Push Security Requirements

Approved Version 1.0 – 09 Aug 2011

Open Mobile Alliance

OMA-RD-PushSecurity-V1_0-20110809-A

Contents

Figures

Tables

1. Scope (Informative)

The scope of this document is to identify the use cases pertinent to the security issues of WAP Push and then define the security requirements for the identified use cases.

2. References

2.1 Normative References

[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

[PPGService] Push Proxy Gateway Service, WAP Forum™, WAP-249-PPGService, URL:http://www.openmobilealliance.org/

[PushArch] Push Architectural Overview, WAP Forum™, WAP-250-PushArchOverview, URL:http://www.openmobilealliance.org/

[PushOTA] "Push OTA Protocol Specification", WAP Forum™, WAP-235-PushOTA, URL:http://www.openmobilealliance.org/

[PushPAP] "Push Access Protocol Specification", WAP Forum™, WAP-247-PAP, URL:http://www.openmobilealliance.org/

2.2 Informative References

[WAPARCH] "WAP Architecture". Open Mobile Alliance™. WAP-210-WAPArch. URL:http//www.wapforum.org/

[OMADictionary] Dictionary for OMA Specifications V3.0.0, URL:http://www.openmobilealliance.org/

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

Authentication	Authentication is the process of identifying the true identity of the entity in question by cryptographic means.
Client	In the context of push, a client is a device (or service) that expects to receive push content from a server. In the context of pull a client, it is a device initiates a request to a server for content or data.
Enroll	To register a subscriber to a service.
One Shot	One-shot is the instance of the user instructing the client to trust a PPG or PI for a single time upon receiving a push message from an untrusted PPG or PI.
Push Initiator	The entity that originates push content and submits it to the push framework for delivery to a user agent on a client.
Push Proxy Gateway	A proxy gateway that provides push proxy services.
Trusted PI	A PI can be called trusted if the questioning entity has successfully authenticated the PI.
Trusted PPG	A PPG can be called trusted if the questioning entity has successfully authenticated the PPG.

3.3 Abbreviations

ACL	Access Control List
Client	A mobile terminal
NAT	Network address translation
PAP	Push Access Protocol
PI	Push initiator
PPG	Push Proxy Gateway
SIR	Service Initiation Request

4. Introduction (Informative)

WAP Push technology allows the users of the service to be pushed data to their mobile clients. Initially a user will browse to a website that is hosted by the push initiator (PI); the PI will have a service(s) to offer the user. An example push service can be a local weather service where the PI pushes to the user's client a local weather report every morning.

The WAP Push architecture defines three entities, the Push Initiator (PI), the Push Proxy Gateway (PPG) and the client. When pushing connection-less (as described below) content to a user's client the PI interacts with a PPG using the Push Access Protocol [PushPAP], the PPG in turn compiles the Push message and sends it over the air (OTA) to the client.

The WAP Push security specifications currently do not satisfy the security needs of the various players in the industry that provide or wish to provide WAP Push services. It is therefore necessary to define the security requirements for the various use cases for WAP Push.

Ultimately the goal is to have a complete security chain between the Push Initiator (PI) and the client, so that the user is confident that she can receive push messages to her client from trusted sources.

