DS 2.0 Architecture

Approved Version 2.0 – 19 Jul 2011

Open Mobile Alliance

OMA-AD-DS-V2_0-20110719-A

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Use of this document is subject to all of the terms and conditions of the Use Agreement located at http://www.openmobilealliance.org/UseAgreement.html.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE (INFORMATIVE) 4
2. REFERENCES 5
2.1 NORMATIVE REFERENCES 5
2.2 INFORMATIVE REFERENCES 5
3. TERMINOLOGY AND CONVENTIONS 6
3.1 CONVENTIONS 6
3.2 DEFINITIONS 6
3.3 ABBREVIATIONS 6
4. INTRODUCTION (INFORMATIVE) 7
4.1 PLANNED PHASES 7
4.2 SECURITY CONSIDERATIONS 7
5. ARCHITECTURAL MODEL 8
5.1 ARCHITECTURAL DIAGRAM 8
5.2 FUNCTIONAL COMPONENTS AND INTERFACES 8
5.2.1 Components Specified by this Enabler 8
5.2.2 Other Enablers and Components 9
5.2.3 Interfaces Specified in this Enabler 9
5.3 FLOWS 10
5.3.1 Data synchronization Flow 10
5.3.2 Device Information Negotiation Flow 11
5.3.3 Notification Flow 11
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 13
A.1 APPROVED VERSION 2.0 HISTORY 13

Figures

Figure 1: OMA DS logical Architecture Diagram 8

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

1. Scope (Informative)

The scope of this document is to define the architecture for the OMA DS Enabler.

This document details the functional description and architecture for data synchronization within OMA specifications.

This document fulfils the functional capabilities needed to support this service enabler as described in the DS 2.0 Requirements document [DS-RD].

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. References

2.1 Normative References

[DS-RD] "OMA Data Synchronization Requirements", Open Mobile Alliance™, OMA-RD-DS-V2_0, 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 Informative References

[3GPP-SMS] "Technical Realization of the Short Message Service (SMS)", 3GPP TS23.040, URL:http://www.3gpp.org/

[OMA-DICT] "OMA Dictionary", Open Mobile Alliance™, OMA-Dictionary-V2_4, URL:http://www.openmobilealliance.org/

[OMA-DM] "OMA Device Management Enabler", Version 1.2, Open Mobile Alliance™ OMA-ERELD-DM-V1_2, URL:http://www.openmobilealliance.org/

[OMA-EMN] "OMA Email Notification", Open Mobile Alliance™,OMA-Push-EMN-V1_0, URL:http://www.openmobilealliance.org/

[OMA-PUSH-OTA] "Push Over The Air", Open Mobile Alliance™, OMA-WAP-TS-PushOTA-V2_1, URL:http://www.openmobilealliance.org/

[OMA-PUSH-PPG] "Push Proxy Gateway Service", Open Mobile Alliance™, OMA-WAP-TS-PPGService-V2_1, URL:http://www.openmobilealliance.org/

[RFC3265] "SIP Event Notification", June 2002, URL:http://www.ietf.org/rfc/rfc3265.txt

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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

Data Sync Client	A device, user agent, or other entity that acts as the receiver of data synchronization services.
Data Sync Server	An entity that provides resources to clients in response to data synchronization requests.
Data Synchronization	The act of establishing an equivalence between two data collections, where each data element in one item maps to a data item in the other, and their data is equivalent.
Device	See [OMA-DICT]
Message	Atomic unit that contains the SyncML Commands, as well as the related data and meta-information.
Package	A conceptual set of commands that could be spread over multiple messages.
User	See [OMA-DICT]

3.3 Abbreviations

DS	Data Synchronization
HTTP	Hyper Text Transport Protocol
OBEX	Object Exchange Protocol
OMA	Open Mobile Alliance
XML	Extensible Markup Language

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

4. Introduction (Informative)

With the emergence of mobile computing and communications devices, users have access to their personal or professional information and applications, from multiple places (home, work, travel, …) and devices (mobile phones, PDA, computers, network, …). But, on one hand, the information they want may not always be on the device they carry, and on the other hand, they cannot be permanently connected to network to access their data.

The OMA DS Enabler provides a common data synchronization framework and XML-based format, or representation protocol, for synchronizing data on networked devices. The OMA DS Enabler is designed for use between mobile devices that are intermittently connected to the network and network services that are continuously available on the network. The OMA DS Enabler is specifically designed to handle the case where the network services and the device store the data they are synchronizing in different formats or use different software systems.

4.1 Planned Phases

The DS 2.0 enabler release is expected to meet all the requirements defined in [DS-RD] and no additional phases are planned at this stage.

