OMA Device Management Notification Initiated Session

Candidate Version 1.3 – 25 May 2010

Open Mobile Alliance

OMA-TS-DM_Notification-V1_3-20100525-C

Contents

Figures

1. Scope

This document specifies the OMA Device Management Notification Initiation package from the DM Server to the DM Client. A DM Server can use this notification capability to cause the DM client to initiate a connection back to the DM Server.

2. References

2.1 Normative References

[DMNoti12] "OMA Device Management Notification Initiated Session, Version 1.2", Open Mobile Alliance™. OMA-TS-DM_Notification-V1_2.
URL:http://www.openmobilealliance.org

[DMSTDOBJ] "OMA Device Management Standardized Objects, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_StdObj-V1_3.
URL:http://www.openmobilealliance.org

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.9, Open Mobile Alliance™, OMA-IOP-Process-V1_9,
URL:http://www.openmobilealliance.org

[ISO8601] "Data elements and Interchange formats -- Information interchange -- Representation of dates and times" , ISO 8601:2004,
URL:http://www.iso.org/

[PushOTA] "Push Over The Air", Open Mobile Alliance™, OMA_TS-PushOTA-V2_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

[RFC3174] "US Secure Hash Algorithm 1 (SHA1)", Network Working Group. September 2001.
URL:http://www.ietf.org/rfc/rfc3174.txt

[RFC5234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. January 2008.
URL:http://www.ietf.org/rfc/rfc5234.txt

[RFC5627] "Obtaining and Using Globally Routable Agent URIs (GRUUs) in the Session Initiated Protocol (SIP)". J. Rosenberg. October 2009.
URL:http:www.ieft.org/rfc/rfc5627

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

[SYNCOBEXBinding] "SyncML OMA Device Management OBEX Binding Specification", Open Mobile Alliance™, OMA-TS-SyncMLDM_OBEXBinding-V1_23,
URL:http://www.openmobilealliance.org

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.7, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7,
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.

Any reference to components of the DTD’s or XML snippets is specified in this “`typeface`.”

3.2 Definitions

Device	see [OMADICT]
Notification Message	Message sent from the DM Server to DM Client to alert DM Client to initiate a DM session back for management purpose.

3.3 Abbreviations

DM	Device Management
IANA	Internet Assigned Numbers Authority
OMA	Open Mobile Alliance

4. Introduction

Many devices cannot continuously listen for connections from a management server. Other devices simply do not wish to "open a port" (i.e. accept connections) for security reasons. However, most devices can receive unsolicited messages, sometimes called "notifications". Some handsets, for example, can receive SMS messages. Other devices may have the ability to receive other, similar datagram messages.

A DM Server can use this notification capability to cause the DM Client to initiate a connection back to the DM Server. This connection might be over HTTP, WAP, SIP or another transport protocol.

The notification message needs to contain authentication information for the server who sent this notification. The result of receiving such a notification would be for the DM Client to initiate a connection to the DM Server that sent the alert. In this scenario, the DM client needs to verify that this DM Server is among those authorized servers to request such activity.

5. Server Alerted Management Session

This notification message is intended to provide a possibility for the DM Server to alert the DM Client to initiate a management session. Within the notification message the DM Server can tell the DM Client the protocol version and whether the server proposes the session to be a foreground (user interaction) or background (not visible to the end-user) event. It can also tell if the session is happening because server has some management actions to perform or if the user caused the start of the session. The server MUST also send a digest within the notification message that is included to prevent any Denial of Service (DoS) attacks.

Figure 1 describes the message flow how the server alerts management session.

