Abstract

This document describes the LLIDL interface description for the Virtual World Region Agent Protocol (VWRAP) Client Application Launch message format. 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.

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 August 16, 2010.

Copyright Notice

Copyright (c) 2010 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 (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Introduction ........................................... 3
   1.1. Requirements Language ............................ 3
2. The VWRAP Client Application Launch Message Format ........ 3
3. Message Flow ......................................... 4
4. Processing Expectations ............................... 6
5. IANA Considerations ................................ 6
6. MIME Type Registrations ............................. 7
   6.1. MIME Type Registration for application/calm+xml .... 7
   6.2. MIME Type Registration for application/calm+json ... 8
   6.3. MIME Type Registration for application/calm+binary .. 9
7. Security Considerations ............................. 10
8. References .......................................... 11
   8.1. Normative References ............................ 11
   8.2. Informative References ........................... 11
8. Authors’ Addresses .................................. 12
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. The problem in using desktop applications with "web auth" technologies is that desktop applications do not generally have a URL 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 successful 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 could then launch the client desktop 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 Virtual World Region Agent Protocol (VWRAP) Authentication [I-D.hamrick-vwrap-authentication] 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 VWRAP Client Application Launch Message Format

The Client Application Launch message is an LLSD [I-D.hamrick-vwrap-type-system] message, defined by the LLIDL below, but is identified with a unique MIME type (described 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.
; note that the &request defined here uses named types &authenticator;
; and &identifier which are defined in
; draft-hamrick-vwrap-authentication-00

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

%% launch_request << &request

Figure 1 : VWRAP Client Application Launch Message

3. Message Flow

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

Two techniques for processing a client application launch message are
defined. The first requests a one time "single use only" secret from
an agent domain. This secret is used to authenticate the client to
the agent domain. The second technique uses possession of a web
capability to authenticate the client. The message flow for both
techniques is the same.

Figure 2 below shows message flows between four conceptual entities.
It is provided for expository purposes only; implementers may choose
to combine conceptual entities into fewer reified components. That
is, nothing in this specification should be interpreted to require
four distinct, deployed entities.
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 VWRAP Client Applications SHOULD register themselves as the helper application for the three MIME types listed in IANA Considerations (Section 5) below.

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

1. Web Client to Web Server Authentication / Authorization The process of launching an VWRAP 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 or LoginURL Capability 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 or the LoginURL web capability.

The exact mechanism for this request 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 or LoginURL Capability Response  The agent domain responds with a One Time Password or web capability. If the one time password is used, the password SHOULD be a sequence of unguessable octets, thought 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 or web capability 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. VWRAP Authentication  In response to receipt of the Client Application Launch Message, the client application uses the information in the message to begin the VWRAP Authentication process and initial placement of the user’s avatar in the virtual world.

4. Processing Expectations

When a client application receives a client application launch message, it is expected to request a seed capability from the service endpoint from in the loginurl specified in message. The loginurl is expected to identify the service endpoint for an agent_login resource defined in the VWRAP Trust Model and User Authentication [I-D.hamrick-vwrap-authentication] specification. The client SHOULD pass the &authenticator and &identifier map entries to the agent_login resource unaltered.

5. IANA Considerations

In accordance with [RFC5226], this document registers the following mime types:
See the MIME Type Registrations section (Section 6) below for detailed information on MIME Type registrations.

6. MIME Type Registrations

This section provides media-type registration applications (as per RFC 4288 [RFC4288].)

6.1. MIME Type Registration for application/calm+xml

To: ietf-types@iana.org
Subject: Registration of media type application/calm+xml

Type name: application
Subtype name: calm+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. When encoding binary data using RFC 4648 [RFC4648], characters outside the base alphabet are explicitly allowable and should be ignored.

Security Considerations: The VWRAP 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 VWRAP 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: calmx
- Macintosh File Type Code(s): CALX

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

Intended Usage: COMMON

Author: IESG

Change Controller: IESG

6.2. MIME Type Registration for application/calm+json

To: ietf-types@iana.org

Subject: Registration of media type application/calm+json

Type name: application

Subtype name: calm+json

Required Parameters: none

Optional Parameters: none

Encoding Considerations: Use of Unicode is Mandatory  
ECMA-262 [ECMA262r5] requires the use of Unicode, but allows the use of UTF-8, UTF-16 or UTF-32 character encodings.

Security Considerations: The VWRAP 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 VWRAP 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: calmj

  Macintosh File Type Code(s): CALJ

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

Intended Usage: COMMON

Author: IESG

Change Controller: IESG

6.3. MIME Type Registration for application/calm+binary

To: ietf-types@iana.org

Subject: Registration of media type application/calm+binary

Type name: application

Subtype name: calm+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 VWRAP 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 VWRAP 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

7. Security Considerations

Security considerations for this specification are, fortunately, either simple or beyond the scope of this document. [RFC 3552] 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.

8. References
8.1. Normative References

[ECMA262r5]
ECMA International, "Standard ECMA-262, 5th Edition :

[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-vwrap-authentication]
Chu, T., Hamrick, M., and M. Lentczner, "VWRAP Trust Model
and User Authentication",
draft-hamrick-vwrap-authentication-00 (work in progress),
February 2010.

[I-D.hamrick-vwrap-type-system]
Brashears, A., Hamrick, M., and M. Lentczner, "VWRAP :
Abstract Type System for the Transmission of Dynamic
Structured Data", draft-hamrick-vwrap-type-system-00 (work
in progress), February 2010.

[OPENID]
OpenID Foundation, "OpenID Authentication 2.0 - Final",
2007.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail
Extensions (MIME) Part One: Format of Internet Message
Bodies", RFC 2045, November 1996.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail
Extensions (MIME) Part Two: Media Types", RFC 2046,
November 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

[RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data
Encodings", RFC 4648, October 2006.

8.2. Informative References

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H.,
Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext


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
Phone: +1 408 123 4560
Email: john.hurliman@intel.com