4.2 Security Considerations

An objective of OMA DS is to provide a framework for secure operation. The OMA DS enabler itself does not define any new security schemes. Instead, it provides the framework to challenge authentication, authorization and inclusion of encrypted data in an OMA DS Package. The OMA DS Enabler will support a list of common protocol layer encryption/decryption techniques to ensure secure data transmission. In addition, the originator and recipient MAY use the security mechanisms of the underlying transport to authenticate each other and to provide a secure transport for the exchange of OMA DS Packages.

The detailed security mechanism will be defined in the technical specifications at the later stage.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5. Architectural Model

5.1 Architectural Diagram

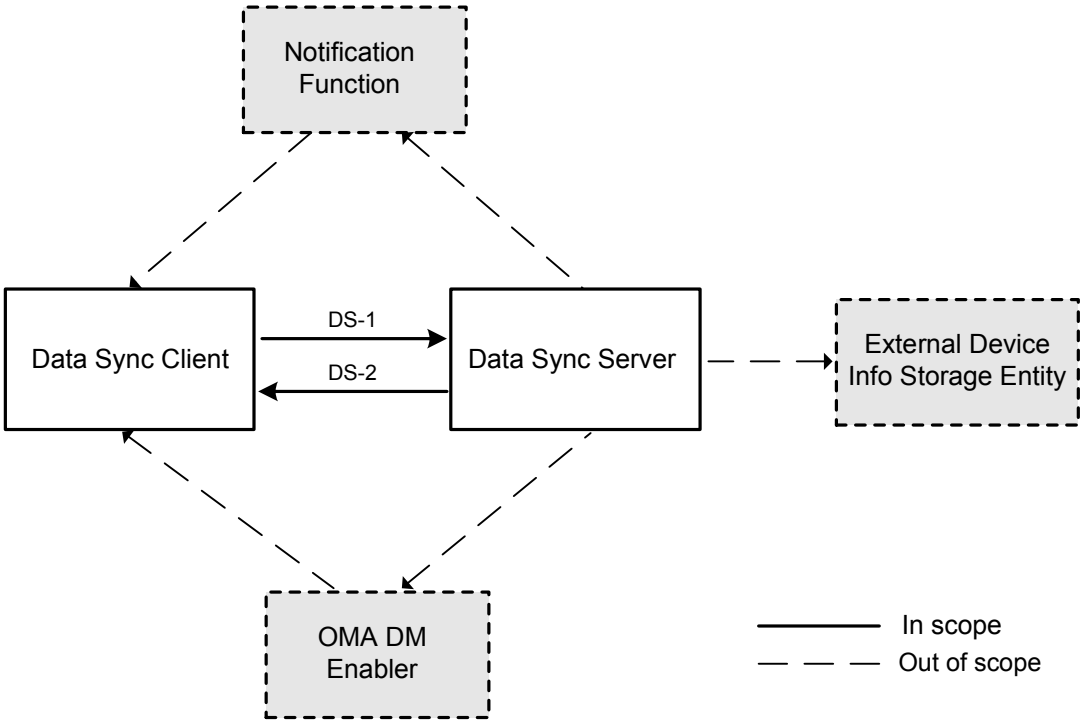

Figure 1: OMA DS logical Architecture Diagram

5.2 Functional Components and Interfaces

5.2.1 Components Specified by this Enabler

5.2.1.1 Data Sync Client

The Data Sync Client is the entity that sends the data synchronization related commands, possibly including payload data to the Data Sync Server. It SHALL also be able to receive responses from the Data Sync Server and to receive some data synchronization commands from the server side.

The Data Sync Client can initiate a session with the Data Sync Server directly.

5.2.1.2 Data Sync Server

The Data Sync Server is the entity that receives the data synchronization messages (operations) possibly including payload data from the Data Sync Client. The Data Sync Server SHALL also be able to send the responses to the commands if needed and to send some data synchronization messages as commands to the client.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The Data Sync Server does not have a defined mechanism in the protocol to directly initiate a session with the Data Sync Client. The Data Sync Server needs to send notification message to the Data Sync Client first, then the Data Sync Client can initiate a session back to the Data Sync Server.

In most of the cases, compared with Data Sync Client, Data Sync Server has some additional functions, for example, conflict resolution, determine appropriate data synchronization mechanism, and maintain the mapping table for data items.

5.2.2 Other Enablers and Components

5.2.2.1 Notification Function

The Notification Function is used to send notification message to the Data Sync Client. Based on the notification message information, the Data Sync Client can initiate a connection to the Data Sync Server. The notification message can be transported over various channels. It can be PUSH, SMS, EMN, SIP PUSH etc.

5.2.2.2 OMA DM Enabler

The OMA DM Enabler is used to provision synchronization settings for Data Sync Client.

