IMS Device Configuration and Supporting Services

Version 4.0

28 June 2017

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

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
CP AC	Client Provisioning Application Characteristic
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
OMNA	Open Mobile Naming Authority, registry available at: http://www.openmobilealliance.org
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

Term	Description
UAS	User Agent Server
UE	User Equipment
UI	User Interface
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, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO) http://www.3gpp.org
[2]	[PRD-IR.88]	GSMA PRD IR.88 - “LTE and EPC Roaming Guidelines”, Version 15.0, 03 November 2016 http://www.gsma.com/
[3]	[PRD-RCC.07]	GSMA PRD RCC.07 “Rich Communication Suite 7.0 Advanced Communications Services and Client Specification”, Version 8.0, 28 June 2017 http://www.gsma.com
[4]	[PRD-RCC.14]	GSMA PRD RCC.14 “Service Provider Device Configuration”, Version 5.0, 28 June 2017 http://www.gsma.com
[5]	[RFC2119]	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. 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

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

A client supporting IMS Device Configuration and Supporting Services shall indicate the support by inclusion of an "*app*" HTTP GET request parameter as defined in [PRD-RCC.14] with the value of the OMA DM Management Object Identifier assigned by the Open Mobile Naming Authority (OMNA) for the IMS Management Object (MO) defined in [3GPP TS 24.167], i.e. “*urn:oma:mo:ext-3gpp-ims:1.0*”.

Services based on IMS may define

- MOs for their service configuration which results in additional "app" HTTP GET request parameter values
- service specific HTTP GET request parameters.

For details about request parameters for IMS based services refer to the corresponding service documentation.

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.

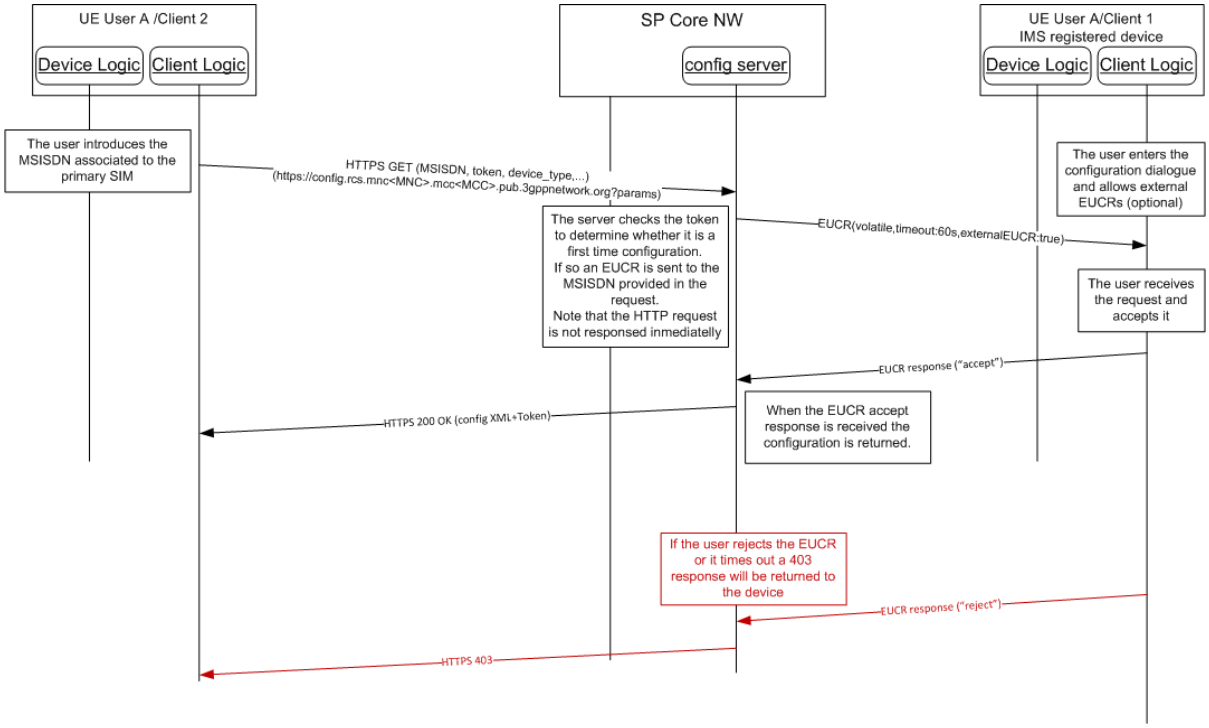

Figure 1: Alternative HTTP configuration for additional devices: First time configuration using EUCR

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:

