



Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services

2nd Committee Draft, 11 September, 2006 (WD11)

6 **Document identifier:**

7 oasis-dss-1.0-profiles-asynchronous-processing-spec-cd-r2

8 **Location:**

9 <http://docs.oasis-open.org/dss/v1.0/>

10 **Editor:**

11 Andreas Kuehne, *individual*

12 **Contributors:**

13 Trevor Perrin, *individual*

14 Pieter Kasselman, *Betrusted*

15 Tommy Lindberg, *individual*

16

17

18 **Abstract:**

19 This draft profiles the OASIS DSS core protocol for asynchronous processing. This profile is

20 intended to be generic, so it may be combined with other profiles freely.

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

23 **Status:**

24 This is a **Public Review Draft** produced by the OASIS Digital Signature Service Technical
25 Committee. Comments may be submitted to the TC by any person by clicking on "Send A
26 Comment" on the TC home page at:

27 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss.

28 For information on whether any patents have been disclosed that may be essential to

29 implementing this specification, and any offers of patent licensing terms, please refer to the
30 Intellectual Property Rights section of the Digital Signature Service TC web page at

31 <http://www.oasis-open.org/committees/dss/ipr.php>.

32 Table of Contents

33	1	Introduction	3
34	1.1	Notation	3
35	1.2	Namespaces	3
36	1.3	Overview (Non-normative)	4
37	2	Profile Features.....	5
38	2.1	Identifier.....	5
39	2.2	Scope	5
40	2.3	Relationship To Other Profiles	5
41	2.4	Signature Object.....	5
42	2.5	Transport Binding	5
43	2.6	Security Binding	5
44	3	Polling Protocol	6
45	3.1	Element <PendingRequest>	6
46	4	Profile of Signing Protocol.....	8
47	4.1	Element <SignRequest>	8
48	4.1.1	Element <OptionalInputs>	Error! Bookmark not defined.
49	4.1.2	Element <InputDocuments>	Error! Bookmark not defined.
50	4.2	Element <SignResponse>	8
51	4.2.1	Element <Result>	Error! Bookmark not defined.
52	4.2.2	Element <ResultMajor>	8
53	4.2.3	Element <OptionalOutputs>	8
54	4.2.4	Element <SignatureObject>.....	9
55	5	Profile of Verifying Protocol.....	10
56	5.1	Element <VerifyRequest>	10
57	5.1.1	Element <OptionalInputs>	Error! Bookmark not defined.
58	5.1.2	Element <SignatureObject>.....	10
59	5.1.3	Element <InputDocuments>	10
60	5.2	Element <VerifyResponse>	10
61	5.2.1	Element <Result>	Error! Bookmark not defined.
62	5.2.2	Element <ResultMajor>	10
63	5.2.3	Element <OptionalOutputs>	10
64	6	References.....	10
65	6.1	Normative	12
66		Appendix A. Revision History	15
67		Appendix B. Notices	16

68 1 Introduction

69 This is an *abstract profile*. Further profiles will build on this one to provide a basis for
70 implementation and interoperability.
71 This draft profiles the OASIS DSS core protocol for asynchronous processing. Although most
72 applications of the OASIS Digital Signature Service supply the results immediately there is a
73 demand for deferred delivering of results. E.g. the German Signature Law explicitly requires the
74 commitment of the certificate holder or at least a time slot for the certificate holder to deny the
75 signing request [SigG].
76 Another use case for a asynchronous protocol may arise in a verification request if a minimum
77 latency between creation and verification has to be respected.
78 This profile is intended to be generic, so it may be combined with other profiles freely.
79 A protocol for asynchronous processing is already defined in the XML Key Management
80 Specification [XKMS]. This profile borrows ideas from the XKMS protocol for the OASIS Digital
81 Signature Service.
82 The following sections describe how to understand the rest of this document.

83 1.1 Notation

84 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,
85 “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this specification are to be
86 interpreted as described in IETF RFC 2119 [RFC 2119]. These keywords are capitalized when
87 used to unambiguously specify requirements over protocol features and behavior that affect the
88 interoperability and security of implementations. When these words are not capitalized, they are
89 meant in their natural-language sense.
90 This specification uses the following typographical conventions in text: <ns : Element>,
91 Attribute, Datatype, OtherCode.

