Standardized Connectivity Management Objects
WAP Proxy Parameters

For use with OMA Device Management

Approved Version 1.0 – 24 Oct 2008

Open Mobile Alliance

OMA-DDS-DM_ConnMO_WAPProxy-V1_0-20081024-A

Contents

Figures

Tables

1. Scope

1.1 Connectivity Object – WAP Proxy

This document defines WAP Proxy specific parameters that are used together with the standardized connectivity management object [CONNMO] in order to have a complete standardized Proxy management object for WAP Proxy in the OMA DM management tree.

While this WAP Proxy object is optional for any OMA DM implementation, their widespread use will simplify the management of basic WAP Proxy parameters in mobile terminals.

The object is defined using the OMA DM Device Description Framework [DMTND]. The object has standardized points of extension to permit implementation-specific parameters to accompany the standardized parameters. This added flexibility is intended to encourage the use of the standardized object while not unnecessarily restricting individual vendor innovations.

2. References

2.1 Normative References

[CONNMO] *Standardized Connectivity Management Objects, Version 1.0,* Open Mobile Alliance™, OMA-DDS-DM_ConnMO_V1_0-D, URL:http://www.openmobilealliance.org

[DMTND] *Device Management Tree and Description, Version 1.2*, Open Mobile Alliance™, OMA-TS-DM-DMTND-V1_2, 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

2.2 Normative Authorities of Reference

Various parameters specified in the management objects defined in this document rely on an authority outside the scope of this specification to supply the set of acceptable values and value formats. In such references to external authority, only the directly cited material is referenced, not the entire external specification. The following authorities of reference are cited in this document:

[E2ESEC] *"WAP Transport Layer E2E Security Specification",* WAP Forum, WAP-187-TransportE2Esec, URL: http://www.openmobilealliance.org

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

[RFC791] *"Internet Protocol",* Postel, J., September 1981, URL:http://www.ietf.org/rfc/rfc791.txt

[RFC2373] *"IP Version 6 Addressing Architecture",* Hinden, R and S. Deering, July 1998, URL:http://www.ietf.org/rfc/rfc2373.txt

[RFC2396] *"Uniform Resource Identifiers (URI): Generic Syntax",* T.Berners-Lee, et al., August 1998,URL: http://www.ietf.org/rfc/rfc2396.txt

[RFC2617] *RFC2617, HTTP Authentication: Basic and Digest Access Authentication,* URL; http://www.ietf.org/rfc/rfc2617.txt

[AUTH-RFC3513-ADDR] *RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture*, §§2.2, 2.3 The Internet Society, 2003, URL:http://www.ietf.org/rfc/rfc3513.txt

2.3 Informative References

N/A

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

See the DM Tree and Description [DMTND] document for definitions of terms related to the management tree.

3.3 Abbreviations

ME	Mobile Equipment
OMA	Open Mobile Alliance

4. Introduction

Usually over time network protocols grow and are replaced as the market cycle plays out. Connectivity Management Object [CONNMO] is structured in such a way as to be resilient to the addition of new bearer and proxy types without requiring wholesale replacement of the object definitions. In this way, the common structure survives into future versions of the management objects thus easing the burden of transition from old bearer types to new.

This document specifies WAP Proxy specific part of the general Proxy management object and it also allows for vendor specific extensions.

5. Justification

This Reference Release includes several Management Object definitions for use, in conjunction with the OMA Device Management Enabler, to manage data network connectivity settings for mobile terminals over common bearer and proxy types.

5.1 Standardized Connectivity Management

Providing a standardized set of management objects for configuration of data network connectivity through the OMA Device Management system will improve the usability and customer experience of mobile terminals that rely upon data services. As proposed, the management object definitions may be used in conjunction with OMA Device Management Candidate and Approved Enabler Releases over a variety of transports including: HTTP, HTTPS, OBEX over IrDA, OBEX over Bluetooth, and various forms of Smart Card.

5.2 Application-Neutral

Producing these management object definitions in an application-neutral fashion, we avoid reinvention of solutions to the same set of problems for each of new application that requires data connectivity. This reduces the connectivity parameters that an application must define to a simple reference node, ConRef (Connectivity Reference).

5.3 Bearer-Neutral

By presenting the specifications in two parts, a bearer-neutral part and bearer-specific bindings, we reinforce the OMA principle of network neutrality while providing specificity where needed but without bias for or against any particular network type.

6. WAP Proxy Specific Management Object

6.1 Introduction

A general introduction of the connectivity management object is given in the connectivity management object document [CONNMO] as well as the needed compliance rules. This document specifies the WAP Proxy specific subtree that is placed under the general Proxy management object in order to enable the WAP Proxy specific parameter manipulation.

6.2 Definitions realated to Proxy MO

The WAP proxy subtree specified in this document MUST be placed under the ProxyParams node in [CONNMO].

ProxyType

The *ProxyType* node value specified in [CONNMO] MUST be "WAP".

AddrType

The AddrType value in the NAP MO specified in [ConnMO] MUST be from the table below:

AddrType	**Description**
IPv4	An IPv4 address [AUTH-RFC791] represented in string form dotted-decimal CIDR notation (default)
IPv6	An IPv6 address represented in string form as in [AUTH-RFC3513-ADDR]

Table 1: Proxy Address Types

AuthType

When the WAP Proxy acts as an HTTP Proxy, the AuthType value in the NAP MO specified in [ConnMO] MUST be from the table below:

AuthType	**Description**
HTTP-BASIC	HTTP basic authentication done according to [RFC2617]
HTTP-DIGEST	HTTP digest authentication done according to [RFC2617]

Table 2: Proxy Authentication Protocol Types

6.3 Graphical Representation (Informative)

The following figure provides the structure of WAP Proxy specific parameter sub-tree.

