Push Client - Application Interface

Approved Version 1.1 – 22 Nov 2011

Open Mobile Alliance

OMA-TS-PushCAI-V1_1-20111122-A

Contents

1. Scope

This specification defines the Push Application Interface through which Push Applications can access OMA Push enabler services. The interface specified in this document defines functions and data formats supporting:

- registration of Push Applications with an OMA Push Client
- the subsequent delivery of Push events to the Push Application

2. References

[BCAST-SvcGuide] “Service Guide for Mobile Broadcast Services”. Open Mobile Alliance™. OMA-TS-BCAST_ServiceGuide-V1_0. URL:http://www.openmobilealliance.org

[PushMO] "Push Management Object". Open Mobile Alliance™. OMA-TS-Push_MO-V1_1. URL: http://www.openmobilealliance.org/

[PushMsg] "Push Message Specification". Open Mobile Alliance™. OMA-TS-Push_Message-V2_3. URL: http://www.openmobilealliance.org/

[PushOTA] "Push OTA Protocol Specification". Open Mobile Alliance™. OMA-WAP-TS-PushOTA-V2_3. URL:http://www.openmobilealliance.org/

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”. S. Bradner. March 1997. URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. URL:http://www.ietf.org/rfc/rfc2234.txt

[SIPPush] “Push using SIP”. Open Mobile Alliance™. OMA-TS-SIP_Push-V1_0. URL: http://www.openmobilealliance.org/

[TS23.041] "Technical realization of Cell Broadcast Service (CBS)". 3rd Generation Partnership Project (3GPP). URL:http://www.3gpp.org

[TS26.346] 3GPP “Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS)”. URL: http://www.3gpp.org

[UAPROF] "Wireless Application Group User Agent Profile Specification", Open Mobile Alliance™, OMA-UAProf-v2_0. URL: URL: http://www.openmobilealliance.org/

[UAProfSchema] OMA User Agent Profile Schema (latest), Open Mobile Alliance™, http://www.openmobilealliance.org/Technical/schemas.aspx

2.1 Informative References

[IANA] "Internet Assigned Numbers Authority", URL: http://www.iana.org/

[OMADICT] “Dictionary for OMA Specifications”, Open Mobile Alliance™, OMA-ORG-Dictionary, URL:http://www.openmobilealliance.org/

[OMNA] "OMA Naming Authority". Open Mobile Alliance™. URL: http://www.openmobilealliance.org/OMNA.aspx

3. Terminology and Conventions

3.1 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].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Application	An implementation of a related set of functions that perform useful work, often enabling one or more services [OMADICT]
Application-Level Addressing	the ability to address push content between a particular user agent on a client and push initiator on a server
Bearer Network	a network used to carry the messages of a transport-layer protocol between physical devices. Multiple bearer networks may be used over the life of a single push session.
Client	A device, user agent, or other entity that acts as the receiver of a service [OMADICT]
Contact Point	address information that describes how to reach a push proxy gateway, including transport protocol address and port of the push proxy gateway.
Content	Digitized work that is processed, stored, or transmitted. It includes such things as text, presentation, audio, images, video, executable files, etc. Content may have properties such as media type, mime type, etc [OMADICT]
Content Encoding	when used as a verb, content encoding indicates the act of converting a data object from one format to another. Typically the resulting format requires less physical space than the original, is easier to process or store, and/or is encrypted. When used as a noun, content encoding specifies a particular format or encoding standard or process.
Content Format	actual representation of content.
Device	Equipment which is normally used by users for communications and related activities. The definition can be extended to cover remote monitoring applications where there is no user present, but the communications to and from the remote monitor use the same communications channels as when used by users [OMADICT]
End-user	see "user"
Multicast Message	a push message containing a single address which implicitly specifies more than one OTA client address.
Point-to-Multipoint Push	Push content delivery to a group of users through the OTA-PTM Push-OTA protocol variant.
Push Access Protocol	a protocol used for conveying content that should be pushed to a client, and push related control information, between a Push Initiator and a Push Proxy/Gateway.
Push Client –Application Interface	A device-internal interface provided by Push Clients, via which Push applications can register for Push services with application-specified options, and receive notifications of Push events.
Push Framework	the entire push system. The push framework encompasses the protocols, service interfaces, and software entities that provide the means to push data to user agents in the client.
Push Initiator	An entity or service that initiates Push content delivery to Push clients [OMADICT]
Push OTA Protocol	a protocol used for conveying content between a Push Proxy/Gateway and a certain user agent on a client.
Push Proxy Gateway	a proxy gateway that provides push proxy services
Push Session	An active point-to-point transport protocol session over which push operations can be executed.

