3GPP TS 24.623 V17.2.0 (2022-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services (Release 17)

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

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

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguousand is notused in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document defines a protocol used for manipulating data related to supplementary services. The protocol is based on the eXtensible Markup Language (XML) Configuration Access Protocol (XCAP)RFC 4825 [8]. A new XCAP application usage is defined for the purpose of manipulating the supplementary services data. The common XCAP related aspects that are applicable to supplementary 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).

The present document is applicable to User Equipment (UE) and Application Servers (AS) which are intended to support XCAP application usage for manipulating data related to supplementary services.

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] Void.

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

[3] Void.

[4] Void.

[5] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[6] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[7] Void.

[8] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[9] Void

[10] Void.

[11] IETF RFC 5875 (May 2010): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".

[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".

[14] OMA-TS-XDM_Core-V1_1-20080627-A: "XML Document Management (XDM) Specification".

[15] 3GPP TS 23.003: "Numbering, addressing and identification".

[15A] 3GPP TS 31.103: "Characteristics of the IP multimedia services identity module (ISIM) application".

[15B] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[16] 3GPP TS 24.315: "IP Multimedia Subsystem (IMS) Operator Determined Barring (ODB); Stage 3".

[17] 3GPP TS 33.141: "Presence service; Security".

[18] IETF RFC 6665 (July 2012): "SIP-Specific Event Notification".

[19] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".

[20] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[22] 3GPP TS 24.424: "Management Object (MO) for Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services (SS)".

[23] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[24] 3GPP TS 22.011: "Service accessibility".

[25] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[26] 3GPP TS 29.292: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem (IMS) and MSC Server for IMS Centralized Services (ICS)".

[27] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[28] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for subscriber certificates".

[29] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[30] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[31] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[32] 3GPP TS 24.244: "Wireless LAN control plane protocol for trusted WLAN access to EPC".

[33] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[34] 3GPP TS 24.502: "Access to the 3GPP 5G Core Network (5GCN) via non-3GPP access networks".

[35] IETF RFC 7230 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[36] IETF RFC 7231 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[37] IETF RFC 7232 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[38] IETF RFC 7233 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".

[39] IETF RFC 7234 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Caching".

[40] IETF RFC 7235 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[41] IETF RFC 7616 (September 2015): "HTTP Digest Access Authentication".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [20] and IETF RFC 4825 [8] apply.

SS configuration via XCAP:supplementary services (SS) configuration based on XCAP protocol sent over the Ut interface.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.011 [24] apply:

3GPP PS data off
3GPP PS data off exempt service

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.229 [25] apply:

3GPP PS data off status

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.501 [33] apply:

NG-RAN

3.2 Abbreviations

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

5GCN	5G Core Network
5GS	5G System
AP	Authentication Proxy
AS	Application Server
AUID	Application Unique ID
EPS	Evolved Packet System
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
IMS	IP Multimedia Subsystem
IP-CAN	IP Connectivity Access Network
ISDN	Integrated Services Digital Network
MIME	Multipurpose Internet Mail Extensions
MMI	Man-Machine Interface
NAF	Network Application Function
NGN	Next Generation Network
NG-RAN	Next Generation Radio Access Network
ODB	Operator Determined Barring
PS	Packet Switched
PSTN	Public Switched Telephone Network

SS	Supplementary Service
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier
WPA	Wrong Password Attempts
XCAP	XML Configuration Access Protocol
XML	eXtended Markup Language
XUI	XCAP User Identifier

4 Architecture for manipulating supplementary services settings

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

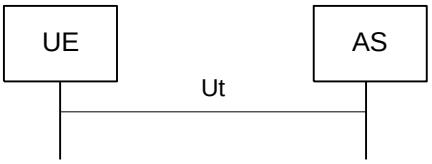

Figure 1: Ut interface

Manipulation of supplementary 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 3GPP TS 33.222 [6].

NOTE: The Network Application Function (NAF) can be an AS.

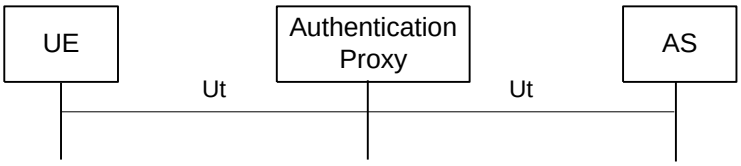

Figure 2: Authentication proxy in the Ut interface path

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 (see IETF RFC 7230 [35], IETF RFC 7231 [36], IETF RFC 7232 [37], IETF RFC 7233 [38], IETF RFC 7234 [39] and IETF RFC 7235 [40]). XCAP uses the HTTP methods PUT, GET, and DELETE to operating on XML documents stored in the server.

In the case of supplementary 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 supplementary services.

XCAP (see IETF RFC 4825 [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 the supplementaryservices. 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.

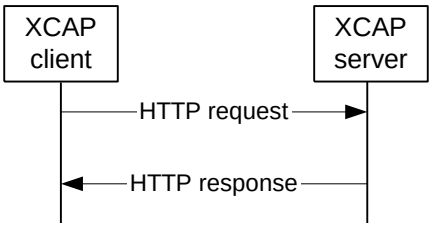

Figure 3: XCAP architecture

According to XCAP (see IETF RFC 4825 [8]), each application that makes use of XCAP defines its own XCAP application usage. The present document defines an supplementaryservices XCAP application usage in clause 6. This application usage defines the XML schemaW3C REC-xmlschema-1-20010502 [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 accessing the XCAP application usage as described in clause 6.2.

For systems where Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is used, the UE shall support the authentication mechanisms specified in 3GPP TS 33.222 [6] and 3GPP TS 24.109 [5].

For systems where Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is not used, the UE shall support IETF RFC 7616 [41] in all procedures of ETSI TS 183 038 [12] where HTTP digest authentication support is specified and shall support the TLS profile specified in 3GPP TS 33.310 [21] annex E in all procedures of ETSI TS 183 038 [12] where TLS support is specified.

