



German Signature Law Profile of the OASIS Digital Signature Service

Committee Draft, 21 August, 2004
(Working Draft 03)

Document identifier:

oasis-dss-1.0-profiles-german-signature-law-spec-cd-01

Location:

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

Editor:

Andreas Kuehne, individual <kuehne@klup.de>

Contributors:

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

Abstract:

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

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>.

26 **Table of Contents**

27 1 Introduction 3
28 1.1 Notation 3
29 1.2 Namespaces 3
30 2 Profile Features 4
31 2.1 Identifier 4
32 2.2 Scope 4
33 2.3 Relationship To Other Profiles 4
34 2.4 Signature Object 4
35 2.5 Transport Binding 4
36 2.6 Security Binding 4
37 3 Profile of Signing Protocol 5
38 3.1 Element <SignRequest> 5
39 3.1.1 Element <OptionalInputs> 5
40 3.1.2 Element <InputDocuments> 5
41 3.2 Element <SignResponse> 6
42 3.2.1 Element <Result> 6
43 3.2.2 Element <OptionalOutputs> 6
44 3.2.3 Element <SignatureObject> 6
45 4 Profile of Verifying Protocol 7
46 4.1 Element <VerifyRequest> 7
47 4.1.1 Element <OptionalInputs> 7
48 4.1.2 Element <SignatureObject> 7
49 4.1.3 Element <InputDocuments> 7
50 4.2 Element <VerifyResponse> 7
51 4.2.1 Element <Result> 7
52 4.2.2 Element <OptionalOutputs> 7
53 5 Profile of Server Processing Rules 9
54 6 Editorial Issues 10
55 7 References 11
56 7.1 Normative 11
57 Appendix A. Revision History 12
58 Appendix B. Notices 13
59

60 1 Introduction

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

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

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

72 1.1 Notation

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

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

81 1.2 Namespaces

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

85 This schema is associated with the following XML namespace:

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

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

88

89 Conventional XML namespace prefixes are used in this document:

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

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

95 2 Profile Features

96 2.1 Identifier

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

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

102 2.2 Scope

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

104 2.3 Relationship To Other Profiles

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

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

112 2.4 Signature Object

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

115 2.5 Transport Binding

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

117 2.6 Security Binding

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

119 3 Profile of Signing Protocol

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

122 3.1 Element <SignRequest>

123 3.1.1 Element <OptionalInputs>

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

126 3.1.1.1 Element <SignedProperties>

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

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

133 3.1.1.1.1 Requesting SignerRole

134 Value for `Identifier` element:

135

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

137

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

141

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

143 3.1.1.2 Element < ClaimedIdentity >

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

146 3.1.2 Element <InputDocuments>

147 The client MUST NOT send <DocumentHash> input documents. The client MUST send
148 <Document> input documents explicitly.

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

152 **3.2 Element <SignResponse>**

153 **3.2.1 Element <Result>**

154 This profile defines no additional <ResultMinor> codes.

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

156 **3.2.2 Element <OptionalOutputs>**

157 This profile does not define any additional outputs.

158 **3.2.3 Element <SignatureObject>**

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

160

161

162 4 Profile of Verifying Protocol

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

165

166 4.1 Element <VerifyRequest>

167 4.1.1 Element <OptionalInputs>

168 This profile does not introduce any additional input elements.

169 4.1.2 Element <SignatureObject>

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

171 4.1.3 Element <InputDocuments>

172 The client MUST send <Document> input documents. The client MUST NOT send
173 <DocumentHash> input documents.

174

175 4.2 Element <VerifyResponse>

176 4.2.1 Element <Result>

177 This profile defines no additional <ResultMinor> codes.

178 4.2.2 Element <OptionalOutputs>

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

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

182 4.2.2.1 Element <Document>

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

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

186 4.2.2.2 Element <SignerRole>

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

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

192 Value for Identifier element:

193

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

195

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

197

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

199

200

201

202 **5 Profile of Server Processing Rules**

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

206

207

208

209 **6 Editorial Issues**

210 The enumeration of all requirements given by the german signature law and its regulations wasn't
211 done. On one hand this would be redundant regarding the existing documents, on the other hand
212 errors or misinterpretations may be introduced.

213 7 References

214 7.1 Normative

- 215 **[Core-XSD]** T. Perrin et al. *DSS Schema*. OASIS, **(MONTH/YEAR TBD)**
- 216 **[DSSCore]** T. Perrin et al. Digital Signature Service Core Protocols and Elements. OASIS,
217 **(MONTH/YEAR TBD)**
- 218 **[RFC 2119]** S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. IETF
219 RFC 2396, August 1998.
- 220 <http://www.ietf.org/rfc/rfc2396.txt>.
- 221 **[XML-ns]** T. Bray, D. Hollander, A. Layman. Namespaces in XML. W3C
222 Recommendation, January 1999.
- 223 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
- 224 **[XMLSig]** D. Eastlake et al. XML-Signature Syntax and Processing. W3C
225 Recommendation, February 2002.
- 226 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
- 227
- 228 **[SigG]** Framework for Electronic Signatures, Amendment of Further Regulations Act
229 (Signaturgesetz – SigG).
- 230 http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/119.pdf
- 231
- 232 **[SigV]** Electronic Signature Ordinance (Signaturverordnung – SigV).
- 233 http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/120.pdf
- 234
- 235 **[Algorithms]** Suitable Cryptographic Algorithms
- 236 http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/03/index.html
- 237
- 238 **[Async]** Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services.
239 OASIS, **(MONTH/YEAR TBD)**
- 240
- 241
- 242

Appendix A. Revision History

Rev	Date	By Whom	What
wd-01	2004-02-28	Andreas Kuehne	Initial version
wd-02	2004-04-05	Andreas Kuehne	Added attribute certificates as <SignerRoles>

Appendix B. Notices

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

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

257 Copyright © OASIS Open 2003. All Rights Reserved.

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

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

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