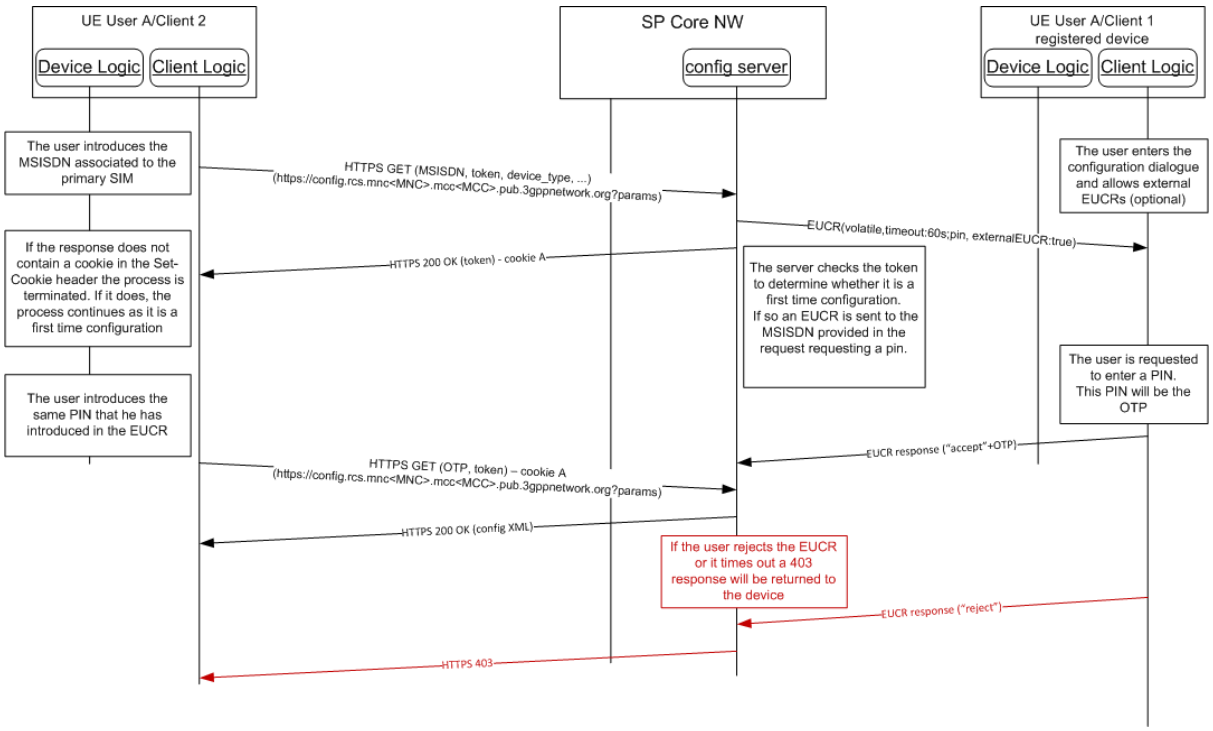

Figure 2: Alternative configuration for additional devices: First time configuration EUCR with PIN

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 the type parameter set to *request a HTTP reconfiguration* and the optional data parameter as specified in section 3.1.4.

If the client receives a EUCR system request with

- a type parameter requesting a HTTP reconfiguration and
- the value parameter absent or a value parameter present with no fqdn parameter included,

then the client shall perform a HTTP configuration as defined in section 2.2, 2.3, 2.4 and 2.5 of [PRD-RCC.14] depending on client capabilities and current connectivity. The client shall send the HTTP configuration request to the configuration server providing the configuration data for the IMS registration used to receive the EUCR system request. If the IMS registration used to receive the EUCR request is not configured via the Service Provider Device Configuration of [PRD-RCC.14], then the client shall use the default configuration server instead. For definition of default configuration server refer to [PRD-RCC.14].

If the client receives a EUCR system request with

- a type parameter requesting a HTTP reconfiguration and
- the value parameter present and a fqdn parameter included,

then

- if the value of the fqdn parameter value matches an fqdn value received from the home Service Provider configuration server in a fqdn value of the SERVER characteristic as defined in section 4.2 of [PRD-RCC.14], then the client shall perform a HTTP configuration as defined in section 2.2, 2.3, 2.4 or 2.5 of [PRD-RCC.14] depending on client capabilities and current connectivity using the fqdn value, otherwise
- the client shall ignore the request.

2.2 Configuration Parameters

2.2.1 Parameter Definitions

2.2.1.1 IMS core network related configuration

2.2.1.1.1 Endorsement of 3GPP IMS Management Object (MO)

Basic IMS core network related 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.

The following differences with [3GPP TS 24.167] apply:

- The IMS MO parameter Public_user_identity_List is used by the configuration server to configure one or more IMS Public User Identities to be used by the client for the IMS registration. A client registering in IMS using an access over the IMS well-known Access Point Name (APN) defined in [PRD-IR.88] shall ignore the IMS MO parameter Public_user_identity_List.
- The IMS MO parameter Home_network_domain_name is used by the configuration server to configure the operator’s home network domain. A client registering in IMS

using an access over the IMS well-known APN defined in [PRD-IR.88] shall ignore the IMS MO parameter Home_network_domain_name.

- The IMS MO parameter LBO_P-CSCF_Address is used by the configuration server to configure one or more P-CSCF addresses to be used by the client for the P-CSCF discovery procedure. A client registering in IMS using an access over the IMS well-known APN defined in [PRD-IR.88] shall ignore the of the IMS MO parameter LBO_P-CSCF_Address.
- The 3GPP IMS Client Provisioning Application Characteristics (CP AC) is not applicable.