For systems where Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is not used, the UE may support the authentication mechanisms specified in 3GPP TS 33.141 [17] annex D.

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 (3GPP TS 24.109 [5]) to the outgoing HTTP request. If the authentication mechanism specified in 3GPP TS 33.141 [17] annex D is used, the UE shall add a HTTP X-3GPP-Intended-Identity header field.

If the UE supports the optional configuration parameter "Access_Point_Name_Parameter_Reading_Rule", as defined in 3GPP TS 24.167 [19] and has been configured with this parameter, then the UE shall use it to retrieve the access point name to use in the PDP context activation procedure or in the PDN connection procedure for XCAP.

5.2.1.2 Subscription for notification of state changes in XML document

In order to keep the supplementary 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 RFC 5875 [11] and RFC 6665 [18].

5.2.1.3 Policy on access type used for XCAP

The policy on access typeused for the XCAP enables HPLMN control of access used for XCAP messages.

The policy on access type used for the XCAPcan be set to one of the following values:

a) any access type;

b) 3GPP accesses only;

c) EPC or 5GCN via WLAN IP-CAN only;

d) Non-seamless WLAN offload only;

e) 3GPP accesses preferred, non-seamless WLAN offload as secondary; and

f) 3GPP accesses preferred, EPC or 5GCN via WLAN IP-CAN as secondary.

The UE may support the policy on access type used for the XCAP.

If the UE supports the policy on access type used for the XCAP:

a) when the UE needs to send an XCAP request:

   1) if the policy on access type used for the XCAP is set to "any access type", the UE shall send XCAP requests from an IP address associated with a bearer of any access;

   2) if the policy on access type used for the XCAP is set to "3GPP accessesonly":

      A) the UE shall attempt to obtain a PDP context for XCAP as specified in 3GPP TS 24.008 [29] or a EPS bearer context for XCAP as specified in 3GPP TS 24.301 [30] or a 5GS QoS flow using NG-RAN as specified in 3GPP TS 24.501 [33];

      B) if the UE obtains the PDP context for XCAP or the EPS bearer context for XCAP or the 5GS QoS flow using NG-RAN, the UE shall send XCAP requests from an IP address associated with the obtained PDP context for XCAP or the obtained EPS bearer context for XCAP or the 5GS QoS flow using NG-RAN; and

      C) if the UE cannot obtain the PDP context for XCAP or the EPS bearer context for XCAP or the 5GS QoS flow using NG-RAN, the UE shall not send XCAP request;

   3) if the policy on access type used for the XCAP is set to "EPC or 5GCN via WLANIP-CAN only":

      A) the UE shall attempt to associate with a WLAN as specified in 3GPP TS 24.302 [31] or as specified in 3GPP TS 24.502 [34] and the UE shall attempt to obtain:

         - a PDN connection for XCAP as specified in 3GPP TS 24.302 [31], or 3GPP TS 24.244 [32]; or

         - a 5GS QoS flow using WLAN as specified in 3GPP TS 24.502 [34];

      B) if the UE obtains the PDN connection or 5GS QoS flow for XCAP, the UE shall send XCAP requests from an IP address associated with the PDN connection or 5GS QoS flow for XCAP; and

      C) if the UE cannot obtain the PDN connection or 5GS QoS flow for XCAP, the UE shall not send an XCAP request;

   4) if the policy on access type used for the XCAP is set to "Non-seamless WLAN offloadonly":

      A) the UE shall attempt to associate with a WLAN as specified in 3GPP TS 24.302 [31];

B) if the UE associates with a WLAN and the WLAN is either untrusted non-3GPP access or the UE established NSWO via TWAN, the UE shall send XCAP requests from an IP address associated with the WLAN; and

C) if the UE cannot associate with a WLAN or the UE associates with TWAN and NSWO is not available, the UE shall not send an XCAP request;

5) if the policy on access type used for the XCAP is set to "3GPP accesses preferred, non-seamless WLAN offload as secondary":

A) the UE shall attempt to obtain a PDP context for XCAP as specified in 3GPP TS 24.008 [298] or a EPS bearer context for XCAP as specified in 3GPP TS 24.301 [30] or a 5GS QoS flow for XCAP as specified in 3GPP TS 24.501 [33];

B) if the UE obtains the PDP context for XCAP or the EPS bearer context for XCAPor a 5GS QoS flow for XCAP, the UE shall send XCAP requests from an IP address associated with the obtained PDP context for XCAP or the obtained EPS bearer context for XCAP; and

C) if the UE cannot obtain the PDP context for XCAP or the EPS bearer context for XCAPor a 5GS QoS flow for XCAP:

i) the UE shall attempt to associate with a WLAN as specified in 3GPP TS 24.302 [31];

ii) if the UE associates with a WLAN and the WLAN is either untrusted non-3GPP access or the UE established NSWO via TWAN, the UE shall send XCAP requests from an IP address associated with the WLAN; and

iii) if the UE cannot associate with a WLAN or the UE associates with TWAN and NSWO is not available, the UE shall not send an XCAP request; and

6) if the policy on access type used for the XCAP is set to "3GPP accesses preferred, EPC or 5GCN via WLAN IP-CAN as secondary":

A) the UE shall attempt to obtain a PDP context for XCAP as specified in 3GPP TS 24.008 [29] or a EPS bearer context for XCAP as specified in 3GPP TS 24.301 [30] or a 5GS QoS flow using NG-RAN as specified in 3GPP TS 24.501 [33];

B) if the UE obtains the PDP context for XCAP or the EPS bearer context for XCAP or the 5GS QoS flow for XCAP, the UE shall send XCAP requests from an IP address associated with the obtained PDP context for XCAP or the obtained EPS bearer context for XCAP or the 5GS QoS flow using NG-RAN; and

C) if the UE cannot obtain the PDP context for XCAP or the EPS bearer context for XCAP or the 5GS QoS flow using NG-RAN:

i) the UE shall attempt to associate with a WLAN as specified in 3GPP TS 24.302 [31] or as specified in 3GPP TS 24.502 [34] and the UE shall attempt to obtain:

- a PDN connection for XCAP as specified in 3GPP TS 24.302 [31], or 3GPP TS 24.244 [32]; or

- a 5GS QoS flow using WLAN as specified in 3GPP TS 24.502 [34];

ii) if the UE obtains the PDN connection or 5GS QoS flow for XCAP, the UE shall send XCAP requests from an IP address associated with the PDN connection or 5GS QoS flow for XCAP; and

iii) if the UE cannot obtain the PDN connection or 5GS QoS flow for XCAP, the UE shall not send an XCAP request; and

b) the UE may support being configured with the policy on access type used for the XCAPusing one or more of the following methods:

a) the $EF_{XCAPConfigData}$ file described in 3GPP TS 31.102 [15B];

b) the $EF_{XCAPConfigData}$ file described in 3GPP TS 31.103 [15A]; and

c) the AccessForXCAP node of 3GPP TS 24.424 [22].