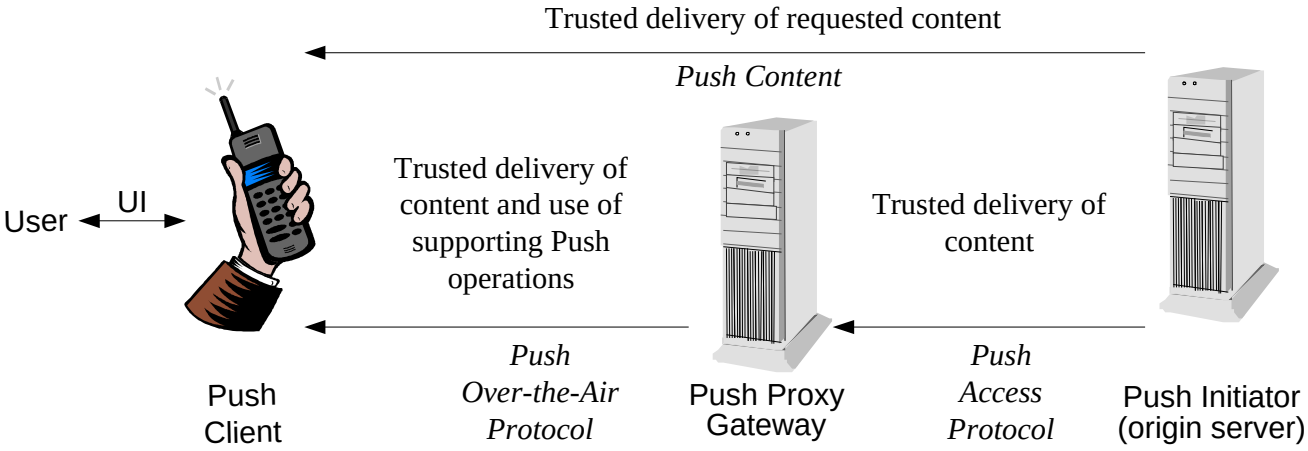


Figure 1: Push Framework

The diagram above shows the four entities within the WAP Push architecture. The security/trust relationships between these entities are a key aspect of Push security. These relationships, and the related key issues addressed herein are:

- The user *should* be able to trust that the PI will deliver content as requested from the PI. Currently this may not be the case.
- The user *should* be able to trust that the PPG will deliver content as requested from PI's and supporting Push-OTA operations, e.g. Session Initiation Request. Currently this may not be the case.
- The PI *should* be able to trust that the PPG will not modify Push content beyond the requirements of conversion to format required by the target push client and the Push-OTA protocol. Currently this may not be the case.

The interactions between the PI and the PPG will generally be sent over a connected oriented protocol e.g. HTTP and will be able to utilise established Internet security protocols such as SSL etc. to provide confidentiality, integrity and authentication. Interactions between the PPG and the client can be carried out in two ways:

- Connection-less Push
- Connection-oriented Push

Connection-less push can be carried out using OTA methods and are described in the Push OTA specification [PushOTA]. The most common interface for Push OTA is SMS. Currently, the push specifications do not address the security issues when using connection-less push.

It is assumed that when using connection oriented push the underlying security protocols for the respective bearers are utilised, e.g. if over HTTP then use SSL. However, issues such as NAT and terminals having public IP addresses will be looked at for security related issues.

4.1 Threat analysis

Explanation of the security risks:

- Unauthorized session initiation: attempt to cause a device to setup a Push session (via SIR [PushOTA]) to an unauthorized PPG. The intent of unauthorized session initiation can be to initiate one of the other attacks, to discover information about the user (information theft), or to spam the user.
- Since SIR [PushOTA] is typically delivered over SMS, the risk of unauthorized SIR delivery over an IP bearer is probably low, but this needs to be verified.
- Harmful content delivery: delivery of any content that disrupts the user's service or threatens the network. The intent of harmful content delivery can be service disruption, theft, to cause offence to the user or virus deployment. It can involve direct processing of the Push content on the device, or tricking the device/user into retrieving harmful content.
- Denial of service: repeated Push message delivery that disrupts the user's service. The intent of denial of service can be to harass a user, or annoy the user into switching network providers.
- Unauthorized Push: attempt to deliver Push content that has not been requested.

The following table shows a threat analysis evaluation for the different scenarios when using WAP Push.

High: Relatively simple to do, although may not be common. Ability of network to block is low.
Medium: Takes more work
Low: Difficult to realise, network measures easy to take.