2.2.1.2 Additional IMS core network related parameters

This specification defines the following additional IMS core network related configuration parameters:

Configuration parameter	Description	GSMA IMS usage
IMS Mode Authentication Type	Specifies the requested mechanism to be used for IMS. Values are defined for: • IMS Authentication and Key Agreement (AKA) • SIP DIGEST (without Transport Layer Security [TLS]) A client registering in IMS using an access over the IMS well-known APN defined in [PRD-IR.88] shall ignore the parameter.	Mandatory Parameter,
Realm	Realm to use for authentication (Digest mode only) A client registering in IMS using an access over the IMS well-known APN defined in [PRD-IR.88] shall ignore the parameter.	Optional parameter It is Mandatory if IMS Mode Authentication Type is set to Digest.
Realm User Name	Realm username to use for authentication (Digest mode only) A client registering in IMS using an access over the IMS well-known APN defined in [PRD-IR.88] shall ignore the parameter.	Optional parameter It is Mandatory if IMS Mode Authentication Type is set to Digest.
Realm User Password	Realm user password to use for authentication (Digest mode only) A client registering in IMS using an access over the IMS well-known APN defined in [PRD-IR.88] shall ignore the parameter.	Optional parameter It is Mandatory if IMS Mode Authentication Type is set to Digest.

Configuration parameter	Description	GSMA IMS usage
Transport Protocols: Signalling Cellular	Controls the transport protocol used to carry the SIP signalling when connecting over PS cellular access in the home network and EPC integrated Wi-Fi. The following values are defined: • SIPoUDP – SIP over UDP transport (default value) • SIPoTCP –SIP over TCP transport • SIPoTLS – SIP over TLS transport	Optional parameter
Transport Protocols: Signalling Roaming	Controls the transport protocol used to carry the SIP signalling when connecting over PS cellular access outside of the home network. The following values are defined: • SIPoUDP – SIP over UDP transport (default value) • SIPoTCP –SIP over TCP transport • SIPoTLS – SIP over TLS transport	Optional parameter
Transport Protocols: Signalling Wi-Fi	Controls the transport protocol used to carry the SIP signalling when connecting over non-3GPP access. The following values are defined: • SIPoUDP – SIP over UDP transport • SIPoTCP – SIP over TCP transport • SIPoTLS – SIP over TLS transport (default value)	Optional parameter
Transport Protocols: Real Time Media Cellular	Controls the transport protocol to carry the real time media when connecting over PS cellular access in the home network and EPC integrated Wi-Fi. The following values are defined: • RTP – Real-time Transport Protocol (default value) • SRTP – Secure Real-time Transport Protocol	Optional parameter
Transport Protocols: Real Time Media Roaming	Controls the transport protocol to carry the real time media when connecting over PS cellular access outside of the home network. The following values are defined: • RTP – Real-time Transport Protocol (default value) • SRTP – Secure Real-time Transport Protocol	Optional parameter
Transport Protocols: Real Time Media Wi-Fi	Controls the transport protocol to carry the real time media when connecting over non-cellular access. The following values are defined: • RTP – Real-time Transport Protocol • SRTP – Secure Real-time Transport Protocol (default value)	Optional parameter

Configuration parameter	Description	GSMA IMS usage
Transport Protocols: Discrete Media Cellular	Controls the transport protocol used to carry discrete media when connecting over PS cellular access in the home network and EPC integrated Wi-Fi. The following values are defined: • MSRPoTCP –MSRP over TCP transport (default value) • MSRPoTLS – MSRP over TLS transport	Optional parameter
Transport Protocols: Discrete Media Roaming	Controls the transport protocol used to carry discrete media when connecting over PS cellular access outside of the home network. The following values are defined: • MSRPoTCP – MSRP over TCP transport (default value) • MSRPoTLS – MSRP over TLS transport	Optional parameter
Transport Protocols: Discrete Media Wi-Fi	Controls the transport protocol used to carry discrete media when connecting over non-3GPP access. The following values are defined: • MSRPoTCP – MSRP over TCP transport • MSRPoTLS – MSRP over TLS transport (default value)	Optional parameter

Table 2: Additional IMS Core/SIP related configuration parameters

2.2.1.3 End User Confirmation parameters

This specification defines 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 by the client to authorise the sender of EUCRs and as the destination address for the sending of EUCR responses	Optional Parameter

Table 3: End user confirmation configuration parameters

2.2.1.4 Multidevice configuration parameters

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

Configuration parameter	Description	GSMA IMS usage
uuid_Value	Provides a Universally Unique IDentifier (UUID) to be used as the instance ID of SIP requests and responses based on the rule defined in section 2.4.2 of [PRD-RCC.07].	Optional Parameter

Table 4: Multi-device configuration parameters

2.2.1.5 Configuration management parameters

This specification defines the following configuration parameters for the management of client configuration data:

