

IMS Device Configuration and Supporting Services
Version 1.0
02 February 2015

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Confidential - Full, Rapporteur, and Associate Members

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2015 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Scope 4
1.3 Abbreviations 4
1.4 References 5
1.5 Conventions 6
2 Configuration 6
2.1 Mechanism Extensions 6
2.1.1 HTTP GET method Parameters 6
2.1.2 Configuration of additional devices using the same identity 6
2.1.3 (Re)configuration triggers 9
2.2 Configuration Parameters 10
2.2.1 Parameter introduction 10
2.2.2 Parameter Definition 12
3 IMS Service Supporting Enablers 24
3.1 End User Confirmation Requests 24
3.1.1 End User Confirmation Request 25
3.1.2 End User Confirmation Response 28
3.1.3 End User Notification Request 29
3.1.4 End User System Request 30
3.1.5 Example Use Case 1: Accepting terms and conditions 32
3.1.6 Example Use Case 2: Notification 33
Annex A Document Management 34
A.1 Document History 34
A.2 Other Information 34

1 Introduction

1.1 Overview

This document describes the configuration of Internet Protocol Multimedia Subsystem (IMS) based devices using the mechanism described in [PRD-RCC.14]. It also introduces some services to support this configuration that may be useful for other aspects of device management.

1.2 Scope

This document covers both the device and network aspects of the configuration. It only describes the generic IMS parts of the configuration. Service specific aspects need to be described in documents relating to that service (for example Permanent Reference Document (PRD) RCC.07 for Rich Communication Services [RCS] based services). It only covers the User-Network Interface (UNI) aspects and does not deal with the internal network and device aspects of the provisioning.

1.3 Abbreviations

Term	Description
AKA	Authentication and Key Agreement
EUCR	End User Confirmation Request
GRUU	Globally Routable User agent Uniform resource identifier
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure
IMEI	International Mobile Station Equipment Identity
IMS	Internet Protocol Multimedia Subsystem
ISIM	Internet Protocol Multimedia Services Subscriber Identity Module
MO	Management Object
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MTU	Maximum Transmission Unit
OTP	One Time Password
PCO	Protocol Configuration Options
PDP	Packet Data Protocol
PRD	Permanent Reference Document
RCS	Rich Communication Services
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
TLS	Transport Layer Security
UAS	User Agent Server
UE	User Equipment
UI	User Interface

Term	Description
UNI	User-Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
UUID	Universally Unique IDentifier
UX	User Experience
XML	Extensible Markup Language
XSD	Extensible Markup Language Schema Definition

1.4 References

Ref	Doc Number	Title
[1]	[3GPP TS 24.167]	3GPP TS 24.167 Release 12, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO) http://www.3gpp.org
[2]	[3GPP TS 24.229]	3GPP TS 24.229 Release 10, 3rd Generation Partnership Project; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) http://www.3gpp.org
[3]	[PRD-IR.88]	GSMA PRD IR.88 - "LTE Roaming Guidelines" 9.0 23 January 2013 http://www.gsma.com/
[4]	[PRD-RCC.14]	GSMA PRD RCC.14 HTTP-based Service Provider Device Configuration, Version 1.0, 01 November 2014 http://www.gsma.com
[5]	[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[6]	[RFC3261]	SIP (Session Initiation Protocol) IETF RFC http://tools.ietf.org/html/rfc3261
[7]	[RFC3428]	Session Initiation Protocol (SIP) Extension for Instant Messaging IETF RFC http://tools.ietf.org/html/rfc3428
[8]	[RFC4122]	The Universally Unique IDentifier (UUID) URN Namespace IETF RFC http://tools.ietf.org/html/rfc4122
[9]	[RFC4483]	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages IETF RFC http://tools.ietf.org/html/rfc4483
[10]	[OMA CP Cont]	Provisioning Content, Approved Version 1.1 – 28 Jul 2009 OMA-WAP-TS-ProvCont-V1_1-20090728-A http://www.openmobilealliance.com

1.5 Conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in [RFC2119].

2 Configuration

2.1 Mechanism Extensions

2.1.1 HTTP GET method Parameters

No additional Hyper-Text Transfer Protocol (HTTP) GET method parameters are defined for generic IMS service configuration. Services based on IMS may define some service specific parameters in the documents describing them though.

2.1.2 Configuration of additional devices using the same identity

In addition to the Short Message Service (SMS) based mechanism defined in section 2.4 of [PRD-RCC.14] for authenticating a configuration request from a secondary device intending to use a primary device’s identity, a Service Provider configuring devices in an IMS environment can rely on End User Confirmation Requests (EUCR) as described in the following sections.

2.1.2.1 Using End User Confirmation Request alternative

As an alternative to the use of SMS to confirm the identity of the user the Service Provider could choose to use the EUCR, see section 3.1.

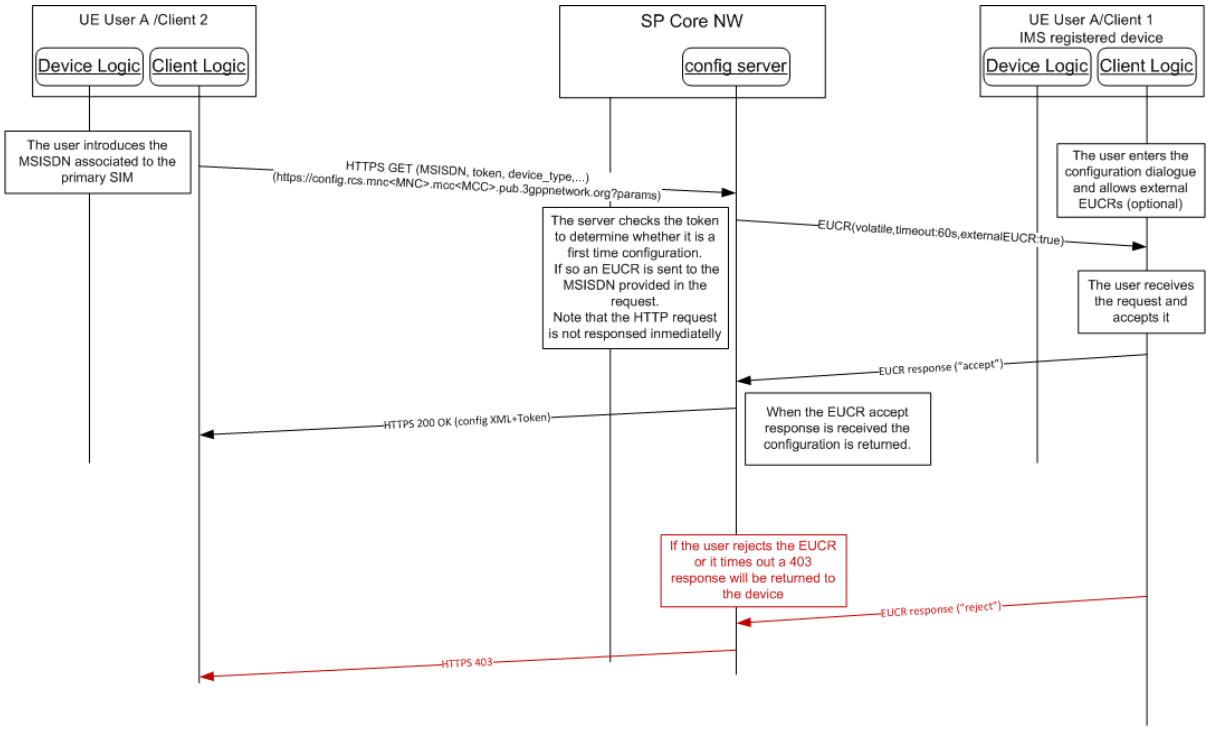

Figure 1: Alternative HTTP configuration for additional devices: First time configuration using EUCR

