Open Grid Protocol : Client Application Launch Message

draft-hamrick-ogp-launch-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 28, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document describes the LLIDL interface description for the Open Grid Protocol (OGP) Client Application Launch message format.
Internet-Draft  OGP : Client Application Launch Message  June 2009

Messages in this format are intended to be used in conjunction with standard web authentication or authorization technologies such as OpenID or OAuth. This document describes the message format, the processing expectations and three MIME types that may be used to identify requests to initiate a virtual worlds session.

Table of Contents

1.  Introduction .................................................. 3
   1.1.  Requirements Language .................................. 3
2.  The OGP Client Application Launch Message Format ............ 3
3.  Processing Expectations ....................................... 4
4.  IANA Considerations .......................................... 6
5.  MIME Type Registrations ....................................... 6
   5.1.  MIME Type Registration for application/ogpcal+xml ....... 7
   5.2.  MIME Type Registration for application/ogpcal+json .... 8
   5.3.  MIME Type Registration for application/ogpcal+binary ... 9
6.  Security Considerations ....................................... 10
7.  References .................................................... 10
   7.1.  Normative References .................................... 10
   7.2.  Informative References ................................... 11
Authors’ Addresses ................................................. 11
1. Introduction

Web authentication protocols such as OpenID [OPENID] and web authorization protocols such as OAuth [I-D.hammer-oauth] are of increasing interest to the internet community. They have great utility in web-based application environments. Best practice for their use in conjunction with applications that do not expose a HTML rendering interface is less clear. Virtual World (VW) client applications, for instance, are often implemented as "desktop applications" instead of "web apps". This introduces difficulty in using web based authentication and authorization protocols to initiate a virtual world session.

OpenID and OAuth traditionally use a HTTP redirect [RFC2616] after user or token authentication to begin an authorized session with a web application. Desktop applications do not generally have a URI to act as the target of HTTP redirection.

One possible solution to this problem is to register a unique MIME type [RFC2046] with the user’s web browser and following succesful user or token authentication, redirect the user’s web browser to a resource with that MIME type. Upon receipt of such a resource, a properly configured web browser should launch the client application.

This document describes the format of a web resource suitable for signaling the user’s web browser to launch a virtual world client application that uses Open Grid Protocol (OGP) Authentication [I-D.hamrick-ogp-auth] to establish a session between the client application and network resources implementing the virtual world.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. The OGP Client Application Launch Message Format

The Client Application Launch message is an LLSD [I-D.hamrick-llsd] message, defined by the LLIDL below. It may be transmitted in XML, JSON or Binary format, at the web server’s convenience. Compliant client applications SHOULD support XML, JSON and Binary serialization formats.
& authenticator = {
    type: 'hash',
    algorithm: 'sha256',
    secret: binary
}

& identifier = {
    type: 'account',
    account_name: string,
    first_name: string,
    last_name: string
}

& identifier = {
    type: 'agent',
    first_name: string,
    last_name: string
}

& request = {
    authenticator: & authenticator,
    identifier: & identifier,
    loginuri: uri,
    region: uri
}

%% launch_request -> & request <- undef

Figure 1 : OGP Client Application Launch Message

3. Processing Expectations

The OGP Client Application Launch Message is intended to be sent by a web server to a web browser following successful web authentication. Requirements for web authentication are explicitly not defined in this document, and left as a responsibility of the authenticating web service.

The message flow for receiving a client application launch message is as follows:
0. Registering MIME types as Web Browser Helper Applications The technique defined in this document depends on the traditional web browser capability to define a "helper application" when the browser receives a MIME type it cannot handle itself. Compliant OGP Client Applications SHOULD register themselves as the helper application for the three MIME types listed in IANA Considerations (Section 4) below.

The exact technique used to register the client application with the OGP Client Application Launch Message is beyond the scope of this document.

1. Web Client to Web Server Authentication / Authorization The process of launching an OGP client application using a web based authentication or authorization system begins with successful user authentication or token authentication. It is traditional in these systems for the user’s web browser to be redirected to a web based application following authentication. This document assumes the user’s web browser will instead be redirected to an HTTP or HTTPS URI that will eventually respond with a Client Application Launch Message.

The exact nature of the web-based authentication or authorization scheme used is beyond the scope of this document.

2. One Time Password Request Before the web service responsible for communicating the launch message to the user’s web browser may download the message, it must first request a "single use only" shared secret.

The exact technique for requesting the One Time Password is beyond the scope of this document. However, the request from the
authentication service to the agent domain SHOULD contain an account or avatar name known to the agent domain and SHOULD be communicated over a secure channel.

3. One Time Password Response The agent domain responds with a One Time Password. The password SHOULD be a sequence of unguessable octets, though the exact encoding and transport of the request is beyond the scope of this document.

4. Client Application Launch Download After the One Time Password is passed from the agent domain to the authorization service, it is included in the Client Application Launch Message along with an account or avatar identifier, a login URI for the agent domain and an initial region URI indicating the avatar’s initial location in the virtual world.

