Signature Policy Profile of the OASIS Digital Signature Services Version 1.0

Committee Draft 01

18 May 2009

Specification URIs:
This Version:
http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.doc
http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.html
http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.pdf
(Authoritative)

Previous Version:
N/A

Latest Version:
http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy.doc
http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy.html
http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy.pdf

Technical Committee:
OASIS Digital Signature Services eXtended (DSS-X) TC

Chair(s):
Juan Carlos Cruellas, *UPC-DAC* <cruellas@ac.upc.ede>
Stefan Drees, Individual Member, <stefan@drees.name>.

Editor(s):
Juan Carlos Cruellas, , *UPC-DAC,* <pvde@sonnenglanz.net>

Related work:
This specification is related to:

- OASIS Digital Signature Service Core Protocols, Elements and Bindings. Version 1.0.

Abstract:
TBC

Status:
This document was last revised or approved by the OASIS DSS-X TC on the above date. The level of approval is also listed above. Check the “Latest Version” location noted above for possible later revisions of this document.

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-x/.

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-x/ipr.php.

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

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

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

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

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names and abbreviations here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

NOTICES **3**

TABLE OF CONTENTS **4**

1 INTRODUCTION **5**

1.1 TERMINOLOGY 5
1.2 NAMESPACES 5
1.3 NORMATIVE REFERENCES 6
1.4 NON NORMATIVE REFERENCES 6

2 OVERVIEW **7**

2.1 PROFILE FEATURES 8
2.1.1 Scope *8*
2.1.2 Relationship To Other Profiles *8*
2.1.3 Element <dss:SignatureObject> *8*
2.2 PROFILE OF SIGNING PROTOCOL 8
2.2.1 Element <dss:SignRequest> *8*
2.2.1.1 Element <dss:OptionalInputs> 8
2.2.1.1.1 New Optional Inputs 8
2.2.1.1.1.1 Optional Input <GenerateUnderSignaturePolicy> 8
2.2.1.1.1.2 Optional Input <ReturnSupportedSignaturePolicies> 9
2.2.2 Element <dss:SignResponse> *9*
2.2.2.1 Element <dss:Result> 9
2.2.2.2 Element <dss:OptionalOutputs> 10
2.2.2.2.1.1 Optional Output <UsedSignaturePolicy> 10
2.2.2.2.1.2 Optional Output <SupportedSignaturePolicies> 10
2.3 PROFILE OF VERIFYING PROTOCOL 10
2.3.1 Element <dss:VerifyRequest> *10*
2.3.1.1 Element <dss:OptionalInputs> 10
2.3.1.1.1 New Optional Inputs 11
2.3.1.1.1.1 Optional Input <VerifyUnderSignaturePolicy> 11
2.3.2 Element <dss:VerifyResponse> *11*
2.3.2.1 Element <dss:OptionalOutputs> 11
2.3.2.1.1 New Optional Outputs 12
2.3.2.1.1.1 Optional Input <VerifiedUnderSignaturePolicy> 12

3 CONFORMANCE **13**

3.1 CONFORMANCE LEVEL 1 13
3.2 CONFORMANCE LEVEL 2 13

A. REVISION HISTORY **14**

1 Introduction

ETSI has specified formats for Advanced Electronic Signatures (AdES) built on XML signatures as specified [XMLSig] -TS 101 903: “XML Advanced Electronic Signatures (XAdES)- and CMS signatures – TS 101 733: “CMS Advanced Electronic Signatures (CAdES)”-.

The DSS signing and verifying protocols are defined in [DSSCore]. The “Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0” [AdES-DSS] profiles [DSSCore] for requesting generation and verification of AdES signatures to a centralized server.

AdES signatures may contain explicit identifiers of Signature Policy, which provides rules for generating and verifying these signatures.

This document extends [DSSCore] protocol specifying a number of operations for managing generation and verification of electronic signatures under the rules established by a Signature Policy, as identified in [SigPol-DSS-Req].

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **Error! Reference source not found.**.

1.2 Namespaces

All schema listings in the current document are excerpts from the schema file [SigPol-DSS-XSD]. 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-x:1.0:profiles:SignaturePolicy:schema#`

The table below lists the namespaces referenced in this specification.

Prefix	Namespace	Specification(s)
ds	`http://www.w3.org/2000/09/xmldsig#`	**[XMLSig]**
dss	`urn:oasis:names:tc:dss:1.0:core:schema`	**[DSSCore]**
xades	`http://uri.etsi.org/01903/v1.3.2#`	**[XAdES]**
dssades	`urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#`	**[AdES-DSS]**
xs	`http://www.w3.org/2001/XMLSchema`	**[XMLSchema]**
vr	`urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#`	**[DSSVerRep]**

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].