The process is very similar to the one described for SMS:

1. As an option, the device implementation/client will offer the possibility to the user to perform manual provisioning as in the SMS mechanism.
2. The user is prompted for the Mobile Subscriber Integrated Services Digital Network Number (MSISDN) or Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) of the primary device and the Service Provider associated with the primary Subscriber Identity Module (SIM) as in the SMS mechanism.
3. The device performs the HTTP configuration using the same GET parameters as in the SMS mechanism.
4. At this point the HTTP configuration server is able to identify whether this is a first time request:

    a) If the token value is empty, then the request is identified as a first time configuration.
    b) If the token has a value, it is checked against the HTTP server database. If successful, from this point the procedure is identical to the one described in section 2.2.2 and 2.2.3 of [PRD-RCC.14].

NOTE1: There is no further authentication of the additional device or the user that starts the configuration process. Appropriate security measures to prevent malicious usage should be implemented on the configuration server.

5. An EUCR flow starts for a first-time registration

    a) In case of malicious usage by another person via the Internet, the EUCR method may block the UI (by unwanted EUCR popups) on the device registered for IMS. Therefore, the following optional user dialogue is recommended.
    If implemented on the IMS-registered mobile device, the user enters a UI dialogue to start the configuration of additional IMS devices. This dialogue sets the mobile device into a mode that allows EUCRs initiated from an external source. This external source is in this case the user's additional device to configure.

NOTE2: If activation and de-activation of that mode is not implemented on the mobile device, all EUCRs are allowed and shown to the user and also the EUCRs related to the configuration of the device.

    b) A volatile EUCR is sent to the MSISDN or SIP URI provided in the HTTP request. The EUCR includes the attribute externalEUCR set to true.

NOTE3: The HTTP request is not answered immediately.

