Specification Information Note

WAP-235_101-PushOTA-20020612-a

Version 12-Jun-2002

for

Wireless Application Protocol
WAP-235-PushOTA-20010425-a
Push OTA Protocol
Version 25-Apr-2001

A list of errata and updates to this document is available from the WAP Forum™ Web site, http://www.wapforum.org/, in the form of SIN documents, which are subject to revision or removal without notice.

This document is available online in PDF format at http://www.wapforum.org/.

Known problems associated with this document are published at http://www.wapforum.org/.

Comments regarding this document can be submitted to the WAP Forum™ in the manner published at http://www.wapforum.org/.

Contents

1. Scope

This document provides changes and corrections to the following document files:

- WAP-235-PushOTA-20010425-a

It includes changes from the following change requests:

- CR-WAP-235-PUSHOTA-20010425-A-PUSHDC-20020206
- CR-WAP-235-PUSHOTA-20010425-A-ERICSSON-20020404
- CR-WAP-235-PUSHOTA-20010425-A-ERICSSON-20020605

2. Notation

In the subsections describing the changes new text is underlined. Removed text has marks. The presented text is copied from the specification. Text that is not presented is not affected at all. The change descriptions may also include editor's notes similar to the one below. The notes are not part of the actual changes and must not be included in the changed text.

Editor's note: Framed notes like these only clarify where and how the changes shall be applied.

3. X-WAP-CPITAG Header Value and Minor Clarifications

3.1 Change Classification

Class 2 – Bug Fixes

3.2 Change Summary

- A reference is added to the end of section 7.2.5.2 for clarification.
- The value of the `X-Wap-CPITag` header is an octet string, which may contain values with special meanings in HTTP (e.g. LWS, CR and LF). This header value must be encoded to avoid that it is parsed incorrectly; base64 is selected for this purpose.
- The `algorithm` parameter in RFC 2617 defaults to MD5. Since SHA-1 is used in the affected specification, the aforementioned parameter cannot be left out; it must be explicitly set to SHA-1.
- Section 8.4 is changed to reflect the change of the `X-Wap-CPITag` header value.

3.3 Change Description

Editor's note: On page 23

7.2.5.2. Registration Validation

[...]

In contrast, if the assumed CPITag does not match the terminal's current CPITag, the terminal SHOULD silently discard the message body of the request (i.e. the push content). If the message body is discarded, the terminal MUST convey its CPITag to the PPG by including the `X-Wap-CPITag` header in the response. If it accepts the message body it SHOULD include the `X-Wap-CPITag` header in the response (see also the introduction to section 7.2.5 for additional explanation on CPI information lookup using the CPITag during registration validation).

[...]

Editor's note: On page 24

7.2.5.3. The X-Wap-CPITag Header

[...] The ABNF [RFC2234] format of the header is:

```
X-Wap-CPITag = "X-Wap-CPITag" ":" CPItag
CPItag = *OCTET
```

The `CPItag` value is a four octet truncated hash of the CPI encoded using base64, and MUST be computed as follows:

- concatenate all CPI header (see section 7.2.5.5) values that are sent in the response
- apply a hashing algorithm that generates at least a four octet hash on the concatenated value. The SHA-1 [SHA] algorithm is RECOMMENDED.
- use the first four octets of the output
- generate the `CPITag` by base64-encoding these four octets

[...]

Editor's note: On page 29

7.2.6.2.2.1. X-Wap-Authenticate Header

[...]

- `algorithm` MUST be "SHA-1"

[...]

7.2.6.2.2.2. X-Wap-Authorization Header

[...]

- `algorithm` MUST be "SHA-1"

[...]

Editor's note: On page 39

8.4. SIA Content Based Protocol Data Unit

[...]

The CPITag field is used to convey a list of CPITags assumed to be valid by the PPG. Each CPITag is represented by the 4 octets (non-encoded, i.e. not encoded using base64) previously sent from the terminal to the PPG in the `X-Wap-CPITag` header (see section 7.2.5.3). The first element in the list of CPITags is interlinked with the first contact point specified in the *Contact Points* field for which the *ProtOpts* identifier indicates that the CPITag is present, the second element in the list of CPITags is interlinked with the second contact point for which the *ProtOpts* identifier indicates that the CPITag is present, and so on. [...]

4. Port Numbers

4.1 Change Classification

Class 2 – Bug Fixes

4.2 Change Summary

- References to the WDP specification are added.
- Port number usage when PO-TCP and TO-TCP are used is amended/clarified.

4.3 Change Description

Editor's note: On page 17

6.2.1 Connectionless Push

The connectionless push must be performed through WSP S-Unit-Push [WSP], which is one of WSP connectionless session service primitives. Two registered WDP ports [WDP], secure and non-secure ports, are reserved in every client capable of connectionless push.