1.3 Normative References

[AdES-DSS] OASIS Standard, "*Advanced* Electronic *Signature Profiles of the OASIS Digital Signature Service Version 1.0".* April 2007 http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf.

[CAdES] CMS Advanced Electronic Signatures. ETSI TS 101 733, January 2007.

[Core-XSD] OASIS Standard, *DSS Schema*. February 2007.

[DSS Core] OASIS Standard, "Digital Signature Service Core Protocols, Elements and Bindings. Version 1.0" April 2007. http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf.

[DSSCore] OASIS Standard, *Digital Signature Service Core Protocols and Elements*. February 2007.

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[RFC 3001] M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3001, November 2000.

[RFC 3852] R. Housley. Cryptographic Message Syntax (CMS) , IETF RFC 3852, July 2004.

[SigPol-DSS-XSD] OASIS Standard, "Signature Policy Profile Schema".,

[XAdES] Advanced Electronic Signatures. ETSI TS 101 733. March 2006.

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

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

[XMLSchema] Henry S. Thompson, David Beech, Murray Maloney, Noah Mendelson. *XML Schema Part 1: Structures Second Edition.* http://www.w3.org/TR/xmlschema-1/, W3C Recommendation 28 October 2004.

[DSSVerRep] Ingo Henkel, Detlef Hühnlein. *Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0*

1.4 Non Normative References

[SigPol-DSS-Req] Juan Carlos Cruellas. *Requirements for specifying the Signature Policy Profile of the OASIS Digital Signature Services*, OASIS, November 2007

2 Overview

This profile supports a number of operations for managing generation and verification of electronic signatures under the rules established by a Signature Policy, as identified in [SigPol-DSS-Req].

For the generation of electronic signatures, the following operations apply:

SignRequest. This operation supports:

- Requesting generation of a signature under a certain signature policy, allowing clients to explicitly identify that signature policy in the request. This identification may be through the usage of both, a URI or an OID.
- Passing to the server the location and/or the digest of the electronic document where the signature policy is specified .
- Requesting to the server the incorporation within the signature to be generated the identifier of the signature policy under which it has been created, using syntaxes defined in [XAdES] or [CAdES].
- Requesting also a list of the supported signature policies supported by the server.

SignResponse. This operation supports delivery of:

- Electronic signatures with the identifier of the signature policy under which they have been generated.
- Indication of the signature policy under which the signature has been generated within `<dss:SignResponse>`.
- Digest of the electronic document where the signature policy is defined, as a double check facility for the client.
- A code error in case the server may not sign with the requested signature policy.
- The list of supported signature policy identifiers.

For electronic signature verification (and updating) the following operations apply:

VerifyRequest. This operation supports requests for:

- Request the verification of a signature under a certain signature policy, if the signature does not contain an identifier of such policy, by using an identifier of that policy.
- Requesting signature verification under the signature policies identified within the signature, if any identifier is present there.
- Passing to the server the location and/or the digest of the electronic document where the signature policy is specified.
- Requesting return of explicit indication of the signature policies under which the electronic signatures have been verified.
- Requesting also a list of the supported signature policies supported by the server.

VerifyResponse. This operation supports delivery of:

Indication of the signature policies under which the server has verified the electronic signatures mentioned above.

Digest of the electronic document where the signature policy is defined, as a double check facility for the client.

A code error in case the server may not verify the electronic signature(s) with the requested signature policy(ies).

The list of supported signature policy identifiers.

2.1 Profile Features

2.1.1 Scope

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

2.1.2 Relationship To Other Profiles

The profile in this document is based on the [DSSCore]. The profile in this document may be implemented.

This profile provides means for the explicit management of signature policies with [DSSCore] and other existing profiles like [AdES-DSS], and as such, it may be used in conjunction with these specifications.

2.1.3 Element <dss:SignatureObject>

This profile supports requests for generation and verification of electronic signatures under a given signature policy.

Although this specification does not impose any constraint the format of the signatures generated by the servers or sent to the servers for verification, it nicely fits with formats of advanced signatures as defined in [XAdES] and [CAdES].

2.2 Profile of Signing Protocol

2.2.1 Element <dss:SignRequest>

This clause profiles the <dss:SignRequest> element.

2.2.1.1 Element <dss:OptionalInputs>

This profile does not impose any restrictions on any optional input specified in the [DSSCore] or other profiles.

This profile defines a new Optional Input as indicated below.