6. The End User Confirmation Request is received by the device and will be handled as follows:

    a) If the device does allow external End User Confirmation Requests, it will be shown in the User Interface (UI). The user may accept it, in which case a 200 OK response is sent as described in section 2.2.2 of [PRD-RCC.14]. The response will also contain a token to be used in subsequent and future requests:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
        <characteristic type="TOKEN">
                <parm name=”token” value=”X”/>
                <parm name=”validity” value=”Y”/>
        </characteristic>
        <characteristic type="VERS">
                <parm name=”version” value=”Z”/>
                <parm name=”validity” value=”W”/>
        </characteristic>
        <characteristic type="APPLICATION">
                ….
        </characteristic>
</wap-provisioningdoc>
```

Table 1: HTTPS configuration of additional devices using EUCR: First time response to the HTTPS request.

b) If the device does allow external EUCRs but the user rejects the EUCR or the timer expires, the server will reply with an HTTP 403 response and the process is concluded (the device is not configured as an end result).
c) If the device does not allow external EUCRs, it shall ignore the request or reject it. As in b) the server will reply with an HTTP 403 response and the additional device is not configured.

NOTE4: there is no further authentication of the additional device or the user that starts the configuration process (i.e. the initial Hyper-Text Transfer Protocol Secure [HTTPS] request). If misused via the Internet, a EUCR may block an IMS user’s UI (by unwanted popups) on the device associated with the primary SIM. Therefore, appropriate security measures to prevent such malicious usage should be implemented.

2.1.2.2 Using EUCR with PIN alternative

The Service Provider can add an extra layer of security by using the pin request feature in the EUCR.

Using this alternative, the flow is similar as the SMS process described in section 2.4 or [PRD-RCC.14] except that instead of sending the One-Time Password (OTP) in the SMS, the OTP is chosen by the user and typed into both devices:

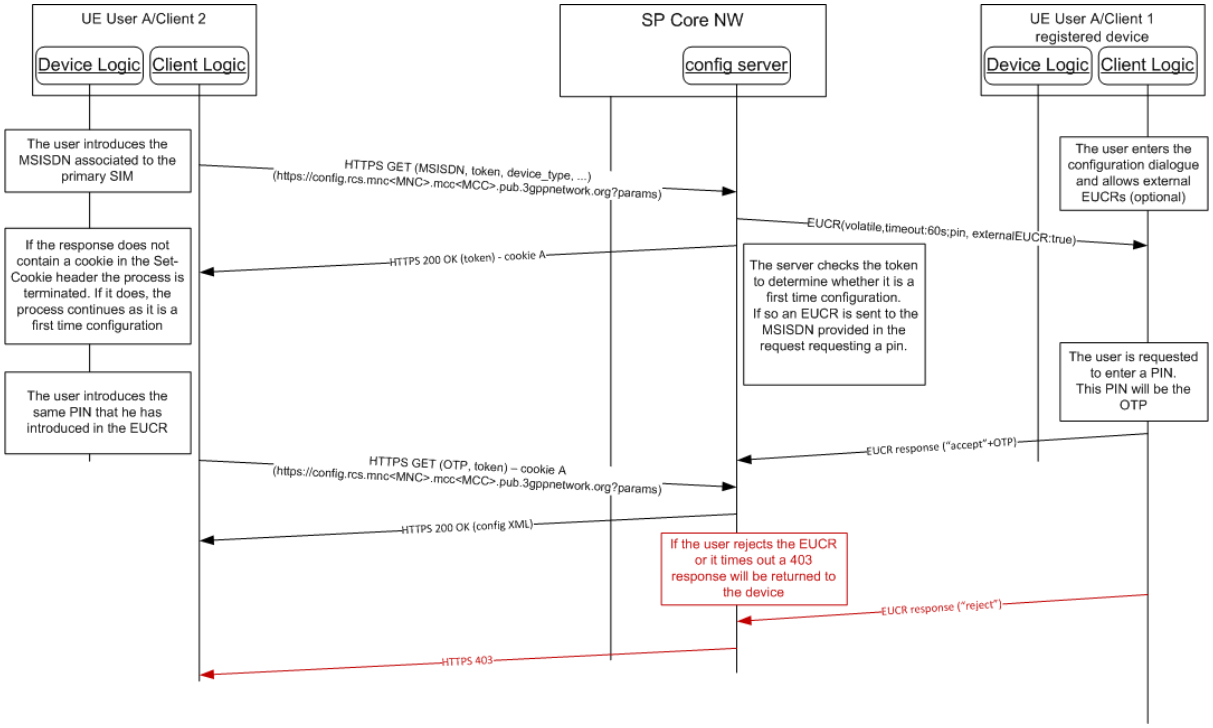

Figure 2: Alternative configuration for additional devices: First time configuration EUCR with PIN

NOTE: There is no further authentication of the additional device or the user that starts the configuration process (i.e. the initial HTTPS request). If misused via Internet, EUCR may block an IMS user's UI (by unwanted popups) on the device associated with the primary SIM. Therefore, appropriate security measures to prevent such malicious usage should be implemented.

2.1.3 (Re)configuration triggers

In addition to the SMS based triggers defined in section 3 or [PRD-RCC.14] for devices supporting IMS also IMS based options shall be available to initiate the configuration from the network side.

2.1.3.1 Reconfiguration via EUCR request

A reconfiguration can be triggered by the network by sending a EUCR system request with type *urn:gsma:rcs:http-configuration:reconfigure*[1] as specified in section 3.1.

When the client receives such request, it shall take the following actions:

1. Reply to the request with a 200 OK response
2. Perform a HTTP configuration setting the version and validity parameters to 0 (i.e. for example in the case of a first-time configuration).
3. If active, deactivate service(s) for which the settings have changed as specified for those services and apply configuration (e.g. de-register from the IMS network as specified in section 2.2.2 for changes to the IMS settings).
4. Register back to the IMS network with the received settings.

[1] Includes "rcs" for historic reasons

2.2 Configuration Parameters

2.2.1 Parameter introduction

2.2.1.1 IMS Core / SIP related configuration

Configuration for access over IMS APN

2.2.1.1.1

For access over the IMS Access Point Name (APN) defined in [PRD-IR.88], the own SIP or tel URI configured through the management object referred to in section 2.2.1.1.2 will not be used, but rather be received in the 200 OK response to the SIP REGISTER request and the SIP Proxy is provided in Protocol Configuration Options (PCO) information received during Packet Data Protocol (PDP) context activation. If the device only supports IMS access over that APN, those values shall not be configured.

Endorsement of 3GPP IMS Management Object (MO)

2.2.1.1.2

Basic IMS/SIP client parameters are defined in 3GPP TS “IMS 3GPP IMS Management Object (MO)” [3GPP TS 24.167]. They are populated by the Service Provider according to the deployment conditions of the IMS core network providing access to the Service Provider’s IMS based services.

Also, it should be noted that:

- Both a SIP and a tel URI may be configured for a user with the following clarifications:
    - The configured values should not be used in the non-REGISTER transactions; instead the client uses one of the SIP or tel URIs provided in the P-Associated-URI header field returned in the 200 OK to the SIP REGISTER request as described in [3GPP TS 24.229]
    - The user’s own tel URI and/or SIP URI identities are configured through the Public_user_identity parameters defined in [3GPP TS 24.167][2].
    - The public identity used for IMS registration is built according to the procedure defined in [3GPP TS 24.229].
    - When the device has either Internet Protocol Multimedia Services Subscriber Identity Module (ISIM) or Universal Subscriber Identity Module (USIM) present and the IMS client has access to the ISIM or USIM, it does not rely on the SIP URI and tel URI configuration parameters.
    - If the device has neither ISIM nor USIM present or is not able to access to it, a SIP URI must be configured. This URI is used for REGISTER transactions.
    - Configuration of the tel URI is optional

[2] The private identity (*Private_user_identity*), public identity (*Public_user_identity_List/<X>/Public_user_identity*) and domain (*Home_network_domain_name*) objects mentioned in [3GPP TS 24.167] are defined as read-only and these parameters should be obtained by the User Equipment (UE) using the procedures described [3GPP TS 24.229]. This specification makes an exception to that definition and considers them writable during the autoconfiguration process.

- The SIP proxy is configured through the parameters hosted by the LBO_P-CSCF_Address sub-tree defined in [3GPP TS 24.167].

Specific Provisioning parameters

This specification includes the following additional IMS Core/SIP related configuration parameters:

2.2.1.1.3

Configuration parameter	Description	GSMA IMS usage
IMS Mode Authentication Type	Specifies the type of authentication support for SIP. NOTE: In “IETF” Digest authentication is assumed. Accepted values are: • Early IMS • IMS Authentication and Key Agreement (AKA) • SIP DIGEST (without Transport Layer Security [TLS])	Mandatory Parameter, NOTE: a client with ISIM/USIM access always uses IMS AKA when using cellular PS access and shall ignore this parameter when using that access