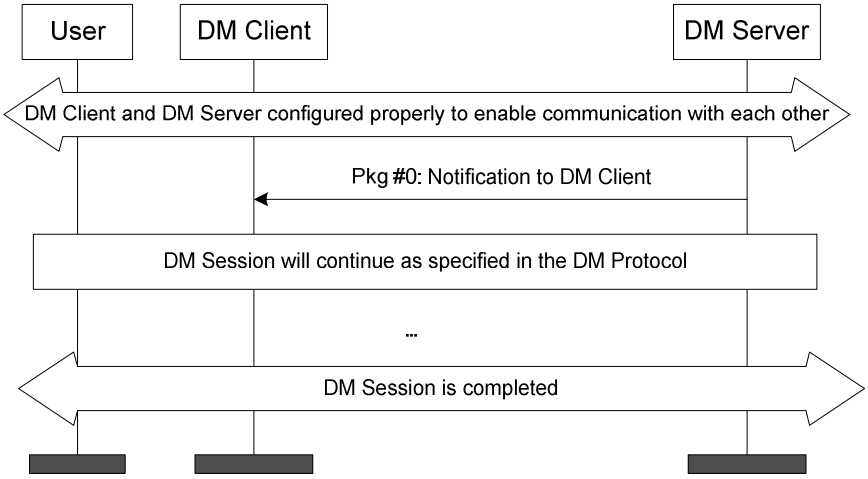

Figure 1: Flow of the Server Alerted Management session

The message flow presented above is one Device Management session. This means that all messages have the same OMA DM Session ID.

6. Structure of DM Notification

Package#0 is the default format used for the Notification Message. This default format can be used if this document does not describe a special format for initialization purposes.

The following figure describes the format of the General Package #0.

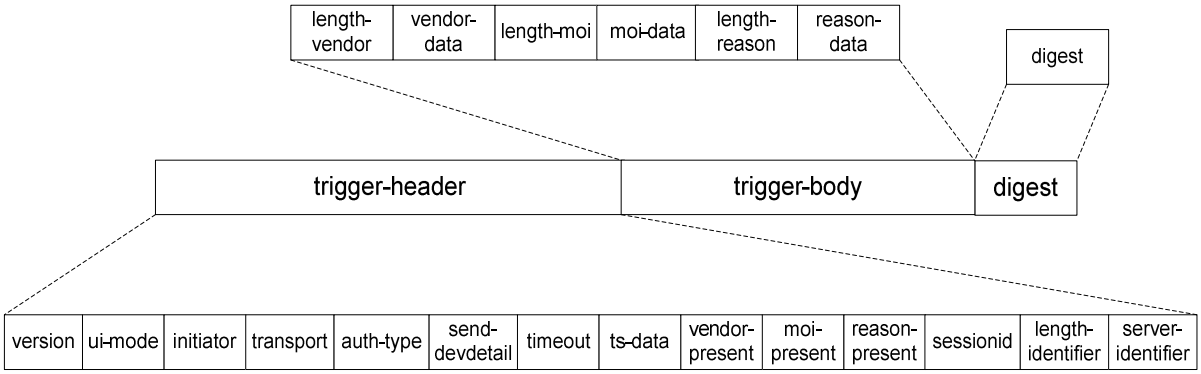

Figure 2: Format of the DM Notification Message (Package#0)

The MIME type for this version of DM Notification Message is *application/vnd.syncml.dm.notification* and the Content-Type code for that is *0x58.* Byte order for DM Notification Message is Big Endian (Network order).

The DM Client MUST support the notification format from DM 1.2 [DMNoti12].

6.1 Syntax for the DM Notification

The following ABNF [RFC5234] defines the syntax for the DM Notification Message. The order and the size of the fields MUST be same as specified in the following syntax of the DM Notification Message.

