Network Working Group
Request for Comments: 3504
Category: Informational

D. Eastlake
Motorola

March 2003

Internet Open Trading Protocol (IOTP)
Version 1, Errata

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 (2003). All Rights Reserved.

Abstract

Since the publication of the RFCs specifying Version 1.0 of the Internet Open Trading Protocol (IOTP), some errors have been noted. This informational document lists these errors and provides corrections for them.

Table of Contents

1. Introduction..... 2
2. DTD Errata..... 2
   2.1 PackagedContent Element..... 2
   2.2 The Element called Attribute..... 3
3. Other Errata..... 3
   3.1 Re: Combining Authentication Transactions with other Transactions..... 3
   3.2 Type attribute of Element called Attribute..... 3
4. Security Considerations..... 4
5. References..... 4
6. Acknowledgements..... 4
7. Author's Address..... 5
8. Full Copyright Statement..... 6

1. Introduction

The Internet Open Trading Protocol (IOTP), Version 1.0, is specified in [RFC 2801, 2802, 2803]. It provides a payment system independent framework for Internet commerce oriented to consumer to business transactions. It provides mechanism for different portions of the business function, such as fulfillment or payment handling, to be distributed or outsourced. It does not require a prior relationship between the consumer and business.

Several errors have been noted in the IOTP v1.0 specification, particularly RFC 2801, which was the largest RFC ever issued. These are listed, with their fix, in this document.

2. DTD Errata

2.1 PackagedContent Element

Attribute types are swapped.

OLD/INCORRECT:

```
!ELEMENT PackagedContent (#PCDATA) >
<!ATTLIST PackagedContent
          Name              CDATA     #IMPLIED
          Content           NMTOKEN   "PCDATA"
          Transform   (NONE|BASE64)  "NONE" >
```

NEW/CORRECT:

```
<!ELEMENT PackagedContent (#PCDATA) >
<!ATTLIST PackagedContent
           Name           NMTOKEN     #IMPLIED
           Content        CDATA       "PCDATA"
           Transform   (NONE|BASE64)  "NONE" >
```

2.2 The Element called Attribute

Incorrect element content specification syntax.

OLD/INCORRECT:

```
<!ELEMENT Attribute ( ANY ) >
<!ATTLIST Attribute
          type                NMTOKEN            #REQUIRED
          critical        ( true | false )       #REQUIRED
>
```

NEW/CORRECT

```
<!ELEMENT Attribute ANY >
<!ATTLIST Attribute
          type                NMTOKEN            #REQUIRED
          critical        ( true | false )       #REQUIRED
>
```

3. Other Errata

3.1 Re: Combining Authentication Transactions with other Transactions

Section 9.1.13. page 234, restarted->continued:

OLD/INCORRECT:

if the Authentication transaction is successful, then the original IOTP Transaction is restarted

NEW/CORRECT:

if the Authentication transaction is successful, then the original IOTP Transaction is continued

3.2 Type attribute of Element called Attribute

Section 7.19.1, Page 150, insufficient list of signature types:

OLD/INCORRECT:

There must be one and only one Attribute Element that contains a Type attribute with a value of IOTP Signature Type and with content set to either: OfferResponse, PaymentResponse, DeliveryResponse, AuthenticationRequest, AuthenticationResponse, PingReq or PingResponse; depending on the type of the signature.

NEW/CORRECT:
There must be one and only one Attribute Element that contains a Type attribute with a value of IOTP Signature Type and with content set to either: OfferResponse, PaymentResponse, DeliveryResponse, AuthenticationRequest, AuthenticationResponse, PingReq, PingResponse, AuthenticationStatus, InquiryRequest, or InquiryResponse; depending on the type of the signature.

AND a similar change extending the list of values in Section 12.1, Page 262.

And at Section 6.1.2, Page 82, add the following:

AuthenticationStatus	any role
InquiryRequest	any role
InquiryResponse	any role

4. Security Considerations

The errata listed herein are not particularly security related. Never the less, incorrect implementations due to uncorrected errors in the specification may compromise security.

5. References

[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 2803] Maruyama, H., Tamura, K. and N. Uramoto, "Digest Values for DOM (DOMHASH)", RFC 2803, April 2000.

6. Acknowledgements

Thanks to the following people for reporting or responding to reports of these errata:

Harald Barrera Dubois, Yoshiaki Kawatsura, Chun Ouyang

7. Author's Address

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

8. Full Copyright Statement

Copyright (C) The Internet Society (2003). 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.