Scenarios Type of Risk	Public IP Addresses	Private IP Addresses	PI Policy at Operator or Authorized 3rd party PPG		Network-Initiated Mobile Terminated SMS	Mobile Originated SMS
			Open	Access Controlled		
Unauthorized session initiation	Low	Low	None	None	High	High
Harmful content delivery	High	Medium	High	High to low (1)	High	High
Denial of service	High	Medium	High	High to low (1)	High	High
Unauthorized Push	High	Medium	High	High to low (1)	High	High

Table Notes:

1. Effective access controls can significantly reduce the risk.

Explanation of the scenarios:

- Public IP Device Addresses
    - The mobile network assigns public IP addresses to devices. The operator may provide a PPG or rely upon 3rd party PPGs.
- Private IP Device Addresses
    - The mobile network assigns private IP addresses to devices. The operator typically provides a PPG, since delivery of Push from 3rd party PPGs is complicated by private-to-public network address translation (NAT)
- Open PI Policy at Operator or Authorized 3rd party PPG
    - The PPG provides no special control over Push source, addressing, content types, or quality of service.
- Access Controlled PI Policy at Operator or Authorized 3rd party PPG
    - The PPG provides some level of access control over Push source, addressing, content types, or quality of service.
- Network-Initiated Mobile Terminated SMS
    - The Push messages are initiated by network-based SMS sources, which can include unsecured sources in another carrier's network. No specific controls are assumed per the SMS source, destination, or content.
- Mobile Originated SMS
    - Mobile devices initiate the Push messages. No specific controls are assumed per the SMS source, destination, or content.

5. Use Cases (Informative)

5.1 Actors & their specific issues

Push Initiator[1]

The Push initiator provides a service for the user and carries out the following functions:

- Enroll a user – The Service provides a mechanism for a user to enroll to a service
- Submit a push message to a client via a push proxy gateway.
- Ability to ask for notification, cancellation, replacement and status queries from the Push proxy gateway

The PI can be co-located with a PPG, enabling direct submission of a Push message to the client.

Push Proxy Gateway Operator[1]

A point of contact for the PI and is used to establish connectivity with the client as requested by the PI. The PPG has the following functions:

- Deliver Push content of various MIME types as requested by the PI, and Session Initiation Requests (SIR).
- Controls PPG service access and the Push features available to PI's.
- Ability to provide access control (PI authentication)
- Ability to respond to the PI with the result of the Push request
- Request a target device to establish a WAP session for connection-oriented Push message delivery
- Provide address resolution service

Note that PPG and PI can be co-located, enabling direct submission of a Push message to the client.

Wireless Network Operator

The wireless network operator will provide the following services:

- Ability to provision and pre-configure the client
- Controlling wireless network security

Client

A client is defined in the Push specifications [PushArch].

User

The user is defined in the Push specifications [PushArch]. The user is typically involved in the following scenarios:

- Sign up for a push service – User already in a browsing session and signs up for a service that utilises push (ability to form the trust relationship between the user and PI regardless if it is via the PPG or not)

[1] Note that PPG and PI can be co-located, enabling direct submission of a Push message to the client.

- Cancel a push service
- Refuse a push service
- Receive a push message from a service.
- Manage security decisions related to device settings and the services accessed.

5.2 Use Case A : Allow trusted PPGs and PIs to push content to a client over a connectionless or connection-oriented bearer

	Affected Areas				
	Device	**Connectivity**	**Enabling Services**	**Applications**	**Content**
Tickmarks (X)	X		X	X	
Additional Keywords					

Table 1: Affected Areas for Use Case A

5.2.1 Short Description

This use case describes the client behaviour upon receiving an unauthenticated push message.

5.2.2 Actors

Client, PPG and PI

5.2.2.1 Actor Specific Issues

As listed in section 5.1.

5.2.2.2 Actor Specific Benefits

Wireless Network Operator

Wireless operator benefits by being confident that subscribers are receiving content from sources they trust.

User

The user benefits so that now:

- Does not receive Spam/abusive messages
- The user can be confident that his phone is not vulnerable to attacks by untrusted PPG's or PI's sending active push messages to his client.
- The user can be confident that he will receive the service that he has subscribed to.

5.2.3 Pre-conditions

It is assumed that the client will have a pre-established security association with the PPG or PI so that it is able to authenticate the PPG or PI.