Realm	Realm to use for authentication (Digest mode only)	Optional parameter It is Mandatory if a IMS Mode Authentication Type is set to Digest.
Realm User Name	Realm username to use for authentication (Digest mode only)	Optional parameter It is Mandatory if a IMS Mode Authentication Type is set to Digest.
Realm User Password	Realm user password to use for authentication (Digest mode only)	Optional parameter It is Mandatory if a IMS Mode Authentication Type is set to Digest.
Transport Protocols	Control the transport protocols used for signalling and media on the different access networks supported	Mandatory

Table 2: Additional IMS Core/SIP related configuration parameters

2.2.1.2 End User Confirmation parameters

This specification includes the following specific configuration parameters targeting the EUCR configuration (see section 3.1) which only need to be supported by devices supporting EUCR:

Configuration parameter	Description	GSMA IMS usage
END USER CONF REQ ID	This is the URI that is used to identify the sender of the EUCRs.	Optional Parameter

Table 3: End user confirmation configuration parameters

2.2.1.3 Multidevice configuration parameters

This specification includes the following specific configuration parameters targeting the multidevice configuration:

Configuration parameter	Description	GSMA IMS usage
uuid_Value	This is the Universally Unique IDentifier (UUID) value used for sip.instance in the SIP REGISTER request. It is included for the case where an International Mobile Station Equipment Identity (IMEI) is not available to the IMS client or where the might be used by another IMS client on the device already. NOTE: if not provided, the UUID shall be generated as per [RFC4122] section 4.2	Optional Parameter

Table 4: Multi-device configuration parameters

2.2.2 Parameter Definition

2.2.2.1 IMS Sub tree mapping to HTTP

The parameters defined in [3GPP TS 24.167] are mapped as follows:

Configuration parameter in [3GPP TS 24.167]	HTTP XML Characteristic type/Parm name	HTTP XML element type
Node: /<X>	APPLICATION	characteristic
/<X>/AppID	AppID	parm
/<X>/Name	Name	parm
/<X>/ConRefs/	ConRefs	characteristic
/<X>/ConRefs/<X>	Refs	characteristic
/<X>/ConRefs/<X>/ConRef	Conref<X> where <X> is a positive integer value determining the ordering	parm
/<X>/PDP_ContextOperPref	PDP_ContextOperPref	parm

/<X>/P-CSCF_Address	P-CSCF_Address	parm
/<X>/Timer_T1	Timer_T1	parm
/<X>/Timer_T2	Timer_T2	parm
/<X>/Timer_T4	Timer_T4	parm
/<X>/Private_user_identity	Private_User_Identity	parm
/<X>/Public_user_identity_List/	Public_User_Identity_List	characteristic
/<X>/Public_user_identity_List/<X>	Public_user_identities	characteristic
/<X>/Public_user_identity_List/<X>/Public_user_identity	Public_user_identity<X> where <X> is a positive integer value determining the ordering	parm
/<X>/Home_network_domain_name	Home_network_domain_name	parm
/<X>/Ext/	Ext	characteristic
/<X>/ICSI_List/	ICSI_List	characteristic
/<X>/ICSI_List/<X>	ICSIS	characteristic
/<X>/ICSI_List/<X>/ICSI	ICSI<X> where <X> is a positive integer value determining the ordering	parm
/<X>/ICSI_List/<X>/ICSI_Resource_Allocation_Mode	ICSI_Resource_Allocation_Mode<X> where <X> is a positive integer value determining the ordering	parm
/<X>/LBO_P-CSCF_Address/	LBO_P-CSCF_Address	characteristic
/<X>/LBO_P-CSCF_Address/<X>	LBO_P-CSCF_Addresses	characteristic
/<X>/LBO_P-CSCF_Address/<X>/Address	Address<X> where <X> is a positive integer value determining the ordering	parm
/<X>/LBO_P-CSCF_Address/<X>/AddressType	AddressType<X> where <X> is a positive integer value determining the ordering	parm
/<X>/Resource_Allocation_Mode	Resource_Allocation_Mode	parm
/<X>/Voice_Domain_Preference_E_UTRAN	Voice_Domain_Preference_E_UTRAN	parm
/<X>/SMS_Over_IP_Networks_Indication	SMS_Over_IP_Networks_Indication	parm
/<X>/Keep_Alive_Enabled	Keep_Alive_Enabled	parm
/<X>/Voice_Domain_Preference_UTRAN	Voice_Domain_Preference_UTRAN	parm
/<X>/Mobility_Management_IMS_Voice_Termination	Mobility_Management_IMS_Voice_Termination	parm
/<X>/RegRetryBaseTime	RegRetryBaseTime	parm
/<X>/RegRetryMaxTime	RegRetryMaxTime	parm
/<X>/PhoneContext_List/	PhoneContext_List	characteristic
/<X>/PhoneContext_List/<X>	PhoneContexts	characteristic
/<X>/PhoneContext_List/<X>/PhoneContext	PhoneContext<X> where <X> is a positive integer value determining the ordering	parm

/<X>/PhoneContext_List/<X>/Public_user_identity	Public_User_Identity<X> where <X> is a positive integer value determining the ordering	parm
/<X>/SS_domain_setting	SS_domain_setting	parm
/<X>/PS_domain_IMS_SS_control_preference	PS_domain_IMS_SS_control_preference	parm

Table 5: Mapping of [3GPP TS 24.167] MO to XML elements

NOTE: Given the dependency on [3GPP TS 24.167], **Error! Reference source not found.** shall be updated whenever parameters relevant changes are done to the referred 3GPP specification.

2.2.2.2 IMS sub tree additions

The following additions to the IMS MO sub tree will be included where <*IMS*> corresponds to the <*x*> root node of the IMS MO defined in [3GPP TS 24.167].

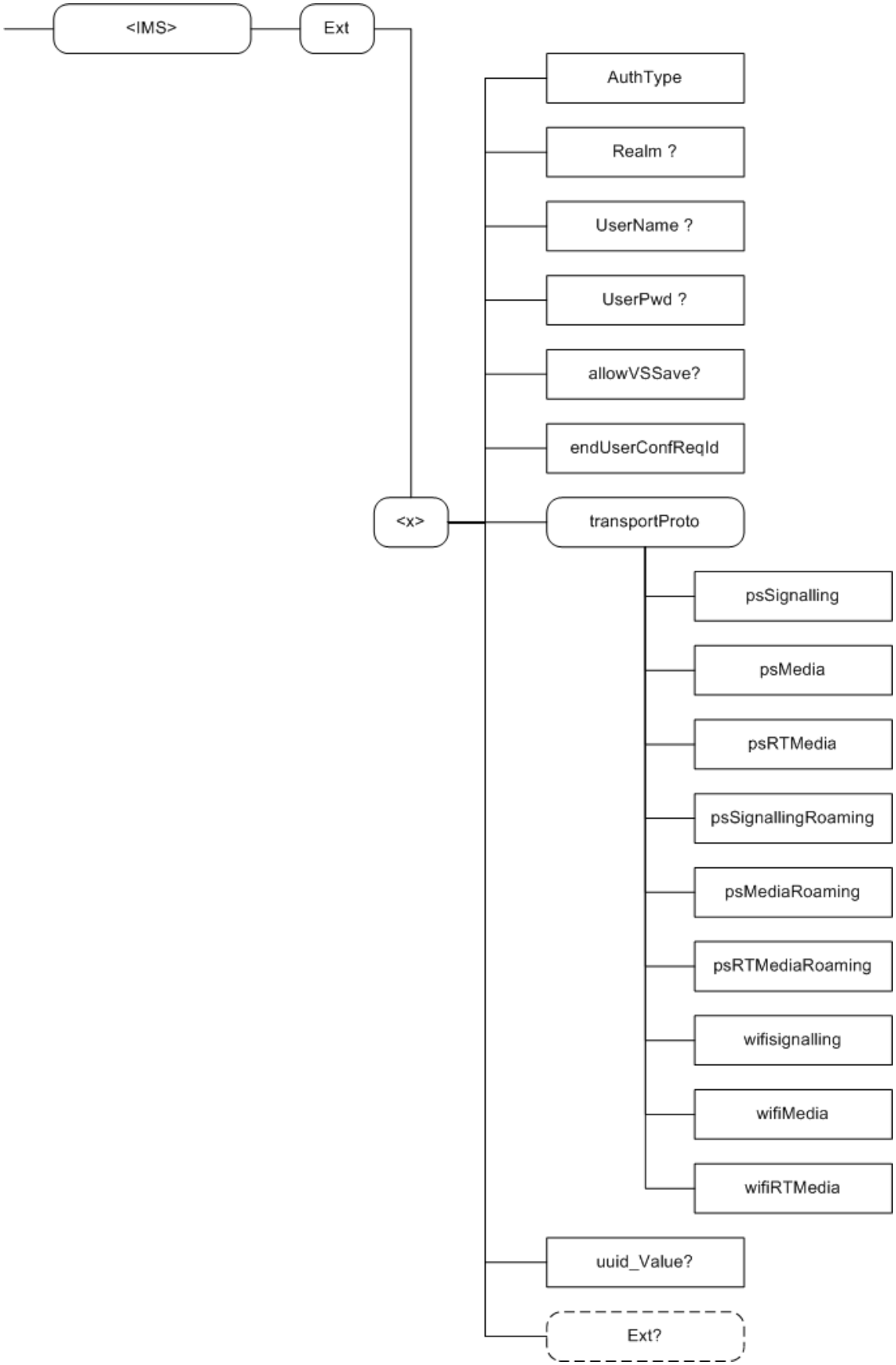

Figure 3: Additions to the IMS MO sub tree

Node: <x>

Under this interior node the parameters related to IMS are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 6: IMS MO sub tree addition IMS node

- Values: N/A
- Associated HTTP Extensible Markup Language (XML) characteristic type: “IMS”

Node: <x>/AuthType

Leaf node that describes the type of IMS authentication for the user

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 7: IMS MO sub tree addition parameters (AuthType)

- Values: ‘EarlyIMS’, ‘AKA’, ‘Digest’
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “AuthType”, given its nature in the HTTP XML document, this parameter is provided as part of the APPAUTH characteristic defined in OMA CP (see [OMA CP Cont]).

Node: <x>/Realm

If the IMS mode for authentication is ‘digest’, this leaf node exists and contains the realm Uniform Resource Locator (URL) affected to the user

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

Table 8: IMS MO sub tree addition parameters (Realm)

- Values: <Realm URL>, example: ‘authenticatorY.operatorX.com’
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “Realm”, given its nature in the HTTP XML document, this parameter is provided as part of the APPAUTH characteristic defined in OMA CP (see [OMA CP Cont]).

Node: <x>/UserName

If the IMS mode for authentication is ‘Digest’, this leaf node exists and contains the realm User name assigned to the user for IMS authorization/registration

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	No Get, No Copy

Table 9: IMS MO sub tree addition parameters (UserName)

- Values: <user name assigned to the user for IMS authentication/registration purpose>, Example: “Alice”
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “UserName”, given its nature in the HTTP XML document, this parameter is provided as part of the APPAUTH characteristic defined in OMA CP (see [OMA CP Cont]).

Node: <x>/UserPwd