<trigger-message> ::= <trigger><digest>

<trigger> ::= <trigger-header><trigger-body>

<trigger-header> ::= <version><ui-mode><initiator><transport><auth-type><send-devdetail><timeout><vendor-present><moi-present><reason-present><future-use><sessionid><length-identifier><server-identifier>
*<version> ::= 10*BIT* ; 'Device Management Version'
<ui-mode> ::= <not-specified> / <background> / ; 'Background/Informative/
<informative> / <user-interaction> ; User Interaction session'
<not-specified> ::= "00" ; '2*bit value "0"'
<background> ::= "01" ; '2*bit value "1"'
<informative> ::= "10" ; '2*bit value "2"
<user-interaction> ::= "11" ; '2*bit value "3"'
<initiator> ::= <user> / <server> ; 'User/Server initiated'
<user> ::= "0" ; '1*bit value "0"'
<server> ::= "1" ; '1*bit value "1"'
<transport>::=<not-specified> / <HTTP> / <HTTPS> ; 'transport bindings'
<not-specified> ::= "00" ; '2*bit value "0"'
<HTTP>::="01" ; '2*bit value "1"'
<HTTPS>::="10" ; '2*bit value "2"'
<auth-type>::=<not-specified> / <HTTP-DIGEST> / ; 'authentication type

<DIGEST> / <HMAC>
<not-specified> ::="00" ; '2*bit value "0"'
<HTTP-DIGEST>::="01" ;'2*bit value "1"'
<DIGEST>::="10" ;'2*bit value "2"'
<HMAC>::="11" ;'2*bit value "3"'
<send-devdetail> ::=<send> / <not-send> ; if DevDetail information is required
<send>::="1" ; '1*bit value "1"'
<not-send>::="0" ; '1*bit value "0"'
*<timeout> ::=3*BIT* ; the days to keep the <sessionid> valid

*<ts-data> ::= 16*CHAR* ;
Current server time in UTC in ISO8601 formed text
*<vendor-present> ::= 1*BIT* ; Whether Vendor Specific Info is present ('1') or not-present ('0') in trigger body
*<moi-present> ::= 1*BIT* ; Whether MOI is present ('1') or not-present ('0') in trigger body
*<reason-present> ::= 1*BIT* ; 'Whether reason for connection is present ('1') or not-present ('0') in trigger body'
*<sessionid> ::= 16*BIT* ; 'Session identifier'
*<length-identifier> ::= 8*BIT* ; 'Server Identifier length'
*<server-identifier> ::= <length-identifier>*CHAR* ; 'Server Identifier'
<trigger-body> ::=<length-vendor><vendor-data><length-moi><moi-data><length-reason><reason-data>

*<length-vendor> ::= 16*BIT* ; 'Vendor Specific Info Length'
*<vendor-data> ::= <length-vendor>*BYTE* ; 'Vendor Specific Info'
*<length-moi> ::= 8*BIT* ; 'MO Identifier length'
*<moi-data> ::= <length-moi>*BYTE* ; 'MO Identifier for MO to be managed'
*<length-reason> ::= 16*BIT* ; 'Reason for Connection Length'
*<reason-data> ::= <length-reason>*BYTE* ; 'Reason for Connection Data'

*<digest> ::= 160*BIT* ; 'Digest data'

6.2 Description of the fields

6.2.1 Trigger Message

The <*trigger-message*> field specifies the DM Notification Message causing the DM Client to connect to the DM Server.

6.2.2 Trigger

The <*trigger*> field is container for the trigger-header and trigger-body fields.

6.2.3 Header of the Trigger Message

The <trigger-header> field specifies the header of the DM Notification Message.

6.2.4 Body of the Trigger Message

The <trigger-body> field specifies the body of the DM Notification Message.

6.2.5 Version Information

The <version> field specifies the version of the DM Notification message sent by the DM Server. This value is specified by using the 10 bits in the Notification Message. The supported version is counted as <notification message version> = DEC (version)/10, i.e. first the bit value is transferred to the numeric and then divided by ten. Therefore the biggest possible version is '102.3' and the version '1.0' is specified as '0000001010'.

Notification Messages conforming to this version of the specification MUST have <version> field 10-bit binary value '0000001100' and the version is '1.2".

NOTE: This is not the DM protocol version, but the Notification message version.

6.2.6 User Interaction Mode

The <ui-mode> field specifies the DM Server recommendations whether the server wants the management session to be executed in background or show a notification to the user. This value is specified using 2 bits. A DM Client SHOULD follow this recommendation.