[...]

6.2.2 Connection-Oriented Push

[...]

The push session can use either secure or non-secure transport services. Server-side port numbers are reserved in [WDP] for both options. WTLS MUST be used if the secure transport service is required. The secure transport service is required if either the port number in a contact point is a registered secure port [WDP] or the secure transport is indicated in a pre-existing list of contact points for PPGs.

Editor's note: On page 21

7.2.4.1.1 The TO-TCP Method

This method allows a TCP connection established by the terminal towards the PPG to be used as the active TCP connection (this implies that the terminal must be prepared to receive HTTP requests on this connection). The destination port (in order of precedence) is:

- a port specified in SIR (if present)
- a provisioned port (if so provisioned), or another port agreed by some implementation specific means
- one of the registered push ports (non-secure/secure)

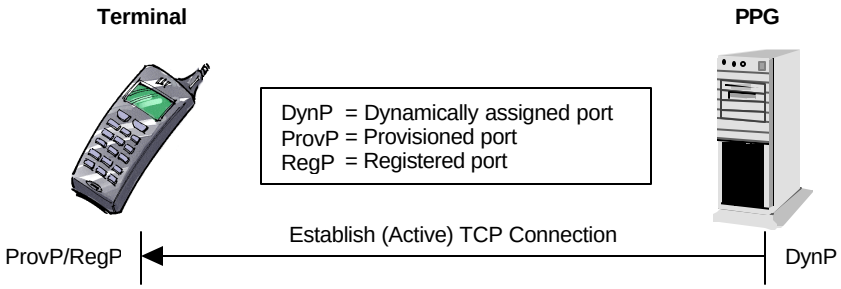
[...]

7.2.4.1.2 The PO-TCP Method

This method assumes that the terminal has IP connectivity with the network (or that the PPG can initiate the IP connectivity establishment procedure via the network), and its IP address is known by the PPG. A TCP connection established by the PPG towards the terminal is used as the active TCP connection. The destination port (in order of precedence) is:

- a provisioned port (if so provisioned), or another port agreed by some implementation specific means
- one of the registered push ports (non-secure/secure)
-

Editor's note: Replace figure 6 on page 21 with the following one:



[...]**Editor's note:** On page 40

Appendix A. Static Conformance Requirements (Normative)

A.1 Client/Terminal Features

Item	Function	Reference	Status	Requirement
OTA-CL-C-002	Non-secure Port for connectionless push	0	M	WDP-RP-C-001
OTA-CL-C-003	Secure Port for WTLS for connectionless push	0	O	OTA-CL-C-001 AND WDP-RP-C-002 AND WTLS:MCF AND WTLS:WTLS-C007

Editor's note: On page 42

A.2 Server/PPG Features

Item	Function	Reference	Status	Requirement
OTA-WSP-S-003	Use non-secure transport service	0	O	WDP-RP-S-004
OTA-WSP-S-004	Use secure transport service with WTLS	0	O	WDP-RP-S-006 AND WTLS:MCF

5. AUTH-PARAM Directive

5.1 Change Classification

Class 2 – Bug Fixes

5.2 Change Summary

Section 7.2.6.2.2 is not in line with the extension mechanism specified in RFC 2617 since it only specifies possible parameter values, but no parameter name as required by the mentioned RFC. This change introduces the `x-wap-auth-status` parameter name.

5.3 Change Description

Editor's note: On page 28

7.2.6.2.2 Terminal Authentication

[...]
If the terminal does not accept the challenge sent by the PPG it MUST respond with status code 412 "Precondition Failed" and include an `auth-param` directive [RFC2617] in the `X-Wap-Authorization` header with the following ABNF [ABNF] definition:

```
x-wap-auth-status = "x-wap-auth-status" "=" x-wap-auth-status-value

x-wap-auth-status-value = "failed_retry" | "failed_noretry"
```

The token "`failed_retry`" indicates that the PPG MAY retry the request by sending the `X-Wap-Authenticate` header anew. If the field is set to "`failed_noretry`", the PPG MUST NOT re-send the `X-Wap-Authenticate` header.

If the PPG does not accept the credentials supplied by the terminal it MUST re-send the request and include the `X-Wap-Authenticate` header with the `x-wap-auth-status` field value set to the token "`failed_retry`" or "`failed_noretry`". The token "`failed_retry`" indicates that the terminal MUST either retry to authenticate itself by re-sending the `X-Wap-Authorization` header or terminate the connection with the PPG. If the field is set to "`failed_noretry`", the terminal MUST terminate the connection.