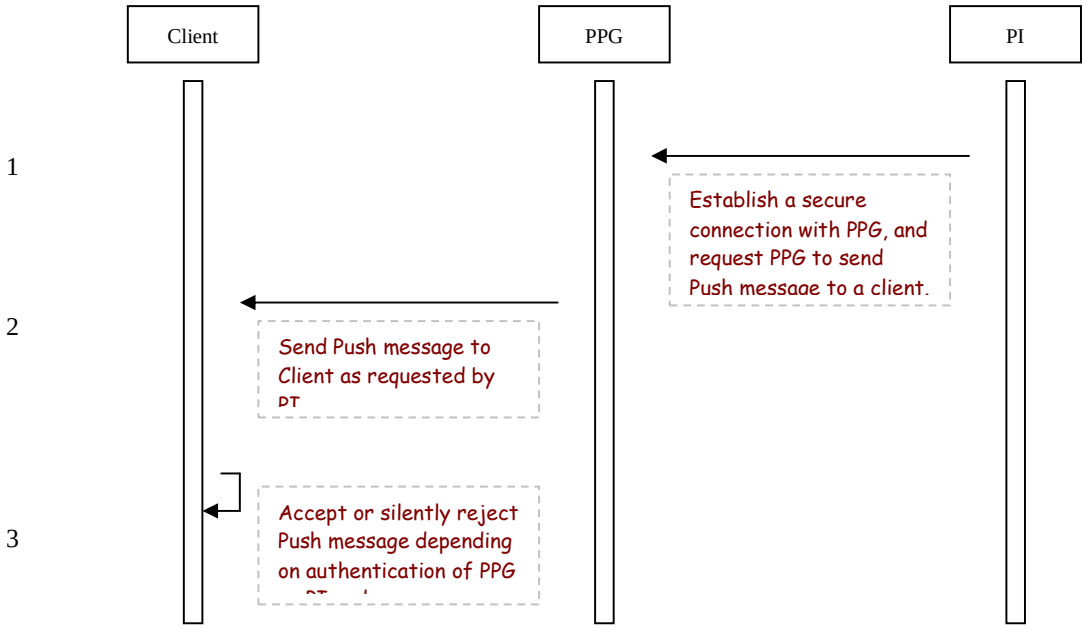
5.2.4 Post-conditions

Depending on the success of the authentication procedure, the client will decide to accept or silently reject an incoming push message.

5.2.5 Normal Flow

1. The PI establishes a (possibly secure[2]) connection with the PPG and requests it to send a connection-less Push message to a particular client.
2. The PPG compiles the push message as requested by the PI and pushes it to the client.
3. The client accepts or silently rejects the push message based on its trust relationship with the PPG or PI.

Sequence diagram for use case:



5.2.6 Alternative Flow

None

5.2.7 Operational and Quality of Experience Requirements

None.

[2] A secure connection refers to the security of the underlying protocol that PAP is running over e.g. if over TCP/IP then SSL can be used.

5.3 Use Case B: Allow users to decide whether a PPG or PI can be trusted to deliver content to their client

	Affected Areas				
	Device	**Connectivity**	**Enabling Services**	**Applications**	**Content**
Tickmarks (X)	X		X	X	
Additional Keywords					

Table 2: Affected Areas for Use Case B

5.3.1 Short Description

When users sign up for new Push-enabled services, they may need to update client-based Push access controls. Clients should support the easy update of Push access controls, e.g. via a menu available from the Client browser while in the browser session.

5.3.2 Actors

User, client and PI

5.3.2.1 Actor Specific Issues

As listed in section 5.1.

5.3.2.2 Actor Specific Benefits

User

The user benefits by having the flexibility of being able to choose a service from a PI he wishes.

5.3.3 Pre-conditions

It is assumed that the user does not already have a provisioned trusted PPG or PI on his client that will deliver the Push content that the user wishes to subscribe the service from.

5.3.4 Post-conditions

A new PPG or PI security relationship is added to the client so that the PPG or PI can authenticate itself to the client when sending push messages..

