Extended Incident Handling Working Group
draft-ietf-inch-rid-soap-01.txt
Expires: October 20, 2006

Kathleen M. Moriarty
MIT Lincoln Laboratory
April 20, 2006

IODEF/RID over SOAP

Status of this Memo

Abstract

Documents intended to be shared among multiple constituencies must share a common format and transport mechanism. The Incident Object Description Exchange Format (IODEF) defines a common XML format for document exchange. This draft outlines the SOAP wrapper for all IODEF documents and extensions to facilitate an interoperable and secure communication of documents. The SOAP wrapper allows for flexibility in the selection of a transport protocol. The transport protocols will be provided through existing standards and SOAP binding, such as SOAP over HTTP(S) and SOAP over BEEP.

TABLE OF CONTENTS

1. Introduction

The Incident Object Description Exchange Format (IODEF) [RFCXXX] describes an XML document format for the purpose of exchanging data between CSIRTS or those responsible for security incident handling for network providers. The defined document format provides an easy way for CSIRTS to exchange data in a way which can be easily parsed. In order for the IODEF documents to be shared between entities, a uniform method for transport is necessary. SOAP will provide a layer of abstraction and enable the use of multiple transport protocol bindings. IODEF documents and extensions will be contained in an XML Real-time Inter-network Defense (RID) [RFCXXXX] envelope inside the body of a SOAP message. The RIDPolicy class of RID (e.g., policy information that may affect message routing) will appear in the SOAP message header.

HTTPS or HTTP/TLS has been selected as the REQUIRED SOAP binding for exchanging IODEF/RID messages. The primary reason for selecting HTTPS is due to the existence of multiple successful implementations of SOAP over HTTP, and to its being widely understood. Excellent tool support exists to ease the development of applications using SOAP over HTTP. BEEP may actually be better suited as a transport for RID messages containing IODEF documents, but does not yet have wide adoption. Standards exist for the HTTPS or HTTP/TLS binding for SOAP. A standard is in development for SOAP over BEEP, [RFC****]. Standards MUST be followed when implementing transport bindings for RID communications.

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. SOAP Wrapper

IODEF/RID documents, including all supported extensions, intended to be shared between CSIRTS or NPs MUST use a SOAP wrapper, along with a supported transport protocol binding, for transport. The transport is independent of the wrapper. SOAP will be used to provide the messaging framework and can make distinctions as to how messages should be handled by each participating system. SOAP has been selected because of the flexibility it provides for binding with transport protocols, which can be independent of the IODEF/RID messaging system.

As defined by the SOAP messaging specifications [18], the IODEF document plus any extensions will be in the SOAP body of the message. The SOAP header contains information pertinent to all

participating systems that receive the message, including the ultimate destination, any intermediate hosts, and message processing policy information. Depending on the message or

document being transported, there may be a case, such as with RID messages, in which a host may only need to view the SOAP header and not the SOAP body and is, therefore, acting as a SOAP intermediary node. An example of this would be if one RID system was sending a communication to a RID system for which there was no direct trust relationship, an intermediate RID system may be used to provide the trusted patch between the communicating systems. This intermediate system may not need to see the contents of the SOAP body. Therefore, the elements or classes needed by all participating systems MUST be in the SOAP header, specifically the RIDPolicy class. Each participating system receiving an incident handling IODEF document is an ultimate destination and has to parse and view the entire IODEF document to make necessary decisions.

The SOAP specifications for intermediate and ultimate nodes MUST be Followed; for example, a message destined for an intermediate node would contain the attribute env:role with the value http://www.w3c.org/2003/05/soap-envelope/role/next. Also in accordance with the SOAP specifications, the attribute of env:mustUnderstand has a value of "true" to ensure each node processes the header blocks consistent with the specifications for IODEF.