If the UE is configured with both the AccessForXCAP node of 3GPP TS 24.424 [22] and the $EF_{XCAPConfigData}$ file described in 3GPP TS 31.102 [15B] or 3GPP TS 31.103 [15A], then the $EF_{XCAPConfigData}$ file shall take precedence.

NOTE: Precedence for files configured on both the USIM and ISIM is defined in 3GPP TS 31.102 [15B].

5.2.1.4 Policy on authenticationmechanism used for XCAP

The policy on authenticationmechanism used for the XCAP enables the network to choose authentication mechanism for the Ut reference point.

The policy on authentication mechanism used for the XCAPcan be set to one of the following values:

a) GBA_ME;

b) GBA_U;

c) GBA_Digest; and

d) SSC (support for subscriber certificates).

The UE may support the policy on authentication mechanism used for the XCAP.

If the UE supports the policy on authentication mechanism for the XCAP, when the UE needs to send an HTTP request:

a) if the policy on authentication mechanism used for the XCAP is set to "GBA_ME", the UE shall use GBA_ME authentication mechanism as defined in 3GPP TS 33.220 [27];

b) if the policy on authentication mechanism used for the XCAP is set to "GBA_U", the UE shall use GBA_U authentication mechanism as defined in 3GPP TS 33.220 [27];

c) if the policy on authentication mechanism used for the XCAP is set to "GBA_Digest", the UE shall use GBA_Digest authentication mechanism as defined in 3GPP TS 33.220 [27]; or

d) if the policy on authentication mechanism used for the XCAP is set to "SSC", the UE shall use SSC authentication mechanism as defined in 3GPP TS 33.221 [28].

The UE may support being configured with the policy on authentication mechanism used for the XCAP using the AuthenticationForXCAP node of 3GPP TS 24.424 [22].

5.2.2 Authentication Proxy (AP)

5.2.2.1 Introduction

An Authentication Proxy is an HTTP/1.1 (see IETF RFC 7230 [35], IETF RFC 7231 [36], IETF RFC 7232 [37], IETF RFC 7233 [38], IETF RFC 7234 [39] and IETF RFC 7235 [40]) 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. 3GPP TS 33.222 [6] provides further architectural authentication details.

NOTE: Multiple APs can exist between the UE and the AS, and the UE can obtain a list of different AP addresses via DNS query.

5.2.2.2 Authentication

5.2.2.2.0 General

On receiving an HTTP request, the AP shall first determine the mechanism used to authenticate the user. If the Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is used, the AP shall attempt to authenticate the user via the mechanisms specified in 3GPP TS 33.222 [6] and the AP shall follow the procedures indicated in clause 5.2.2.2.1. For systems where Generic Authentication Architecture specified in 3GPP TS 33.222 [6] is not used, the AP shall attempt to authenticate the user according to IETF RFC 7616 [41] (ETSI TS 183 038 [12] provides guidelines for the Authentication Proxy) or 3GPP TS 33.141 [17] annex D.

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 IETF RFC 7616 [41] for authentication;

c) if the HTTP request contains an X-3GPP-Intended-Identity header field (3GPP TS 24.109 [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 (3GPP TS 24.109 [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 3GPP TS 33.222 [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 3GPP TS 33.222 [6] and IETF RFC 7616 [41]; 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 3GPP TS 24.109 [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 providing the XCAP application usage as described in clause 6.2.

For systems where Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is used, the AS shall support the authentication mechanisms specified in 3GPP TS 33.222 [6] and 3GPP TS 24.109 [5].

For systems where Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is not used, the AS shall support IETF RFC 7616 [41] in all procedures of ETSI TS 183 038 [12] where HTTP digest authentication support is specified and shall support the TLS profile specified in 3GPP TS 33.310 [21] annex E in all procedures of ETSI TS 183 038 [12] where TLS support is specified.

Procedures regarding Operator Determined Barring (ODB) are defined in 3GPP TS 24.315 [16].

For systems where Generic Authentication Architecturespecified in3GPP TS 33.222 [6] is not used, the AS may support the authentication mechanisms specified in 3GPP TS 33.141 [17] annex D.

5.2.3.2 Authentication and authorization

5.2.3.2.0 General

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 (3GPP TS 24.109 [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 (3GPP TS 24.109 [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 of authentication mechanisms specified in 3GPP TS 33.222 [6] and 3GPP TS 24.109 [5] in case Generic Authentication Architecture is selected, or as described in clause 5.2.3.2.1 or 3GPP TS 33.141 [17] annex D otherwise.

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 IETF RFC 7616 [41]. 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 IETF RFC 7616 [41]; 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 "xcap-diff", 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 RFC 5875 [11] and RFC 6665 [18].

5.2.3.4 Validation against service capability

On receiving a XCAP request to modify service settings for a supplementary service, the AS shall check whether service capability fragments within the simservs document for the subscription of the sender for the XCAP request are available. If a service capability fragment within the simservs documentis available, the AS shall validate the XCAP

request against constraints defined in that service capability fragment and only accept modifications that are allowed by the service capability fragment. If the validation fails, the AS shall respond with a HTTP 409 (Conflict) response as defined in IETF RFC 4825 [8].

