Authorization Framework for Network APIs Requirements

Candidate Version 1.0 – 10 Sep 2013

Open Mobile Alliance

OMA-RD-Autho4API-V1_0-20130910-C

Contents

Tables

1. Scope (Informative)

The Authorization Framework for Network APIs will enable a resource owner owning network resources exposed by the Network APIs and RESTful APIs, to authorize third-party applications (desktop, mobile and web applications) to access these resources via that API on the resource owner's behalf.

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

[RCSREQ] "Rich Communication Suite -- RCS API Detailed Requirements 1.1, 17 October 2011", GSM Association, 2011.

URL:http://www.gsma.com/rcs/wp-content/uploads/2012/03/rcsapirequirementsv11.pdf.

[RFC6749] "The OAuth 2.0 Authorization Framework", D. Hardt, October 2012, URL:http://www.ietf.org/rfc/rfc6749.txt

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/

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 Abbreviations

API	Application Program Interface
Autho4API	Authorization Framework for Network APIs
GSMA	Global System for Mobile communications Association
OMA	Open Mobile Alliance
RCS	Rich Communication Suite
RC_API	APIs for Rich Communications
TLS	Transport Layer Security

4. Introduction (Informative)

OMA RESTful Network APIs may be complemented with a common delegated authorization framework based on OAuth 2.0, for access of third party applications via those APIs.

The Delegated Authorization framework will enable a user owning network resources exposed by an OMA RESTful API, to authorize third-party applications (desktop, mobile and web applications) to access these resources via that API on the user's behalf.

4.1 Version 1.0

The main objective is to re-use OAuth 2.0 specifications, by referencing and profiling the specifications as needed for use by OMA RESTful APIs and extend (if required so) OAuth 2.0. Additional extensions, but not changes to OAuth 2.0, may be included in order to meet the scope.

5. Authorization Framework for Network APIs release description (Informative)

This release defines a commonly reusable, lightweight, Web-friendly delegated authorization framework for OMA RESTful APIs. This authorization framework is based on OAuth 2.0.

5.1 End-to-end Service Description

This authorization framework will allow granting authorization to different types of applications (desktop, mobile and web applications), taking into account their specific characteristics.

6. Requirements (Normative)

This section captures the requirements for the enabler Autho4API. The main share of the requirements originates from the GSM Association's RCS API (Rich Communication Suite) requirements related to authorization, which are accessible in document [RCSREQ].

The OMA enabler Autho4API covers the referenced authorization related requirements, but is intended to provide a more generic authorization approach applicable to a broad range of RESTful Network APIs.

To model that, this document references the applicable requirements related to authorization from [RCSREQ], and defines additional requirements.

6.1 High-Level Functional Requirements

This section contains the High Level requirements for the enabler Autho4API.

The following requirements apply:

Label	Description	Release
Autho4API-HLF-001	The Authorization Framework SHALL not prevent an instance of an application from accessing multiple resources owned by the same owner.	Autho4API V1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

6.1.1.1 Authentication

Authentication (of user, application, or developer) is out of the scope for the enabler Autho4API.

6.1.1.2 Authorization

6.1.1.2.1 Generic authorization

This section contains the generic authorization requirements for the enabler Autho4API.

The following requirements from GSMA RCS [RCSREQ] apply to this enabler:

Label	Description	Release
Autho4API-RCAZ-001	This requirement maps to the requirement UNI-AUT-001 from GSMA RCS document [RCSREQ]	Autho4API V1.0
Autho4API-RCAZ-002	This requirement maps to the requirement UNI-AUT-002 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-003	This requirement maps to the requirement UNI-AUT-003 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-004	This requirement maps to the requirement UNI-AUT-004 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-005	This requirement maps to the requirement UNI-AUT-007 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-006	This requirement maps to the requirement UNI-AUT-010 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-007	This requirement maps to the requirement UNI-AUT-013 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-008	This requirement maps to the requirement UNI-AUT-014 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCAZ-009	This requirement maps to the requirement UNI-AUT-016 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Autho4API-RCAZ-010	This requirement maps to the requirement UNI-AUT-019 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Table 2: Generic Authorization Requirements – from GSMA RCS

In addition, the following requirements apply:

Label	Description	Release
Autho4API-AZ-001	The Authorization Framework SHALL support one-time access tokens, depending on the type of the request (e.g. charging).	Autho4API V1.0
Autho4API-AZ-002	The Authorization Framework SHALL validate the access token received from the third-party application and ensure it has not expired and that its scope covers the requested resource.	Autho4API V1.0
Autho4API-AZ-003	The Authorization Framework MAY facilitate presenting to the resource owner the trustworthiness of the third-party application before the resource owner grants the third-party application access to his/her network resources.	Autho4API Future versions
Autho4API-AZ-004	The Authorization Framework SHOULD be able to inform the third-party application about the expiry time of an issued access token.	Autho4API V1.0
Autho4API-AZ-005	The Authorization Framework SHOULD support the issuing and processing of access tokens in a specified format, handled as opaque data by the third-party application. In the specified format of the access token it SHOULD be possible to omit parameters impacting user's privacy.	Autho4API V1.0

Table 3: Generic Authorization Requirements

6.1.1.2.2 Specific OAuth 2.0 Authorization

This section contains the specific OAuth 2.0 authorization requirements for the enabler Autho4API.