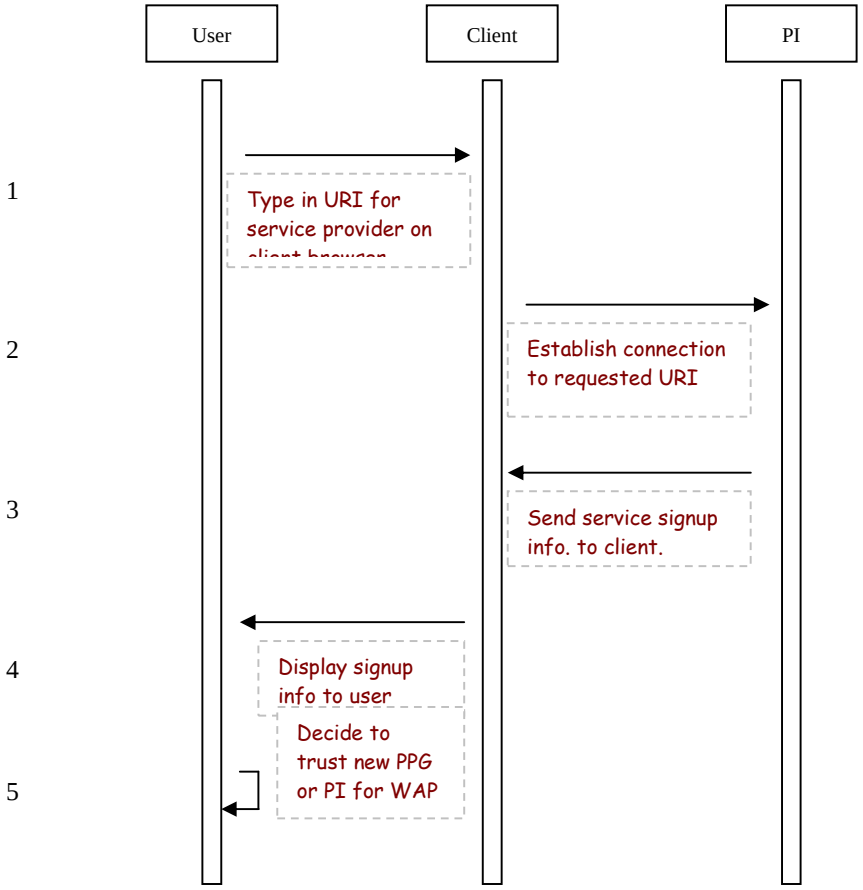
5.3.5 Normal Flow

1,2 & 3. The user initiates the client to connect to a PI to signup for a service.

4. The client displays the signing up information to the user. The signup information may include relevant details necessary to configure the client or enable access via the PPG or information directly from the PI.

5. The user decides whether to reject or accept the service. By accepting the service, a trust relationship can be established between the client and the PPG or the PI.

Sequence diagram for use case:



5.3.6 Alternative Flow

None.

5.3.7 Operational and Quality of Experience Requirements

None.

5.4 Use Case C: Allow users and operators to edit the trusted PPG/PI list

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X		
Additional Keywords					

Table 3: Affected Areas for Use Case C

5.4.1 Short Description

To allow flexible management of Push access controls, Clients should allow the user, wireless network operator, or other authorised Client management entity to define that Push sources are allowed to Push to the Client.

5.4.2 Actors

User, client and wireless operator.

5.4.2.1 Actor Specific Issues

As listed in section 5.1.

5.4.2.2 Actor Specific Benefits

User

- The user has the benefit of setting authorisation controls upon the trusted PPG's or PI's.
- The user has the benefit of editing the trusted PPG or PI list.

Wireless network operator

- The wireless network operator has the ability to update and modify the clients Push settings upon request of the user

5.4.3 Pre-conditions

User wants to update or edit his trusted PPG or PI list.

User is receiving unwanted content via (one of) the PPGs or PIs that he has on his trusted list, or the user is not receiving push content that he is supposed to receive from his trusted PPGs or PIs.

User wants the wireless network operator to update or edit the trusted PPG or PI list on the client.

There needs to be a user friendly identifier for identifying a PPG or PI ID stored on the client.

There needs to be a secure connection between the operator and the client.

5.4.4 Post-conditions

User can successfully update or edit the trusted PPG or PI list.

Wireless network operator can successfully update or edit the trusted PPG or PI list upon the request of the user.