Configuration parameter	Description	GSMA IMS usage
APPREF	The parameter includes the reference identity of an IMS MO instance. The value of the parameter value shall be unique in the scope of the client configuration data. The TO-APPREF configuration parameter included in other Management Objects can be used for referring to an individual instance of an IMS MO in the client configuration data. The value "DEFAULT" shall be used for the APPREF parameter to identify the default IMS MO instance. IMS based services shall use the default IMS MO instance unless configured for another IMS MO instance via a TO-APPREF configuration parameter in their configuration data. Service Providers assigning additional configuration servers using the procedure defined in [PRD-RCC.14] shall ensure uniqueness of the APPREF values across all IMS MO provisioning documents provided by their configuration servers.	Mandatory Parameter

Table 5: Multi-device configuration parameters

2.2.2 Provisioning document of the IMS MO

2.2.2.1 General

IMS Management Objects are conveyed between the configuration server and the client by use of a configuration XML document as defined in section 4 of [PRD-RCC.14]. The IMS Management Object shall be represented in the configuration XML document via the provisioning document defined in this section.

In accordance with the procedure defined in Annex A of [PRD-RCC.14] the AppID value of the provisioning document containing one or more IMS MO instances shall be set to the value assigned by the OMNA for the OMA DM Management Object Identifier of the IMS Management Object (MO) defined in [3GPP TS 24.167], i.e. "*urn:oma:mo:ext-3gpp-ims:1.0*".

Each IMS MO instance contained in an IMS MO provisioning document contains an AppID parameter resulting from the procedure defined in section 2.2.2.2. The value and occurrence of the AppID parameter of an IMS MO instance shall follows the definitions of [3GPP TS 24.167].

2.2.2.2 IMS Sub tree mapping to HTTP

The IMS MO parameters defined in [3GPP TS 24.167] shall be mapped to a provisioning document using the procedure defined in Annex A of [PRD-RCC.14].

2.2.2.3 IMS MO sub tree additions

The additional configuration parameters defined in section 2.2.1 are added to the IMS MO sub tree as depicted in Figure 3. The <*3GPP_IMS*> node corresponds to the <*x*> root node of the IMS MO defined in [3GPP TS 24.167].

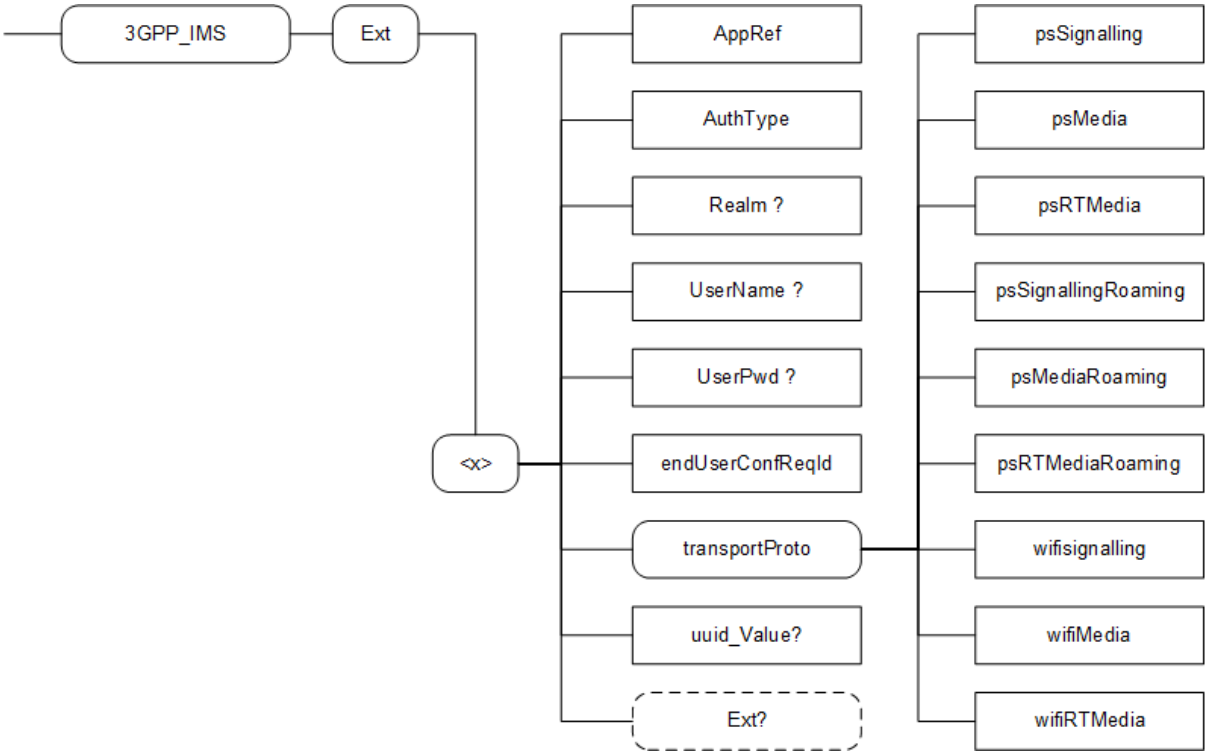

Figure 3: Additions to the IMS MO sub tree

Node: <x>

Under this interior node the additional IMS MO parameters are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 6: IMS MO sub tree addition IMS node

- Values: N/A
- Characteristic/Parameter: GSMA

Node: <x>/AppRef

Leaf node that describes the reference identity of an IMS MO instance.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

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

- Values: <unique reference identity of the IMS MO instance>
  The value "DEFAULT" shall be used to identify the default IMS MO instance in the client configuration.

- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on.
- Characteristic/Parameter: GSMA/AppRef

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 8: IMS MO sub tree addition parameters (AuthType)

- Values: < AKA | Digest >
  AKA IMS Authentication and Key Agreement
  Digest SIP Digest
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Characteristic/Parameter: GSMA/AuthType

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 9: 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.
- Characteristic/Parameter: GSMA/Realm

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 10: IMS MO sub tree addition parameters (UserName)

- Values: <user name assigned to the user for the IMS authentication/registration>, Example: “Alice”
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Characteristic/Parameter: GSMA/UserName

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 11: IMS MO sub tree addition parameters (UserPwd)

- Values: <password assigned to the user for the IMS authentication/registration>, Example: 'secretxyz'
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Characteristic/Parameter: GSMA/UserPwd

Node: <x>/endUserConfReqId

Leaf node that describes the identity of the authorised sender of the EUCR request that is also used as destination address for sending of the EUCR response.

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 12: IMS MO sub tree addition parameters (endUserConfReqId)

- Values: <SIP URI or Tel URI>
  The identity of the authorised sender of the EUCR request and to be used as destination address for sending of the EUCR response
- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on.
- Characteristic/Parameter: GSMA/endUserConfReqId

Node: <x>/transportProto

Under this interior node the parameters related to transport protocol selection are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 13: Transport Protocol sub tree node

- Values: N/A
- Characteristic/Parameter: transportProto

Node: <x>/transportProto/psSignalling

Leaf node that describes the transport protocol used to carry the signalling when connecting over PS cellular access in the home network and EPC integrated Wi-Fi.

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

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

- Values: The possible values are:
    - SIPoUDP (default value)
    - SIPoTCP
    - SIPoTLS
- Post-reconfiguration actions: The client shall unregister if registered in a packet switched access before applying the new configuration and register back using the new parameter. Otherwise, there is no action required by the client apart from storing the new value and applying it from then on.
- Characteristic/Parameter: transportProto/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 in the home network and EPC integrated Wi-Fi.

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

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

- Values: The possible values are:
    - MSRP (default value)
    - MSRPoTLS
- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on for new MSRP sessions.
- Characteristic/Parameter: transportProto/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 in the home network and EPC integrated Wi-Fi.

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

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

- Values: The possible values are:
    - RTP (default value)

  - SRTP

- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on for new real time protocol sessions.
- Characteristic/Parameter: transportProto/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).

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

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

- Values: The possible values are:

  - SIPoUDP (default value)
  - SIPoTCP
  - SIPoTLS

- Post-reconfiguration actions: The client shall unregister if registered in packet switched access outside of the HPLMN before applying the new configuration and register back using the new parameter. Otherwise, there is no action required by the client apart from storing the new value and applying it from then on.
- Characteristic/Parameter: transportProto/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).

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

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

- Values: The possible values are:

  - MSRP (default value)
  - MSRPoTLS

- Post-reconfiguration actions: There is no action required by the client at the time reconfiguration apart from storing the new value and applying it from then on for new MSRP sessions.
- Characteristic/Parameter: transportProto/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).

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

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

- Values: The possible values are:
    - RTP (default value)
    - SRTP
- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on for new real time protocol sessions.
- Characteristic/Parameter: transportProto/psRTMediaRoaming

Node: <x>/transportProto/wifiSignalling

Leaf node that describes the transport protocol used to carry the signalling when connecting over non-3GPP access.

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

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

- Values: The possible values are:
    - SIPoUDP
    - SIPoTCP
    - SIPoTLS (default value)
- Post-reconfiguration actions: The client shall unregister if registered in non-3GPP access before applying the new configuration and register back using the new parameter. Otherwise, there is no action required by the client the apart from storing the new value and applying it from then on.
- Characteristic/Parameter: transportProto/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 non-3GPP access

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

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

- Values: The possible values are:
    - MSRP
    - MSRPoTLS (default value)
- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on for new MSRP sessions.
- Characteristic/Parameter: transportProto/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 non-3GPP access.

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

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

- Values: The possible values are:
    - RTP
    - SRTP (default value)
- Post-reconfiguration actions: There is no action required by the client at the time of reconfiguration apart from storing the new value and applying it from then on for new real time protocol sessions.
- Characteristic/Parameter: transportProto/wifiRTMedia

Node: <x>/uuid_Value

Leaf node that describes the UUID to be used as the instance ID in the contact address of SIP requests and responses based on the rule defined in section 2.4.2 of [PRD-RCC.07].