92 1.2 Namespaces

93 The structures described in this specification are contained in the schema file [XYZ-XSD]. All
94 schema listings in the current document are excerpts from the schema file. In the case of a
95 disagreement between the schema file and this document, the schema file takes precedence.
96 This schema is associated with the following XML namespace:

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

98 If a future version of this specification is needed, it will use a different namespace.
99

100 Conventional XML namespace prefixes are used in this document:

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

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

107 **1.3 Overview (Non-normative)**

- 108 This profile defines a simple mechanism for asynchronous signing and verification requests. This
109 profile is similar to the asynchronous processing protocol defined in the XKMS spec [[XKMS](#)].
- 110 In the first call the client supplies its input values as defined in the core and the applied profiles.
111 The server may reply synchronously with the appropriate result.
- 112 On the other hand the server may reply with an 'empty' result, giving the `<ResultMajor>` code
113 'Pending' and a `<async:ResponseID>` element as an `<OptionalOutput>`. The server
114 generates the value of the `<async:ResponseID>` on its own.
- 115 The client may initiate a `<PendingRequest>` call from time to time with the
116 `<async:ResponseID>` of the initial response included in the `<async:ResponseID>` element
117 within the `<dss:OptionalInputs>`.
- 118 When the server finally succeeds with its processing the results will be delivered to the client with
119 its next polling call. In this case the `<ResultMajor>` must not be 'Pending' but the
120 `<ResultMajor>` resulting from the request processing.
- 121 A notification mechanism isn't defined yet, but may be subject to following versions of this profile.
- 122

123 **2 Profile Features**

124 **2.1 Identifier**

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

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

127 **2.2 Scope**

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

129 **2.3 Relationship To Other Profiles**

130 This profile is based directly on the **[DSSCore]**.

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

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

133 **2.4 Signature Object**

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

135 **2.5 Transport Binding**

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

137 **2.6 Security Binding**

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

139 **3 Polling Protocol**

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

143 **3.1 Element <PendingRequest>**

144 The <PendingRequest> element is sent by the client to request the result from a pending
145 signature or verification initiated earlier. It contains the following attributes and elements inherited
146 from <RequestBaseType> :

147 RequestID [Optional]

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

150 Profile [Optional]

151 This attribute indicates a particular DSS profile. It may be used to select a profile if a server
152 supports multiple profiles, or as a sanity-check to make sure the server implements the profile
153 the client expects. In this special case of a <PendingRequest> the required profile
154 information is already defined within the initial call to the server. So Profile MUST be
155 omitted in a <PendingRequest>. Consequently there MUST NOT be any
156 <AdditionalProfile> optional input elements in a <PendingRequest>.

157 <OptionalInputs> [Optional]

158 Any additional inputs to the request. This element may be used e.g. for authentication data.

159 In addition to <RequestBaseType> the <PendingRequest> element defines the following
160 <ResponseID> element:

161 **3.1.1 Element <OptionalInputs>**

162 This profile defines the new input element of <async:ResponseID>.

163

164 <async:ResponseID>

165 To correlate subsequent <PendingRequest> calls to the initial request the
166 <async:ResponseID> element is introduced by this profile. The client MUST take care of the
167 value returned by the initial <SignRequest> in <async:ResponseID>.

168 **3.2 Element <Response>**

169 The <PendingRequest> may response with a generic <Response> in cases where the service is
170 unable to specialise down to <SignResponse> or <VerificationResponse>.

171 This will happen when the service doesn't recognise the given ResponseID. The
172 <ResultMinor> is set to the special value of ResponseIdUnknown.

173

174 Urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:
175 ResponseIdUnknown

176

177 The <ResultMajor> code in this case is RequesterError . This result code shows up only in
178 response to a <PendingRequest>.

179 In the case of successful interpretation of the ResponseID attribute the service returns a
180 <SignResponse> or <VerifyResponse> as intended by the initial request.