SOAP messages are typically a one-way conversation. Transmittal of Incident information to another RID host in the form of a Report message is the single case within RID where a one way communication is specified. The arrival of an IODEF/RID Report document in a SOAP message is simply an assertion that a described incident occurred. In the case of other RID message types to support incident handling, two SOAP messages may be exchanged to enable bi-directional communication. Request/response pairs defined by RID include TraceRequest/TraceAuthorization/Result, Investigation/Result, and IncidentQuery/Report.

3. Transport Protocol Bindings

The SOAP binding will be used for message transport. One agreed-upon protocol, HTTPS, MUST be implemented by all RID systems and other protocols may be used. The use of a single transport binding supported by all systems sending and receiving RID messages and extensions of IODEF will enable interoperability between participating CSIRTS and NPs. Other protocol bindings may be defined in separate documents.

3.1 SOAP over HTTP/TLS

SOAP over HTTP/TLS is widely supported, as are ancillary tools such as the Web Services Description Language (WSDL), hence the

selection of SOAP over HTTP/1.1 over TLS as Mandatory for transport of RID communications. Security is provided through the RID specification and all REQUIRED RID security MUST be implemented. TLS offers additional security at the transport layer; this

security SHOULD be used.

BCP 56 contains a number of important considerations when using HTTP for application protocols. These include the size of the payload for the application, whether the application will use a web browser, whether the protocol should be defined on a port other than 80, and if the security provided through HTTPS suits the needs of the new application.

It is acknowledged within the scope of these concerns that HTTPS is not ideally suited for IODEF/RID transport, as the former is a client-server protocol and the latter a message-exchange protocol; however, the ease of implementation for services based on SOAP over HTTP outweighs these concerns. Consistent with BCP 56, IODEF over SOAP over HTTP/TLS will require its own TCP port assignment from IANA.

Every RID system participating in a consortium MUST listen for HTTPS connections on the assigned port, as the requests and responses in a RID message exchange transaction may be significantly separated in time. If a RID message is answered immediately, or within a generally accepted HTTP client timeout (about thirty seconds), the listening system SHOULD return the reply message in the HTTP response body; otherwise, it must initiate a connection to the requesting system and send its reply in an HTTP request.

If the HTTP response body sent in reply to a RID message does not contain a RID message itself, the response body SHOULD be empty, and RID clients MUST ignore any response body that is not an expected RID message. This provision applies ONLY to HTTP response bodies; unsolicited HTTP requests (such as Reports not preceded by an IncidentQuery) are handled according to the message exchange pattern described in RID.

RID systems SHOULD use HTTP/1.1 persistent connections as described in RFC 2616 to minimize TCP connection setup overhead. RID systems SHOULD support chunked transfer encoding on the HTTP server side to allow the implementation of clients that do not need to precalculate message sizes before constructing HTTP headers.

3.2 SOAP over BEEP

SOAP over BEEP is an optional transport binding for IODEF/RID. A RID system supporting BEEP MAY attempt to use SOAP over BEEP on first connection with a peer; if the peer does not support SOAP over BEEP, the initiating peer MUST fall back to SOAP over HTTPS, and SHOULD note that the peer does not support BEEP, to avoid

attempting to use BEEP in future communications.

BEEP has certain implementation advantages over HTTP/TLS for this application; however, the protocol has not been widely implemented.

Communication between participating RID systems is on a server-to-server basis, for which BEEP is better suited than HTTP. Incident handling may at times require immediate action; thus, a protocol with low overhead and minimum bandwidth requirements is desirable.

To provide equivalent transport-layer security to HTTP/TLS, the BEEP TLS profile MUST be supported and SHOULD be used.

4. Examples

The examples below, parallel to the examples in section 4.5 of the RID document, demonstrate how the structure of RID messages fits into SOAP containers as outlined in this document for each message type. Of particular note in each is the duplication of the RID policy information in both the SOAP header and SOAP body. The first example includes the full RID message and associated IODEF-Document; following examples omit the IODEF-Document and refer to it in a comment. The IODEF-Document must be present, and the elements required are outlined in the RID specification.

