



German Signature Law Profile of the OASIS Digital Signature Service Version 1.0

OASIS Standard

11 April 2007

Specification URIs:

This Version:

http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-v1.0-os.html

http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-v1.0-os.pdf

http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-v1.0-os.doc

Latest Version:

http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-v1.0-os.html

http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-v1.0-os.pdf

http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-v1.0-os.doc

Technical Committee:

OASIS Digital Signature Services TC

Chair(s):

Nick Pope, Thales eSecurity

Juan Carlos Cruellas, Centre d'aplicacions avançades d'Internet (UPC)

Editor(s):

Andreas Kuehne, individual

Related work:

This specification is related to:

- [oasis-dss-core-spec-v1.0-os](#)

Abstract:

This document defines protocol profiles and processing profiles for the purpose of creating and verifying German Signature Law signatures.

35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53

Status:

This document was last revised or approved by the membership of OASIS on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/dss/>.

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 Technical Committee web page (<http://www.oasis-open.org/committees/dss/ipr.php>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/dss/>.

The non-normative errata page for this specification is located at www.oasis-open.org/committees/dss/.

54 **Notices**

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

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

67 Copyright © OASIS® 1993–2007. All Rights Reserved. OASIS trademark, IPR and other policies
68 apply.

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

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

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

85 The names "OASIS" are trademarks of OASIS, the owner and developer of this specification, and
86 should be used only to refer to the organization and its official outputs. OASIS welcomes
87 reference to, and implementation and use of, specifications, while reserving the right to enforce
88 its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for
89 above guidance.

90

91 **Table of Contents**

92 1 Introduction 5
93 1.1 Terminology..... 5
94 1.2 Normative References 5
95 1.3 Non-Normative References..... 6
96 1.4 Namespaces 6
97 2 Profile Features..... 7
98 2.1 Identifier..... 7
99 2.2 Scope 7
100 2.3 Relationship To Other Profiles 7
101 2.4 Signature Object..... 7
102 2.5 Transport Binding..... 7
103 2.6 Security Binding 7
104 3 Profile of Signing Protocol..... 8
105 3.1 Element <SignRequest> 8
106 3.1.1 Element <OptionalInputs> 8
107 3.1.1.1 Element <SignedProperties> 8
108 3.1.1.1.1 Requesting SignerRole 8
109 3.1.1.2 Element < ClaimedIdentity > 8
110 3.1.2 Element <InputDocuments> 8
111 3.2 Element <SignResponse> 9
112 3.2.1 Element <Result> 9
113 3.2.2 Element <OptionalOutputs> 9
114 3.2.3 Element <SignatureObject> 9
115 4 Profile of Verifying Protocol..... 10
116 4.1 Element <VerifyRequest> 10
117 4.1.1 Element <OptionalInputs> 10
118 4.1.2 Element <SignatureObject>..... 10
119 4.1.3 Element <InputDocuments> 10
120 4.2 Element <VerifyResponse> 10
121 4.2.1 Element <Result> 10
122 4.2.2 Element <OptionalOutputs> 10
123 4.2.2.1 Element <Document>10
124 4.2.2.2 Element <SignerRole>.....10
125 5 Profile of Server Processing Rules 12
126 A. Acknowledgements 13
127

128 1 Introduction

129 This DSS profile is to support creation and validation of qualified signatures according to the
130 guidelines given by the german signature law (SigG) **[SigG]** and its associated regulations
131 **[SigV]**. The EU certified that the german signature law complies with the european legal
132 framework. So this DSS profile may be used as a template for national profiles all over Europe.

133 The DSS signing and verifying protocols are defined in **[DSSCore]**. As defined in that document,
134 these protocols have a fair degree of flexibility and extensibility. This document defines a protocol
135 profile of these protocols that limit their flexibility to comply with the given SigG regulations. It also
136 defines processing profiles that govern how clients and servers should behave when using these
137 protocol.

138 However, these profiles still leave certain things undefined. You cant understand this profile as a
139 definition of an interface. Thus further profiles will build on / implement the ones in this document.

140 1.1 Terminology

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

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

149 1.2 Normative References

150 **[Core-XSD]** S Drees et al. *DSS Schema*. OASIS, February 2007.

151 **[DSSCore]** S Drees et al. *Digital Signature Service Core Protocols and Elements*. OASIS,
152 February 2007.

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

155 **[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML*.
156 <http://www.w3.org/TR/1999/REC-xml-names-19990114>, W3C Recommendation, January 1999.

157 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*.
158 <http://www.w3.org/TR/1999/REC-xml-names-19990114>, W3C Recommendation, February 2002.

159 **[SigG]** *Framework for Electronic Signatures, Amendment of Further Regulations Act*
160 (*Signaturgesetz – SigG*).

161 <http://www.bundesnetzagentur.de/media/archive/3612.pdf>

162 **[SigV]** *Electronic Signature Ordinance (Signaturverordnung – SigV)*.

163 <http://www.bundesnetzagentur.de/media/archive/3613.pdf>

164 **[Algorithms]** *Suitable Cryptographic Algorithms*

165 http://www.bundesnetzagentur.de/enid/87813fdad06a8c942d819a8058fc7c16,0/Publications_and
166 [_Notifications/Suitable_Algorithms_z8.html](http://www.bundesnetzagentur.de/enid/87813fdad06a8c942d819a8058fc7c16,0/Publications_and)

167 **[Async]** *Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services*.
168 OASIS, February 2007

169 **1.3 Non-Normative References**

170 **1.4 Namespaces**

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

174 This schema is associated with the following XML namespace:

175 `urn:oasis:names:tc:dss:1.0:profiles:germanSignatureLaw`

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

177

178 Conventional XML namespace prefixes are used in this document:

- 179 • The prefix `dss:` (or no prefix) stands for the DSS core namespace **[Core-XSD]**.
180 • The prefix `ds:` stands for the W3C XML Signature namespace **[XMLSig]**.

