

1 Digital Signature Web Service 2 Interface

3 1 Introduction

4 This document describes an RPC interface for a centralized digital signature web service that
5 enforces policy controls on who can request signatures for specific transactions. The signature is
6 calculated using a private key owned by the web service for the purpose of producing an
7 "organization" signature. Thus, anyone within the organization authorized to obtain an
8 "organization" signature can obtain it simply by request to the web service.

9 1.1 Motivation

10 A digital signature provides:

11 **Authentication:**

12 A digital signature is unique to the private key used in its creation, and as a result it
13 provides strong authentication of an individual when that individual signs a contract or e-
14 business transaction.

15 **Support for Non-repudiation:**

16 Once a contract or transaction has been digitally signed, the signer cannot disclaim or
17 "repudiate" the signature after the fact. This means, for example, that both parties to an
18 online purchase are bound to the terms of the deal - and thus that both parties to the
19 transaction are protected from online fraud.

20 **Data integrity:**

21 Included in a digital signature is protection of the signed data against any accidental or
22 intentional tampering of the data. For example, the value of an online transaction cannot
23 be compromised without detection, once it has been digitally signed.

24 Most current implementations of digital signatures bind the public key with a specific individual
25 that is responsible for the content of any data signed with the corresponding private key.
26 However, there is a need, especially in the web services paradigm, for signatures that represent
27 "organizations" (not individuals within organizations) and this need is becoming more apparent
28 over time. Distributing the "organization" private key among all end users authorized to use it
29 creates a number of security concerns. It makes sense then to provide a centralized service
30 which applies all "organization" signatures using a private key unique to the organization. Thus,
31 this document describes an RPC interface for a centralized digital signature web service that
32 enforces policy controls on who can request signatures for specific transactions.

33 2 Terminology

34 The key words *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*,
35 and *optional* in this document are to be interpreted as described in [RFC2119].

36 3 General Interface Design Issues

37 The major design goals of this specification are simplicity, extensibility and efficiency.

38 3.1 Related Standards

39 This specification seeks to leverage both existing and emerging web service standards whenever
40 possible. The following are particularly noted as relevant standardization efforts.

41 3.1.1 Existing Standards

42 [WSDL](#) – Defines how abstract interfaces and their concrete realizations are defined.

43 [SOAP](#) – Defines how to invoke remote interfaces.

44 [UDDI](#) – Defines how web services are published, queried and found using standardized
45 directories.

46 [SSL/TLS](#) – Defines secure transport mechanisms.

47 [URL](#) – Defines URI (includes URL) syntax and encoding

48 Character set encoding

49 [XML Digital Signatures](#) – Defines how portions of an XML document are digitally signed.

50 [SAML](#) – Defines how authentication and authorization information may be exchanged.

51 [P3P](#) – Defines how a Producer/entity may publish its privacy policy so that a Consumer could
52 enforce End-User privacy preferences.

53 3.1.2 Emerging Standards

54 [XML Encryption](#) – Defines how to encrypt/decrypt portions of an XML document.

55 [WS-Security](#) – Defines how document level security standards apply to SOAP messages.

56 [XACML](#) – Defines a syntax for expressing authorization rules.

57 4 Digital Signature Interfaces

58 Digital signature interfaces define all operations by the Digital Signature Server that produce a
59 digital signature upon request by a Digital Signature Client.

60 4.1 envelopingSignXmlData

61 The **envelopingSignXmlData()** operation returns an enveloping XML Digital Signature on the
62 provided XML markup data.

```
63 envelopingSignXmlDataResponse =  
64 envelopingSignXmlData(toBeSignedXmlData);
```

65 Where:

66 `toBeSignedXmlData` is the XML markup data to be signed. It is of type **string**.

67

68 `envelopingSignXmlDataResponse` is the XML markup of the enveloping signature on
69 `toBeSignedXmlData` computed by the Digital Signature Server. It is of type **string**.

70

71 This operation SHOULD be invoked only if the requester is authorized to request digital
72 signatures from the Digital Signature Server.

73 4.2 envelopingSign

74 The **envelopingSign()** operation returns an enveloping XML Digital Signature on the data
75 pointed to by the given URI.

```
76 envelopingSignResponse = envelopingSign(toBeSignedUri);
```

77 Where:

78 `toBeSignedUri` is the URI pointing to the data to be signed. It is of type **string**.

79

80 `envelopingSignResponse` is the XML markup of the enveloping signature on the data pointed to
81 by `toBeSignedUri` computed by the Digital Signature Server. It is of type **string**.

82

83 This operation SHOULD be invoked only if the requester is authorized to request digital
84 signatures from the Digital Signature Server.

85 4.3 detachedSign

86 The **detachedSign()** operation returns a detached XML Digital Signature on the data pointed to
87 by the given URI.

```
88 detachedSignResponse = detachedSign(toBeSignedUri);
```

89 Where:

90 `toBeSignedUri` is the URI pointing to the data to be signed. It is of type **string**.