NOTE: The XML schema for a service capability fragment for a supplementary service is defined in the respective supplementary service specification.

5.3 Roles

5.3.1 XCAP client

5.3.1.1 Introduction

The XCAP client is a logical function as defined in IETF RFC 4825 [8]. The XCAP client provides the means to manipulate the general data, such as configuration settings related to supplementary services.

In order to manipulate XCAP resources stored on the XCAP server, the XCAP client uses the XCAP Root URI as defined in clause 13.9.1 of 3GPP TS 23.003 [15]. The UE implementing the XCAP client can be provisioned with an XCAP Root URI as specified in Appendix C in OMA-TS-XDM_Core-V1_1-20080627-A [14].

NOTE: In order to be able to manipulate XCAP resources stored on the XCAP server, the XCAP client needs to know the user's directory name. It is assumed that this value is 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 supplementary services

5.3.1.2.1 General

When the XCAP client intends to manipulate a resource list, the XCAP client shall generate an HTTP PUT, HTTP GET or HTTP DELETE request in accordance with IETF RFC 4825 [8] and the supplementary services application usage specified in clause 6 of the present document. The XCAP client may attempt to manipulate resources for one or more supplementary services per request.

IETF RFC 4825 [8] describes the usage of a locally cached copy of resource lists. The XCAP client shall ensure that a modification of a resource list is performed using a version of the resource list that is synchronized with the resource list that is stored in the XCAP server.

NOTE 1: One mechanism to ensure that the locally cached version of a resource list is the same as the version of the resource list on the XCAP server is the usage of If-Match header field for conditional operations as defined in IETF RFC 4825 [8] by the XCAP client.

When the XCAP client needs to provide a password in order to request the manipulation of a resource list, the XCAP client shall include an XCAP User Identifier (XUI) in the Request-URI of an HTTP PUT request containing:

1) a SIP URI representing the public user identity of the served user; and

2) in the password portion of the SIP URI, the current password.

NOTE 2: The password provided by the user is a common password for all applicable supplementary services.

5.3.1.2.2 U E temporarily prevented from manipulating supplementary service settings via XCAP

Ifthe XCAP client receives a HTTP 403 (Forbidden) response to an HTTP PUT, HTTP GET or HTTP DELETE request, the XCAP client should not retry to manipulate the supplementary service settings via XCAP for a certain time period.

NOTE 1: If the UE is not configured for supplementary service management as specified in 3GPP TS 24.167 [19], the UE canuse another mechanism or domain (if available) to manipulate the supplementary services configuration settings (e.g. CS domain).

NOTE 2: The certain time period that the XCAP client does not retry the manipulation of supplementary services settings via XCAP depends on the type of terminal that implements the XCAP client (e.g. XCAP clients residing on mobile terminals can retry after a power-off/power-on orafter detection of achange of USIM/ISIM).

5.3.1.2.3 Supplementary service settings manipulation errors

If the XCAP client receives an HTTP 409 (Conflict) response to an XCAP request (within an HTTP PUT request or HTTP DELETE request) where the request contained changes to the *simservs* XML document (as defined in clause 6.1) then the XCAP client shall not attempt to resend the request with the same contents but if there are smaller portion of the change that are appropriate to make then the XCAP client should attempt to resend thesesmaller portions of changes to the *simservs* XML document, with each smaller portion contained within its own XCAP request (each within an HTTP PUT request or HTTP DELETE request, as appropriate).

NOTE 1: The functionality desired bythe user and the XCAP client implementation can determine how and whether to reapportion changes to the *simservs* XML document in a new XCAP request from a previous XCAP request. One example could be to align portions of changes to known supplementary service boundaries.

NOTE 2: An XCAP client might receive an HTTP 409 (Conflict) response for reasons other than a supplementary service subscription error e.g. as defined in IETF RFC 4825 [8]. Indication of the specific reason for the error is not defined in the current version of the present document.

5.3.1.2.4 HTTP retrywhen no response is received

If no response is received within a certain time period, after the XCAP client has sent out anHTTP requestand the XCAP client has different IP addresses available, the XCAP client may retry the requestusing one of the other IP addresses.

NOTE: The certain time period before the XCAP client retries the request depends on the configuration of the terminal that implements the XCAP client.

5.3.1.3 Password change

NOTE 1: 3GPP TS 22.030 [23] describes the MMI used when a user wishes to change a password when performing supplementary service control via the CS domain. This requires the user to input the current password, the new password and the new password (again). For password change via the CS domain, the network performs the verification of the new password with the new password (again). For password change via IMS, it is assumed that the user will still provide the current password, the new password and the new password (again) but the verification of the new password with the new password (again) will be carried out by the application on the UE. The details of this verification are out of scope of the present document.

When changing a password, the UE shall send an HTTP POST request, and shall include:

a) in the Request-URI an XUI including:

   1) a SIP URI representing the public user identity of the served user; and

   2) in the password portion of the SIP URI the current password;

b) the node selector in the Request-URI indicating the simservs XCAP resource; and

c) in the body a <password-change> element including a <new-password> element containing the new password.

NOTE 2: The current password and new password are common passwords for all applicable supplementary services.

The UE may also request a password check by sending an HTTP POST request as above, but without the <new-password> element.

NOTE 3: There is no useful semantics for a UE to request a password check, but for IMS centralised services as specified in 3GPP TS 29.292 [26] this is needed for compatibility with CS procedures.

5.3.2 XCAP server

5.3.2.1 Introduction

The XCAP server is a logical function as defined in IETF RFC 4825 [8]. The XCAP server can store data related to the configuration of supplementary services. The XCAP server shall provide or deny authorization to access XCAP resources by authenticated users. It is an operator configurable option in the XCAP server as to which supplementary services (if any) are provisioned for a subscription and what constraints (if any) apply to settings for provisioned supplementary services.

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.

The XCAP server shall support conditional processing as specified in IETF RFC 4825 [8] based on If-Match header field.

Afterwards the XCAP server shall perform the requested action and generate a response in accordance with IETF RFC 4825 [8] and the supplementary services application usage specified in clause 6.

