OMA Delegated Authentication Profile

Candidate Version 1.1 – 30 Nov 2010

Open Mobile Alliance

OMA-TS-Delegated_Authentication_Profile-V1_1-20101130-C

© 2010 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.

© 2010 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 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 7
4.1 VERSION 1.1 7
5. DELEGATED AUTHENTICATION PROFILE 8
5.1 OPENID WITH GBA 8
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 9
A.1 APPROVED VERSION HISTORY 9
A.2 DRAFT VERSION 1.1 HISTORY 9
APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) 10
B.1 SCR FOR DELEGATED_AUTHENTICATION CLIENT 10
B.2 SCR FOR DELEGATED_AUTHENTICATION SERVER 10

© 2010 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

This specification defines an OMA profile of existing mechanisms related to delegated authentication for web service to provide SSO experience for users during accessing web services as well as to allow users to control their public identifiers on the Web.

© 2010 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

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

[3GPP TR 33.924] "Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking", 3GPP TR 33.924, http://www.3gpp.org

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, URL:http://www.openmobilealliance.org/

© 2010 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

None

3.3 Abbreviations

3GPP	Third Generation Partnership Project
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
OpenID	Open IDentity
OMA	Open Mobile Alliance
SDO	Standards Development Organization
SSO	Single Sign On

© 2010 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

Delegated Authentication for web service is to provide SSO experience for users during accessing web services as well as to allow users to control their public identifiers on the Web.

4.1 Version 1.1

TS-Delegated_Authentication_Profile v1.1 profiles GBA interworking with OpenID to provide GBA-based delegated authentication for web services.

© 2010 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. Delegated Authentication Profile

5.1 OpenID with GBA

In networks where GBA is deployed, the profile of GBA interworking with OpenID SHALL be used for delegated authentication for web services, as defined in [3GPP TR 33.924].

Note that other delegated authentication mechanisms could be profiled in future versions of this specification after they are finished in other SDOs.

© 2010 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 History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft Version 1.1 History

Document Identifier	Date	Sections	Description
Draft Versions: OMA-TS-Delegated_Authentication_Profile-V1_1	30 Apr 2010	All	OMA-ARC-SEC-2010-0036R01-INP_SEC_CF1.1_TS_Delegated_Authentication_Skeleton
	01 Jun 2010	1	OMA-ARC-SEC-2010-0044R01-CR_SEC_CF1.1_TS_Delegated_Authentication_Scope
	10 Jun 2010	All	OMA-ARC-SEC-2010-0048R02-CR_OpenID_GBA_in_Delegated_Authentication_Scope.doc
	01 Sep 2010	All	OMA-ARC-SEC-2010-0081-CR_DelegatedAuthentication_Profile_SCR.doc; OMA-ARC-SEC-2010-0080R02-CR_DelegatedAuthentication_Profile_Note.doc; OMA-ARC-SEC-2010-0079R01-CR_DelegatedAuthentication_Profile_Introduction.doc;
	03 Oct 2010	2, 3	OMA-ARC-SEC-2010-0091-CR_DelegatedAuthentication_Profile_Abbreviation OMA-ARC-SEC-2010-0093R01-CR_Delegated_Authentication_Profile_Bibliography
	29 Oct 2010	2	OMA-ARC-SEC-2010-0109-CR_CONR_SEC_CF1.1_TS_Delegated_Authn_Profile_F001
Candidate Version: OMA-TS-Delegated_Authentication_Profile-V1_1	30 Nov 2010	All	Status changed by TP: OMA-TP-2010-0472-INP_SEC_CF_V1_1_ERP_for_Candidate_Approval

© 2010 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 B. Static Conformance Requirements (Normative)

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

B.1 SCR for Delegated_Authentication Client

Item	Function	Reference	Requirement
Delegated_Authentication-C-001-O	Delegated Authentication for web services in networks where GBA is deployed conform to [3GPP TR 33.924]	Section 5.1	

B.2 SCR for Delegated_Authentication Server

Item	Function	Reference	Requirement
Delegated_Authentication-S-001-O	Delegated Authentication for web services in networks where GBA is deployed conform to [3GPP TR 33.924]	Section 5.1	

© 2010 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.