91

92 `detachedSignResponse` is the XML markup of the detached signature on the data pointed to by
93 `toBeSignedUri` computed by the Digital Signature Server. It is of type **string**.

94

95 This operation SHOULD be invoked only if the requester is authorized to request digital
96 signatures from the Digital Signature Server.

97 **4.4 envelopedSign**

98 The **envelopedSign()** operation returns an enveloped XML Digital Signature on the data pointed
99 to by the given URI.

```
100     envelopedSignResponse = envelopedSign(toBeSignedUri,  
101     signaturePosition);
```

102 Where:

103 `toBeSignedUri` is the URI pointing to the data to be signed. It is of type **string**. The data being
104 pointed to MUST be XML markup.

105

106 `signaturePosition` is the name of an XML element in the resource to be signed to be used as
107 the insertion point for the signature by the Digital Signature Server. If null, the signature is
108 inserted as the first child element under document root. It is of type **string**.

109

110 `envelopedSignResponse` is the XML markup of the enveloped signature on the data pointed to
111 by `toBeSignedUri` computed by the Digital Signature Server. It is of type **string**.

112

113 This operation SHOULD be invoked only if the requester is authorized to request digital
114 signatures from the Digital Signature Server.

115 **4.5 envelopedSignXmlData**

116 The **envelopedSignXmlData()** operation returns an enveloped XML Digital Signature on the
117 XML markup data in the request.

```
118     envelopedSignXmlDataResponse =  
119     envelopedSignXmlData(toBeSignedXmlData, signaturePosition);
```

120 Where:

121 `toBeSignedXmlData` is the XML markup data to be signed. It is of type **string**.

122

123 `signaturePosition` is the name of an XML element in the resource to be signed to be used as
124 the insertion point for the signature by the Digital Signature Server. If null, the signature is
125 inserted as the first child element under document root. It is of type **string**.

126

127 `envelopedSignXmlDataResponse` is the XML markup of the enveloped signature on the data
128 pointed to by `toBeSignedUri` computed by the Digital Signature Server. It is of type **string**.

129

130 This operation SHOULD be invoked only if the requester is authorized to request digital
131 signatures from the Digital Signature Server.

132 5 Security

133 Digital Signature Servers will be exposed to many of the same security issues as other web
134 service systems. For a representative summary of security concerns, refer to the [Security and](#)
135 [Privacy Considerations](#) document produced by the [XML-Based Security Services Oasis TC](#).

136

137 The Digital Signature Web Server MUST only produce a signature upon request from an
138 authorized digital signature requester. Thus, the requester MUST be authenticated and policy
139 controls determining who is authorized MUST be enforced.

140 5.1 Authentication of Consumer

141 Digital Signature Server authentication of a requester may be achieved at the transport level
142 through the use of client certificates in conjunction with SSL/TLS.

143 5.2 Authentication of Digital Signature Server

144 Since the requester will likely be sending sensitive data to the Digital Signature Server to be
145 signed, the Server should be authenticated before the data is sent. Authentication of the server
146 may be achieved at the transport level through the use of server certificates in conjunction with
147 SSL/TLS.

148 5.3 Confidentiality & Message Integrity

149 SSL/TLS may be used to ensure the contents of messages are neither tampered with nor
150 decipherable by an unauthorized third party.

151

152 For Digital Signature Server - requester communications, the use of SSL/TLS is provided by the
153 Server's WSDL declaring an https: endpoint.

154 5.4 Access control

155 A Digital Signature Server MUST implement access control mechanisms that restrict which end
156 entities are authorized to request digital signatures on documents.