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

Table 23: IMS MO sub tree addition parameters (uuid_Value)

- Values: <UUID value as defined in [RFC4122]>
- Post-reconfiguration actions: The client shall unregister before applying the new configuration and register back using the new parameter.
- Characteristic/Parameter: GSMA/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 24: IMS MO sub tree addition Service Provider Extension Node

- Values: N/A
- Characteristic/Parameter: Ext

2.2.2.4 Summary structure

An example provisioning document containing the parameters of the IMS MO defined in [3GPP TS 24.167] and the additional parameters (shown in blue) is shown in Table 25. Note that Table 25 is an example and as such non-normative.

```
<characteristic type="APPLICATION">
        <parm name="AppID" value="urn:oma:mo:ext-3gpp-ims:1.0"/>
        <characteristic type="3GPP_IMS">
                <parm name=”AppID” value=”ap2001”/>
                <parm name="Name" value="X"/>
                <characteristic type="ConRefs">
                        <characteristic type="NODE">
                                <parm name="ConRef" value="X"/>
                        </characteristic>
                        <characteristic type="NODE">
                                <parm name="ConRef" 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="NODE">
                                <parm name="Public_User_Identity" value="X"/>
                        </characteristic>
                        <characteristic type="NODE">
                                <parm name="Public_User_Identity" value="X"/>
                        </characteristic>
                 </characteristic>
                <parm name="Home_network_domain_name" value="X"/>
                <characteristic type="Ext">
                        <characteristic type="GSMA">
                                <parm name="AppRef" value="X"/>
                                <parm name="AuthType" value="X"/>
                                <parm name="Realm" value="X"/>
                                <parm name="UserName" value="X"/>
                                <parm name="UserPwd" value="X"/>
                                <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>
        <characteristic type="ICSI_List">
            <characteristic type="NODE">
                <parm name="ICSI" value="X"/>
                <parm name="ICSI_Resource_Allocation_Mode" value="X"/>
            </characteristic>
            <characteristic type="NODE">
                 <parm name="ICSI" value="X"/>
                <parm name="ICSI_Resource_Allocation_Mode" value="X"/>
            </characteristic>
        </characteristic>
        <characteristic type="LBO_P-CSCF_Address">
            <characteristic type="NODE">
                <parm name="Address" value="X"/>
                <parm name="AddressType" value="X"/>
            </characteristic>
            <characteristic type="NODE">
                 <parm name="Address" value="X"/>
                <parm name="AddressType" 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="NODE">
                <parm name="PhoneContext" value="X"/>
                <parm name="Public_User_Identity" value="X"/>
            </characteristic>
            <characteristic type="NODE">
                <parm name="PhoneContext" value="X"/>
                <parm name="Public_User_Identity" value="X"/>
            </characteristic>
        </characteristic>
        <parm name="SS_domain_setting" value="X"/>
        <parm name="PS_domain_IMS_SS_control_preference" value="X"/>
        <characteristic type="Media_type_restriction_policy">
            <characteristic type=”NODE”>
                <parm name=”Media_type” value=”X”/>
                <parm name=”IP_CAN” value=”X”/>
                <parm name=”ICSI” value=”X”/>
                <parm name=”Roaming” value=”X”/>
            </characteristic>
            <characteristic type=”NODE”>
                <parm name=”Media_type” value=”X”/>
                <parm name=”IP_CAN” value=”X”/>
```

```
                        <parm name=”ICSI” value=”X”/>
                        <parm name=”Roaming” value=”X”/>
                    </characteristic>
                </characteristic>
                <characteristic type=”Default_EPS_bearer_context_usage_restriction_policy”>
                    <characteristic type=”NODE”>
                        <parm name=”Media_type” value=”X”/>
                        <parm name=”ICSI” value=”X”/>
                    </characteristic>
                    <characteristic type=”NODE”>
                        <parm name=”Media_type” value=”X”/>
                        <parm name=”ICSI” value=”X”/>
                    </characteristic>
                </characteristic>
                <characteristic type=”Reliable_18x_policy”>
                    <characteristic type=”NODE”>
                        <parm name=”Send_18x_Reliably” value=”X”/>
                        <parm name=”ICSI” value=”X”/>
                    </characteristic>
                    <characteristic type=”NODE”>
                        <parm name=”Send_18x_Reliably” value=”X”/>
                        <parm name=”ICSI” value=”X”/>
                    </characteristic>
                </characteristic>
                <!-- extensible for IMS MO parameters defined in [3GPP TS 24.167] -->
                <!-- by use of the mapping rule defined in Annex A of [PRD-RCC.14]. -->
            </characteristic>
</characteristic>
```

Table 25: IMS sub tree provisioning document structure (non-normative)