181 **4 Profile of Signing Protocol**

182 **4.1 Element <SignRequest>**

183 No additional elements of <SignRequest> defined by this profile.

184 **4.2 Element <SignResponse>**

185 **4.2.1 Element <ResultMajor>**

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

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

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

194 In case an asynchronous service is unable to reply in a synchronous manner and a request to
195 this service is made without profiling the call as asynchronous (using the given profile identifier
196 within the `Profile` attribute or the `<AdditionalProfiles>` element), the service returns a
197 <ResultMajor> of `RequesterError` and a <ResultMinor> of:

198 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:`
199 `asynchronousOnly`

200

201 **4.2.2 Element <OptionalOutputs>**

202 This profile defines the new optional output element of <async:ResponseID>.

203

204 <async:ResponseID>

205 To correlate subsequent <PendingRequest> calls to the initial request the
206 <async:ResponseID> element is introduced by this profile. The service will generate a suitable
207 value on its own behalf. So the client MUST take care of the value returned in
208 <async:ResponseID> for subsequent <PendingRequest>.

209

210 If the server returns the <ResultMajor> code

211 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pen-`
212 `ding`

213 the contents of the <OptionalOutputs> element children other than
214 <async:ResponseID> are undefined.

215

216 If the server returns the <ResultMajor> code

217 `urn:oasis:names:tc:dss:1.0:resultmajor:Success`

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

220

221 **4.2.3 Element <SignatureObject>**

222 If the server returns the <ResultMajor> code

223 urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending
224 the content of the <SignatureObject> element is undefined.

225

226 If the server returns the <ResultMajor> code

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

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

230 **5 Profile of Verifying Protocol**

231 **5.1 Element <VerifyRequest>**

232 **5.1.1 Element <OptionalInputs>**

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

234 **5.1.2 Element <SignatureObject>**

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

236 **5.1.3 Element <InputDocuments>**

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

238 **5.2 Element <VerifyResponse>**

239 **5.2.1 Element <ResultMajor>**

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

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

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

248 In case an asynchronous service is unable to reply in a synchronous manner and a request to
249 this service is made without profiling the call as asynchronous (using the given profile identifier
250 within the `Profile` attribute or the <AdditionalProfiles> element), the service returns a
251 <ResultMajor> of RequesterError and a <ResultMinor> of:

252 `urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:
253 asynchronousOnly`

254

255 **5.2.2 Element <OptionalOutputs>**

256 This profile defines the new optional output element of <async:ResponseID>.

257

258 <async:ResponseID>

259 To correlate subsequent <PendingRequest> calls to the initial request the
260 <async:ResponseID> element is introduced by this profile. The service will generate a suitable
261 value on its own behalf. So the client MUST take care of the value returned in
262 <async:ResponseID> for subsequent <PendingRequest>.

263

264 If the server returns the <ResultMajor> code
265 urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending
266 the contents of the <OptionalOutputs> element children other than <async:ResponseID>
267 are undefined.

268

269 If the server returns the <ResultMajor> code
270 urn:oasis:names:tc:dss:1.0:resultmajor:Success
271 the <OptionalOutputs> MUST contain the results defined by the accompanying profiles as
272 expected in synchronous operation.

273 **6 Appendix**

274 **6.1 Example**

275

276 Example of an initial signing request :

```
277 <dss:SignRequest  
278   Profile="urn:oasis:names:tc:dss:1.0:profile:dss_interop"  
279     RequestID="I0d2f1de663c75dc52f468e678af1bfd6"  
280     xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">  
281   <dss:OptionalInputs>  
282     <dss:SignatureType>...</dss:SignatureType>  
283     <dss:AdditionalProfile>  
284       urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing  
285     </dss:AdditionalProfile>  
286   </dss:OptionalInputs>  
287   <dss:InputDocuments>  
288     <dss:Document ID="..." RefType="..." RefURI="...">  
289     ...  
290     </dss:Document>  
291   </dss:InputDocuments>  
292 </dss:SignRequest>
```