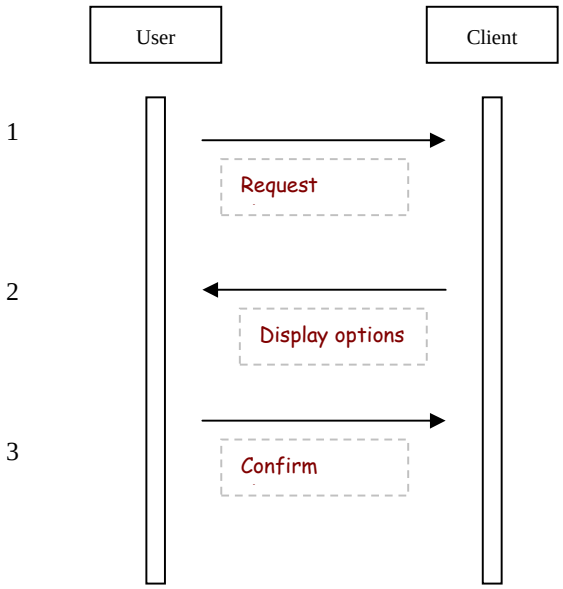
5.4.5 Normal Flow

1. The user scrolls through the options on the client to display edit options for his trusted PPG or PI list.
2. The client displays the options available to the user for each PPG or PI. The following options are displayed to the user for each PPG or PI in the list:
   - Always trust(PPG or PI is always trusted)
   - Always ask (The client will prompt the user for permission when a push message is sent from this PPG or PI)
   - Delete (Delete the PPG or PI)

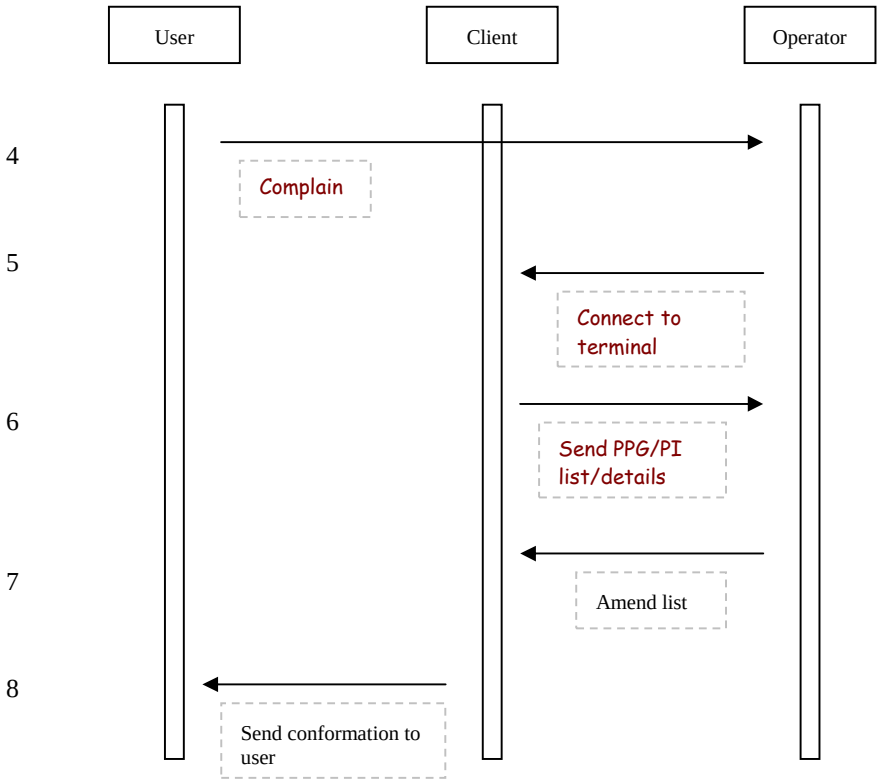
   The user chooses one of the options.
3. The user confirms changes.

Customer care scenario (5.4.5a)

4. The user calls the customer care of the operator because he is receiving unwanted content via the PPGs or PIs that he had on his trusted list or not receiving push content that he was supposed to receive from the trusted PPG or PI.
5. The operator makes a connection to the client (this will have to take place over a secure channel).
6. The client sends the trusted PPG or PI list to the operator.
7. Operator updates the client and provisions it either with a default list or deletes the appropriate PPG or PI.
8. The client sends a confirmation to the user that the list has been updated.