5. Web Browser Launches Client Application When the user’s web browser receives the Client Application Launch Message, it forwards the contents of the message AND the message’s MIME type to the registered Client Application.

6. OGP Authentication In response to receipt of the Client Application Launch Message, the client application uses the information in the message to begin the OGP Authentication process and initial placement of the user’s avatar in the virtual world.

4. IANA Considerations

In accordance with [RFC5226], this document registers the following mime types:

application/ogpcal+xml

application/ogpcal+json

application/ogpcal+binary

See the MIME Type Registrations section (Section 5) below for detailed information on MIME Type registrations.

5. MIME Type Registrations

This section provides media-type registration applications (as per RFC 4288 [RFC4288].)
5.1. MIME Type Registration for application/ogpcal+xml

To: ietf-types@iana.org

Subject: Registration of media type application/ogpcal+xml

Type name: application

Subtype name: ogpcal+xml

Required Parameters: none

Optional Parameters: none

Encoding Considerations: The Extensible Markup Language (XML) specification allows for the use of multiple character sets. The character set used to encode the body of the message is defined as part of the XML header. If no character set is indicated in the XML header, compliant systems MUST assume UTF-8.

Security Considerations: The OGP Client Application Launch Request Message contains sensitive information. Compliant systems SHOULD ensure the confidentiality of the communications media between the web authentication service and the OGP agent domain as well as that between the web authentication service and the user’s web browser.

Interoperability Considerations: While it is possible for compliant implementations to specify the use of character sets other than UTF-8, such systems MUST accept UTF-8 input and SHOULD generate UTF-8 output.

Published specification: this specification.

Applications that use this media type: Virtual world, tele-presence and content management systems related to "virtual reality" systems.

Additional Information:

Magic Number(s): none

File Extension: calx

Macintosh File Type Code(s): CALX
5.2. MIME Type Registration for application/ogpcal+json

To: ietf-types@iana.org

Subject: Registration of media type application/ogpcal+json

Type name: application

Subtype name: ogpcal+json

Required Parameters: none

Optional Parameters: none

Encoding Considerations: Use of UTF-8 is Mandatory

RFC 4627 : The application/json Media Type for JavaScript Object Notation (JSON) [RFC4627] allows the use of UTF-8, UTF-16 and UTF-32. This specification REQUIRES the use of UTF-8.

Security Considerations: The OGP Client Application Launch Request Message contains sensitive information. Compliant systems SHOULD ensure the confidentiality of the communications media between the web authentication service and the OGP agent domain as well as that between the web authentication service and the user’s web browser.

Interoperability Considerations: Note that unlike RFC 4627, this specification REQUIRES the use of UTF-8.

Published specification: This specification.

Applications that use this media type: Virtual world, tele-presence and content management systems related to "virtual reality" systems.

Additional Information:
5.3. MIME Type Registration for application/ogpcal+binary

To: ietf-types@iana.org

Subject: Registration of media type application/ogpcal+binary

Type name: application

Subtype name: ogpcal+binary

Required Parameters: none

Optional Parameters: none

Encoding Considerations: LLSD Binary Serialization REQUIRES the use of binary content-transfer-encoding. Section 5 of RFC 2045 [RFC2045] describes the binary Content-Transfer-Encoding header field. This specification REQUIRES the use of this header to alert intermediary systems that information being included in the message should be interpreted as binary data with no end-of-line semantics which could be considerably longer than allowed in an RFC 821 transport.

Security Considerations: The OGP Client Application Launch Request Message contains sensitive information. Compliant systems SHOULD ensure the confidentiality of the communications media between the web authentication service and the OGP agent domain as well as that between the web authentication service and the user’s web browser.
Interoperability Considerations: none

Published specification: This specification.

Applications that use this media type: Virtual world, tele-presence and content management systems related to "virtual reality" systems.

Additional Information:

Magic Number(s): none

File Extension: calb

Macintosh File Type Code(s): CALB

Person & email address to contact for further information: Meadhbh Hamrick <infinity@lindenlab.com>

Intended Usage: COMMON

Author: IESG

Change Controller: IESG

6. Security Considerations

Security considerations for this specification are, fortunately, either simple or beyond the scope of this document. RFC 3552 [RFC3552] describes several aspects to use when evaluating the security of a specification or implementation. The authors believe most common security concerns users of this specification will encounter are more appropriately considered as transport, network or link layer issues. Or, as higher level "application security" issues.

7. References

7.1. Normative References

[I-D.hammer-oauth]
Hammer-Lahav, E. and B. Cook, "The OAuth Core Protocol",
draft-hammer-oauth-02 (work in progress), March 2009.

[I-D.hamrick-ogp-auth]
Chu, T., Hamrick, M., and M. Lentczner, "Open Grid


7.2. Informative References


Authors’ Addresses

Meadhbh Siobhan Hamrick
Linden Research, Inc.
945 Battery St.
San Francisco, CA  94111
US

Phone: +1 650 283 0344
Email: infinity@lindenlab.com

John Hurliman
Intel Corporation
3600 Juliette Lane
Santa Clara, CA  95051
US

Email: john.hurliman@intel.com