293

294 The request above may result in an response like this :

```
295 <dss:SignResponse RequestID="I0d2f1de663c75dc52f468e678af1bfd6"  
296   Profile="urn:oasis:names:tc:dss:1.0:profile:dss_interop"  
297   xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"  
298  
299   xmlns:async="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing  
300   :1.0">  
301   <dss:Result>  
302     <dss:ResultMajor>  
303  
304     urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:  
305     Pending  
306     </dss:ResultMajor>  
307   </dss:Result>  
308   <dss:OptionalOutputs>  
309  
310   <async:ResponseID>I517f0e98752098c7245f2892f59ef9fc</async:ResponseID>  
311   </dss:OptionalOutputs>  
312 </dss:SignResponse>
```

313 The server return a <dss :ResultMajor> value 'Pending' with no Signature returned. So the client
314 will send a PendingRequest using the value of <async:ResponseID> from this response. A
315 PendingRequest may look like this :

```
316 <async:PendingRequest RequestID="If82506cfa678bedf2cdc1549f5970641"  
317   xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
```

```
318
319     xmlns:async="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing
320     :1.0">
321     <dss:OptionalInputs>
322       <dss:AdditionalProfile>
323         urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0
324       </dss:AdditionalProfile>
325
326     <async:ResponseID>I517f0e98752098c7245f2892f59ef9fc</async:ResponseID>
327   </dss:OptionalInputs>
328 </async:PendingRequest>
```

329

330 The server may respond with a <dss:ResultMajor> value ‘Pending’ again. But finally server side
331 processing will be finished and the server replies such a Response :

```
332 <dss:SignResponse RequestID="If82506cfa678bedf2cdc1549f5970641"
333   Profile="urn:oasis:names:tc:dss:1.0:profile:dss_interop"
334   xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
335   <dss:Result>
336     <dss:ResultMajor>
337       urn:oasis:names:tc:dss:1.0:resultmajor:Success
338     </dss:ResultMajor>
339   </dss:Result>
340   <dss:SignatureObject>
341     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
342       ...
343       </ds:Signature>
344     </dss:SignatureObject>
345 </dss:SignResponse>
```

346

347

348

349 **7 References**

350 **7.1 Normative**

- 351 [Core-XSD] T. Perrin et al. *DSS Schema*. OASIS, (**MONTH/YEAR TBD**)
352 [DSSCore] T. Perrin et al. *Digital Signature Service Core Protocols and Elements*. OASIS,
353 (**MONTH/YEAR TBD**)
354 [RFC 2119] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. IETF
355 RFC 2119, March 1997.
356 <http://www.ietf.org/rfc/rfc2119.txt>.
357 [XML-ns] T. Bray, D. Hollander, A. Layman. *Namespaces in XML*. W3C
358 Recommendation, January 1999.
359 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
360 [XMLSig] D. Eastlake et al. *XML-Signature Syntax and Processing*. W3C
361 Recommendation, February 2002.
362 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
363 [SigG] Framework for Electronic Signatures, Amendment of Further Regulations Act
364 (Signaturgesetz – SigG), 21 May 2001.
365 http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/119.pdf
366
367 [XKMS2] Phillip Hallam-Baker *XML Key Management Specification (XKMS 2.0)* W3C
368 Candidate Recommendation, 5 April 2004.
369 <http://www.w3.org/TR/2004/CR-xkms2-20040405/>
370
371
372

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
Wd-06	2005-12-11	Andreas Kuehne	Profile aligned with the new core specification.
Wd-07	2006-01-21	Andreas Kuehne	Simplified the responseld mechanism by dropping the requestId attribute. The service generates the responselds on his own.
Wd-08	2006-03-31	Andreas Kuehne	Samples added
Wd-09	2006-05-12	Andreas Kuehne	Added a new resultminor for async services unable to respond to a sync call.
Wd-10	2006-07-08	Andreas Kuehne	Fixed a minor asymmetric documentation of ResultMinor of 'asynchronousOnly' (see Action Item 06-06-12-01)
Wd-11	2006-08-31	Andreas Kuehne	Updated reference to RFC 2119

374 **Appendix B. Notices**

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

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

387 Copyright © OASIS Open 2006. *All Rights Reserved.*

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

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

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