

INTERNET DRAFT
Obsoletes [RFC 2935](#)
Expires April 2004

Donald E. Eastlake 3rd
Motorola
Chris Smith
October 2003

Internet Open Trading Protocol (IOTP) HTTP Supplement
<[draft-ietf-trade-iotp-http2-00.txt](#)>

Status of this Memo

Distribution of this document is unlimited. Comments should be sent to the IETF TRADE working group <ietf-trade@lists.elistx.com>. This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#). 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>.

Copyright Notice

Copyright (C) 2003, The Internet Society. All Rights Reserved.

Abstract

Internet Open Trading Protocol (IOTP) messages will be carried as Extensible Markup Language (XML) documents. As such, the goal of mapping to the transport layer is to ensure that the underlying XML documents are carried successfully between the various parties. This document describes that mapping for the Hyper Text Transport Protocol (HTTP), Versions 1.0 and 1.1, and the location of HTTP based IOTP services using the SRV domain name system resource record.

Table of Contents

Status of this Memo.....	1
Copyright Notice.....	1
Abstract.....	1
Table of Contents.....	2
1 . Introduction.....	3
2 . HTTP Servers and Clients.....	3
3 . HTTP Net Locations.....	3
4 . Consumer Clients.....	4
4.1 Starting the IOTP Client and the Merchant IOTP Server..	4
4.2 Ongoing IOTP Messages.....	5
4.3 Stopping an IOTP Transaction.....	5
5. Starting the Payment handler and Deliverer IOTP Servers.	6
6 . Security Considerations.....	7
7 . IANA Considerations.....	7
Changes from RFC 2935	7
Normative References.....	8
Informative References.....	8
Authors Addresses.....	9
Full Copyright Statement.....	9
File name and Expiration.....	10

1. Introduction

Internet Open Trading Protocol (IOTP) [[RFC2801](#)] messages are carried as XML [[XML](#)] documents. As such, the goal of mapping to the transport layer is to ensure that the underlying XML documents are carried successfully between the various parties.

This document describes that mapping for the Hyper Text Transport Protocol (HTTP), Versions 1.0 and 1.1 [RFCs 1945, 2616], and the location of IOTP services using the SRV domain name system resource record [RFC 2782, [draft-ietf-trade-srv-higher-services](#)].

There may be future documents describing IOTP over email (SMTP), TCP, cable TV, or other transports.

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](#)].

2. HTTP Servers and Clients

The structure of IOTP maps onto the structure of HTTP in the following way:

The merchant, payment handler, delivery handler, and customer care roles are all represented by HTTP servers. Each may be represented by a separate server, or they may be combined in any combination.

The consumer role is represented by an HTTP client, possibly a browser.

Note: A Merchant, may act in the role of a consumer, for example to deposit electronic cash. In this case the Merchant, as an organization rather than as a role, would need to be supported by an HTTP client.

3. HTTP Net Locations

The Net Locations specified by URIs [[RFC 2396](#)] within the IOTP specification or by a domain name at which a service is required. If a secure connection is required or desired a secure channel that both the HTTP Server and Client support MUST be used. Examples of such channels are SSL version 3 or TLS [[RFC 2246](#)].

To locate an IOTP service at a domain name, the SRV DNS resource

record is used as describe in [[draft-ietf-trade-srv-higher-services](#)]. The higher level service tokens to be used are as follows:

Service	Token
customer	_iotp-customer
merchant	_iotp-merchant
payment	_iotp-payment
delivery	_iotp-delivery
care	_iotp-care

4. Consumer Clients

In most environments, the consumer agent will initially be an HTML browser. However, current browsers do not provide the needed capability to act as an agent for the consumer for an IOTP ptransaction. This leads to two requirements:

- a method of starting and passing control to the IOTP client, and
- a method of closing down the IOTP client cleanly and passing control back to the HTML browser once the IOTP Transaction has finished.

4.1 Starting the IOTP Client and the Merchant IOTP Server

At some point, the HTTP client at the consumer will send an HTTP request that is interpreted as an "IOTP Startup Request" by the Merchant HTTP server. This might, for example, be the result of clicking on a "pay" button. This message is a stand-in for a request message of some form and the Merchant Server will respond with the first IOTP Message in the form of an XML document.

The MIME type for all IOTP messages is: "APPLICATION/IOTP"; however "APPLICATION/X-IOTP" has been in use for experimentation and development and SHOULD also be recognized. See [section 7](#) below for the MIME type registration template for APPLICATION/IOTP. Because HTTP is binary clean, no content-transfer-encoding is required. (See [[RFC 2376](#)] re the application/xml type which has some similar considerations.)

This HTTP response will be interpreted by the HTML browser as a request to start the application associated with MIME type "APPLICATION/IOTP", and to pass the content of this message to that application.

At this point, the IOTP client will be started and have the first message.

IOTP messages are short-lived. Therefore, the HTTP server SHOULD avoid having its responses cached. In HTTP V1.0, the "nocache" pragma can be used. This can be neglected on SSL/TLS secured connections which are not cached and on HTTP POST requests in HTTP v1.1 as in v1.1 POST responses are not cached.