5.2.2.3 External Device Info Storage Entity

The External Device Info Storage Entity is used as an optional external storage for device information. This entity is used for the Data Sync Server to retrieve Data Sync Client's device information. OMA DS Enabler will provide methods to negotiate device information between Data Sync Client and Server. One of the possibilities is as following: During the sync initialization, the Data Sync Client MAY send a URI which points to its device information for retrieval. The method how to retrieve it is out of scope of OMA DS Enabler.

5.2.3 Interfaces Specified in this Enabler

5.2.3.1 The DS-1 Interface

The DS-1 interface is exposed by the Data Sync Server for data synchronization requests or responses.

The DS-1 interface can be used to request/receive server device information, or to request/receive the data items from the Data Sync Server.

Also, the DS-1 interface can be used for the Data Sync Client to initiate a session with the Data Sync Server.

5.2.3.2 The DS-2 Interface

The DS-2 interface is exposed by the Data Sync Client for data synchronization requests or responses.

The DS-2 interface can be used to request/receive client device information, or to request/receive the data items from the Data Sync Client.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.3 Flows

5.3.1 Data synchronization Flow

This flow describes the two-way data synchronization. In normal case, the DS Client and the DS Server will exchange information about their modified data. For the one-way data synchronization, the flow is similar.

Figure 2 shows the normal flow for this scenario:

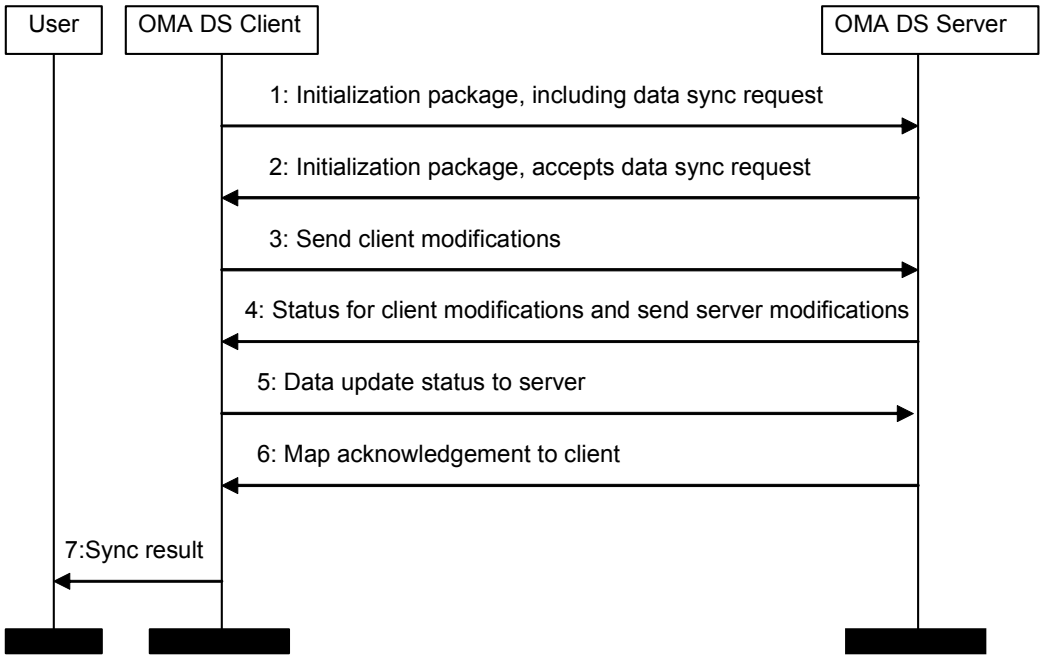

Figure 2: Normal Two-way Data Synchronization Flow

The detailed flow is as the following:

Step 1: The client sends the initialization package to the server, including authentication information, device information and data sync request. The request includes data sync mechanism negotiation parameters, for example, direction, change log valid information, ID valid information.

Step 2: The server authenticates the client, analyses the data sync request and determines an appropriate data sync mechanism. Then the server sends the initialization package to the client, including authentication information, device information and response for the data sync request.

Step 3: The client sends modified data to the server.

Step 4: The server compares the data and updates its database with the data from the client. Then the server returns status for the client modifications and sends server modifications to the client.

Step 5: The client updates its database with the data from the server, and sends the map status to the server.

Step 6: The server returns the map acknowledgement to the client.

Step 7: The client shows the sync result to the user.

5.3.1.1 Alternative flow 1

Optionally, to avoid conflict (that is, the client modifications also be modified in the server) and save the network resource, in step 1, the client can send the characteristic information of the modified data in the initialization

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

package. In step2, According to the characteristic information from the client, the server can decide what part of data the client needs to send, and send back the response.

