NGN PSTN/ISDN simulation services XCAP application usage

6.1 Structure of the XML document

XCAP provides for the existence of application usages that define the conventions and constrains related to the manipulation of XML documents in an XCAP server. The present document defines an NGN PSTN/ISDN simulation services XCAP application usage. This application usage is common for a variety of PSTN/ISDN simulation services defined by NGN Release 1. Further releases may extend this application usage when deemed practical.

The present document follows a modular approach, as depicted in figure 4. We provide for the existence of a *simservs* XML document that contains the data associated to one or more NGN PSTN/ISDN simulation services. The *simservs* XML document is composed of a common part, defined by the present document, and a number of XML fragments corresponding to each of the NGN PSTN/ISDN simulation services. This modular approach has significant advantages. Particularly, it is versatile enough to allow any number of configurations. For example, in one configuration, an XCAP server might be managing a given server. In this case, the *simservs* XML document will contain one subtree per service. In another configuration, each service is managed in its own XCAP server, case in which the XML document in each XCAP server will contain the common parts and a single XML subtree that manages the service. Yet in a third configuration the XCAP server stores several XML documents, each document managing one or more services.

The XML schema for the *simservs* XML document, including the common parts, is specified in clause 6.3. This XML schema allows for each of the individual XML schemas pertaining to a particular service to import the common parts XML schema. Each XML fragment affects the settings of a PSTN/ISDN simulation service (or group of related PSTN/ISDN simulation services). The XML schema of each of the PSTN/ISDN simulation services is specified in its own specification. A template of the XML schema for a PSTN/ISDN simulation service is provided in clause 6.4.
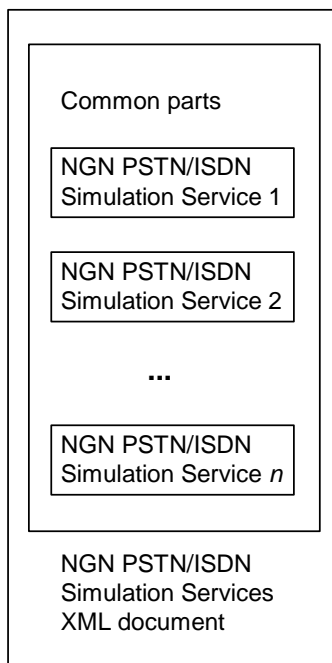
Figure 4: Structure of an NGN PSTN/ISDN simulation services XML document

The *simservs* XML document starts with a <simservs> root XML element that can contain one or more child elements pertaining to PSTN/ISDN simulation services. Each of these service elements can contain an "active" attribute that indicates whether the service is activated or not. When the "active" attribute is absent on a service element, it indicates that the service is activated. Elements and attributes from different namespaces can be present as well.

6.2   XCAP application usage

XCAP requires application usages to fulfil a number of steps in the definition of such application usage. The reminder of this clause specifies the required definitions of the NGN PSTN/ISDN simulation services XCAP Application Usage.

Application Unique ID (AUID): Each XCAP application usage is associated with a unique name called the Application Unique ID (AUID). The AUID defined by this application usage falls into the vendor-proprietary namespace of XCAP AUID, where ETSI is considered a vendor.

The AUID allocated to the NGN PSTN/ISDN simulation services XCAP application usage is:

<p align="center">simservs.ngn.etsi.org</p>

XML schema: Implementations in compliance with the present document shall implement the XML schema that includes the XML Schema defined in clause 6.3. Additionally, each PSTN/ISDN simulation service (or group of them) is modelled with a XML fragment that is validated according to a specific XML schema. The XML schema that affects the settings of the related service is specified in the specification of the given PSTN/ISDN simulation service. Clause 6.4 provides a template that shall be included in XML Schema that also includes the XML Schema defined in clause 6.3 along with inclusion of XML schema defined by each of the PSTN/ISDN simulation services that implement XML schemas for data manipulation. Additionally the schema in clause 6.3 contains the specification of a number of common service specific elements and types, the semantics and applicability of these elements is described in the service specifications that use them.

Default namespace: XCAP requires application usages to declare the default namespace. The default namespace of the NGN PSTN/ISDN simulation services XCAP application usage is:

<p align="center">http://uri.etsi.org/ngn/params/xml/simservs/xcap</p>

MIME type: The MIME type of NGN PSTN/ISDN simulation services XML documents is:

<p align="center">application/simservs+xml</p>

Validation constraints: The present document does not specify any additional constraint beyond those defined by XCAP [8]. Note, however, that each of the supplementary services may specify additional constraints on each of the XML subdocuments.

Data semantics: The XML schema does not accept URIs that could be expressed as a relative URI reference causing a resolution problem. However, each of the supplementary services should consider if relative URIs are allowed in the subdocument tree, and in that case, they should indicate how to resolve relative URI references. In the absence of further indications, relative URI references should be resolved using the document URI as the base of the relative URI reference.