If the IMS mode for authentication is ‘Digest’, this leaf node exists and contains the User password assigned to the user for IMS authorization/registration

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	No Get, No Copy

Table 10: IMS MO sub tree addition parameters (UserPwd)

- Values: <password assigned to user for IMS authentication/registration purpose>, Example: ‘secretxyz’
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “UserPwd”, given its nature in the HTTP XML document, this parameter is provided as part of the APPAUTH characteristic defined in OMA CP (see [OMA CP Cont]).

Node: <x>/endUserConfReqId

Leaf node that describes the identity (*P-Asserted-Identity*) used for sending the end user confirmation request.

This node shall be supported by IMS devices supporting EUCR as described in section 3.1.

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get, Replace

Table 11: IMS MO sub tree addition parameters (endUserConfReqId)

- Values: Values: The identity (P-Asserted-Identity) used for sending the end user a confirmation request
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML parameter ID: “endUserConfReqId”

Node: <x>/transportProto

Under this interior node the parameters related to roaming are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 12: Transport Protocol sub tree node

- Values: N/A
- Associated HTTP XML characteristic type: “transportProto”

Node: <x>/transportProto/psSignalling

Leaf node that describes the transport protocol used to carry the signalling when connecting over PS cellular access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 13: IMS MO sub tree addition parameters (psSignalling)

- Values: The possible values are:
    - SIPoUDP
    - SIPoTCP
    - SIPoTLS
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “psSignalling”

Node: <x>/transportProto/psMedia

Leaf node that describes the transport protocol used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over PS cellular access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 14: IMS MO sub tree addition parameters (psMedia)

- Values: The possible values are:
    - MSRP
    - MSRPoTLS
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “psMedia”

Node: <x>/transportProto/psRTMedia

Leaf node that describes the transport protocol used to carry the real time media (e.g. Video Share) when connecting over PS cellular access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 15: IMS MO sub tree addition parameters (psRTMedia)

- Values: The possible values are:
    - RTP
    - SRTP
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “psRTMedia”

Node: <x>/transportProto/psSignallingRoaming

Leaf node that describes the transport protocol used to carry the signalling when connecting over PS cellular access through a visited network (roaming scenario).

NOTE: The “psSignallingRoaming” parameter is defined as a temporary workaround to address PS roaming related issues identified in live deployments.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 16: IMS MO sub tree addition parameters (psSignallingRoaming)

- Values: The possible values are:
    - SIPoUDP
    - SIPoTCP
    - SIPoTLS
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “psSignallingRoaming”

Node: <x>/transportProto/psMediaRoaming

Leaf node that describes the transport protocol used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over PS cellular access through a visited network (roaming scenario).

NOTE: The “psMediaRoaming” parameter is defined as a temporary workaround to address PS roaming related issues identified in live deployments.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 17: IMS MO sub tree addition parameters (psMediaRoaming)

- Values: The possible values are:
    - MSRP
    - MSRPoTLS
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “psMediaRoaming”

Node: <x>/transportProto/psRTMediaRoaming

Leaf node that describes the transport protocol used to carry the real time media (e.g. Video Share) when connecting over PS cellular access through a visited network (roaming scenario).

NOTE: The “psRTMediaRoaming” parameter is defined as a temporary workaround to address PS roaming related issues identified in live deployments.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 18: IMS MO sub tree addition parameters (psRTMediaRoaming)

- Values: The possible values are:
    - RTP
    - SRTP
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “psRTMediaRoaming”

Node: <x>/transportProto/wifiSignalling

Leaf node that describes the transport protocol used to carry the signalling when connecting over Wi-Fi.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 19: IMS MO sub tree addition parameters (wifiSignalling)

- Values: The possible values are:
    - SIPoUDP
    - SIPoTCP
    - SIPoTLS
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “wifiSignalling”

Node: <x>/transportProto/wifiMedia

Leaf node that describes the transport protocol used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over Wi-Fi access

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 20: IMS MO sub tree addition parameters (wifiMedia)

- Values: The possible values are:
    - MSRP
    - MSRPoTLS
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “wifiMedia”

Node: <x>/transportProto/wifiRTMedia

Leaf node that describes the transport protocol used to carry the real time media (e.g. Video Share) when connecting over Wi-Fi access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

Table 21: IMS MO sub tree addition parameters (wifiRTMedia)

- Values: The possible values are:
    - RTP
    - SRTP
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “wifiRTMedia”

Node: <x>/uuid_Value

Leaf node that describes the UUID value that shall be included in the SIP REGISTER request as value for the sip.instance feature tag to support identifying the configured client in a multidevice approach. In this case the UUID is generated by the Service Provider network following the algorithm described in [RFC4122].

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get, Replace

Table 22: IMS MO sub tree addition parameters (uuid_Value)

- Values: A string containing the UUID value

- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Associated HTTP XML characteristic type: “uuid_Value”

Node: <x>/Ext

An extension node for Service Provider specific parameters. Clients that are not aware of any extensions in this subtree (e.g. because they are not Service Provider specific) should not instantiate this tree.

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Table 23: IMS MO sub tree addition Service Provider Extension Node

- Values: N/A
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration as described in [PRD-RCC.14].
- Associated HTTP XML characteristic type: “Ext”

2.2.2.3 Summary structure

The HTTP configuration XML structure associated with the IMS parameters resulting from the parameters coming from the IMS MO defined in [3GPP TS 24.167] mapped in section 2.2.2.1 and the additional specific parameters (shown in blue) introduced in section 2.2.2.2 is presented in the table below