The following requirements from GSMA RCS [RCSREQ] apply to this enabler:

Label	Description	Release
Autho4API-RCOAZ-001	This requirement maps to the requirement UNI-OAU-001 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-002	This requirement maps to the requirement UNI-OAU-002 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-003	This requirement maps to the requirement UNI-OAU-003 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-004	This requirement maps to the requirement UNI-OAU-004 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-005	This requirement maps to the requirement UNI-OAU-005 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-006	This requirement maps to the requirement UNI-OAU-006 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-007	This requirement maps to the requirement UNI-OAU-007 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-008	This requirement maps to the requirement UNI-OAU-008 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-009	This requirement maps to the requirement UNI-OAU-009 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-010	This requirement maps to the requirement UNI-OAU-010 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCOAZ-011	This requirement maps to the requirement UNI-OAU-011 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Autho4API-RCOAZ-012	This requirement maps to the requirement UNI-OAU-012 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Table 4: Specific OAuth 2.0 Authorization Requirements – from GSMA RCS

In addition, the following requirements apply:

Label	Description	Release
Autho4API-OAZ-001	Values that specify the scope of an OAuth 2.0 access token SHALL conform to [RFC6749], regardless of where those values are defined.	Autho4API V1.0
Autho4API-OAZ-002	The Authorization Framework SHALL be able to accept and process values that specify the scope of an OAuth 2.0 access token, regardless where those values are defined, as long as they were defined in conformance with [RFC6749].	Autho4API V1.0
Autho4API-OAZ-003	The Authorization Framework SHOULD define guidelines or facilitate mechanisms to manage values that specify the scope of an OAuth 2.0 token, to support both such values defined via standards as well as such values defined as extensions to the standard values by Service Providers.	Autho4API V1.0

Table 5: Specific OAuth 2.0 Authorization Requirements

6.1.1.3 Data Integrity

Data integrity is out of scope.

6.1.1.4 Confidentiality

Credentials (e.g., access token) may be transmitted in the HTTP request and response with clear-text format. IETF OAuth2.0 [RFC6749] requires TLS must be supported when transporting the access token.

The following confidentiality requirements apply for the enabler Autho4API:

Label	Description	Release
Autho4API-CONF-001	The Authorization Framework SHALL support confidentiality of the authorization grant and access token when they are transported in plain-text.	Autho4API v1.0
Autho4API-CONF-002	The Authorization Framework MAY support confidentiality of the user information (e.g., user email address, mobile phone number, etc.) transported between the third-party application and the Authorization Framework.	Autho4API v1.0

Table 6: Confidentiality Requirements

6.1.2 Charging Events

Charging events are out of scope.

6.1.3 Administration and Configuration

This section contains the administration and configuration requirements for the enabler Autho4API.

The following requirements from GSMA RCS [RCSREQ] apply to this enabler:

Label	Description	Release
Autho4API-RCADM-001	This requirement maps to the requirement UNI-AUT-006 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCADM-002	This requirement maps to the requirement UNI-AUT-011 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCADM-003	This requirement maps to the requirement UNI-AUT-017 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Autho4API-RCADM-004	This requirement maps to the requirement UNI-AUT-018 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Table 7: Administration and Configuration Requirements – from GSMA RCS

6.1.4 Usability

This section contains the usability requirements for the enabler Autho4API.

The following requirements from GSMA RCS [RCSREQ] apply to this enabler:

Label	Description	Release
Autho4API-RCUSE-001	This requirement maps to the requirement UNI-AUT-008 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCUSE-002	This requirement maps to the requirement UNI-AUT-009 from GSMA RCS document [RCSREQ].	Autho4API V1.0
Autho4API-RCUSE-003	This requirement maps to the requirement UNI-AUT-012 from GSMA RCS document [RCSREQ].	Autho4API Future Versions

Table 8: Usability Requirements – from GSMA RCS

6.1.5 Interoperability

Out of scope.

6.1.6 Privacy

This section contains the privacy requirements for the enabler Autho4API.

The following requirements from GSMA RCS [RCSREQ] apply to this enabler:

Label	Description	Release
Autho4API-RCPRV-001	This requirement maps to the requirement UNI-AUT-005 from GSMA RCS document [RCSREQ].	Autho4API V1.0

Table 9: Privacy Requirements – from GSMA RCS

In addition, the following privacy requirements apply for the enabler Autho4API:

Label	Description	Release
Autho4API-PRV-001	The Authorization framework SHALL NOT require a user to reveal to third-party applications her/his identities (e.g. MSISDN) he/she uses to authenticate to the service provider.	Autho4API V1.0

Table 10: Privacy Requirements

6.1.7 Shared Multi-Service Provider Scenarios

This section contains the requirements to satisfy when one or a set of RESTful Network APIs are offered by several Service Providers in a shared manner. In this context, shared means that the relationship of the Application developer is with a single entity, i.e.: not with each Service Provider individually.