5.3.2.3 User not allowed to manipulate settings via XCAP

If the username identified by the XUI in the HTTP PUT, HTTP GET or HTTP DELETE request, is not allowed to manipulate settings via XCAP, then the XCAP server shall respond with a HTTP 403 (Forbidden) response.

NOTE: If the UE is not configured for supplementary service management as specified in 3GPP TS 24.167 [19], it is expected that operators do not configure their XCAP servers to return the HTTP 403 error response code for any other reason than specified above.

5.3.2.4 Supplementary Service subscription errors

If the subscription associated with the username identified by the XUI in a received HTTP PUT or HTTP DELETE request is allowed to manipulate settings via XCAP and is either not provisioned with one or more supplementary services indicated in the XML document contained within the request or is provisioned but the indicated configuration is not in compliance with one or more operator defined constraints or the subscription option "control of supplementary service" to "by the service provider", then the XCAP server shall respond with an HTTP 409 (Conflict) response and shall not update the settings.

NOTE: An XCAP server might send an XCAP client an HTTP 409 (Conflict) response for reasons other than a supplementary service subscription error e.g. as defined in IETF RFC 4825 [8]. Indication of the specific reason for the error is not defined in the current version of the present document.

5.3.2.5 Password management

5.3.2.5.1 General

Password management procedures at the XCAP server consist of two independent procedures:

- password check; and
- password change;

The password check procedure is used for verifying the current password stored against the user:

- when the user requests a password check;
- when the user requests a password change; and
- when the user requests modification of a supplementary service configuration document for a service that has password control.

The password change procedure is used by the XCAP server to set a new password for the user.

The XCAP server shall maintain a Wrong Password Attempts (WPA) counter.

When the password is set by the service provider the XCAP server shall reset the WPA counter to zero.

If the XCAP server receives a password that does not match the current password stored for the service, the XCAP server shall increment the WPA counter by 1.

If a password check passes at the XCAP server, the XCAP server shall reset the WPA counter to zero. If the WPA counter exceeds the value three, the XCAP server shall set the subscription option "control of supplementary service" to "by the service provider".

5.3.2.5.2 Password check

If a password is required (e.g. for supplementary service configuration or for password change) and the XUI contains a password in the password portion of the SIP URI, the XCAP server shall verify that the password in the request matches that stored for the user.

If a password is required, and the XCAP server receives a request:

- where the XUI is not a SIP URI;
- where the XUI is a SIP URI and the request does not contain a password in the password portion of the SIP-URI; or
- where the XUI is a SIP URI, the request contains a password in the password portion of the SIP-URI and the password does not match the current password stored for the user;

then the XCAP server shall respond with an HTTP 409 (Conflict) response.

When the XCAP server responds with an HTTP 409 (Conflict) response where the XUI in the received request is not a SIP URI , the XCAP server shall include an <incorrect-xui-format> element in the HTTP 409 (Conflict) response.

When the XCAP server responds with an HTTP 409 (Conflict) response where the XUI is a SIP URI, the WPA counter has not exceeded 3 and:

- if the password is missing in the request, the XCAP server shall include a <password-required> element; and
- if the password is not correct, the XCAP server shall include an <incorrect-password> element.

If the XCAP server receives a request for

- a password check;
- a password change; or
- modification of a supplementary service,

and the user has the subscription option "control of supplementary service" set to "by the service provider", the XCAP server shall reject the request with an HTTP 403 (Forbidden) response.

5.3.2.5.3 Password change

If the XCAP server receives an HTTP POST request populated as in clause 5.3.1.3 and the subscription option "control of supplementary service" is set to a value of "by the service provider",then the XCAP server shall respond with an HTTP 403 (Forbidden) response.

When the XCAP server receives an HTTP POST request populated as in clause 5.3.1.3, and the subscription option "control of supplementary service" is set to a value of "by subscriber using a password", the AS shall determine if the user is authorized to change the password by asserting that the received current password is correct as described in clause 5.3.2.5.2, and if so replace the currently used password with the new password.The new password is stored in an implementation specific way such that the password cannot be retrieved by the user.

6 Supplementary services XCAP application usage

6.1 Structure of the XML document

XCAP provides for the existence of application usages that define the conventions and constraints related to the manipulation of XML documents in an XCAP server. The present document defines a supplementary services XCAP application usage.

NOTE 1: Further releases can extend this application usage when deemed practical.

The present document follows a modular approach, as depicted in figure 4, that provides for the existence of a *simservs* XML document that contains the data associated to one or more supplementary services. The *simservs* XML document is composed of a common part, defined by the present document, and a number of XML fragments each corresponding to one or more supplementary services.

NOTE 2: 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 of the present document. 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 one or more supplementary services. The XML schema of each of the supplementary services is specified in its own specification. A template for this XML schema is provided in clause 6.4 of the present document.

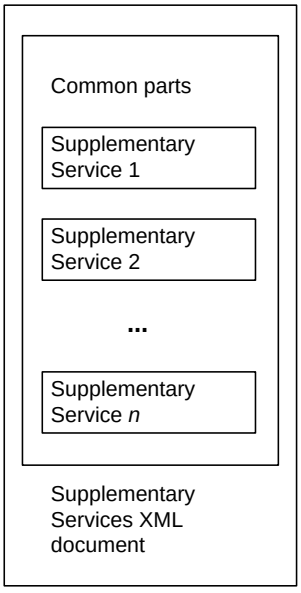

Figure 4: Structure of a supplementary services XML document

The *simservs* XML document starts with a <simservs> root XML element that can contain one or more child elements pertaining to supplementary 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. Services may also include capability elements that are read-only. These elements indicate which capabilities the network has provisioned for a user.