```
<characteristic type="APPLICATION">
        <parm name=”AppID” value=”X”/>
        <parm name=”Name” value=”X”/>
        <parm name=”AppRef” value=”IMS-Settings”/>
        <characteristic type=”ConRefs”>
              <characteristic type=”Refs”>
                    <parm name=”ConRef1” value=”X”/>
                    <parm name=”ConRef2” value=”X”/>
                    …
              </characteristic>
        </characteristic>
        <parm name=”PDP_ContextOperPref” value=”X”/>
        <parm name=”Timer_T1” value=”X”/>
        <parm name=”Timer_T2” value=”X”/>
        <parm name=”Timer_T4” value=”X”/>
        <parm name=”P-CSCF_Address” value=”X”/>
        <parm name=”Private_User_Identity” value=”X”/>
        <characteristic type=”Public_User_Identity_List”>
              <characteristic type=”Public_user_identities”>
                    <parm name=”Public_User_Identity1” value=”X”/>
                    <parm name=”Public_User_Identity2” value=”X”/>
                    …
              </characteristic>
        </characteristic>
        <parm name=”Home_network_domain_name” value=”X”/>
        <characteristic type=”Ext”>
```

```
            <parm name=”endUserConfReqId” value=”X”/>
            <characteristic type=” transportProto”>
                  <parm name=”psSignalling” value=”X”/>
                  <parm name=”psMedia” value=”X”/>
                  <parm name=”psRTMedia” value=”X”/>
                  <parm name=”psSignallingRoaming” value=”X”/>
                  <parm name=”psMediaRoaming” value=”X”/>
                  <parm name=”psRTMediaRoaming” value=”X”/>
                  <parm name=”wifiSignalling” value=”X”/>
                  <parm name=”wifiMedia” value=”X”/>
                  <parm name=”wifiRTMedia” value=”X”/>
            </characteristic>
            <parm name=”uuid_Value” value=”X”/>
            <characteristic type=”Ext”/>
      </characteristic>
      <characteristic type=”ICSI_List”>
            <characteristic type=”ICSIs”>
                  <parm name=”ICSI1” value=”X”/>
                  <parm name=”ICSI_Resource_Allocation_Mode1” value=”X”/>
                  <parm name=”ICSI2” value=”X”/>
                  <parm name=”ICSI_Resource_Allocation_Mode2” value=”X”/>
            </characteristic>
      </characteristic>
      <characteristic type=”LBO_P-CSCF_Address”>
            <characteristic type=”LBO_P-CSCF_Addresses”>
                  <parm name=”Address1” value=”X”/>
                  <parm name=”AddressType1” value=”X”/>
                  <parm name=”Address2” value=”X”/>
                  <parm name=”AddressType2” value=”X”/>
                  …
            </characteristic>
      </characteristic>
      <parm name=”Resource_Allocation_Mode” value=”X”/>
      <parm name=”Voice_Domain_Preference_E_UTRAN” value=”X”/>
      <parm name=”SMS_Over_IP_Networks_Indication” value=”X”/>
      <parm name=”Keep_Alive_Enabled” value=”X”/>
      <parm name=”Voice_Domain_Preference_UTRAN” value=”X”/>
      <parm name=”Mobility_Management_IMS_Voice_Termination” value=”X”/>
      <parm name=”RegRetryBaseTime” value=”X”/>
      <parm name=”RegRetryMaxTime” value=”X”/>
      <characteristic type=”PhoneContext_List”>
            <characteristic type=”PhoneContext_List”>
                  <parm name=”PhoneContext1” value=”X”/>
                  <parm name=”Public_User_Identity1” value=”X”/>
                  <parm name=”PhoneContext2” value=”X”/>
                  <parm name=”Public_User_Identity2” value=”X”/>
                  …
            </characteristic>
      </characteristic>
      <parm name="SS_domain_setting" value="X"/>
      <parm name="PS_domain_IMS_SS_control_preference" value="X"/>
      <characteristic type=”APPAUTH”>
            <parm name=”AuthType” value=”X”/>
            <parm name=”Realm” value=”X”/>
            <parm name=”UserName” value=”X”/>
            <parm name=”UserPwd” value=”X”/>
      </characteristic>
</characteristic>
```

Table 24: IMS sub tree associated HTTP configuration XML structure

2.2.2.4 Inclusion in the HTTP XML document

The IMS configuration is included as follows in the configuration document:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
        <characteristic type="VERS">
                <parm name=”version” value=”X”/>
                <parm name=”validity” value=”Y”/>
        </characteristic>
        <characteristic type="TOKEN">
                <parm name=”token” value=”U”/>
                <parm name=”validity” value=”V”/>
        </characteristic>
        <characteristic type="MSG">                    -- This section is OPTIONAL
                <parm name=”title” value=”R”/>
                <parm name=”message” value=”S”/>
                <parm name=”Accept_btn” value=”X”/>
                <parm name=”Reject_btn” value=”X”/>
        </characteristic>
        <characteristic type="APPLICATION">
                <parm name=”AppID” value=”ap2001”/>
                <parm name=”Name” value=”IMS Settings”/>
                <parm name=”AppRef” value=”IMS-Settings”/>
                        …       -- see section 2.2.2.2
        </characteristic>
        <characteristic type="APPLICATION">
                <parm name=”AppID” value=”apXYZ”/>
                <parm name=”Name” value=”My IMS APP settings”/>
                <parm name=”AppRef” value=”MyIMSApp-Settings”/>
                <characteristic type=”IMS”>
                        <parm name=”To-AppRef” value=”IMS-Settings”/>
                </characteristic>
                <characteristic type=”xx”>
                        …
                </characteristic>
                <characteristic type=”yy”>
                        …
                </characteristic>
                …
        </characteristic>
</wap-provisioningdoc>
```

Table 25: Complete IMS HTTP configuration XML structure

3 IMS Service Supporting Enablers

3.1 End User Confirmation Requests

The following section provides a framework that will allow the Service Provider to inform the end user about a certain situation by opening a dialog in the device presenting all the available information and asking the user to confirm or decline the proposed request.

NOTE: Support for the framework described in this section is not mandatory for all IMS devices, but may be mandated in specifications describing specific IMS-based services (e.g. RCS) either explicitly or implicitly by mandating the support of other enablers depending on it (e.g. configuration as described in section 2.1.2).

The End User Confirmation Request is implemented using a SIP MESSAGE[3] method containing a XML payload type "*application/end-user-confirmation-request+xml*" that will be sent by the Service Provider serving the end user to their IMS device/client. A specific device can be addressed using a Globally Routable User agent URI (GRUU) or a sip.instance feature tag. If the user is required to answer from every device, the devices should be addressed individually using a GRUU or a sip.instance feature tag.

Upon the reception of the SIP MESSAGE, the end user terminal will check the *P-Asserted-Identity* of the incoming message and match it against the configured URI for the service (END USER CONF REQ ID) as defined in **Error! Reference source not found.** and extract the request information from the XML payload body. A dialog or notification will be displayed to the End User (User Experience [UX] dependent) showing the confirmation request and related information.

The End User Confirmation Response will be encapsulated in an XML body with a payload type "*application/end-user-confirmation-response+xml*" and returned back to the Service Provider in a new SIP MESSAGE.

3.1.1 End User Confirmation Request

The information contained in the end user confirmation request is the following

- Id: Unique identifier of the request.
- Type: Determines the behaviour of the receiving device. It can take one of the following two values:
  - *Volatile*, the answer shall be returned inside of a new SIP MESSAGE request. The request may time out without end user input, in which case it will be discarded.
  - *Persistent*, the answer shall be returned inside of a new SIP MESSAGE request. The confirmation request does not time out.
- Pin: Determines whether a pin is requested to the end user. It can take one of the following two values: true or false. If the attribute is not present it shall be considered as false. This pin request can be used to add a higher degree of confirmation and can be used to allow certain operations for example parental control.

[3] Please take into account that according to [RFC3428], the size of MESSAGE requests outside of a media session MUST NOT exceed 1300 bytes, unless the UAC has positive knowledge that the message will not traverse a congestion-unsafe link at any hop, or that the message size is at least 200 bytes less than the lowest MTU (Maximum Transmission Unit) value found en route to the User Agent Server (UAS). Larger payloads may be sent by the Service Provider in the initial confirmation request and/or ack (Acknowledgement) using content-indirection as specified in [RFC4483]. Therefore, this shall be supported by the devices/clients.