4.1. Example TraceRequest message

This TraceRequest is identical to the TraceRequest example in Section 4.5.1.1 of RID and would be sent from a CSIRT reporting a denial-of-service attack in progress to its upstream NP. This request asks the upstream to continue the trace and to rate-limit traffic closer to the source.

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
  <SOAP-ENV:Header>
    <iodef-rid:RID
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>TraceRequest</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>Inter-Consortium
          </iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>RIDSystem</iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.20.1.2
          </iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
```

```
    </iodef-rid:RID>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <iodef-rid:RID
```

```
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>TraceRequest</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>Inter-Consortium
          </iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>RIDSystem</iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.20.1.2
          </iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
        <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
        <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-UPSTREAM-NP</iodef:Name>
        <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
        <iodef:Email>csirt-for-upstream-np@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.20.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
    </iodef-rid:RID>
    <iodef:IODEF-Document version="1.0">
      <iodef:Incident restriction="need-to-know" purpose="handling">
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
        <iodef:IncidentData>
          <iodef:Description>Host involved in DOS attack
            </iodef:Description>
          <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
          <iodef:DetectTime>2004-02-02T22:49:24+00:00
            </iodef:DetectTime>
          <iodef:ReportTime>2004-02-02T23:20:24+00:00
            </iodef:ReportTime>
```

```
          <iodef:Assessment>
            <iodef:Impact severity="low" completion="failed"
               type="none"/>
          </iodef:Assessment>
```

```
<iodef:Contact role="creator" role="irt" type="organization">
  <iodef:name>CSIRT-FOR-OUR-DOMAIN</iodef:name>
  <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
</iodef:Contact>
<iodef:Contact role="tech" type="organization">
  <iodef:name>Constituency-contact for 10.1.1.2</iodef:name>
  <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
</iodef:Contact>
<iodef:History>
  <iodef:HistoryItem type="notification">
    <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
      CSIRT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
    <iodef:Description>
      Notification sent to next upstream NP closer to
      10.1.1.2</iodef:Description>
    <iodef:DateTime>2001-09-14T08:19:01+00:00
    </iodef:DateTime>
  </iodef:HistoryItem>
</iodef:History>
<iodef:EventData>
  <iodef:System category="source">
    <iodef:Service>
      <iodef:port>38765</iodef:port>
    </iodef:Service>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">10.1.1.2
      </iodef:Address>
    </iodef:Node>
  </iodef:System>
  <iodef:System category="target">
    <iodef:Service>
      <iodef:port>80</iodef:port>
    </iodef:Service>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.168.1.2
      </iodef:Address>
    </iodef:Node>
  </iodef:System>
  <iodef:Expectation priority="high"
         category="rate-limit-host">
    <iodef:Description>Rate limit traffic close to source
    </iodef:Description>
  </iodef:Expectation>
  <iodef:Record>
  <iodef:RecordData>
  <iodef:RecordItem type="ipv4-packet">
   450000522ad90000ff06c41fc0a801020a010102976d0050103e020810
```

```
 d94a1350021000ad6700005468616e6b20796f7520666f722063617265
 66756c6c792072656164696e67207468697320524 32e0a
</iodef:RecordItem>
<iodef:Description>"The IPv4 packet included
```

```
              was used in the described attack"
            </iodef:Description>
            </iodef:RecordData>
          </iodef:Record>
        </iodef:EventData>
      </iodef:IncidentData>
    </iodef:Incident>
  </iodef:IODEF-Document>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

4.2 Example InvestigationRequest Message

This InvestigationRequest is identical to the InvestigationRequest example in section 4.5.2.1 of the RID specification and would be sent in a situation similar to that of example 4.1, when the source of the attack is known.