Customer care scenario (5.4.5b)



5.4.6 Alternative Flow

None

5.4.7 Operational and Quality of Experience Requirements

None

6. Requirements

6.1 High-Level System Requirements (Normative)

REQ-1	It SHALL be possible for the client to authenticate the PPG or PI as the originator of a WAP push message (from use cases in sections 5.2.1/2).
REQ-2	The client SHALL silently reject all push messages in which neither the PPG nor the PI is authenticated
REQ-3	The client MAY accept push messages from an unauthenticated PPG if instead a security association exists between the client and the PI, and the PI is authenticated in the push message.
REQ-4	The user MUST be able to manage the relationship with PPGs and PIs in order to control the Push services.
REQ-5	The user MAY be able to edit a trusted PPG or PI list. The following options MUST be made available to the user: (Note: The term trusted "trusted PPG or PI list" is not intended to imply or restrict the technical solution(s) to these requirements) 1. To trust the PPG or PI, but user prompting required for each Push Message 2. To trust the PPG or PI, user prompting not required 3. Delete PPG or PI Note: It is suggested that the default option when adding a new PPG/PI be set to 1.
REQ-6	All device management exchange between the client and the wireless network operator MUST be authenticated and, integrity protected. Device management exchanges between the client and wireless network operator MAY be confidentiality protected. (Use case 5.4.5b).

Table 4: High-Level System Requirements

6.1.1 Security

REQ-7	The security mechanisms SHALL prevent or limit common protocol attacks such as: ▪ PPG/PI address spoofing ▪ Replay attacks ▪ Denial of service attacks

Table 5: High-Level System Requirements – Security Items

6.1.2 Charging

None

6.1.3 Administration and Configuration

REQ-8	It MUST be possible for the user to efficiently and easily set up a security association with the PPG or PI in a user-friendly way.

Table 6: High-Level System Requirements – Administration Items

6.1.4 Usability

REQ-9	Client controls for and behaviour for PPG or PI trust management SHOULD NOT impact the usability of WAP devices. Client controls for PPG or PI trust management MUST be configurable such that users can lower the level of intrusiveness, or disable intrusive messages.

Table 7: High-Level System Requirements – Usability Items

6.1.5 Interoperability

None

6.1.6 Privacy

None

6.2 System Elements (Informative)

Push Security requirements should be addressed within the current Push Architecture framework [PushArch]. In summary the PI is typically an application that runs on an ordinary web server. It communicates with the PPG using the Push Access Protocol (PAP) over HTTP. The PPG [PPGservice] uses the Push Over-The-Air (OTA) Protocol to deliver the push content to the client. Figure 1 illustrates the Push Framework.

PAP [PushPAP] is based on standard Internet protocols; XML is used to express the delivery instructions, and the push content can be any MIME media type.

As mentioned, the PPG is responsible for delivering the push content to the client. In doing so it potentially may need to translate the client address provided by the PI into a format understood by the mobile network, store the content if the client is currently unavailable, etc. The PPG does more than deliver messages. For example, it may notify the PI about the final outcome of a push submission and optionally handle cancellation, replace, or client capability requests from the PI.

The Push Over-The-Air (OTA) [PushOTA] protocol is the part of the Push Framework that is responsible for transporting content from the PPG to the client and its user agents. It is designed to run on top of HTTP (OTA-HTTP), WSP (OTA-WSP), or other protocols (as yet unspecified)

6.2.1 Push Proxy Gateway

The Push Proxy Gateway (PPG) is the entity that does most of the work in the Push framework. Its responsibilities include acting as an access point for content pushes from the Internet to the mobile network, and everything associated therewith (authentication, address resolution, etc).

As the PPG is the entry point to a mobile network, it may implement network access-control policies about who is able to gain access to the network, i.e. who is able to push content and who is not, and under which circumstances, etc.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
Approved Version: OMA-RD-PushSecurity-V1_0-20110809-A	09 Aug 2011	Status changed to Candidate by TP: OMA-TP-2011-0282-INP_Push_V2_2_ERP_for_Final_Approval