2.2.2.5 Inclusion in the HTTP XML document

The IMS MO provisioning document is included in the configuration XML document as illustrated in Table 26. Note that Table 26 is an example and as such non-normative.

```
<?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">                    <!-- This section is OPTIONAL -->
        <parm name="token" value="U"/>
    </characteristic>
    <!-- Potentially additional optional characteristics such as MSG, User and Access Control -->
    <!-- see [PRD-RCC.14] -->
    <characteristic type="APPLICATION">
        <parm name=”AppID” value=”urn:oma:mo:ext-3gpp-ims:1.0”/>
        <characteristic type="3GPP_IMS">
            <parm name=”AppID” value=”ap2001”/>
            <parm name=”Name” value=”Default IMS Settings”/>
            <characteristic type="Ext">
                <characteristic type="GSMA">
                    <parm name=”AppRef” value=”DEFAULT”/>
                    <!-- see Table 25 -->
                </characteristic>
            </characteristic>
```

```
                <!-- see Table 25 -->
            </characteristic>
            <characteristic type="3GPP_IMS">
                <parm name="AppID" value="ap2001"/>
                <parm name="Name" value="IMS Settings"/>
                <characteristic type="Ext">
                    <characteristic type="GSMA">
                        <parm name="AppRef" value="IMS-Settings"/>
                        <!-- see Table 25 -->
                    </characteristic>
                </characteristic>
                <!-- see Table 25 -->
            </characteristic>
        </characteristic>
        <characteristic type="APPLICATION">
            <parm name="AppID" value="apXYZ"/>
            <parm name="Name" value="My IMS APP settings"/>
            <characteristic type="IMS">
                <parm name="To-AppRef" value="IMS-Settings"/>
            </characteristic>
            <!-- service specific data -->
        </characteristic>
        <characteristic type="APPLICATION">
            <parm name="AppID" value="urn:foo:mo:bar:1.0"/>
            <parm name="Name" value="My other IMS APP settings"/>
            <parm name=”To-AppRef” value=”DEFAULT”/>
            <characteristic type="yy">
                <!-- service specific data -->
            </characteristic>
            <!-- additional service data -->
        </characteristic>
</wap-provisioningdoc>
```

Table 26: Complete configuration XML document structure (non-normative)

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 application specific XML payload documents based on bi-directional SIP MESSAGE[1] method transport between the RCS client and the server of the Service Provider serving the end user.

For End User Confirmation requests sent to the client, the Server Provider's server shall send the SIP MESSAGE request to the user's client based on the public user identity. A specific device of the user 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 with the content-type set to a XML payload type value defined for EUCR, the client shall match the value of the *P-Asserted-Identity* of the incoming SIP MESSAGE request against the value of the configuration parameter END USER CONF REQ ID as defined in Table 3.

If the values do not match, the client shall reply to the SIP MESSAGE with a 403 Forbidden response and discard the content of the message.

If the values match the client shall reply to the SIP MESSAGE with a 200 OK response and extract the request information from the XML payload body.

For End User Confirmation responses sent from the client to the Service Provider's server the client shall send the SIP MESSAGE to the address provided in the value of the configuration parameter END USER CONF REQ ID as defined in Table 3.

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

[1] 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 on 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.

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.
- 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 be done either 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, the 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 27: 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 28: 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 29: 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 30: 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 31: System Request XSD

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

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

Table 32: List of generic System Requests

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

The trigger-data of the system request to trigger a HTTP reconfiguration is defined as follows:

```
trigger-data = parm [ "," parm ]
parm = fqdn-parm | extension
fqdn-parm = fqdn-key "=" fqdn-value
fqdn-key = "fqdn"
fqdn-value = realm ; for encoding of realm refer to [RFC4282]
extension = 1*(parm-chars)
parm-chars = %x20-2B | %x2D-7E
```