Push Whitelist	a list stored in the Terminal of PPG addresses and/or SMSC addresses that are authorised to push Content to the Terminal.
Registration	refers to a procedure where the PPG becomes aware of the terminal's current capabilities and preferences.
Registration Context	a state where the PPG is aware of at least the last capabilities and preferences conveyed from the terminal.
Server	An entity that provides resources to clients in response to requests [OMADICT]
Terminal	see "client".
Terminal-ID	an identifier that is used by a PPG to uniquely identify a terminal.
User	An entity which uses services. Example: a person using a device as a portable telephone [OMADICT]
User agent	Any software or device that acts on behalf of a user, interacting with other entities and processing resources [OMADICT]
WAP Push	Push content delivery to a specific user via the WAP1 (OTA-WSP) or WAP2 (OTA-HTTP) Push-OTA protocol variants.
XML	The Extensible Markup Language is a World Wide Web Consortium (W3C) standard for Internet markup language, of which WML is one such language [OMADICT]

3.3 Abbreviations

ABNF	Augmented Backus-Naur Form
BCAST	OMA Broadcast Services
CPI	Capability and Preference Information
CBS	Cell Broadcast Service
CSD	Circuit Switched Data
DNS	Domain Name Server
GPRS	General Packet Radio Service
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
MBMS	Multimedia Broadcast/Multicast Service
MSISDN	Mobile Station International Subscriber Directory Number
OMA	Open Mobile Alliance
OTA	Over The Air
OTA-HTTP	(Push) OTA over HTTP
OTA-SIP	(Push) OTA over SIP
OTA-HTTP-TLS	OTA-HTTP over TLS
OTA-PTM	(Push) OTA over Point-to-Multipoint
OTA-SIP	(Push) OTA over SIP
OTA-WSP	(Push) OTA over WSP

PDP	Packet Data Protocol
PDU	Protocol Data Unit
PI	Push Initiator
PO-TCP	PPG Originated TCP connection establishment method
PPG	Push Proxy Gateway
PTM	Point-to-Multipoint
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
SHA-1	Secure Hash Algorithm 1
SIA	Session Initiation Application
SIP	Session Initiation Protocol
SIR	Session Initiation Request
SMS	Short Message Service
SMSC	Short Message Service Centre
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TO-TCP	Terminal Originated TCP connection establishment method
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security

4. Introduction

The OMA Push architecture enables a Push Client to register for Push-based services on behalf of Push applications, and to subsequently deliver Push events to the Push application. The Push Client may use various over-the-air (OTA) protocols and data bearers in providing Push service.

Historically, Push Clients have been implemented as embedded software functions in mobile devices, with pre-defined support for specific Push applications, e.g. browsers, Multimedia Messaging clients, Instant Messaging clients, etc. The Push Client typically registers as needed on behalf of these pre-defined Push applications, and includes its capabilities on their behalf in the vendor-published User Agent Profile for the device. While this approach has supported well the growth of Push-based services for typical embedded Push applications, it does not support the dynamic enhancement of devices for new Push applications and services, e.g. through installation of downloadable applications and OMA service enabler clients.

