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.

Table of Contents

1 Introduction

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

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

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

1.1 Notation

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

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

1.2 Namespaces

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

This schema is associated with the following XML namespace:

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

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

Conventional XML namespace prefixes are used in this document:

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

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

2 Profile Features

2.1 Identifier

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

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

2.2 Scope

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

2.3 Relationship To Other Profiles

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

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

2.4 Signature Object

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

2.5 Transport Binding

This profile does not specify or constrain the transport binding.

2.6 Security Binding

This profile does not specify or constrain the security binding.

3 Profile of Signing Protocol

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

3.1 Element <SignRequest>

3.1.1 Element <OptionalInputs>

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

3.1.1.1 Element <SignedProperties>

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

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

3.1.1.1.1 Requesting SignerRole

Value for Identifier element:

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

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

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

3.1.1.2 Element < ClaimedIdentity >

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

3.1.2 Element <InputDocuments>

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

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

3.2 Element <SignResponse>

3.2.1 Element <Result>

This profile defines no additional `<ResultMinor>` codes.

Is a ‘Intentionally rejected by the certificate holder’ a specific ResultMinor code ?

3.2.2 Element <OptionalOutputs>

This profile does not define any additional outputs.

3.2.3 Element <SignatureObject>

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

4 Profile of Verifying Protocol

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

4.1 Element <VerifyRequest>

4.1.1 Element <OptionalInputs>

This profile does not introduce any additional input elements.

4.1.2 Element <SignatureObject>

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

4.1.3 Element <InputDocuments>

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

4.2 Element <VerifyResponse>

4.2.1 Element <Result>

This profile defines no additional <ResultMinor> codes.

4.2.2 Element <OptionalOutputs>

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

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

4.2.2.1 Element <Document>

The server MUST return the <Document> input documents.

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

4.2.2.2 Element <SignerRole>

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

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

Value for Identifier element:

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

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

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

5 Profile of Server Processing Rules

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

6 Editorial Issues

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

7 References

7.1 Normative

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

[DSSCore] T. Perrin et al. Digital Signature Service Core Protocols and Elements. OASIS, **(MONTH/YEAR TBD)**

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

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

[XML-ns] T. Bray, D. Hollander, A. Layman. Namespaces in XML. W3C Recommendation, January 1999.

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

[XMLSig] D. Eastlake et al. XML-Signature Syntax and Processing. W3C Recommendation, February 2002.

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

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

http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/119.pdf

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

http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/120.pdf

[Algorithms] Suitable Cryptographic Algorithms

http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/03/index.html

[Async] Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services. OASIS, **(MONTH/YEAR TBD)**

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

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

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