The values the User Interaction mode can have:

- Not specified – Indicates that the DM Server doesn't have a recommendation to this element. The bit value MUST be "00".
- Background management action – Indicates that the DM Server recommends the management action SHOULD be done as a background event. The bit value MUST be "01".
- Informative management action – Indicates that the DM Server recommends the client to display an informative notification or maybe emitting a beep sound announcing the beginning of the provisioning session to the device user. The bit value MUST be "10".
- User Interaction before the management action – Indicates that the DM Server recommends the DM Client to prompt the device user for acceptance of the offered management session before the management session takes place. The bit value MUST be "11".

6.2.7 Initiator of the Management Action

The <initiator> field specifies how the DM Server has interpreted the initiation of the management action, either because the end user requested it or because the DM Server has management actions to perform. This value is specified using 1 bit. A DM Client SHOULD follow this recommendation.

The values the Initiator of the Management action can have:

- Client (End User) Initiated management action – Indicates that the end user caused the device management session to start. The bit value MUST be "0".
- Server Initiated management action – Indicates that the DM Server caused the device management session to start. The bit value MUST be "1".

6.2.8 Transport Binding

The <transport> field indicates the desired transport binding to be used for connection between DM Client and Server in subsequent DM session. This value is specified using 2 bits.

The values of the <transport> field can have:

- Not Specified - Indicates no transport binding has been specified. It is up to the client to choose appropriate transport binding to use. The bit value MUST be "00"
- HTTP - Indicates the HTTP transport binding. The bit value MUST be "01"

- HTTPS - Indicates the HTTPS transport binding. The bit value MUST be “10”.

6.2.9 Authentication Type

The <auth-type> field indicates the authentication type for the DM Client to find the corresponding password and nonce within the DM Account Management Object [DMSTDOBJ] in order to calculate the digest for notification message. This value is specified using 2 bits.

The values of the <auth-type> field can have:

- <not-specified> - Indicates the authentication type was not specified. The bit value MUST BE “00”
- HTTP-DIGEST - Indicates the HTTP-DIGEST authentication type. The bit value MUST be “01”
- DIGEST - Indicates the DIGEST authentication type. The bit value MUST be “10”.
- HMAC - Indicates the HMAC authentication type. The bit value MUST be “11”.

6.2.10 SendDevDetail

The <SendDevDetail> field specifies whether the information within DevDetail MO needs to be sent to DM Server within subsequent management session. This value is specified using 1 bit.

The values of this field are as follows:

- Send – Indicates that the DM Server requires the DevDetail MO to be sent by DM Client in subsequent management session. The bit value MUST be “1”. The DM Client MUST send the DevDetail MO to the DM Server when it initiates the management session.
- Not Send - Indicates that the DM Server does not require the DevDetail MO. The bit value MUST be“0”.

6.2.11 Timeout of the Notification Message

The <timeout> field specifies the number of days that the DM Server will keep the <sessionid> within the Notification Message valid. After the <sessionid> has expired and the DM Client still initiates the management session, the DM Server MAY reject the session. This value is specified by using 3 bits. A timeout value of zero indicates there is no timeout.

6.2.12 Timestamp

The <ts-data> field specifies the current server time in UTC in the form of “YYYYMMDDThhmmssZ” as defined in [ISO8601]. The data in this field MUST be 16 bytes in length.

The DM Client MAY ignore this notification if the message is older than the number of days specified in <timeout>. The age of the message is determined by comparing the value of <ts-data> and the current date and time on the device.

This value MAY also be used to prevent replay attack.

6.2.13 Information Present in Trigger Body

There are several 1 bit fields defined to indicate what is present in the trigger body as follows:

- <vendor-present>: Indicate whether the Vendor Specific Info is present in trigger body respectively.
- <moi-present>: Indicate whether the MO Identifier is present in trigger body.
- <reason-present>: Indicate whether the reason for connection is present in trigger body.

The value of above fields is described below:

- Present – Indicates that the corresponding information is present in trigger body. The bit value MUST be “1”.

