



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

## Committee Specification

13 February 2007

### Specification URIs:

#### This Version:

[http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german\\_signature\\_law-spec-cs-v1.0-r1.html](http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-cs-v1.0-r1.html)

[http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german\\_signature\\_law-spec-cs-v1.0-r1.pdf](http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-cs-v1.0-r1.pdf)

#### Latest Version:

[http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german\\_signature\\_law-spec-cs-v1.0-r1.html](http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-cs-v1.0-r1.html)

[http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german\\_signature\\_law-spec-cs-v1.0-r1.pdf](http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-german_signature_law-spec-cs-v1.0-r1.pdf)

### 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-cs-v1.0-r1](#)

### Abstract:

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

### Status:

This document was last revised or approved by the OASIS Digital Signature Services TC 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.

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

40 For information on whether any patents have been disclosed that may be essential to  
41 implementing this specification, and any offers of patent licensing terms, please refer to  
42 the Intellectual Property Rights section of the Technical Committee web page  
43 (<http://www.oasis-open.org/committees/dss/ipr.php>).

44 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/dss)  
45 [open.org/committees/dss](http://www.oasis-open.org/committees/dss).

46

47 The non-normative errata page for this specification is located at [www.oasis-](http://www.oasis-open.org/committees/dss)  
48 [open.org/committees/dss](http://www.oasis-open.org/committees/dss).

49

---

## Notices

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

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

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

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

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

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

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

86

## Table of Contents

88	1	Introduction .....	5
89	1.1	Terminology.....	5
90	1.2	Normative References .....	5
91	1.3	Non-Normative References.....	6
92	1.4	Namespaces .....	6
93	2	Profile Features.....	7
94	2.1	Identifier.....	7
95	2.2	Scope .....	7
96	2.3	Relationship To Other Profiles .....	7
97	2.4	Signature Object.....	7
98	2.5	Transport Binding.....	7
99	2.6	Security Binding .....	7
100	3	Profile of Signing Protocol.....	8
101	3.1	Element <SignRequest> .....	8
102	3.1.1	Element <OptionalInputs> .....	8
103	3.1.1.1	Element <SignedProperties> .....	8
104	3.1.1.1.1	Requesting SignerRole .....	8
105	3.1.1.1.2	Element < ClaimedIdentity >.....	8
106	3.1.2	Element <InputDocuments> .....	8
107	3.2	Element <SignResponse> .....	9
108	3.2.1	Element <Result> .....	9
109	3.2.2	Element <OptionalOutputs> .....	9
110	3.2.3	Element <SignatureObject>.....	9
111	4	Profile of Verifying Protocol.....	10
112	4.1	Element <VerifyRequest> .....	10
113	4.1.1	Element <OptionalInputs> .....	10
114	4.1.2	Element <SignatureObject>.....	10
115	4.1.3	Element <InputDocuments> .....	10
116	4.2	Element <VerifyResponse> .....	10
117	4.2.1	Element <Result> .....	10
118	4.2.2	Element <OptionalOutputs> .....	10
119	4.2.2.1	Element <Document> .....	10
120	4.2.2.2	Element <SignerRole>.....	10
121	5	Profile of Server Processing Rules .....	12
122	A.	Acknowledgements .....	13
123			

---

## 124 1 Introduction

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

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

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

### 136 1.1 Terminology

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

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

### 145 1.2 Normative References

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

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

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

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

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

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

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

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

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

160 **[Algorithms]** Suitable Cryptographic Algorithms

161 [http://www.bundesnetzagentur.de/enid/87813fdad06a8c942d819a8058fc7c16,0/Publications\\_and](http://www.bundesnetzagentur.de/enid/87813fdad06a8c942d819a8058fc7c16,0/Publications_and)  
162 [\\_Notifications/Suitable\\_Algorithms\\_z8.html](http://www.bundesnetzagentur.de/enid/87813fdad06a8c942d819a8058fc7c16,0/Publications_and)

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

165 **1.3 Non-Normative References**

166 **1.4 Namespaces**

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

170 This schema is associated with the following XML namespace:

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

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

173

174 Conventional XML namespace prefixes are used in this document:

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

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

---

## 180 2 Profile Features

### 181 2.1 Identifier

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

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

### 187 2.2 Scope

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

### 189 2.3 Relationship To Other Profiles

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

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

### 197 2.4 Signature Object

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

### 200 2.5 Transport Binding

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

### 202 2.6 Security Binding

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

---

## 204 3 Profile of Signing Protocol

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

### 207 3.1 Element <SignRequest>

#### 208 3.1.1 Element <OptionalInputs>

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

##### 211 3.1.1.1 Element <SignedProperties>

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

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

##### 218 3.1.1.1.1 Requesting SignerRole

219 Value for `Identifier` element:

220

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

222

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

226

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

##### 228 3.1.1.2 Element < ClaimedIdentity >

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

#### 231 3.1.2 Element <InputDocuments>

232 The client MUST NOT send <DocumentHash> input documents. The client MUST send  
233 <Document> input documents explicitly.

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



237 **3.2 Element <SignResponse>**

238 **3.2.1 Element <Result>**

239 This profile defines no additional <ResultMinor> codes.

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

241 **3.2.2 Element <OptionalOutputs>**

242 This profile does not define any additional outputs.

243 **3.2.3 Element <SignatureObject>**

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

245

246

---

## 247 4 Profile of Verifying Protocol

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

250

### 251 4.1 Element <VerifyRequest>

#### 252 4.1.1 Element <OptionalInputs>

253 This profile does not introduce any additional input elements.

#### 254 4.1.2 Element <SignatureObject>

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

#### 256 4.1.3 Element <InputDocuments>

257 The client MUST send <Document> input documents. The client MUST NOT send  
258 <DocumentHash> input documents.

259

### 260 4.2 Element <VerifyResponse>

#### 261 4.2.1 Element <Result>

262 This profile defines no additional <ResultMinor> codes.

#### 263 4.2.2 Element <OptionalOutputs>

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

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

##### 267 4.2.2.1 Element <Document>

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

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

##### 271 4.2.2.2 Element <SignerRole>

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

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

277 Value for Identifier element:

278

279

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

280

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

282

283

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

284

285

286

---

287 **5 Profile of Server Processing Rules**

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

291

292

293

---

294 **A. Acknowledgements**

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

297 **Participants:**

298 Trevor Perrin, individual

299