This specification enables Push Clients to optionally offer a means for Push applications to register for Push services with application-specified options for the Push service, including:

- Providing an application name, which can be a unique identifier usable by OMA Push entities in service matching
- A Push Application ID, which associates the application with an OMNA-registered Push service type or an unregistered (proprietary) Push service type
- A specified application event handler for reception of Push events
- A selection of Push Servers (e.g. Push Proxy Gateways or Push Application Servers) from which the Push Client should request service and expect Push events
- Push protocols and data bearers to use for Push Client registration and Push event reception
- Push event addressing at the Push Client, via which the Push Client can be directed to receive Push events at standard or alternate ports for specific bearers
- A set of content types which the Push application is compatible with, which may be used by the Push Client to negotiate capabilities with a Push Server

This registration and event reception interface enables the dynamic extension of the OMA Push enabler to new applications and OMA service enablers as described above.

4.1 Version 1.0

Version 1.0 includes all of the functionality described in section 4.

4.2 Version 1.1

Version 1.1 includes functionality supporting Point-to-Multipoint Push, and support for the Push Service Registration procedure defined in [PushOTA].

5. Push Client - Application Interface (Push-CAI)

The term Push-CAI is used in this specification to refer to a generic interface defined as a set of functions and related data formats enabling the high-level capabilities described in section 4, which comprise overall:

- Push application registration with the Push Client, and subsequent deregistration if required
- Push Client delivery of Push events to the Push application

The Push-CAI is defined in an implementation-agnostic manner, since the implementation of the Push-CAI in specific devices will depend upon the application programming environments and runtime environments supported by the devices. Thus definition of a specific application programming interface (API) is out of scope for this specification. However to support the basic set of interface functionality called for in this specification, the Push-CAI makes the following assumptions about the interaction capabilities of the Push Client and Push applications:

- The Push Client supports some means of being invoked for registration of the Push application. This can be for example through a callable function or a service access point to which interface messages can be directed.
- The Push application, through the execution environment, supports some means of being invoked for Push event delivery from the Push Client. Similar to the Push Client registration function, the Push application may provide this through a callback function or a service access point to which interface messages can be directed.

5.1 Push Application Registration

Push applications register with the Push Client through delivery of an Application Registration request to the Push Client, and receiving an Application Registration response. The Application Registration may be successful or unsuccessful depending upon the Push Client's ability to handle the Push application's specified options.

Note: interface parameter data types given below are the recommended types for support by specific API implementations. Where no data type is given, the type is expected to be API implementation-specific.

The Push application must include the following parameters in the Application Registration request:

- pushApplicationID (string): an [OMNA] registered or unregistered (proprietary) Push Application ID to be associated with the Push application.

The Push application may include the following parameters as options in the Application Registration request:

- Application ID (anyURI): "name" of the application, recommended as a unique identifier in the form of a URI registered by the Push application developer.
- Event Handler: handler for incoming Push events, defined per the capabilities of the device execution environment and Push application preferences. May be unspecified if the device execution environment provides default mechanisms for Push event delivery to the Push application.
- Whitelist (structure): set of addresses from which Push events should be accepted per [PushMO]. If unspecified, the Push Client default whitelist (if any) is assumed to be compatible with the Push application.
- one of:
    - Push Service Registration URI (anyURI): the address where the Push Client should execute the Push Service Registration procedure [PushOTA], to receive applicable connection profile(s) for the Push service
    - Connection Profile (structure): one or more set of options for Push event delivery, including