- Not-Present – Indicates that the corresponding information is not present in trigger body. The bit value MUST be "0".

6.2.14 Session Identifier

The <sessionid> field specifies the identifier of the OMA DM session associated with the DM Message. This value is specified by using the 16 bits in the Notification Message. The Session ID MUST be different between different Notification Messages and the DM Client MUST use this Session ID when it connects to the DM Server. If DM Client receives the same Session ID several times from the same DM Server, it is enough for a DM Client to initiate only one management session.

When preparing the OMA DM Message for connection to the DM server, the binary session ID value from the Notification Message, in the unsigned hexadecimal range of 1 through FFFF, SHALL be mapped to a string of hexadecimal digits (chosen from the numeric digits "0"-"9" and the upper-case letters "A"-"F") of between one and four characters in length, inclusive, and placed in the SessionID element of the OMA DM message. Leading zeros MUST NOT be included. A value of zero MUST NOT be used.

6.2.15 Length of the Identifier

The <length-identifier> field specifies the length of the Server Identifier of the management server. The value of the Length Identifier is calculated as the Length of the server-identifier in bytes = DEC (length-identifier). The value of this field is specified using 16 bits.

6.2.16 Server Identifier

The <server-identifier> field specifies the Server Identifier of the DM Server. This is the same identifier as in the DMAcc [DMSTDOBJ].

6.2.17 Vendor Specific Information Length

The <length-vendor> field specifies the length of the vendor specific information in bytes. The value of this field is specified using 16 bits. If the value of <vendor-present> is "0", then <length-vendor> field MUST NOT be present in the notification message.

6.2.18 Vendor Specific Information

The <vendor-data> field is used to specify vendor specific information. If the value of <vendor-present> is "0", then <vendor-data> field MUST NOT be present in the notification message.

6.2.19 Length of the MO Identifier

The <length-moi> field specifies the length of the MO Identifier for MO to be managed in bytes. This value is specified by using 8 bits. If the value of <moi-present> is "0", then <length-moi> field MUST NOT be present in the notification message.

6.2.20 MO Identifier

The <moi-data> field specifies the MO Identifier for the MO to be managed. If the value of <moi-present> is "0", then <moi-data> field MUST NOT be present in the notification message.

6.2.21 Length of the Reason for Connection

The <length-reason> field specifies the length of the reason for connection information in bytes. This value is specified by using 16 bits. If the value of <reason-present> is "0", then <length-reason> field MUST NOT be present in the notification message.

6.2.22 Reason for Connection

The <reason-data > field specifies the reason for connection information. If the value of <reason-present> is “0”, then <reason-data> field MUST NOT be present in the notification message. If the <reason-data> field is present, the DM Client MAY display this information to the user prior to starting a management session.

6.2.23 Digest

The <*digest-data*> field specifies the SHA-1 digest of the notification message [RFC3174]. The digest is computed as digest-data = H(server-secret:trigger). The server-secret is the same value in the SRVCRED/AAuthData for that server’s DM Account.

7. OMA Device Management Transport Dependant Profiles

The following sections illustrate the transport dependant profiles for sending a Notification Message from a DM Server to a DM Client. At least one of the profiles below MUST be supported.

7.1 Package #0 delivered using WAP Push

Package #0 MAY be sent to the DM Client using the Push OTA Protocol over WSP (OTA-WSP) [PushOTA] with the following additional rules:

- The package MUST be sent using the non-secure connectionless push.
- The application-id code 0x07 MUST be used.
- The Content-Type code 0x58 MUST be used.
- Other headers may be included; however the total length of the header MUST NOT exceed 48 bytes (to ensure that there is sufficient space for the payload).

7.1.1 Using non WAP Push capable devices

If the receiver is not a WAP device, it is very unlikely that any other application would be active on the same port, which has been publicly registered with IANA. The decoding of the message headers is very straightforward even if the device lacks a full WAP stack and therefore the device MUST examine if the message has been sent to the default WAP push port (2948) and if the Application-ID and the MIME type are one assigned to the OMA DM Notification Initiation Package. If this information is correct then the message MUST be routed to the OMA Device Management application.