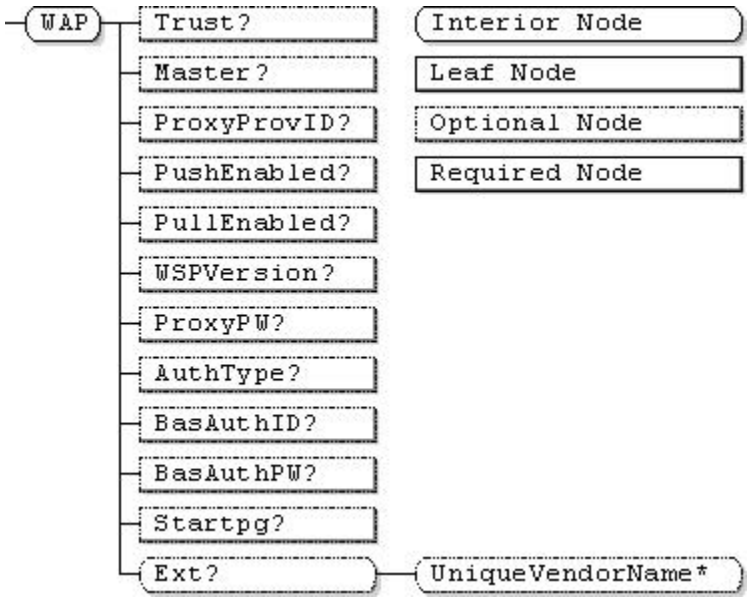

Figure 1. WAP Proxy specific parameters

6.4 Node descriptions

…/ProxyParams/WAP

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node specifies the WAP Proxy specific management object for a *Proxy* management object. Management Object Identifier for the WAP MO MUST be: “urn:oma:mo:oma-connmo-wap:1.0”.

WAP/Trust

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

The Trust leaf node can be used to define that a particular proxy is trusted. If the value is “True” then this proxy is trusted. If the value is “False” or this node does not exist then this proxy is not trusted. For example, provisioning information received from the trusted proxy can be accepted. Note that it is possible that the user does not have a trusted proxy. The trusted proxy does not have to be the home (default) proxy.

WAP/Master

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If the leaf node is “True” a particular proxy is allowed to send navigation documents to the device, using the Proxy Navigation Mechanism defined in [E2ESEC].

ProxyProvID

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The ProxyProvID leaf node is used to verify the identity of a proxy when using certificate based server authentication. If server certificate authentication is used, and the ProxyProvID has been defined, then service credentials of the certificate MUST match the ProxyProvID. The format MUST be either a fully qualified Internet domain name (i.e. hostname as defined in section 3.2.2 of [RFC2396]) or a globally unique IP address (IPv4 [RFC791] in decimal format with dots as delimiters or IPv6 [RFC2373], as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters).

PushEnabled

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If the value is “True”, then this proxy will support push. The ME is consequently advised to enable push. If the value is “False” or not present then this proxy will not support push.

PullEnabled

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If the value is “True” then this proxy will support pull. If the value is “False” or not present then this proxy will not support pull.

WSPVersion

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The WSPVersion indicates the WSP encoding version that the proxy in question supports. The format of this parameter is an integer representing the major version number followed by a “.” and an integer representing the minor version number.

ProxyPW

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	No Get

The ProxyPW indicates the authentication password for the proxy. ProxyId [CONNMO] and ProxyPW are used as authentication parameters for push proxy authentication to the client.

AuthType

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The AuthType parameter links the ProxyID [CONNMO] and ProxyPW to an authentication method. Possible values are "HTTP-BASIC" and "HTTP-DIGEST" [PushOTA].

BasAuthID

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The BasAuthID indicates the basic authentication identifier for the startpage.

BasAuthPW

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	No Get

The BasAuthPW indicates the basic authentication password for the startpage.

Startpg

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The Startpg value MUST be an absolute URI [RFC2396] and defines the homepage or start page associated with the services accessible from the proxy. The Startpg MAY be used to provide different services to different users. If the scheme is missing from the Startpg parameter, then “http” is assumed.

Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node designates a branch of the Proxy parameters sub-tree into which vendor extensions MAY be added, permanently or dynamically. Ext sub trees, such as this one, are included at various places in the DM connectivity management objects to provide flexible points of extension for implementation-specific parameters. However, vendor extensions MUST NOT be defined outside of one of these `Ext` sub-trees.

Ext/UniqueVendorName

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node is supplied by a vendor to distinguish their extension from those of other vendors. The *UniqueVendorName* SHOULD be a trademark or company name controlled by each vendor to ensure uniqueness. The structure of any sub-tree below a *UniqueVendorName* interior node is implementation-specific.

7. Operational Considerations

ConnMO is normatively dependent on the DM 1.2 specifications. However, this normative dependency should not be seen as restricting these MO definitions only to DM clients implementing that version of the DM enabler.

For example, a management authority may exchange ConnMO data-files using means not specifically defined in the DM 1.2 enabler.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-DDS-DM_ConnMO_WAPProxy-V1_0-20081024-A	24 Oct 2008	Approved by OMA Technical Plenary: Ref TP#: OMA-TP-2008-0405-INP_ConnMO_V1_0_RRP_for_Notification_and_Final_Approval