

Network Working Group
Request for Comments: 3354
Category: Informational

D. Eastlake, III
Motorola
August 2002

Internet Open Trading Protocol Version 2 Requirements

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This document gives requirements for the Internet Open Trading Protocol (IOTP) Version 2 by describing design principles and scope and dividing features into those which will, may, or will not be included.

Version 2 of the IOTP will extend the interoperable framework for Internet commerce capabilities of Version 1 while replacing the XML messaging and digital signature part of IOTP v1 with standards based mechanisms.

Table of Contents

1. Introduction	2
2. Design Principles and Scope	2
3. Requirements	2
4. Security Considerations	4
References	4
Authors Addresses	5
Full Copyright Statement	6

1. Introduction

Version 2 of the Internet Open Trading Protocol (IOTP) will extend the interoperable framework for Internet commerce capabilities of Version 1 [RFC 2801] as described in Section 3 below. In addition, it will replace the ad hoc XML messaging and digital signature [RFC 2802] parts of IOTP v1 with standards based mechanisms [RFC 3275].

This document gives requirements for the Internet Open Trading Protocol (IOTP) Version 2 by describing design principles and scope and dividing features into those which will, may, or will not be included.

2. Design Principles and Scope

1. The specification must describe the syntax and processing necessary for an extension of the interoperable framework for Internet commerce described in IOTP V1.0 [RFC 2801].
2. Keep changes to IOTP V1.0 to a minimum.
3. Maintain all existing functionality of IOTP V1.0.
4. Test all XML DTDs and/or Schemas and XML examples in the specification to insure that they are well-formed.
5. Create usage/implementation guidance information, probably as a separate document.
6. It should be designed to work well with other protocols such as ECML [RFC 3106].
7. IOTP Version 2 should be developed as part of the broader Web design philosophy of decentralization, URIs, Web data, and modularity /layering / extensibility. [Berners-Lee, WebData] In this context, this standard should take advantage of existing provider (and infrastructure) primitives.

3. Requirements

IOTP Version 2 will include the following:

1. Be a superset of IOTP Version 1.
2. Provide for the Dynamic Definition of Trading Sequences. I.E., transactions will not be limited, as with v1, to a single payment and a single delivery with delivery occurring after payment.

Instead, it will be possible to propose an arbitrary sequence of transaction steps.

3. Include specification of an Offer Request Block.
4. Support Improved Problem Resolution (extend to cover presentation of signed receipt to customer support party, better defined Customer Care role, etc.).
5. Add provisions to indicate and handle a payment protocol not tunneled through IOTP.
6. Add support for server based wallets.

The following may be include in IOTP v2:

1. Support Repeated/ongoing payments. For example, a means to specify that a customer approval covers not only the instant purchase but also some limited number of future purchase with some total or per purchase spending limit.
2. Enhanced Server to Server messages. For example, a means for a Delivery Handler to inform a Payment Handler that goods have actually shipped, which may be a pre-condition for making a charge against a credit card.
3. Include the ability to add both fields and attributes to existing trading blocks in addition to the present ability to add entirely new trading blocks.

The following are out of scope for IOTP version 2:

1. Legal or regulatory issues surrounding the implementation of the protocol or information systems using it.
2. Design of an XML Messaging Layer. Instead, whatever is or appears most likely to become the standard XML messaging layer will be used. This includes a standard enveloping, addressing, and error reporting framework.
3. Design of XML Digital Signatures. Instead, the existing standard [RFC 3275] will be used.

4. Security Considerations

As provided above, IOTP v2 will provide optional authentication via standards based XML Digital Signatures [RFC 3275]; however, neither IOTP v1 nor v2 provide a confidentiality mechanism. Both require the use of secure channels such as those provided by TLS [RFC 2246] or IPSEC for confidentiality and depend on the security mechanisms of any payment system used in conjunction with them to secure payments.

References

- [Berners-Lee] "Axioms of Web Architecture: URIs",
<<http://www.w3.org/DesignIssues/Axioms.html>>, "Web Architecture from 50,000 feet",
<<http://www.w3.org/DesignIssues/Architecture.html>>.
- [RFC 2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
- [RFC 2246] Dierks, T. and C. Allen, "The TLS Protocol: Version 1.0", RFC 2246, January 1999.
- [RFC 2801] Burdett, D., "Internet Open Trading Protocol - IOTP Version 1.0", RFC 2801, April 2000.
- [RFC 2802] Davidson, K. and Y. Kawatsura, "Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP)", RFC 2802, April 2000.
- [RFC 3106] Eastlake, D. and T. Goldstein, "ECML v1.1: Field Names for E-Commerce", RFC 3106, April 2001.
- [RFC 3275] Eastlake, D., Reagle, J. and D. Solo, "XML-Signature Syntax and Processing", RFC 3275, March 2002.
- [WebData] "Web Architecture: Describing and Exchanging Data",
<<http://www.w3.org/1999/04/WebData>>.
- [XML] "Extensible Markup Language (XML) 1.0 (Second Edition)", <<http://www.w3.org/TR/1998/REC-xml>>, T. Bray, J. Paoli, C. M. Sperberg-McQueen.

Author's Addresses

Donald E. Eastlake 3rd
Motorola
155 Beaver Street
Milford, MA 01757 USA
Phone: +1-508-851-8280 (w)
 +1-508-634-2066 (h)
EMail: Donald.Eastlake@motorola.com

Full Copyright Statement

Copyright (C) The Internet Society (2002). 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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