7.2 Package #0 over OBEX

Local Notification Initiated Session over OBEX is done inside the PUT command of the OBEX protocol. This happens in the same way as sending the DM messages over OBEX to a SyncML client (See the SyncML OBEX Binding specification [OBEXBinding]).

7.3 Package #0 over SIP Push

Package #0 MAY be sent to the DM Client using the Push OTA Protocol over SIP (OTA-SIP) [SIPPush] with the following additional rules:

- The DM Client MUST register with the SIP/IP Core as soon as practical.
- If GRUU [RFC5627] is supported on the device, then it MUST be used in the registration process.
- The Content-Type MUST be used '*application/vnd.syncml.dm.notification'* in text format.
- "syncml.dm" SHALL be used for "g.oma.eventappid" media feature tag.
- "SIP MESSAGE method (Pager-Mode)" SHALL be used to deliver the Package #0 message.

7.4 Package #0 over HTTP Push

Package #0 MAY be sent to the DM Client using the Push OTA Protocol over HTTP (OTA-HTTP) [PushOTA] with the following additional rules:

- The Content-Type MUST be used '*application/vnd.syncml.dm.notification'* in text format.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
N/A	N/A	No prior 1.3 version.

A.2 Draft/Candidate Version 1.3 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-DM_Notification-V1_3	15 Oct 2008	All	Baseline to v1.3 using OMA-TS-DM_Notification-V1_2_1-20080617-A.
	12 Jan 2009	2.1, 7.3	Applied OMA-DM-DM13-2008-0002R02-CR_SipNotification.
	01 Jun 2009	2.1, 7	Applied OMA-DM-DM13-2009-0024R03-CR_Notification_Push_Update.
	14 Aug 2009	6.1, 6.2	Applied OMA-DM-DM13-2009-0046R02-CR_Notification_Body_Extension with comment from R&A
	09 Sep 2009	6.1, 6.2	Applied OMA-DM-DM13-2009-0060R03-CR_Authentication_Type OMA-DM-DM13-2009-0076R01-CR_Transport_Binding.
	18 Nov 2009	All	Applied OMA-DM-DM13-2009-0081-CR_Notification_Cleanup
	10 Dec 2009	6.2.6, B.2	Applied OMA-DM-DM13-2009-0103R02-CR_Notification_Message_Version
	11 Dec 2009	All	Applied OMA-DM-2009-0066-CR_DM_1.3_TS_Notification_Clerical
	07 Jan 2010	All	Clerical changes from Closure Review.
	27 Jan 2010	All	Applied OMA-DM-DM13-2010-0010R01-CR_Notification_Cleanup Editorial clean-up by DSO
	10 Feb 2010	All	Applied OMA-DM-DM13-2010-0030-CR_PresentBits OMA-DM-DM13-2010-0024R01-CR_Notification_Cleanup.
	11 Feb 2010	2.1, A.2	Editorial changes
	14 Apr 2010	All	Applied OMA-DM-DM13-2010-0049-CR_Nonce_Resync_Security OMA-DM-DM13-2010-0060R02-CR_Notification_Hash
	15 Apr 2010	All	Corrected the notification MIME type.
	26 Apr 2010	2.1	Editorial clean-up of formatting
	04 May 2010	All	Applied OMA-DM-DM13-2010-0075-CR_Notification_MIME Language set to English UK.
	05 May 2010	All	[DMStdObj] changed to [DMSTDOBJ]
Candidate Version OMA-TS-DM_Notification-V1_3	25 May 2010	N/A	Status changed to Candidate by TP Ref # OMA-TP-2010-0221-INP_DM_V1.3_ERP_and_ETR_for_Candidate_approval

Appendix B. Static Conformance Requirements (Normative)