Naming conventions: By default, NGN PSTN/ISDN simulation services XML documents are stored under the user's Home Directory (which is located under the "users" sub-tree). In order to facilitate the manipulation of an NGN PSTN/ISDN simulation services XML document, we define a default XML file name:

<p align="center">simservs.xml</p>

Resource interdependencies: The present document does not specify additional resource interdependency beyond those specified in the XML schema and beyond any resource interdependency that may be specified in each of the NGN PSTN/ISDN simulation services.

Authorization policies: The default XCAP [8] authorization policy is used in the application usage defined by the present document.

NOTE: The default policy indicates that the creator of the XML document is the one authorized to manipulate it.

6.3 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
           xmlns:ss="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           elementFormDefault="qualified"
           attributeFormDefault="unqualified">

<!-- The element "simservs" maps to the Common Parts of an NGN PSTN/ISDN  Simulation services
document -->

   <xs:element name="simservs">
      <xs:annotation>
         <xs:documentation>XML Schema for data manipulation of ETSI
                           NGN PSTN/ISDN Simulation Services
         </xs:documentation>
      </xs:annotation>
      <xs:complexType>
         <xs:sequence>
            <xs:element ref="ss:absService" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="extensions" minOccurs="0">
               <xs:complexType>
                  <xs:sequence>
                     <xs:any namespace="##other" processContents="lax"
                        minOccurs="0" maxOccurs="unbounded"/>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
         </xs:sequence>
         <xs:anyAttribute namespace="##any" processContents="lax"/>
      </xs:complexType>
   </xs:element>

   <xs:element name="absService" abstract="true" type="ss:simservType"/>

   <xs:complexType name="simservType">
      <xs:attribute name="active" type="xs:boolean"
                    use="optional" default="true" />
      <xs:anyAttribute namespace="##any" processContents="lax"/>
   </xs:complexType>

   <!-- service specific IETF common policy condition elements-->
   <xs:element name="anonymous" type="ss:empty-element-type"/>
   <xs:element name="presence-status" type="ss:presence-status-activity-type"/>
   <xs:element name="media" type="ss:media-type"/>
   <xs:element name="communication-diverted" type="ss:empty-element-type"/>
```

```
<xs:element name="rule-deactivated" type="ss:empty-element-type"/>
<xs:element name="not-registered" type="ss:empty-element-type"/>
<xs:element name="busy" type="ss:empty-element-type"/>
<xs:element name="no-answer" type="ss:empty-element-type"/>
<xs:element name="not-reachable" type="ss:empty-element-type"/>
<xs:element name="roaming" type="ss:empty-element-type"/>

<!-- service specific type declarations -->
<xs:simpleType name="media-type" final="list restriction">
   <xs:restriction base="xs:string"/>
</xs:simpleType>
<xs:simpleType name="presence-status-activity-type" final="list restriction">
   <xs:restriction base="xs:string"/>
</xs:simpleType>
<xs:complexType name="empty-element-type"/>

</xs:schema>
```

6.4 Template for a PSTN/ISDN simulation service XML schema

PSTN/ISDN simulation services that implement XCAP operations to manipulate the data associated to its service shall base their XML schema in the following template. Replace "ServiceName" with the name or acronym of the actual service.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
   xmlns:ss="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
              elementFormDefault="qualified"
              attributeFormDefault="unqualified">

   <xs:element name="ServiceName" substitutionGroup="ss:absService">
      <xs:annotation>
        <xs:documentation>Template of a PSTN/ISDN Simulation
                          Service XML Schema
        </xs:documentation>
      </xs:annotation>

      <!-- If the service needs to add children elements or attributes -->
      <!-- it can use the following complexType for such purpose -->
      <xs:complexType>
         <xs:complexContent>
            <xs:extension base="ss:simservType">
                  <xs:sequence>
                     <!-- service specific elements can be defined here -->
                  </xs:sequence>
                  <!-- service specific attributes can be defined here -->
            </xs:extension>
         </xs:complexContent>
      </xs:complexType>

   </xs:element>
</xs:schema>
```

Annex A (informative):
Bibliography

- ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

Annex B (informative):
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2005-09					Publication as **ETSI TS 183 023**		1.1.1
2006-03					Publication as ETSI TS 183 023		1.2.1
2007-04					Publication as ETSI TS 183 023		1.3.1
2008-01					Publication as ETSI TS 183 023		1.4.0
2008-01					Conversion to **3GPP TS 24.423**		1.4.1
2008-03	CT#39	CP-080087			Version 1.4.1 approved in CP-080087 and version 7.0.0 created by MCC for publication	1.4.1	7.0.0

History

Document history		
V7.0.0	April 2008	Publication