The following requirements apply to this enabler:

Label	Description	Release
Autho4API-MSP-001	The Authorization Framework SHOULD support seamless access of a client Application to a RESTful Network API exposed by a particular Service Provider, in an environment where multiple Service Providers expose the same RESTful Network API, without the need for the client Application to know the details of the selected Service Provider	Autho4API V1.0
Autho4API-MSP-002	In the scenario described in AUTHO4API-MSP-001, an Application SHOULD be able to gain access rights and later access to protected RESTful Network API resources using the same procedures as in the scenario in which an Application deals individually with the Service Provider exposing the RESTful Network API.	Autho4API V1.0
Autho4API-MSP-003	In the scenario described in AUTHO4API-MSP-001, for privacy/regulatory reasons, it SHOULD be possible for the Application to gain access to the RESTful Network APIs without knowing the Service Provider of the Resource Owner	Autho4API V1.0
Autho4API-MSP-004	The Authorization Framework SHALL NOT prevent the particular Service Provider to perform authentication and token issuance in accordance with its policy.	Autho4API V1.0

Table 11: Shared Multi-Service Provider Requirements

6.2 Overall System Requirements

Overall system requirements are out of scope.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-Autho4API-V1_0	15 Mar 2011	All	Creates the RD baseline: OMA-ARC_Autho4API-2011-0002R01-INP_Autho4API_RD_Baseline
	23 Mar. 2011	6.1	Incorporates the following CRs: OMA-ARC-Auth4API-2011-0003R02-CR_Authorization_Requirements_from_GSMA_RCS OMA-ARC-Auth4API-2011-0004R01-CR_Privacy_Requirements_from_GSMA_RCS OMA-ARC-Auth4API-2011-0005-CR_Additional_OAuth2.0_Authorization_Requirements
	09 Apr. 2011	6.1.1	Incorporates the following CRs: OMA-ARC-Auth4API-2011-0006R03-CR_Additional_Confidentiality_Requirements OMA-ARC-Auth4API-2011-0007R02-CR_Additional_authorization_requirements
	01 May 2011	6.1	Incorporates the following CRs: OMA-ARC-Autho4API-2011-0019R02-CR_Additional_High_level_Requirement_for_Autho4API OMA-ARC-Autho4API-2011-0021-CR_Changing_Requirement_Labels
	02 May 2011	6.1.6	Incorporates the following CRs: OMA-ARC-Autho4API-2011-0020-CR_Additional_privacy_requirement_for_Autho4API
	04 May 2011	All	Editorial changes and Incorporates the following CRs: OMA-ARC-Autho4API-2011-0022-CR_Autho4API_RD_additional_text OMA-ARC-Autho4API-2011-0023R01-CR_Abbreviation_and_Editorial_Changes
	11 May 2011	6.1.7	Editorial changes and Incorporates the following CRs: OMA-ARC-Autho4API-2011-0017R05-CR_New_requirements_for_Distributed_OAuth_scenarios OMA-ARC-Autho4API-2011-0025 R01
	16 May 2011	6.1.1.2.1	Incorporates the following CRs: OMA-ARC-Autho4API-2011-0024R02-CR_Additional_Auth_requirement_for_Autho4API
	02 June 2011	2 6.1.6 A.2	Editorial changes and Incorporating the following contribution: OMA-ARC-2011-0219-INP_REQinformalReviewON2RDs
	30 June 2011	2	Adding the URL of the reference RCS Requirements.
	10 Nov 2011	2	Replacing the reference GSMA RCS requirements 1.0 with GSMA RCS requirements 1.1
	11 Nov 2011	2	Adding the URL for GSMA RCS requirements 1.1.
	05 Jan 2012	All	Updating Autho4API v1.0 RD to address editorial comments according to OMA-CONRR-Autho4API-V1_0-20120104-D
	02 Feb. 2012	2 6.1.1.4	Addressing consistency review comments A005 and A009 in OMA-CONRR-Autho4API-V1_0-20120201-D
Candidate Version OMA-RD-Autho4API-V1_0	27 Mar 2012	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2012-0124-INP_Autho4API_1_0_ERP_and_ETR_for_Candidate_Approval

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-Autho4API-V1_0	07 Aug 2012	2.1	Incorporated CR; OMA-ARC-SEC-2012-0028-CR_Autho4APIv1.0_RD_Fix_External_Reference Editorial changes.
	10 Oct 2012	6.1.4	Incorporated CR: OMA-ARC-SEC-2012-0033-CR_Autho4API_RD_UEext_Future_Versions Editorial changes
	14 Jun 2013	2.1, 6.1.1.2.2, 6.1.1.4	Incorporated CR: OMA-ARC-SEC-2013-0008-CR_Autho4API_RD_IETF_draft_to_RFC Applied latest template. Editorial changes
Candidate Version OMA-RD-Autho4API-V1_0	10 Sep 2013	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2013-0243-INP_Autho4API_V1_0_ERP_and_ETR_for_Candidate_re_approval