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

B.1 SCR for OMA DM v1.3 Client

Item	Function	Reference	Status	Requirement
SCR-DM-NOTI-C-001	Support of Server-Alerted Management Session	Section 5	O	SCR-DM-NOTI-C-002
SCR-DM-NOTI-C-002	Receiving Notification message	Section 6	O	SCR-DM-NOTI-C-004 OR SCR-DM-NOTI-C-005 OR SCR-DM-NOTI-C-006 OR SCR-DM-NOTI-C-007
SCR-DM-NOTI-C-003	Nonce Synchronisation	Section 5	O	
SCR-DM-NOTI-C-004	Support WAP Push	Section 7.1	O	
SCR-DM-NOTI-C-005	Support OBEX Push	Section 7.2	O	
SCR-DM-NOTI-C-006	Support SIP Push	Section 7.3	O	
SCR-DM-NOTI-C-007	Support HTTP Push	Section 7.4	O	

B.2 SCR for OMA DM v1.3 Server

Item	Function	Reference	Status	Requirement
SCR-DM-NOTI-S-001	Support of Server-Alerted Management Session	Section 5	O	SCR-DM-NOTI-S-002
SCR-DM-NOTI-S-002	Sending of Notification message	Section 6	O	SCR-DM-NOTI-S-005 OR SCR-DM-NOTI-S-006 OR SCR-DM-NOTI-S-007 OR SCR-DM-NOTI-S-008
SCR-DM-NOTI-S-003	Notification message <version> field value is the binary value ‘0000001100’	Section 6.2.6	M	
SCR-DM-NOTI-S-004	Nonce Synchronisation	Section 5	O	
SCR-DM-NOTI-S-005	Support WAP Push	Section 7.1	O	
SCR-DM-NOTI-S-006	Support OBEX Push	Section 7.2	O	
SCR-DM-NOTI-S-007	Support SIP Push	Section 7.3	O	
SCR-DM-NOTI-S-008	Support HTTP Push	Section 7.4	O	

Appendix C. Example of Notification Message (Informative)

Example WAP Push over SMS containing the trigger information:

Binary value	Meaning	Description
06	User-Data-Header (UDHL) Length = 6 bytes	WDP layer (start WDP headers).
05	UDH IE identifier: Port numbers	
04	UDH port number IE length	
0B	Destination port (high)	Port number 2948
84	Destination port (low)	
C0	Originating port (high)	Port number chosen by sender
02	Originating port (low)	WDP layer (end WDP headers)
01	Transaction ID / Push ID	WSP layer (start WSP headers)
06	PDU type (push)	
03	Headerslength (content type+headers)	
C4	Content type code	MIME-Type
AF	X-WAP-Application-ID	
87	Id for urn: x-wap-application:syncml.dm	WSP layer (end WSP headers)
{digest value is 16-bytes}	128-bit digest value	Digest
03, 12, D1,, 00, 00	Binary ‘0000001100’	Version ‘1.2’
	Binary ‘01’	UI-Mode ‘1’
	Binary ‘0’	Initiator ‘0’
	Binary ‘01’	HTTP Transport
	Binary ‘01’	HTTP-Digest Auth Type
	Binary ‘1’	Needs to send DevDetail
	Binary ‘010’	Expiry date: 2 days
	Binary ‘0’	No vendor specific info in body
	Binary ‘0’	No MOI present in body
	Binary ‘1’	Reason for session is present in body
	Binary ‘0000000000000000’	Future DM use
12, 34	Binary ‘0001001000110100’	SessionID 0x1234
12	Binary ‘00010010’	Server Identifier length ‘18’
63, 6F, 6D, 2E, 6D, 67, 6D, 74, 73, 72, 76, 2E, 6D, 61, 6E, 61, 67, 65	String ‘com.mgmtsrv.manage’	Server Identifier
00, 0B	Binary ‘0000000000001011’	Reason for Connection Length is ‘11’
55, 70, 64, 61, 74, 65, 20, 46, 55, 4D, 4F	String ‘Update FUMO’	Reason for session