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 supplementary 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 supplementary services XCAP application usage is:

`simservs.ngn.etsi.org`

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 supplementary 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 supplementary 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 supplementary 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 document namespace: XCAP requires application usages to declare the default document namespace specified in IETF RFC 4825 [8]. The default document namespace of the supplementary services XCAP application usage is:

`http://uri.etsi.org/ngn/params/xml/simservs/xcap`

MIME type: The MIME type of supplementary services XML documents is:

`application/vnd.etsi.simservs+xml`

Validation constraints: The present document does not specify any additional constraint beyond those defined by XCAP RFC 4825 [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: Supplementary services XML documents are stored under the user's Home Directory (which is located under the "users" sub-tree). The filename in the document selector is:

`simservs.xml`

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 supplementary services.

Authorization policies: The following authorization policy applies to the owner of *simservs* XML document:

a) authorised to retrieve any part of the document;

b) unauthorised to create:

   1) new child element(s) to the <simservs> root element; and

   2) new attribute(s) for a child element of the the <simservs> root element;

c) unauthorised to remove:

   1) existing child element(s) from the <simservs> root element; and

2) existing attribute(s) from a child element of the <simservs> root element;

d) unauthorised to replace or remove:

1) read-only child element(s) of the <simservs> root element, their attributes and their content;

e) unauthorised to replace:

1) descendant element(s) of the <simservs> root element that are not allowed to be modified by the service capability fragments as described in clause 5.2.3.4; and

2) attribute(s) within descendant element(s) of the the <simservs> root element that are not allowed to be modified by the service capability fragments as described in clause 5.2.3.4; and

f) authorized to replace element(s) and attribute(s) other than those specified in bullet d).

Users other than the owner of the *simservs* XML document are unauthorised to perform any operation on the document.

Unauthorized manipulation attempts on the *simservs* XML document are rejected with an HTTP 409 (Conflict) response as defined in IETF RFC 4825 [8].

NOTE 1: It is allowed to replace the *simservs* XML document or its <simservs> root element containing read-only child elements provided that the read-only child elements, including their content, are preserved.

NOTE 2: Any child elements of the <simservs> root element of the *simservs* XML document unknown to the XCAP client can be potentially read-only.

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 a supplementary services document -->

    <xs:element name="simservs">
<xs:annotation>
<xs:documentation>XML Schema for data manipulation of Supplementary
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>
<xs:complexType name="provisioned-type">
<xs:attribute name="provisioned" type="xs:boolean"
use="optional" default="true" />
<xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
```

```
<xs:complexType name="supported-media-type">
<xs:choice>
<xs:element name="all-media" type="ss:empty-element-type"/>
<xs:element name="no-media" type="ss:empty-element-type"/>
<xs:sequence maxOccurs="unbounded">
<xs:element name="media" type="ss:media-type"/>
</xs:sequence>
<xs:any namespace="##other" processContents="lax"/>
</xs:choice>
</xs:complexType>

<xs:complexType name="provisioned-target-type">
<xs:choice>
<xs:element name="any-target-type" type="ss:empty-element-type"/>
<xs:element name="telephony-type" type="ss:empty-element-type"/>
<xs:any namespace="##other" processContents="lax"/>
</xs:choice>
</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"/>
    <xs:element name="international" type="ss:empty-element-type"/>
    <xs:element name="international-exHC" type="ss:empty-element-type"/>
    <xs:element name="request-name" type="ss:request-name-type"/>

    <!-- service specific IETF xcap-error elements-->
    <xs:element name="password-required" type="ss:empty-element-type"/>
    <xs:element name="incorrect-password" type="ss:empty-element-type"/>
    <xs:element name="incorrect-xui-format" 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:simpleType name="request-name-type" final="list restriction">
<xs:restriction base="xs:string">
<xs:pattern value="([A-Z])*"/>
</xs:restriction>
</xs:simpleType>



</xs:schema>
```

6.4 Template for a supplementary service XML schema

Supplementary 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
Supplementary 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>
```

6.5 XML schema for password change

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ss="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:annotation>
<xs:documentation xml:lang="en">This schema defines elements for changing a password.
</xs:documentation>
</xs:annotation>
<xs:include schemaLocation="XCAP.xsd"/>
<xs:element name=" password-change" substitutionGroup="ss:absService">
<xs:complexType>
<xs:complexContent>
<xs:extension base="ss:simservType">
<xs:sequence>
<xs:element name="new-password" type="ss:password-type" minOccurs="0"/>
<xs:element name="anyExt" type="ss:anyExtType"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
<xs:simpleType name="password-type">
<xs:restriction base="xs:string">
<xs:pattern value="\d{4}"/>
</xs:restriction>
</xs:simpleType>
<xs:complexType name="anyExtType">
<xs:sequence>
<xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

Annex A (informative):
Void

Annex B (normative): Connectivity Aspects when using XCAP

B.1 Scope

The present annex defines aspects for the connection between UE and the network to be used for XCAP.

B.2 Procedures at the UE

The XCAP connection parameters policy consists of zero or more XCAP connection parameters policy parts.

The XCAP connection parameters policy part consists of an access identifier and an XCAP connection parameters reference. The XCAP connection parameters reference refer to an instance of the <X> interior node specified in OMA-TS-XDM_Core-V1_1-20080627-A [14].

The UE may support the XCAP connection parameters policy.

If the UE supports the XCAP connection parameters policy:

1) if the UE intends to send an XCAP request using an access identified by an access identifier of a XCAP connection parameters policy part, the UE shall send the XCAP request according to the XCAP connection parameters referenced by the XCAP connection parameters reference of the XCAP connection parameters policy part; and

2) the UE may support being configured with the XCAP connection parameters policy using one or more of the following methods:

   a) the $EF_{XCAPConfigData}$ file described in 3GPP TS 31.102 [15B];

   b) the $EF_{XCAPConfigData}$ file described in 3GPP TS 31.103 [15A]; and

   c) in the XCAP_conn_params_policy node of 3GPP TS 24.424 [22]

If the UE is configured with both XCAP_conn_params_policy node of 3GPP TS 24.424 [22] and the $EF_{XCAPConfigData}$ file described in 3GPP TS 31.102 [15B] or 3GPP TS 31.103 [15A], then the $EF_{XCAPConfigData}$ file shall take precedence.