5.3.1.2 Alternative flow 2

Optionally, in case of continuous synchronization, between step 6 and step 7, the client and the server can synchronize additional data as desired, based upon user settings, or receipt of new data.

5.3.1.3 Alternative flow 3

Optionally, after step 7, the client and the server monitor for the receipt of additional data.

5.3.2 Device Information Negotiation Flow

This flow describes the device information negotiation flow. In case that the device has either been upgraded, or the user has selected additional data sections to synchronize, the DS Client and the DS Server can negotiation their device information without performing data synchronization.

Figure 3 shows the device information negotiation flow:

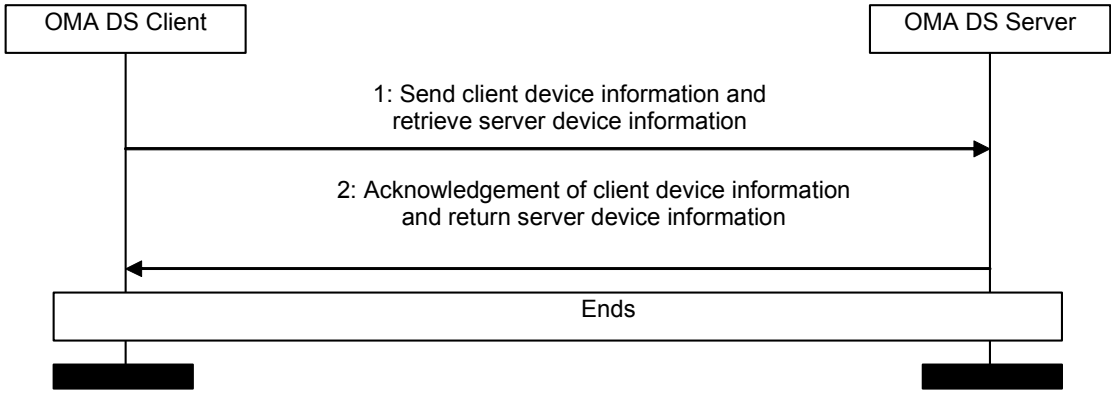

Figure 3: Device Information Negotiation Flow

The detailed flow is as the following:

Step 1: The client sends its device information to the server, and retrieves the server device information.

Step 2: The server sends back acknowledgement of client device information and returns the server device information.

5.3.3 Notification Flow

This flow describes the notification flow.

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 devices, for example, can receive SMS messages. Other devices may have the ability to receive other, similar datagram messages.

A DS Server can use this notification capability to cause the DS Client to initiate a connection back to the synchronization server. The result of receiving such a notification would be for the client to initiate a connection to the synchronization server specified in the notification. For example, the client can initiate a data synchronization or device information negotiation with the server.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Figure 4 shows the notification flow:

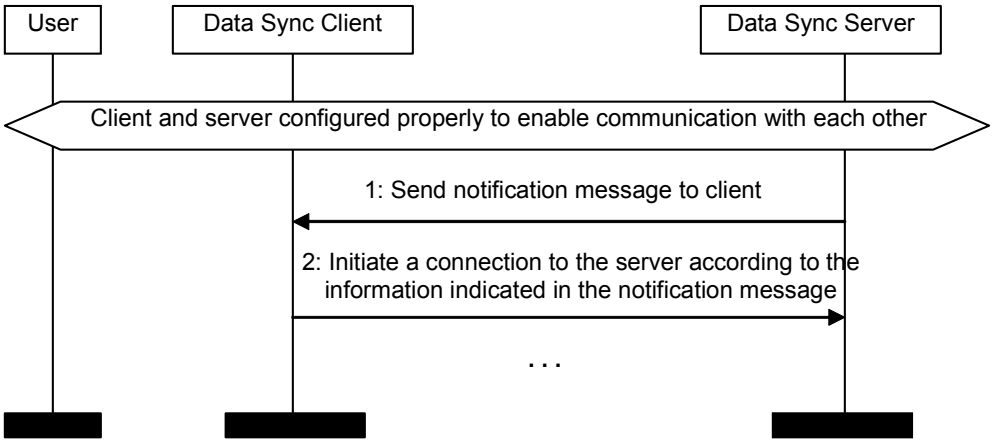

Figure 4. Notification Flow

The detailed flow is as the following:

Step 1: The server sends notification message to the client.

Step 2: According to the information indicated in the notification message, the client initiates a connection with the server.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix A. Change History (Informative)

A.1 Approved Version 2.0 History

Reference	Date	Description
OMA-AD-DS-V2_0-20110719-A	19 Jul 2011	Status changed to Approved by TP: OMA-TP-2011-0258-INP_DS_V2_0_ERP_for_final_Approval

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.