As an example:

```
fqdn=config.rcs.provider.com
```

3.1.5 Example Use Case 1: Accepting terms and conditions

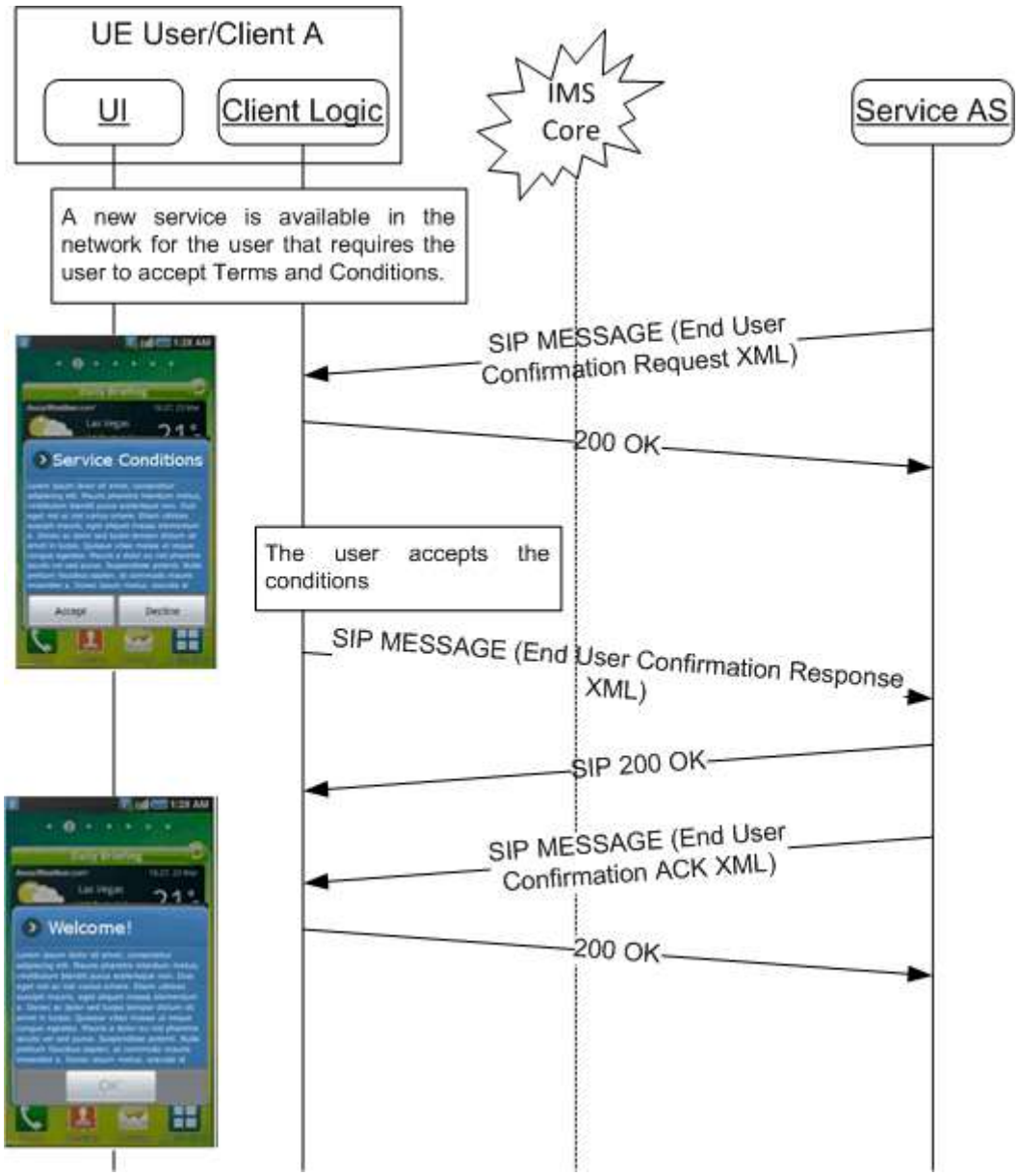

Figure 4: Terms and Condition Use Case example

3.1.6 Example Use Case 2: Notification

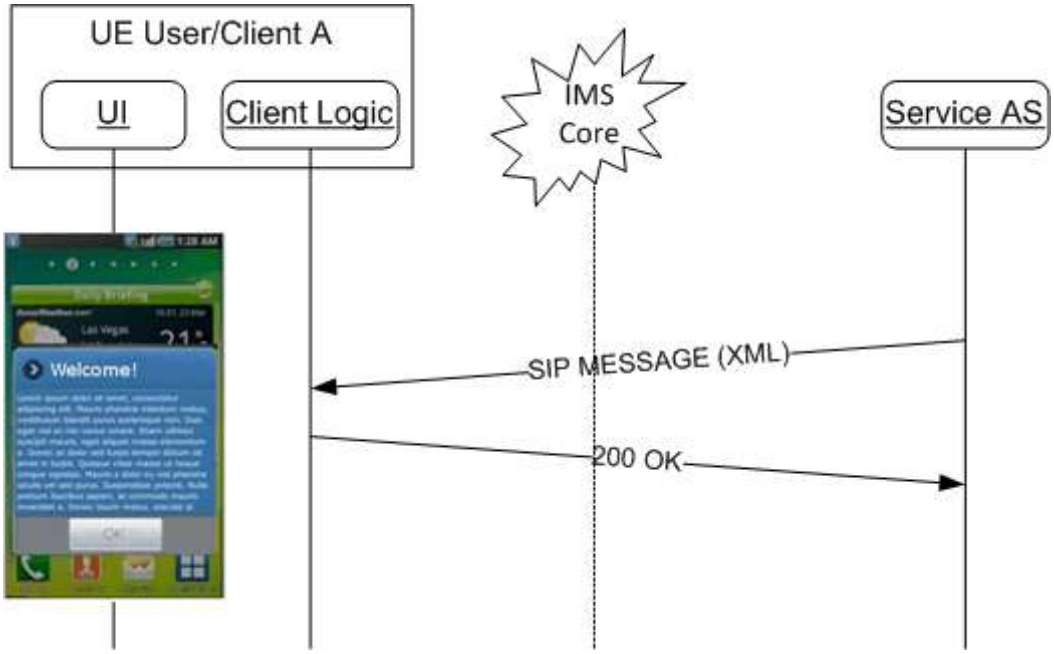

Figure 5: User Notification example

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
2.0	21 March 2016	Include approved CR1002	PSMC	Tom Van Pelt / GSMA
3.0	26 February 2017	Include approved CR1003	PSMC	Tom Van Pelt / GSMA
4.0	28 June 2017	Include approved CR1004	TG	Tom Van Pelt / GSMA

A.2 Other Information

Type	Description
Document Owner	Future Networks Programme, 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.