ETSI TS 124 623 V14.3.0 (2019-07)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Extensible Markup Language (XML)
Configuration Access Protocol (XCAP)
over the Ut interface for Manipulating Supplementary Services
(3GPP TS 24.623 version 14.3.0 Release 14)

Reference
RTS/TSGC-0124623ve30

Keywords
GSM,LTE,UMTS

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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 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 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] 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] 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] Void.

[28] Void.

[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".

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

3.2 Abbreviations

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

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
ODB	Operator Determined Barring
PS	Packet Switched
PSTN	Public Switched Telephone Network
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.

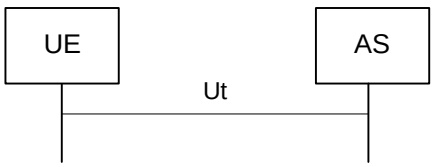

Figure 1: Ut interface

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.

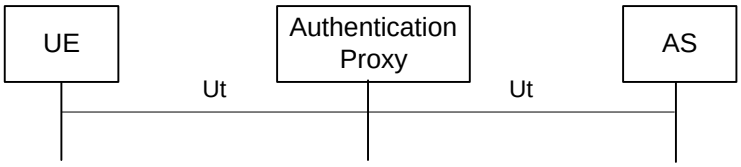

Figure 2: Authentication proxy in the Ut interface path

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 2616 [1]). 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 supplementary 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.

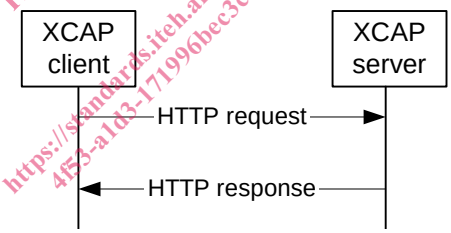

Figure 3: XCAP architecture

According to XCAP (see IETF RFC 4825 [8]), each application that makes use of XCAP defines its own XCAP application usage. The present document defines an supplementary services XCAP application usage in clause 6. This application usage defines the XML schema W3C 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 subclause 5.3.1 accessing the XCAP application usage as described in subclause 6.2.

For systems where Generic Authentication Architecture [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 Architecture [6] is not used, the UE shall support IETF RFC 2617 [3] according to ETSI TS 183 038 [12] 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 according to IETF RFC 2246 [4] is specified.

For systems where Generic Authentication Architecture [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.

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 type used for the XCAP enables HPLMN control of access used for XCAP messages.

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

a) any access type;

b) 3GPP accesses only;

c) EPC 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 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 accesses only":

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];