NOTE: Precedence for files configured on both the USIM and ISIM is defined in 3GPP TS 31.102 [15B].

If the UE does not support the XCAP connection parameters policy, in order to manipulate XCAP resources stored on the XCAP server, a UE can be configured with parameters describing a connection to be used for XCAP. Connection parameters can be configured as specified in appendix C in OMA-TS-XDM_Core-V1_1-20080627-A [14].

Annex C (normative): IP-Connectivity Access Network specific concepts when using EPS to access IM CN subsystem

C.1 Scope

The present annex defines IP-CAN specific requirements for the supplementary services configuration using XCAP/Ut in the IMS, where the IP-CAN is Evolved Packet System (EPS).

C.2 Application usage of XCAP

C.2.1 Procedures at the UE

C.2.1.1 3GPP PS data off

C.2.1.1.1 General

The UE may support the 3GPP PS data off.

If the UE supports the 3GPP PS data off:

a) the UE can be configured with an indication whether the SS configuration via XCAP is a 3GPP PS data off exempt service; and

b) the UE may support being configured with the indication whether the SS configuration via XCAP is a 3GPP PS data off exempt service using one or more of the following methods:

1) the $EF_{3GPPPSDATAOFF}$ described in 3GPP TS 31.102 [15B]; and

2) the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22].

If the UE is configured with both the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22] and the $EF_{3GPPPSDATAOFF}$ described in 3GPP TS 31.102 [15B], then the $EF_{3GPPPSDATAOFF}$ shall take precedence.

C.2.1.1.2 Enforcement

If the 3GPP PS data off status is "active" and the UE is not configured with an indication that SS configuration via XCAP is a 3GPP PS data off exempt service the UE shall not invoke the procedures in clause 5.2.1 and clause 5.3.1 from a UE's contact address containing an IP address associated with an EPS IP-CAN bearer.

Annex D (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IM CN subsystem

D.1 Scope

The present annex defines IP-CAN specific requirements for the supplementary services configuration using XCAP/Ut in the IMS, where the IP-CAN is General Packet Radio Service (GPRS).

D.2 Application usage of XCAP

D.2.1 Procedures at the UE

D.2.1.1 3GPP PS data off

D.2.1.1.1 General

The UE may support the 3GPP PS data off.

If the UE supports the 3GPP PS data off:

a) the UE can be configured with an indication whether the SS configuration via XCAP is a 3GPP PS data off exempt service; and

b) the UE may support being configured with the indication whether the SS configuration via XCAP is a 3GPP PS data off exempt service using one or more of the following methods:

1) the $EF_{3GPPPSDATAOFF}$ described in 3GPP TS 31.102 [15B]; and

2) the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22].

If the UE is configured with both the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22] and the $EF_{3GPPPSDATAOFF}$ described in 3GPP TS 31.102 [15B], then the $EF_{3GPPPSDATAOFF}$ shall take precedence.

D.2.1.1.2 Enforcement

If the 3GPP PS data off status is "active" and the UE is not configured with an indication that SS configuration via XCAP is a 3GPP PS data off exempt service the UE shall not invoke the procedures in clause 5.2.1 and clause 5.3.1 from a UE's contact address containing an IP address associated with a GPRS IP-CAN bearer.

Annex E (normative): IP-Connectivity Access Network specific concepts when using 5GS to access an IM CN subsystem

E.1 Scope

The present annex defines IP-CAN specific requirements for the supplementary services configuration using XCAP/Ut in the IMS, where the IP-CAN is 5GS.

E.2 Application usage of XCAP

E.2.1 Procedures at the UE

E.2.1.1 3GPP PS data off

E.2.1.1.1 General

The UE may support the 3GPP PS data off feature.

If the UE supports the 3GPP PS data off feature, then:

a) the UE can be configured with an indication of whether the SS configuration via XCAP is a 3GPP PS data off exempt service; and

b) the UE may support being configured with the indication of whether the SS configuration via XCAP is a 3GPP PS data off exempt service using one or more of the following methods:

1) the $EF_{3GPPPSDATAOFF}$ described in 3GPP TS 31.102 [15B]; and

2) the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22].

If the UE is configured with both the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22] and the $EF_{3GPPPSDATAOFF}$ described in 3GPP TS 31.102 [15B], then the $EF_{3GPPPSDATAOFF}$ shall take precedence.

In case of SNPN, if the UE supports the 3GPP PS data off:

a) the UE can be configured with:

1) up to two indications of whether the SS configuration via XCAP is a 3GPP PS data off exempt service for each subscribed SNPN whose entry exists in the "list of subscriber data", one indication is valid for the UE camping in the subscribed SNPN, and the other indication is valid for any non-subscribed SNPN the UE is camping in using the subscribed SNPN's credentials; and

2) an indication of whether the SS configuration via XCAP is a 3GPP PS data off exempt servicefor PLMN subscription, valid for any non-subscribed SNPN the UE is camping in using the PLMN subscription; and

b) for a subscribed SNPN whose entry exists in the "list of subscriber data", the UE may support being configured with the indication of whether the SS configuration via XCAP is a 3GPP PS data off exempt service using one or more of the following methods:

1) the SS_XCAP_config_exempt node of 3GPP TS 24.424 [22], if the UE is in the subscribed SNPN.

2) the SS_XCAP_config_exempt_non_subscribed_SNPN node of 3GPP TS 24.424 [22], if the UE is in the non-subscribed SNPN.

For PLMN subscription, the UE may support being configured with the indication of whether the SS configuration via XCAP is a 3GPP PS data off exempt service using the following method:

1) the SS_XCAP_config_exempt_non_subscribed_SNPN node of 3GPP TS 24.424 [22], if the UE is in the non-subscribed SNPN.

When the UE is only configured with the indication valid for the UE camping in the subscribed SNPN, the UE shall use this indication also when the UE is in the non-subscribed SNPN.

E.2.1.1.2 Enforcement

If the 3GPP PS data off status is "active" and the UE is not configured with an indication that SS configuration via XCAP is a 3GPP PS data off exempt service, then the UE shall not invoke the procedures in clause 5.2.1 and clause 5.3.1 from a UE's contact address containing an IP address associated with a 5GS QoS flow using NG-RAN.