157 6 WSDL Interface Definition

```
158 <?xml version="1.0" encoding="utf-8" ?>  
159 <definitions xmlns:s="http://www.w3.org/2001/XMLSchema"  
160           xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"  
161           xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"  
162           xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"  
163           xmlns:tns="urn:DigSig"  
164           targetNamespace="urn:DigSig"  
165           xmlns="http://schemas.xmlsoap.org/wsdl/">  
166  
167 <message name="envelopingSignXmlData">  
168 <part name="toBeSignedXmlData"
```

```

169         xmlns:partns="http://www.w3.org/2001/XMLSchema"
170         type="partns:string" />
171     </message>
172
173     <message name="envelopingSignXmlDataResponse">
174         <part name="result"
175             xmlns:partns="http://www.w3.org/2001/XMLSchema"
176             type="partns:string" />
177     </message>
178
179     <message name="envelopingSign">
180         <part name="toBeSignedUri"
181             xmlns:partns="http://www.w3.org/2001/XMLSchema"
182             type="partns:string" />
183     </message>
184
185     <message name="envelopingSignResponse">
186         <part name="result"
187             xmlns:partns="http://www.w3.org/2001/XMLSchema"
188             type="partns:string" />
189     </message>
190
191     <message name="detachedSign">
192         <part name="toBeSignedUri"
193             xmlns:partns="http://www.w3.org/2001/XMLSchema"
194             type="partns:string" />
195     </message>
196
197     <message name="detachedSignResponse">
198         <part name="result"
199             xmlns:partns="http://www.w3.org/2001/XMLSchema"
200             type="partns:string" />
201     </message>
202
203     <message name="envelopedSign">
204         <part name="toBeSignedUri"
205             xmlns:partns="http://www.w3.org/2001/XMLSchema"
206             type="partns:string" />
207         <part name="signaturePosition"
208             xmlns:partns="http://www.w3.org/2001/XMLSchema"
209             type="partns:string" />
210     </message>
211
212     <message name="envelopedSignResponse">
213         <part name="result"
214             xmlns:partns="http://www.w3.org/2001/XMLSchema"
215             type="partns:string" />
216     </message>
217
218     <message name="envelopedSignXmlData">
219         <part name="toBeSignedXmlData"
220             xmlns:partns="http://www.w3.org/2001/XMLSchema"
221             type="partns:string" />
222         <part name="signaturePosition"
223             xmlns:partns="http://www.w3.org/2001/XMLSchema"
224             type="partns:string" />
225     </message>
226
227     <message name="envelopedSignXmlDataResponse">
228         <part name="result"
229             xmlns:partns="http://www.w3.org/2001/XMLSchema"
230             type="partns:string" />
231     </message>

```

```

232
233 <portType name="DigSigPortType">
234
235   <operation name="envelopingSignXmlData">
236     <input message="tns:envelopingSignXmlData" />
237     <output message="tns:envelopingSignXmlDataResponse" />
238   </operation>
239
240   <operation name="envelopingSign">
241     <input message="tns:envelopingSign" />
242     <output message="tns:envelopingSignResponse" />
243   </operation>
244
245   <operation name="detachedSign">
246     <input message="tns:detachedSign" />
247     <output message="tns:detachedSignResponse" />
248   </operation>
249
250   <operation name="envelopedSign">
251     <input message="tns:envelopedSign" />
252     <output message="tns:envelopedSignResponse" />
253   </operation>
254
255   <operation name="envelopedSignXmlData">
256     <input message="tns:envelopedSignXmlData" />
257     <output message="tns:envelopedSignXmlDataResponse" />
258   </operation>
259
260 </portType>
261
262 <binding name="DigSigSoapBinding" type="tns:DigSigPortType">
263   <soap:binding style="rpc"
264     transport="http://schemas.xmlsoap.org/soap/http" />
265
266   <operation name="envelopedSignXmlData">
267     <soap:operation soapAction="" />
268     <input>
269       <soap:body use="encoded" namespace="urn:Entrust-DigSig"
270         encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
271       />
272     </input>
273     <output>
274       <soap:body use="encoded" namespace="urn:Entrust-DigSig"
275         encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
276       />
277     </output>
278   </operation>
279
280   <operation name="envelopingSignXmlData">
281     <soap:operation soapAction="" />
282     <input>
283       <soap:body use="encoded" namespace="urn:Entrust-DigSig"
284         encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
285       />
286     </input>
287     <output>
288       <soap:body use="encoded" namespace="urn:Entrust-DigSig"
289         encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
290       />
291     </output>
292   </operation>
293
294   <operation name="envelopingSign">

```

```

295     <soap:operation soapAction="" />
296     <input>
297       <soap:body use="encoded" namespace="urn:Entrust-DigSig"
298         encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
299         />
300     </input>
301     <output>
302       <soap:body use="encoded" namespace="urn:Entrust-DigSig"
303         encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
304         />
305     </output>
306 </operation>
307
308 <operation name="detachedSign">
309   <soap:operation soapAction="" />
310   <input>
311     <soap:body use="encoded" namespace="urn:Entrust-DigSig"
312       encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
313       />
314   </input>
315   <output>
316     <soap:body use="encoded" namespace="urn:Entrust-DigSig"
317       encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
318       />
319   </output>
320 </operation>
321
322 <operation name="envelopedSign">
323   <soap:operation soapAction="" />
324   <input>
325     <soap:body use="encoded" namespace="urn:Entrust-DigSig"
326       encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
327       />
328   </input>
329   <output>
330     <soap:body use="encoded" namespace="urn:Entrust-DigSig"
331       encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
332       />
333   </output>
334 </operation>
335 </binding>
336
337 <service name="DigSig">
338   <documentation>todo: add your documentation here</documentation>
339   <port name="DigSigPort" binding="tns:DigSigSoapBinding">
340     <soap:address
341       location="http://my.org/DigSigServer" />
342   </port>
343 </service>
344 </definitions>

```

345 7 References

346 7.1 Normative

347 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
348 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

349 PARTICULAR PURPOSE.