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
  <SOAP-ENV:Header>
    <iodef-rid:RID
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>Investigation</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>PeertoPeer</iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>SourceOfIncident
          </iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.25.1.33
          </iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#208-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
    </iodef-rid:RID>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <iodef-rid:RID
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>Investigation</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>PeertoPeer</iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>SourceOfIncident
```

```
          </iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.25.1.33
          </iodef:Address>
```

```
        </iodef:Node>
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#208-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
        <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
        <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-UPSTREAM-NP</iodef:Name>
        <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
        <iodef:Email>csirt-for-upstream-np@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.20.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
    </iodef-rid:RID>
    <!-- Associated IODEF document follows -->
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

4.3 Example Report

This Report is identical to the Report example in section 4.5.3.1 of the RID specification.

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://www.w2.org/2001/12/soap-envelope">
  <SOAP-ENV:Header>
    <iodef-rid:RID
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>Report</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>PeertoPeer</iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>RIDSystem</iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
        </iodef:Node>
```

```
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#209-1
        </iodef:IncidentID>
```

```
      </iodef-rid:RIDPolicy>
    </iodef-rid:RID>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <iodef-rid:RID
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>Report</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>PeertoPeer</iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>RIDSystem</iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#209-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
        <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
        <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.20.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-REQUESTING-NP</iodef:Name>
        <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
        <iodef:Email>csirt-for-requesting-np@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
    </iodef-rid:RID>
    <!-- Associated IODEF document follows -->
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

4.4 Example IncidentQuery

This IncidentQuery is identical to the IncidentQuery example in Section 4.5.4.1 of the RID specification.

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
  <SOAP-ENV:Header>
    <iodef-rid:RID
```

```
     xmlns:iodef-rid="http://www.ietf.org/iodef/iodef-rid.html"
     xmlns:iodef="http://www.ietf.org/iodef/iodef.html">
      <iodef-rid:RIDPolicy>
        <iodef-rid:MsgType>Report</iodef-rid:MsgType>
        <iodef-rid:PolicyRegion>PeertoPeer</iodef-rid:PolicyRegion>
        <iodef-rid:MsgDesination>RIDSystem</iodef-rid:MsgDestination>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
    </iodef:Node>
        <iodef-rid:TrafficType>RIDSystem</iodef-rid:TrafficType>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#209-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
        <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
        <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.20.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
      <iodef-rid:NPPath>
        <iodef:Name>CSIRT-FOR-REQUESTING-NP</iodef:Name>
        <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
        <iodef:Email>csirt-for-requesting-np@ourdomain</iodef:Email>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
        </iodef:Node>
      </iodef-rid:NPPath>
    </iodef-rid:RID>
    <!-- Associated IODEF document follows -->
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

5. Security Considerations

All security considerations of related documents MUST be considered, including those in the following documents: Requirements for the Format for INcident information Exchange (FINE) [RFCXXXX], the Incident Data Exchange Format Data Model and XML Implementation (IODEF), [RFCXXXX], and Incident Handling: Real-time Inter-network Defense (RID) [RFCXXXX]. The SOAP wrappers described herein are built upon the foundation of these documents; the security considerations contained therein are incorporated by

reference.

5.1 Privacy and Confidentiality

For transport confidentiality, TLS (whether HTTP/TLS or the BEEP TLS profile) MUST be supported and SHOULD be used.

Since multiple bindings for transport may be implemented, RID implementations MUST support XML encryption [4] to encrypt the SOAP body. Since XML encryption is performed at the IODEF document level, not only is the transport encrypted when a document is sensitive or contains sensitive elements, but the stored document is also encrypted. Note that this encryption applies only to the SOAP body; policy information in the SOAP header should remain unencrypted if it is necessary for the intermediate node to dispatch the message. XML encryption protects the IODEF document in the SOAP body from being viewed by any involved SOAP intermediary node.

5.2 Authentication and Identification

For transport authentication and identification, TLS (whether HTTP/TLS or the BEEP TLS profile) MUST be supported and SHOULD be used. Each RID consortium SHOULD use a trusted public key infrastructure (PKI) to manage identities for TLS connections.

Since multiple bindings for transport may be implemented, RID implementations MUST support XML digital signatures [5] to sign the SOAP body; the rationale and implementation here is parallel to that for XML Encryption discussed in section 5.1.