Annex F (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
2008-01					Technically identical copy as **3GPP TS 24.623** as basis for further development.		1.4.2
2008-02					CT1#51 agreed to sent spec for information to plenary		1.4.3
2008-04					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TS C1-081006	1.4.3	1.5.0
2008-05					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TS C1-081616 C1-081894 C1-081916	1.5.0	1.6.0
2008-05					Editorial changes done by MCC	1.6.0	1.6.1
2008-06	CT#40	CP-080333			CP-080333 was approved by CT#40 and version 8.0.0 is created by MCC for publishing	1.6.1	8.0.0
2008-06					Version 8.0.1 created to inlcude attachments (.xml adn .xsd files)	8.0.0	8.0.1
2008-09	CT#41	CP-080533	0001	1	Tidyup .xml and .xsd files	8.0.1	8.1.0
2008-09	CT#41	CP-080533	0002		Applicability statement in scope	8.0.1	8.1.0
2009-06	CT#44	CP-090432	0005	2	Addition of international-communications condition	8.1.0	9.0.0
2009-09	CT#45	CP-090687	0007	1	Validation against capabilities	9.0.0	9.1.0
2009-09	CT#45	CP-090687	0008	1	Supported-media-type	9.0.0	9.1.0
2009-09	CT#45	CP-090687	0010		Supported target type	9.0.0	9.1.0
2009-09	CT#45				Editorial cleanup by MCC	9.1.0	9.1.1
2009-12	CT#46	CP-091040	0012	1	Change of ua-profile package to xcap-diff package	9.1.1	9.2.0
2009-12	CT#46	CP-090928	0013	2	Authorization policy update	9.1.1	9.2.0
2009-12	CT#46	CP-090928	0014	1	Service capabilities fragment	9.1.1	9.2.0
2009-12	CT#46	CP-090928	0015		Correct .xml schema	9.1.1	9.2.0
2011-03	CT#51				Upgrade to Rel-10	9.2.0	10.0.0
2011-09	CT#53	CP-110657	0021		IETF reference updates	10.0.0	10.1.0
2011-12	CT#54	CP-110857	0024	1	Incorrect MIME definition	10.1.0	10.2.0
2012-03	CT#55	CP-120097	0027	1	Connection to be used for XCAP	10.2.0	10.3.0
2012-03	CT#55	CP-120097	0030	1	Configuration of XCAP root URI	10.2.0	10.3.0
2012-09	CT#57				Upgrade to Rel-11	10.3.0	11.0.0
2012-12	CT#58	CP-120816	0032	2	Reference to ODB specification for ut based service configuration	11.0.0	11.1.0
2012-12	CT#58	CP-120817	0031	1	Alignment of authentication mechanisms with SA3 specifications	11.1.0	12.0.0
2013-06	CT#60	CP-130265	0033	1	Addition of "request-name" XML element	12.0.0	12.1.0
2013-09	CT#61	CP-130511	0034	2	Supplementary Services Configuration fallback procedure	12.1.0	12.2.0
2013-12	CT#62	CP-130770	0036	2	Update to RFC 6665	12.2.0	12.3.0
2013-12	CT#62	CP-130763	0038	1	Breaking the "Manipulating supplementary services" clause into two clauses	12.2.0	12.3.0
2013-12	CT#62	CP-130763	0040		XCAP disabling and retry CS domain.	12.2.0	12.3.0
2014-06	CT#64	CP-140330	0046	1	Default document namespace clarification	12.3.0	12.4.0
2014-06	CT#64	CP-140330	0051	2	Conditional operation for XCAP	12.3.0	12.4.0
2014-09	CT#65	CP-140665	0045	10	Handling of Supplementary Service provisioning errors	12.4.0	12.5.0
2014-12	CT#66	CP-140837	0053	1	simservs filename clarification	12.5.0	12.6.0
2014-12	CT#66	CP-140837	0054	2	Ut interface retry when no response received	12.5.0	12.6.0
2015-06	CT#68	CP-150328	0056		Aligning TLS profiles used by CT1 specifications with SA3 agreed TLS profile	12.6.0	13.0.0
2015-12	CT#70	CP-150687	0059		Reference correction	13.0.0	13.1.0

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2016-12	CT#74	CP-160742	0064	1	B	Policy on access type for XCAP	14.0.0
2016-12	CT#74	CP-160742	0065		B	Enforcement of access specific configuration for PDN connection for XCAP	14.0.0
2017-03	CT#75	CP-170131	0066	1	B	Password handling	14.1.0
2017-06	CT#76	CP-171077	0067	3	B	Removal of editors notes for parameters configured on UICC	14.2.0
2017-06	CT#76	CP-171085	0068	1	B	3GPP PS Data Off and Ut/XCAP services configuration	14.2.0
2017-06	CT#76	CP-171086	0069	1	B	Password check procedure	14.2.0
2018-06	SA-80	-	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2018-12	CT#82	CP-183077	0070		F	Password change error handling	16.0.0
2018-12	CT#82	CP-183077	0071	1	B	Authentication mechanisms for Ut reference point	16.0.0
2019-06	CT#84	CP-191117	0074	1	A	Correct references	16.1.0
2019-06	CT#84	CP-191126	0076	1	A	Correct using XCAP and PS Data Off via 5GS	16.1.0
2019-06	CT#84	CP-191126	0078	1	A	Correct policy for XCAP when access type involves 5G	16.1.0
2020-12	CT#90e	CP-203215	0079	1	B	Adding handling of the UE configuration parameter "Access_Point_Name_Parameter_Reading_Rule" for the UE to read the XCAP APN name parameter from correct input source.	17.0.0
2021-12	CT#94e	CP-213031	0080		B	Update of HTTP Digest Access Authentication and reference update for HTTP/1.1 protocol	17.1.0
2022-03	CT#94e	CP-220238	0081	1	B	3GPP PS data off and UE in SNPN	17.2.0