- Subject: text to be displayed as notification or dialog title.
- Text: text to be displayed as body of the dialog.
- Timeout: Time period in seconds during which a volatile request is valid. After the timeout expires, the device shall discard any UX notifications silently.

For volatile type requests an optional timeout attribute may be present in the XML representing the validity period in seconds. If this attribute is not present a default value of 64*T1 seconds (with T1 as defined in [RFC3261]) shall be used.

The EUCR initiates a dialogue to the user on the device. For specific use cases it may be necessary that the user accepts external EUCRs which cannot be authenticated appropriately. This acceptance can either be done by configuration or by entering a specific mode on the device UI and avoids unwanted UI dialogues on the devices caused by malicious usage by other person. One use case described in sections 2.1.2.1 and 2.1.2.2 is the configuration of additional IMS clients via Internet. To identify such messages following attribute is provided:

- externalEUCR: Determines that this is an EUCR initiated by an external unsecure source, e.g. via the Internet. If the optional attribute externalEUCR is set to true in the EUCR and the device does not allow such external EUCRs, the EUCR shall be ignored. An EUCR response shall not be sent back in that case. The device shall show all EUCR requests where the attribute externalEUCR is set to false or does not exist.
  If the device or client has not implemented the processing of the attribute externalEUCR, it shall be ignored and therefore all EUCRs are allowed and shown in the UI.

In addition, to allow Service Providers more flexibility the two following optional button labels will be defined. For backward compatibility: if the optional button labels are not used, default values will be used instead.

- **ButtonAccept:** text to display on the button.
- **ButtonReject:** text to display on the button.

To ensure compatibility with future versions, the IMS client/device shall silently discard any unknown node or attribute in the XML structure.

Several Subject or Text nodes can be present in the XML body to be able to support multiple languages. If more than one element is presented a language (*lang*) attribute must be present with the two letter language codes according to the ISO 639-1. IMS clients shall verify the language attribute and display the text data of the element that matches the current language used by the user. If there is no language matching the user's, the first node of Subject and Text shall be used.

If the type of confirmation request is persistent the Service Provider can send an optional acknowledgement message of the transaction back to the user with a welcome message, an error message or further instructions. This acknowledgement message will be encapsulated in an XML body with a payload type "*application/end-user-confirmation-ack+xml*" and returned in a separate SIP MESSAGE. If the acknowledgement refers to the message which is currently displayed, it shall be discarded even if no answer was sent. This allows sending

a message to all active devices of a user when a response from a single device is sufficient. For that reason it is also possible to send acknowledgements without Subject or textual content.

The following table specifies the XML Schema Definition (XSD) of the XML payload for the EUCR:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xmlns:xml=”http://www.w3.org/XML/1998/namespace”
            elementFormDefault="qualified">
      <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
                  schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
      <xs:element name="EndUserConfirmationRequest">
            <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="Subject" maxOccurs="unbounded"/>
                        <xs:element ref="Text" maxOccurs="unbounded"/>
                        <xs:element ref="ButtonAccept" minOccurs="0" maxOccurs="unbounded"/>
                        <xs:element ref="ButtonReject" minOccurs="0" maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="id" type="xs:string" use="required"/>
                  <xs:attribute name="type" type="xs:string" use="required"/>
                  <xs:attribute name="pin" type="xs:boolean" use="optional"/>
                  <xs:attribute name="timeout" type="xs:integer" use="optional"/>
                  <xs:attribute name="externalEUCR" type="xs:boolean" use="optional"/>
            </xs:complexType>
      </xs:element>
      <xs:element name="Subject">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="Text">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="ButtonAccept">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="ButtonReject">
            <xs:complexType>
```

```
                    <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                            <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                    </xs:simpleContent>
                </xs:complexType>
            </xs:element>
</xs:schema>
```

Table 26: End User Confirmation Request XSD

3.1.2 End User Confirmation Response

The information contained in the End User Confirmation Response is the following:

- **Id**: Unique identifier of the request.
- **Value:** with the end user confirmation. It can take one of the following two values accept or decline.
- **Pin:** if the request has the “pin” attribute set to true, the response will contain the pin value introduced by the user.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xml=”http://www.w3.org/XML/1998/namespace”
           elementFormDefault="qualified">
    <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
               schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
    <xs:element name="EndUserConfirmationResponse">
        <xs:complexType>
            <xs:attribute name="id" type="xs:string" use="required"/>
            <xs:attribute name="value" type="xs:string" use="required"/>
            <xs:attribute name="pin" type="xs:string" use="optional"/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Table 27: End User Confirmation Response XSD

The information contained in the End User Acknowledge Response is the following

- **Id:** Unique identifier of the original request. If the ID matches the ID of the currently shown message, this message shall be discarded even if no answer was sent from the receiving device.
- **Status:** of the End User Confirmation. It can take one of the following two values: ok or error.
- **Subject:** text to be displayed as notification or dialog title
- **Text:** text to be displayed as body of the dialog.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xml=”http://www.w3.org/XML/1998/namespace”
                elementFormDefault="qualified">
        <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
                schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
        <xs:element name="EndUserConfirmationAck">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element ref="Subject" maxOccurs="unbounded"/>
                                <xs:element ref="Text" maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute name="id" type="xs:string" use="required"/>
                        <xs:attribute name="status" type="xs:string" use="required"/>
                </xs:complexType>
        </xs:element>
        <xs:element name="Subject">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:extension base=”xs:string”>
                                        <xs:attribute ref="xml:lang"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
        <xs:element name="Text">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:extension base=”xs:string”>
                                        <xs:attribute ref="xml:lang"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

Table 28: End User Confirmation Acknowledgement XSD

3.1.3 End User Notification Request

To provide more flexibility a Service Provider shall be able to send only notification messages to the end user. This notification message shall be implemented similar to confirmation dialog using a SIP MESSAGE method containing an XML payload type “*application/end-user-notification-request+xml*”. A notification will be displayed to the end user (UX dependent) showing the related information.

The information contained in the end user notification is the following:

- **Id:** Unique identifier of the request.
- **Subject:** text to be displayed as notification or dialog title
- **Text:** text to be displayed as body of the dialog.
- **ButtonOK:** text to display on the button.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xmlns:xml=”http://www.w3.org/XML/1998/namespace”
            elementFormDefault="qualified">
      <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
                  schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
      <xs:element name="EndUserNotification">
            <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="Subject" maxOccurs="unbounded"/>
                        <xs:element ref="Text" maxOccurs="unbounded"/>
                        <xs:element ref="ButtonOK" minOccurs="0" maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="id" type="xs:string" use="required"/>
            </xs:complexType>
      </xs:element>
      <xs:element name="Subject">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="Text">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="ButtonOK">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
</xs:schema>
```

Table 29: End User Notification XSD

3.1.4 End User System Request

It shall be also possible to send a System Request to the IMS client to trigger an internal action based on the type of the request. These requests are not displayed to the user at the UI level. The request is implemented also using a SIP MESSAGE method containing an XML payload body of type “*application/system-request+xml*”.

