



Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services

Committee Draft, 24 December, 2004
(Working Draft 05)

Document identifier:

oasis-dss-1.0-profiles-asynchronous-processing-spec-cd-01

Location:

<http://docs.oasis-open.org/dss/>

Editor:

Andreas Kuehne, *individual* <kuehne@klup.de>

Contributors:

Trevor Perrin, *individual* <trevp@trevp.net>

Pieter Kasselmann, *Betrusted* <pkasselmann@betrusted.com>

Abstract:

This draft profiles the OASIS DSS core protocol for asynchronous processing. This profile is intended to be generic, so it may be combined with other profiles freely.

The protocol is designed to be similar to the asynchronous aspects of the XML Key Management Specification [XKMS].

Status:

This is a **Committee Draft** produced by the OASIS Digital Signature Service Technical Committee. Committee members should send comments on this draft to dss@lists.oasis-open.org.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Digital Signature Service TC web page at <http://www.oasis-open.org/committees/dss/ipr.php>.

Table of Contents

29	1	Introduction.....	3
30	1.1	Notation.....	3
31	1.2	Namespaces	3
32	1.3	Overview (Non-normative)	3
33	2	Profile Features	5
34	2.1	Identifier	5
35	2.2	Scope	5
36	2.3	Relationship To Other Profiles	5
37	2.4	Signature Object	5
38	2.5	Transport Binding.....	5
39	2.6	Security Binding	5
40	3	Polling Protocol	6
41	3.1	Element <PendingRequest>	6
42	4	Profile of Signing Protocol	7
43	4.1	Element <SignRequest>	7
44	4.1.1	Element <OptionalInputs>	7
45	4.1.2	Element <InputDocuments>	7
46	4.2	Element <SignResponse>.....	7
47	4.2.1	Element <Result>	7
48	4.2.2	Element <ResultMajor>	7
49	4.2.3	Element <OptionalOutputs>	8
50	4.2.4	Element <SignatureObject>	8
51	5	Profile of Verifying Protocol	9
52	5.1	Element <VerifyRequest>	9
53	5.1.1	Element <OptionalInputs>	9
54	5.1.2	Element <SignatureObject>	9
55	5.1.3	Element <InputDocuments>	9
56	5.2	Element <VerifyResponse>.....	9
57	5.2.1	Element <Result>	9
58	5.2.2	Element <ResultMajor>	9
59	5.2.3	Element <OptionalOutputs>	9
60	6	References	11
61	6.1	Normative	11
62		Appendix A. Revision History	12
63		Appendix B. Notices.....	13

1 Introduction

64

65 This is an *abstract profile*. Further profiles will build on this one to provide a basis for implementation and
66 interoperability.

67 This draft profiles the OASIS DSS core protocol for asynchronous processing. Although most applications of
68 the OASIS Digital Signature Service supply the results immediately there is a demand for deferred delivering
69 of results. E.g. the German Signature Law explicitly requires the commitment of the certificate holder or at
70 least a time slot for the certificate holder to deny the signing request **[SigG]**.

71 Another use case for a asynchronous protocol may arise in a verification request if a minimum latency
72 between creation and verification has to be respected.

73 This profile is intended to be generic, so it may be combined with other profiles freely.

74 A protocol for asynchronous processing is already defined in the XML Key Management Specification
75 **[XKMS]**. This profile borrows ideas from the XKMS protocol for the OASIS Digital Signature Service.

76 The following sections describe how to understand the rest of this document.

1.1 Notation

77

78 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",
79 "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be
80 interpreted as described in IETF RFC 2119 **[RFC 2119]**. These keywords are capitalized when
81 used to unambiguously specify requirements over protocol features and behavior that affect the
82 interoperability and security of implementations. When these words are not capitalized, they are
83 meant in their natural-language sense.

84 This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`,
85 **Datatype**, `OtherCode`.

1.2 Namespaces

86

87 The structures described in this specification are contained in the schema file **[XYZ-XSD]**. All schema
88 listings in the current document are excerpts from the schema file. In the case of a disagreement between
89 the schema file and this document, the schema file takes precedence.

90 This schema is associated with the following XML namespace:

```
urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0
```

92 If a future version of this specification is needed, it will use a different namespace.

93

94 Conventional XML namespace prefixes are used in this document:

- 95 • The prefix `async` : stands for this profiles namespace **[Core-XSD]**.
- 96 • The prefix `dss` : (or no prefix) stands for the DSS core namespace **[Core-XSD]**.
- 97 • The prefix `ds` : stands for the W3C XML Signature namespace **[XMLSig]**.

98 Applications MAY use different namespace prefixes, and MAY use whatever namespace defaulting/scoping
99 conventions they desire, as long as they are compliant with the Namespaces in XML specification **[XML-ns]**.

1.3 Overview (Non-normative)

100

101 This profile defines a simple mechanism for asynchronous signing and verification requests. This profile is
102 similar to the asynchronous processing protocol defined in the XKMS spec **[XKMS]**.