- Protocol (string): one of “OTA-WSP”, OTA-HTTP”, “OTA-SIP”, “OTA-PTM”, or other implementation-specific value. If unspecified, the default supported protocols are assumed to be compatible with the Push application.
- Bearer Type (string): one of the Push-SupportedBearers defined in [UAProfSchema], or other implementation-specific value. If unspecified, the default supported bearers are assumed to be compatible with the Push application.
- Port (string): a specific port number appropriate for the protocol and bearerType. If unspecified, the default/standard port should be used. Note that the mechanisms for coordination of non-standard port usage are unspecified, e.g. are assumed to occur at the application layer.
- Contact Point (string): the expected source address of Push messages as applicable to the protocol, e.g. for OTA-WSP, OTA-HTTP, OTA-SIP, or OTA-PTM, the IP address, hostname, or URI of the PPG
- Cell BroadcastMessageId (string): for OTA-PTM with CBS bearer, the Cell Broadcast Message Identifier associated with Push messages [TS23.041]
- MBMS User Service Description: for OTA-PTM with MBMS bearer, a MBMS User Service Description element [TS26.346]
- BCAST Access Info: For OTA-PTM with BCAST bearer, a Bcast-Access-Info element [BCAST-SvcGuide]

- Accept (string): a set of MIME types of Push events which the Push application specifically requests subscription to.

The Push Client MUST reject an Application Registration indicating an already-registered Push Application ID, unless:

- the Application Registration is received from the same Push application, or
- the Push Client supports a mechanism to ensure uniqueness in Push application registration with the Push Server, and delivery of Push events intended for the specific Push application, e.g.
  - The OTA-SIP protocol is used. OTA-SIP provides a means to uniquely identify distinct Push applications supporting the same Push Application ID, via a media feature tag indentifying the specific application instance, e.g.
    - in IMS, via the IMS Application Reference Identifier (IARI), as described in [Push-OTA].
    - in non-IMS SIP networks, using the same feature tag name
  - The Push application is registered for event reception at a unique bearer port, by request of the Push application.
  - The Push application’s registration is associated with a specific binding to a Push bearer, e.g. a unique Push Service Registration address, or OTA-PTM over MBMS binding via a unique MBMS User Service Description element

The Push Client MUST reject an Application Registration with an option that is not supported or not currently available.

If it accepts the Application Registration request:

- The Push Client MUST respond to the Push application with an Application Registration response indicating registration was accepted (pending further processing, e.g. registration with a PPG), and
- If the Push application provided a Push Service Registration URI, the Push Client MUST initiate the Push Service Registration procedure [PushOTA]. By default, the Push Client MAY initiate the Push Service Registration procedure using a pre-configured Push Service Registration address.

- If the Push application provided a Connection Profile, the Push Client MUST initiate binding to the requested bearer as applicable, e.g.
    - register with the Push Server (e.g. Push Proxy Gateway, Push Application Server, or BM-SC) for the Push application, as applicable for the protocol and bearer, if supported directly by the Push Client . By default, the Push Client MAY register with a Push Server using a pre-configured connection profile.
    - directly bind to the bearer, if the connection profile indicates a bearer which the Push Client directly supports and for which binding can be completed by device-local action only.
    - bind via a bearer-specific client (e.g. CBS receiver, MBMS receiver, or BCAST client)

In registering with the Push Server, the Push Client MUST follow the procedures defined in [PushOTA] for the protocol and bearer, e.g.:

- use the applicable bearer for the Application Registration
- indicate the new Push Application ID
    - for OTA-HTTP, via the X-Wap-Push-Accept-AppID header provided in the terminal's CPI
    - for OTA-SIP, via inclusion as a Push Resource Identifier in
        - a SIP REGISTER request sent to update the registration with the SIP/IP Core
        - a SIP OPTIONS request sent to update the capabilities requested from the Push Server
- indicate the specified MIME types, if any, via inclusion in
    - for OTA-HTTP, the X-Wap-Push-Accept header provided in the terminal's CPI
    - for OTA-SIP, the SIP OPTIONS request sent to update the capabilities requested from the Push Server

If the local binding or registration fails for any reason, the Push Client MUST respond to the Push application with an Application Registration response indicating an applicable failure reason.

Upon successful completion of Application Registration, including actions taken a Push Server if required, the Push Client MUST respond to the Push application with an Application Registration response indicating registration was successful.