6. IANA Considerations

The IANA is requested to assign TCP ports for RID over SOAP over HTTPS and for RID over SOAP over BEEP.

7. Summary

SOAP provides the wrapper to facilitate the exchange of RID messages. The IETF and W3C standards provide detailed implementation details for SOAP and SOAP protocol bindings. The use of existing standards assists with development and interoperability between RID systems exchanging IODEF documents for incident-handling purposes. HTTPS is the mandatory transport binding for SOAP to be implemented and BEEP is optional.

8. References

[RFC2119] "Key Words for Use in RFCs to Indicate Requirement Levels," S. Bradner, March 1997.

[RFC2246] "The TLS Protocol Version 1.0," T. Dierks, C. Allen, W. Treese, P. Karlton, A. Freier, P. Kocher, January 1999.

[RFC2256] "A Summary of the X.500(96) User Schema for use with LDAPv3," M. Wahl, December 1997.

[RFC2459] "Internet Public Key Infrastructure: Part I: X.509 Certificate and CRL Profile," R. Housley, W. Ford, W. Polk, and D. Solo, January 1999.

[RFC2527] "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework," S. Chokhani, W. Ford, March 1999.

[RFC2616] "Hypertext Transfer Protocol - HTTP/1.1," R. Fielding, J. Gettys, J. Mogul, H. Masinter, P. Leach, and T. Berners-Lee, June 1999.

[RFC3080] "The Blocks Extensible Exchange Protocol Core," M. Rose. March 2001.

[RFC3205] "On the Use of HTTP as a Substrate," K. Moore, February 2002. (BCP56)

[RFC3688] "The IETF XML Registry," M. Mealling, January 2004.

[RFCXXXX] "The Incident Object Data Exchange Format Data Model and XML Implementation," J. Meijer, R. Danyliw, and Y. Demchenko, November 2005.
http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-05.txt

[RFCXXXX] "Requirements for the Format for INcident information Exchange," Y. Demchenko, R. Danyliw, and G. Keeni, February 2006.
http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-07.txt

[RFCXXXX] "Incident Handling: Real-time Inter-network Defense," K. Moriarty, April 2006.
http://www.ietf.org/internet-drafts/draft-ietf-inch-rid-06.txt

[RFCXXXX] "Using the Network Configuration Protocol (NETCONF) Over the Simple Object Access Protocol (SOAP)," T. Goddard, March 2006.
http://www.ietf.org/internet-drafts/draft-ietf-netconf-soap-08.txt

[RFCXXXX] "Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)," E. O'Tuathail, and M. Rose, May 13, 2005.
http://www.ietf.org/internet-drafts/draft-mrose-rfc3288bis-02.txt

[1] "Security in a Web Services World: A Proposed Architecture and Roadmap". IBM and Microsoft, April 2002.
http://www-106.ibm.com/developerworks/webservices/library/ws-secmap

[2] SOAP Version 1.2 Part 0: Primer, W3C Recommendation, http://www.w3c.org/TR/REC-soap12-part0-20030624/, 24 June 2004.

[3] SOAP Version 1.2 Part 1:Messaging Framework. W3C Recommendation, 24 June 2004.

http://www.w3c.org/TR/REC-soap12-part1-20030624/

[4] XML Encryption Syntax and Processing, W3C Recommendation. T. Imamura, B. Dillaway, and E. Simon, December 2002.

[5] XML-Signature Syntax and Processing, W3C Recommendation, M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, February 2002. http://www.w3.org/TR/xmldsig-core/#sec-Design

6.1 Acknowledgments

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

6.2 Author Information

Kathleen M. Moriarty
MIT Lincoln Laboratory
244 Wood Street
Lexington, MA 02420
Phone: 781-981-5500
Email: Moriarty@ll.mit.edu

Brian H. Trammell
CERT Network Situational Awareness
4500 Fifth Avenue
Pittsburgh, PA 15213
Email: bht@cert.org

This work was sponsored by the Air Force under Air Force Contract FA8721-05-C-0002.

"Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government."