103

104 In the first call the client supplies its input values as defined in the core and the applied profiles. The client
105 MUST supply the RequestId attribute to correlate subsequent calls.

106 The server may reply synchronously with the appropriate result.
107 On the other hand the server may reply with an 'empty' result, giving the <ResultMajor> code
108 'Pending'. In this case the client may initiate a <PendingRequest> call from time to time with the
109 RequestId of the initial call included in the OriginalRequestId attribute.
110 When the server finally succeeds with its processing the results will be delivered to the client at its next
111 polling call. In this case the <ResultMajor> must not be 'Pending' but the <ResultMajor>
112 resulting from the request processing.
113
114 A notification mechanism isn't defined yet, but may be subject to following versions of this profile.
115

116 2 Profile Features

117 2.1 Identifier

118 urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing

119 Add an <AdditionalProfile> element containing this URI to use this profile.

120 2.2 Scope

121 This document profiles the DSS signing and verifying protocols defined in [DSSCore].

122 2.3 Relationship To Other Profiles

123 This profile is based directly on the [DSSCore].

124 This profile is an abstract profile which is not implementable directly.

125 This profile is intended to be combined with other profiles freely.

126 2.4 Signature Object

127 This profile does not specify or constrain the type of signature object.

128 2.5 Transport Binding

129 This profile does not specify or constrain the transport binding.

130 2.6 Security Binding

131 This profile does not specify or constrain the security binding.

132 3 Polling Protocol

133 The polling protocol extends the core protocol using the <PendingRequest> element for initiating a polling
134 request. This is different from the initial request because the request specific data was already transmitted.

135 3.1 Element <PendingRequest>

136 RequestID

137 This attribute is used to correlate requests with responses. When present in a request, the server MUST
138 return it in the response.

139

140 OriginalRequestID

141 This attribute is used to correlate initial requests with polling requests. The client MUST supply it with each
142 polling request. Its value must match the RequestID sent in an initial <SignRequest> or <VerifyRequest>
143 message (see sections 4.1 and 5.1).

144

145 The <PendingRequest> element doesn't define any child elements.

146

```
147 <xs:element name="PendingRequest">  
148 <xs:complexType name="PendingRequestType">  
149   <xs:attribute name="RequestID" type="xs:string" use="optional"/>  
150   <xs:attribute name="OriginalRequestID" type="xs:string" use="required"/>  
151 </xs:complexType>  
152 </xs:element>
```

153

154 4 Profile of Signing Protocol

155 4.1 Element <SignRequest>

156 RequestID

157 This attribute is used to correlate requests with responses. [DSSCore] defines this attribute as optional.
158 This profile makes the attribute mandatory: the client MUST supply it with the initial request.

159 4.1.1 Element <OptionalInputs>

160 This profile doesn't interfere with the optional inputs from [DSSCore] or from other profiles.

161 4.1.2 Element <InputDocuments>

162 This profile doesn't interfere with the optional inputs from [DSSCore].
163
164

165 4.2 Element <SignResponse>

166 4.2.1 Element <Result>

167 This profile defines the additional <ResultMinor> codes, which MAY be returned in conjunction with a
168 <ResultMajor> code of RequesterError to provide more detailed error reporting:

169 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:RequestIdInUse`

170 This result value means that an operation with the given RequestId is still in progress. The client may retry
171 with a different RequestId. This result code shows up only in response to a <SignRequest>.
172

173 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:RequestIdRequired`

174 This result value means that this operation requires a RequestId for this Request.
175

176 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:RequestIdUnknown`

177 This result value means that an operation included a RequestId that the server didn't recognize. This result
178 code shows up only in response to a <PendingRequest>.
179

180 4.2.2 Element <ResultMajor>

181 This profile defines the additional <ResultMajor> code, which may show up in response to a
182 <SignRequest> or <PendingRequest>:

183 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending`

184 This result value means that the operation did not finish yet. Subsequent requests may return this result
185 code again. After the server has finished the operation the call will return the signing result indicated by the
186 `urn:oasis:names:tc:dss:1.0:resultmajor:Success` value or an error code.

187 **4.2.3 Element <OptionalOutputs>**

188 This profile doesn't interfere with the optional outputs from [DSSCore]. No new optional outputs are defined
189 by this profile.

190

191 If the server returns the <ResultMajor> code

192 urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending

193 the contents of the <OptionalOutputs> element is undefined.

194

195 If the server returns the <ResultMajor> code

196 urn:oasis:names:tc:dss:1.0:resultmajor:Success

197 the <OptionalOutputs> MUST contain the results defined by the accompanying profiles as expected
198 in synchronous operation.

199

200 **4.2.4 Element <SignatureObject>**

201 If the server returns the <ResultMajor> code

202 urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending

203 the content of the <SignatureObject> element is undefined.