If it accepts an Application Registration containing a whitelist parameter, the Push Client MUST add the specified Push Servers to its current whitelist, for the specific Push application.

The Push Client MUST retain the details of the registration request for future reference in a deregistration process if required.

5.2 Push Application Deregistration

Push applications deregister with the Push Client through delivery of an Application Deregistration request to the Push Client, and receiving an Application Deregistration response. The Application Deregistration may be successful or unsuccessful depending upon validation of the request by the Push Client.

Note: interface parameter data types given below are the recommended types for support by specific API implementations. Where no data type is given, the type is expected to be API implementation-specific.

The Push application must include the following parameters in the Application Deregistration request:

- pushApplicationID (string): an [OMNA] registered Push Application ID that is associated with the Push application.

Note that for API implementations, the Push Application ID may be implicit in the way that the deregistration is requested, e.g. call of a deregister method on a registration object can implicitly refer to the Push Application ID used when the registration object was created.

The Push Client MUST reject an Application Deregistration request if it determines that the requesting Push application is not currently registered for events related to the Push Application ID.

If it accepts the Application Deregistration request, the Push Client MUST deregister with the Push Server (e.g. Push Proxy Gateway or Push Application Server) for the Push application if the applicable Push protocol supports explicit deregistration.

In deregistering with the Push Server, the Push Client MUST:

- use the applicable bearer for the Application Registration
- deliver an updated set of supported Push Application ID's, removing the Push Application ID associated with the deregistered Push application
    - for OTA-HTTP, via exclusion in the X-Wap-Push-Accept-AppID header provided in the terminal's CPI
    - for OTA-SIP, via exclusion as a Push Resource Identifier in
        - a SIP REGISTER request sent to update the registration with the SIP/IP Core
        - a SIP OPTIONS request sent to update the capabilities requested from the Push Server
- deliver an updated set of supported MIME types, if any, removing any MIME types that were solely associated with the deregistered Push application
    - for OTA-HTTP, in the X-Wap-Push-Accept header provided in the terminal's CPI
    - for OTA-SIP, in a SIP OPTIONS request sent to update the capabilities requested from the Push Server

Deregistration with the Push Server MUST NOT affect current registrations of other applications. Thus the actions above will be taken only if the deregistering application is the sole registered application of the type (by Push Application ID), or the sole registered application for specific MIME types.

If the registration had included an update to the Push whitelist, the Push Client MUST remove from the Push whitelist any Push Servers that were solely associated with the deregistered Push application.

If the Push Client accepts the Application Deregistration request and successfully deregisters with the Push Server (if required), the Push Client MUST respond to the Push application with an Application Deregistration response indicating deregistration success,

If the deregistration fails for any reason, the Push Client MUST respond to the Push application with an Application Deregistration response indicating an applicable failure reason,

5.3 Push Event Delivery

Push Clients deliver Push events to Push applications upon reception of the Push event from Push Server.

The Push Client MUST include the following parameters in the Push event:

- content: the Push content received in the Push event from the Push Server
- content-type: the MIME type of the Push content
- application-specific or standard HTTP headers, as received.

6. Security Considerations

Push Clients or the device runtime environment in which they execute MAY enforce unspecified security policies on Push registration requests. Unless such security policies are enforced, the Push Client MUST assume that the Push application is trusted and authorized to request registration with the OMA Push enabler. Note that further security policies may be applied by the network, e.g. Push Server.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-PushCAI-V1_1	22 Nov 2011	Status changed to Approved by TP: OMA-TP-2011-0406-INP_Push_V2_3_ERP_for_Final_Approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1 SCR for Push Client

Item	Function	Reference	Requirement
CAI-C-001-M	Push Application Registration	5.1	
CAI-C-002-M	Push Application Deregistration	5.2	
CAI-C-003-M	Push Event Delivery	5.3	
CAI-C-004-O	Security Considerations	6	