The information contained in the end user notification is the following:

- **Id:** Unique identifier of the request.
- **Type:** Identifying the kind of action to be triggered

- **Data:** Custom information needed to perform the action.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
	<xs:element name="SystemRequest">
		<xs:complexType>
			<xs:attribute name="id" type="xs:string" use="required"/>
			<xs:attribute name="type" type="xs:string" use="required"/>
			<xs:attribute name="data" type="xs:string" use="optional"/>
		</xs:complexType>
	</xs:element>
</xs:schema>
```

Table 30: System Request XSD

The following list shows the defined system requests in this specification:

Type	Data	Action
urn:gsma:rcs:http-configuration:reconfigure	N.A.	Perform an HTTP reconfiguration. See section 2.1.3.1

Table 31: List of generic System Requests

NOTE: Specifications describing IMS services may define other system requests.

3.1.5 Example Use Case 1: Accepting terms and conditions

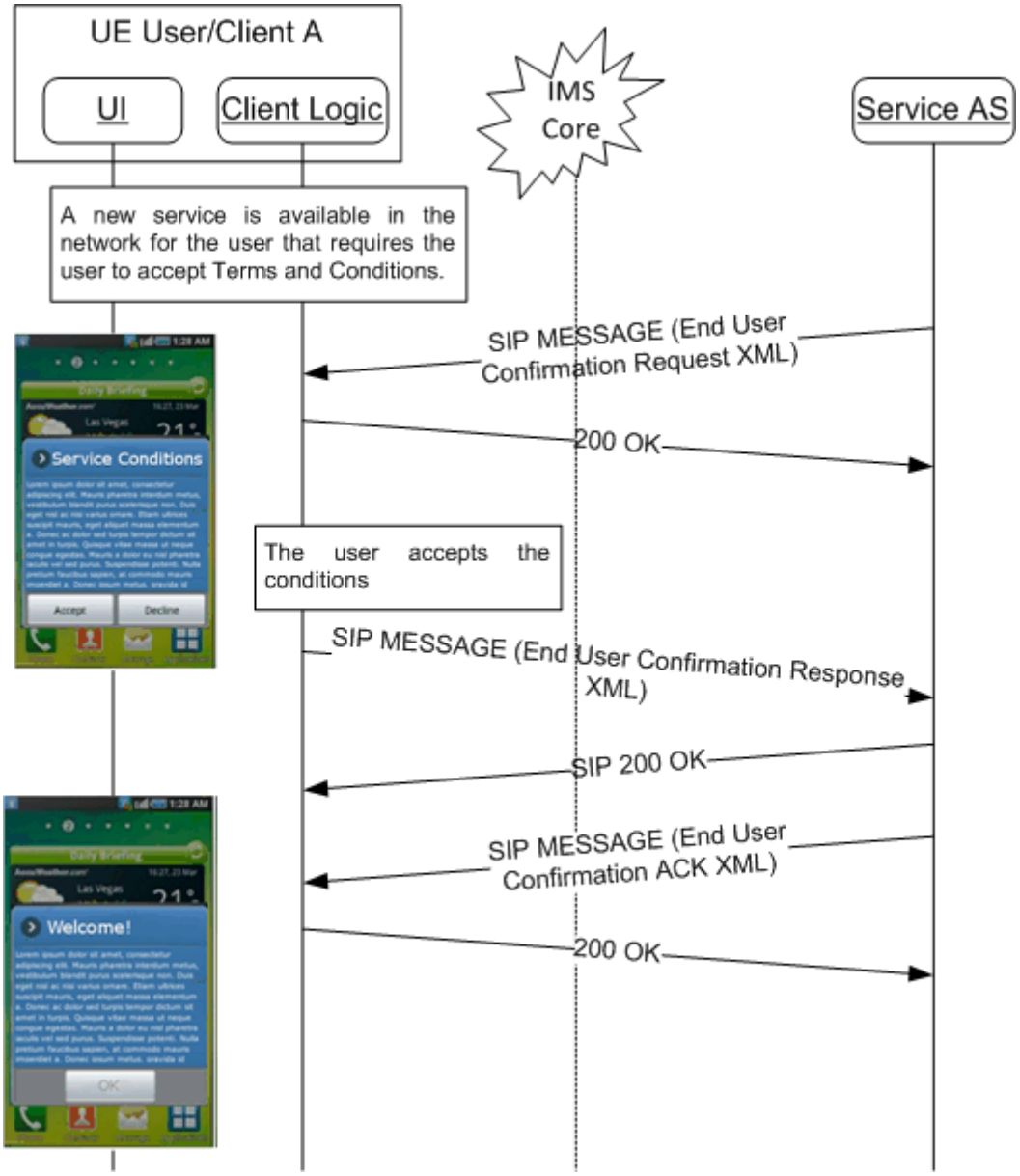

Figure 4: Terms and Condition Use Case example

3.1.6 Example Use Case 2: Notification

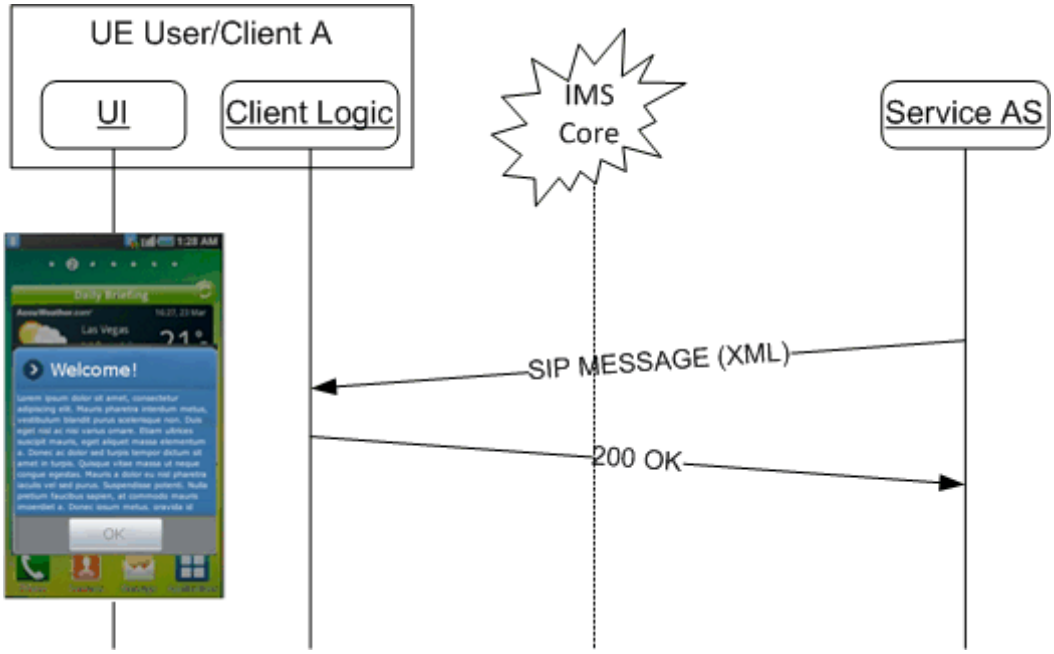

Figure 5: User Notification example

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	02 February 2015	Initial version split from RCC.07 v5.0 to allow for more generic use	PSMC	Tom Van Pelt / GSMA

A.2 Other Information

Type	Description
Document Owner	GSMA Network2020 Programme IP Communications Global Specification Group
Editor / Company	Tom Van Pelt / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.