4.2 Ongoing IOTP Messages

Data from earlier IOTP Messages in a transaction MUST be retained by the IOTP Client so that it may (1) be copied to make up part of later IOTP messages, (2) used in calculations to verify signatures in later IOTP message, (3) be resent in some cases where a request has timed out without response, (4) used as input to the Customer Care role in later versions of IOTP, etc. The way in which the data is copied depends on the IOTP Transaction. The data MUST be retained until the end of the transaction, whether by success, failure, or cancelation, and as long thereafter as it is desired for any of the parties to inquire into it.

The IOTP messages contain Net Locations (e.g. the PayReqNetLocn) which for HTTP will contain the URIs to which the IOTP client MUST send IOTP messages.

Subsequent IOTP messages (XML documents) will be sent using the POST function of HTTP. The HTTP client MUST perform full HTTP POST requests.

The XML documents MUST be sent in a manner compatible with the external encodings allowed by the XML [[XML](#)] specification.

4.3 Stopping an IOTP Transaction

The following should be read in conjunction with [[RFC 2801](#)].

An IOTP Transaction is complete when

- the IOTP client decides to fail the IOTP Transaction for some reason either by canceling the transaction or as a result of discovering an error in an IOTP message received, or
- a "time out" occurs or a connection fails, e.g. a response to an IOTP Message, has not been received after some user-defined period

of Time (including retransmissions).

D. Eastlake, C. Smith

[Page 5]

An IOTP Client which processes an IOTP Transaction which:

- completes successfully (i.e. it has not received an Error Block with a HardError or a Cancel Block) MUST direct the browser to the Net Location specified in SuccessNetLocn in the Protocol Options Component, i.e., cause it to do an HTTP GET with that URL.
- does not complete successfully, because it has received some Error Trading Block, MUST display the information in the Error Message, stop the transaction, and pass control to the browser so that it will do a GET on the Error Net Location specified for the role from which the error was received.
- is cancelled since a Cancel Block has been received, MUST stop the IOTP Transaction and hand control to the browser so that it will do a GET on the on the Cancel Net Location specified for the role from which the Cancel Block was received.
- is in error because an IOTP Message does not conform to this specification, MUST send an IOTP Message containing a Error Trading Block to role from which the erroneous message was received and the ErrorLogNetLoc specified for that role, stop the IOTP Transaction, and hand control to the browser so that it will do a GET from the Error Net Location specified for the role from which the bad message was received.
- has a "time out", MUST display a message describing the time out. May give the user the option of cancelling or retrying and/or may automatically retry. On failure due to time out, treat as an error above.

Each implementation of an IOTP client may decide whether or not to terminate the IOTP Client application immediately upon completing an IOTP Transaction or whether to wait until it is closed down as a result of, for example, user shut down or browser shut down.

5. Starting the Payment handler and Deliverer IOTP Servers

Payment Handler and Deliverer IOTP Servers are started by receiving an IOTP Message which contains:

- for a Payment handler, a Payment Request Block, and
- for a Delivery Handler, a Delivery Request Block

6. Security Considerations

Security of Internet Open Trade Protocol messages is primarily dependent on signatures within IOTP as described in [[RFC 2801](#)] and [[RFC 2802](#)]. Privacy protection for IOTP interactions can be obtained by using a secure channel for IOTP messages, such as SSL/TLS [[RFC 2246](#)].

Note that the security of payment protocols transported by IOTP is the responsibility of those payment protocols, not of IOTP.

7. IANA Considerations

This specification carries forward the specification APPLICATION/IOTP MIME type which has been registered. (See the registration template in [[RFC 2935](#)] and in the IANA records.)

Changes from [RFC 2935](#)

1. Addition of means to locate IOTP services via the SRV resource.
2. Update references for more recent versions.
3. Update author information.

Normative References

[[draft-ietf-trade-srv-higher-services](#)] D. Eastlake, "DNS SRV Location of Higher Level Services"

[RFC 1945] Berners-Lee, T., Fielding, R. and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", [RFC 1945](#), May 1996.

[RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC 2396] Berners-Lee, T., Riedling, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", [RFC 2396](#), August 1998.

[RFC 2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", [RFC 2616](#), June 1999.

[RFC 2801] Burdett, D., "Internet Open Trading Protocol - IOTP Version 1.0", [RFC 2801](#), April 2000.

[XML] Bray, T., Paoli, J. and C. Sperberg-McQueen, "Extensible Markup Language (XML) 1.0 (Second Edition)" <<http://www.w3.org/TR/REC-xml>>, February 1998.

Informative References

[RFC 2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", [RFC 2246](#), January 1999.

[RFC 2376] Whitehead, E. and M. Murata, "XML Media Types", [RFC 2376](#), July 1998.

[RFC 2802] Davidson, K. and Y. Kawatsura, "Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP)", [RFC 2802](#), April 2000

[RFC 2935] Eastlake, D. and C. Smith, "Internet Open Trading Protocol (IOTP) HTTP Supplement", September 2000.

Authors Addresses

Donald E. Eastlake 3rd
Motorola Laboratories
155 Beaver Street
Milford, MA 01757 USA

Phone: +1-508-786-7554 (w)
+1-508-634-2066 (h)
Email: Donald.Eastlake@motorola.com

Chris Smith

Email: smith@interlog.com

Full Copyright Statement

Copyright (c) 2003 The Internet Society, All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

File name and Expiration

This file is [draft-ietf-trade-iotp-http2-00.txt](#).
It expires April 2004.