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

184 2 Profile Features

185 2.1 Identifier

186 `urn:oasis:names:tc:dss:1.0:profiles:germanSignatureLaw`

187 Assign this profile a URI for use in the Profile attribute. Or say “This profile does not specify a
188 URI Identifier”. If this profile inherits from another profile, such that a server implementing this
189 profile could be contacted by a client implementing the super-protocol, mention the super-profile’s
190 identifier as well:

191 2.2 Scope

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

193 2.3 Relationship To Other Profiles

194 The profiles in this document are based on the **[DSSCore]**. The profiles in this document are not
195 implementable directly, but are further profiled by other profiles. The german signature law
196 doesn’t have any limitations on the signature format. So at least one other profile will be used
197 together with this profile.

198 Due to the imposed processing guidelines the server usually needs from hours to days to fulfill a
199 signing request. So this profile will likely be combined with profile for asynchronous processing
200 **[Async]**.

201 2.4 Signature Object

202 This profile supports the creation and verification of signatures as defined in the german signature
203 law and its related regulations.

204 2.5 Transport Binding

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

206 2.6 Security Binding

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

208 3 Profile of Signing Protocol

209 This profile does not introduce any new message elements. Therefore no special schema is
210 defined.

211 3.1 Element <SignRequest>

212 3.1.1 Element <OptionalInputs>

213 This profile introduces a new element within the <OptionalInputs>. There may be zero or more
214 <SignerRole> elements included.

215 3.1.1.1 Element <SignedProperties>

216 The requester MAY request the addition of one or more attribute certificates, embedded in a
217 <SignerRole> element. The requester MUST, in such cases, use `dss:SignedProperties`
218 element.

219 Sections below show profiles for the different `dss:Property` elements that MAY appear as
220 children of `dss:SignedProperties` depending on the property requested. This profile define
221 contents for the `Identifier` and `Value` elements.

222 3.1.1.1.1 Requesting SignerRole

223 Value for `Identifier` element:

224

```
225 urn:oasis:names:tc:dss:1.0:profiles:XAdES:SignerRole
```

226

227 When the value of the role is fixed by the requester, this property will have a value that the server
228 will incorporate to the advanced signature. This profile does not restrict the contents of such a
229 value. Corresponding sub-profiles will define their specific schemas.

230

```
231 <xs:element name="SignerRole" type="dss:AnyType" />
```

232 3.1.1.2 Element < ClaimedIdentity >

233 The requester MUST NOT use the <ClaimedIdentity> element. The Identity of the signer is
234 always given by the subject of the used signing certificate.

235 3.1.2 Element <InputDocuments>

236 The client MUST NOT send <DocumentHash> input documents. The client MUST send
237 <Document> input documents explicitly.

238 The signing certificate holder MUST have the ability to check the content of the documents to be
239 signed. The signing process MUST include at least a time slot for the holder to review the
240 documents and reject the documents optionally.

241 **3.2 Element <SignResponse>**

242 **3.2.1 Element <Result>**

243 This profile defines no additional <ResultMinor> codes.

244 Is a 'Intentionally rejected by the certificate holder' a specific ResultMinor code ?

245 **3.2.2 Element <OptionalOutputs>**

246 This profile does not define any additional outputs.

247 **3.2.3 Element <SignatureObject>**

248 This profile does not introduce any restrictions on the type of signature objects.

249

250

251 4 Profile of Verifying Protocol

252 This profile does not introduce any new message elements. Therefore no special schema is
253 defined.

254

255 4.1 Element <VerifyRequest>

256 4.1.1 Element <OptionalInputs>

257 This profile does not introduce any additional input elements.

258 4.1.2 Element <SignatureObject>

259 This profile does not introduce any restrictions on the type of signature objects.

260 4.1.3 Element <InputDocuments>

261 The client MUST send <Document> input documents. The client MUST NOT send
262 <DocumentHash> input documents.

263

264 4.2 Element <VerifyResponse>

265 4.2.1 Element <Result>

266 This profile defines no additional <ResultMinor> codes.

267 4.2.2 Element <OptionalOutputs>

268 Additionally to the <result> element the input documents are returned.

269 Every attribute certificate given in the <SignedProperties> element during signing time must be
270 returned as on or more <SignerRole> elements.

271 4.2.2.1 Element <Document>

272 The server MUST return the <Document> input documents.

273 The result of the verification has to be related to the input documents directly. Therefore the input
274 documents will be returned as part of the <VerifyResponse> within the <OptionalOutputs>.

275 4.2.2.2 Element <SignerRole>

276 Every attribute certificate included in the <SignedProperties> element of the signature MUST be
277 returned. The attribute certificates are wrapped in a <SignerRole>.

278 The attribute certificates may introduce restrictions regarding the use of the certificates. To
279 appraise the legal value of a signature not only the formal correctness but also the included
280 restrictions must be taken into account.

281 Value for Identifier element:

282

283

```
urn:oasis:names:tc:dss:1.0:profiles:XAdES:SignerRole
```

284

285 The server fills in the value of the incorporated attribute certificates.

286

287

```
<xs:element name="SignerRole" type="dss:AnyType" />
```

288

289

290

291 **5 Profile of Server Processing Rules**

292 The german signature law, its related regulations and the list of applicable algorithms introduces
293 many constraints on the creation and the verification of a signature. A signature service
294 implementing this profile assures that the processing and the results comply with this regulations.

295

296

297

298

A. Acknowledgements

299
300

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

301
302
303

Participants:

Trevor Perrin, individual