204

205 If the server returns the <ResultMajor> code

206 urn:oasis:names:tc:dss:1.0:resultmajor:Success

207 the <SignatureObject> MUST contain the results defined by the accompanying profiles as expected
208 in synchronous operation.

209

210

211

212 5 Profile of Verifying Protocol

213 5.1 Element <VerifyRequest>

214

215 RequestID

216 This attribute is used to correlate requests with responses. The client MUST supply it with the initial request.

217

218 5.1.1 Element <OptionalInputs>

219 This profile doesn't interfere with the optional inputs from [DSSCore] or from other profiles.

220 5.1.2 Element <SignatureObject>

221 This profile doesn't interfere with the element defined from [DSSCore].

222 5.1.3 Element <InputDocuments>

223 This profile doesn't interfere with the element defined from [DSSCore].

224 5.2 Element <VerifyResponse>

225 5.2.1 Element <Result>

226 This profile defines the additional <ResultMinor> code

227 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:RequestIdInUse`

228 . This result value defines that an operation with the given RequestId did not finish yet. The client may retry
229 with a different RequestId.

230

231 This profile defines the additional <ResultMinor> code

232 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:RequestIdRequired`

233 . This result value defines that this operation requires a RequestId for this Request. The client retry with the
234 RequestId defined.

235

236 5.2.2 Element <ResultMajor>

237 This profile defines the additional <ResultMajor> code

238 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending`

239 . This result value defines that the operation did not finish yet. Subsequent requests will return the signing
240 result indicated by the `urn:oasis:names:tc:dss:1.0:resultmajor:Success` value or an
241 error code.

242 5.2.3 Element <OptionalOutputs>

243 This profile doesn't interfere with the optional outputs from [DSSCore]. No new optional outputs are defined
244 by this profile.

245
246 If the server returns the <ResultMajor> code
247 urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending
248 the content of the <OptionalOutputs> element is undefined.
249
250 If the server returns the <ResultMajor> code
251 urn:oasis:names:tc:dss:1.0:resultmajor:Success
252 the <OptionalOutputs> MUST contain the results defined by the accompanying profiles the way are
253 expected in synchronous operation.
254

255

6 References

256

6.1 Normative

257

[Core-XSD] T. Perrin et al. *DSS Schema*. OASIS, (MONTH/YEAR TBD)

258

[DSSCore] T. Perrin et al. *Digital Signature Service Core Protocols and Elements*. OASIS,

259

(MONTH/YEAR TBD)

260

[RFC 2119] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC 2396, August 1998.

261

262

<http://www.ietf.org/rfc/rfc2396.txt>.

263

[XML-ns] T. Bray, D. Hollander, A. Layman. *Namespaces in XML*. W3C Recommendation,

264

January 1999.

265

<http://www.w3.org/TR/1999/REC-xml-names-19990114>

266

[XMLSig] D. Eastlake et al. *XML-Signature Syntax and Processing*. W3C Recommendation,

267

February 2002.

268

<http://www.w3.org/TR/1999/REC-xml-names-19990114>

269

[SigG] Framework for Electronic Signatures, Amendment of Further Regulations Act (Signaturgesetz – SigG), 21 May 2001. http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/119.pdf

270

271

[XKMS2] Phillip Hallam-Baker *XML Key Management Specification (XKMS 2.0)* W3C Candidate Recommendation, 5 April 2004.

272

273

<http://www.w3.org/TR/2004/CR-xkms2-20040405/>

274

275

276

Appendix A. Revision History

Rev	Date	By Whom	What
wd-01	2004-04-17	Andreas Kuehne	Initial version
wd-02	2004-05-09	Andreas Kuehne	Modifying the profile for 'PendingRequest'
wd-03	2004-06-28	Andreas Kuehne	Correlation of initial and subsequent calls optimized
wd-04	2004-08-21	Andreas Kuehne	Added additional return codes. Schema snippets inserted.
Wd-05	2004-11-24	Andreas Kuehne	ResponseMechanism deferred to a later version, no real need now

Appendix B. Notices

279 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might
280 be claimed to pertain to the implementation or use of the technology described in this document or the
281 extent to which any license under such rights might or might not be available; neither does it represent that it
282 has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in
283 OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for
284 publication and any assurances of licenses to be made available, or the result of an attempt made to obtain
285 a general license or permission for the use of such proprietary rights by implementors or users of this
286 specification, can be obtained from the OASIS Executive Director.

287 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
288 other proprietary rights which may cover technology that may be required to implement this specification.
289 Please address the information to the OASIS Executive Director.

290 Copyright © OASIS Open 2003. *All Rights Reserved.*

291 This document and translations of it may be copied and furnished to others, and derivative works that
292 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
293 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
294 this paragraph are included on all such copies and derivative works. However, this document itself does not
295 be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed
296 for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in
297 the OASIS Intellectual Property Rights document must be followed, or as required to translate it into
298 languages other than English.

299 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or
300 assigns.

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