2.2.1.1.1 New Optional Inputs

2.2.1.1.1.1 Optional Input <GenerateUnderSignaturePolicy>

This optional input will specify the signature policy under which the server is requested to generate the electronic signature.

Below follows the schema for this element:

```
<xs:element name="GenerateUnderSignaturePolicy"
type="SignaturePolicyDetailsType"/>

<xs:complexType name="SignaturePolicyDetailsType">
   <xs:sequence>
         <xs:element name="SignaturePolicyIdentifier" type="xs:anyURI"/>
         <xs:element name="SignaturePolicyLocation" type="xs:anyURI"
           minOccurs="0"/>
         <xs:element name="DigestAndAlgorithm"
           type="xades:DigestAlgAndValueType" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>
```

Element <SignaturePolicyIdentifier> contains the identifier of the signature policy as an URI. Signature policies MAY be identified by an URI or by OIDs. Should the signature policy identifier requested by the client be an OID, this element will contain a URN built from the actual value of this OID as specified in [RFC 3001].

Element <SignaturePolicyLocation> is optional and contains the location where the electronic document specifying the identified signature policy may be found.

Element <DigestAndAlgorithm> is optional and contains the digest value of the aforementioned electronic document and the identifier of the digest algorithm used for computing such a value.

2.2.1.1.1.2 Optional Input <ReturnSupportedSignaturePolicies>

This optional input is an empty element, which, when present instructs the server to return within the corresponding <dss:SignResponse> the <SupportedSignaturePolicies> Optional Output identifying all the signature policies supported by this server as described later on in this document.

Below follows the schema for this element:

```
<xs:element name="ReturnSupportedSignaturePolicies" />
```

2.2.2 Element <dss:SignResponse>

This clause profiles the <dss:SignResponse> element.

2.2.2.1 Element <dss:Result>

This profile adds the following <ResultMinor> values to the ones already specified in the [DSSCore] for those cases where the <ResultMajor> code is Success.

urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyNotSupported

The server does not support the signature policy identified in the request.

urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyDigestFailure

The server computed a digest value on the electronic document defining the signature policy that was not equal to the value included in the request,.

urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyIdentifierError

The server concluded that the identifier of the signature policy was not correctly built.

2.2.2.2 Element <dss:OptionalOutputs>

This profile does not impose any restrictions on any optional output specified in the [DSSCore] or other profiles other than those explicitly mentioned in the clauses below.

This profile defines new Optional Outputs as indicated below.

2.2.2.2.1.1 Optional Output <UsedSignaturePolicy>

This optional output will provide to the client details of the signature policy under which the server has actually generated the electronic signature.

Below follows the schema for this element:

```
<xs:element name="UsedSignaturePolicy" type="SignaturePolicyDetailsType"/>
```

No additional constraints are specified for the contents of this element.

2.2.2.2.1.2 Optional Output <SupportedSignaturePolicies>

This optional output will provide to the client details of the signature policies under which the server is able to generate electronic signatures.

Below follows the schema for this element:

```
<xs:element name="SupportedSignaturePolicies">
   <xs:complexType>
          <xs:sequence>
                <xs:element name="SupportedSignaturePolicy"
                  type="SignaturePolicyDetailsType" maxOccurs="unbounded"/>
          </xs:sequence>
   </xs:complexType>
</xs:element>
```

No additional constraints are specified for the contents of `<SuppoertedSignaturePolicy>` elements.

2.3 Profile of Verifying Protocol

2.3.1 Element <dss:VerifyRequest>

This clause profiles the `<dss:VerifyRequest>` element.

2.3.1.1 Element <dss:OptionalInputs>

This profile does not impose any restrictions on any optional input specified in the [DSSCore] or other profiles.

This profile defines a new Optional Input as indicated below.

2.3.1.1.1 New Optional Inputs

2.3.1.1.1.1 Optional Input <VerifyUnderSignaturePolicy>

This optional input allows to instruct the server to use certain signature policy for verifying all (or selected) signatures that do not contain an explicit indication of having been produced under a certain signature policy.

Signatures containing such an explicit indication MUST be verified using the explicitly indicated signature policy, regardless the contents of the optional input specified in this section.

```
<xs:element name="VerifyUnderSignaturePolicy"
type="VerifyUnderSignaturePolicyType"/>

<xs:complexType name="VerifyUnderSignaturePolicyType">
   <xs:sequence>
          <xs:element name="DefaultPolicy" type="SignaturePolicyDetailsType"
minOccurs="0"/>
          <xs:element ref="ExplicitPolicies" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>

<xs:element name="ExplicitPolicies" type="PolicySignaturePairsType" />
<xs:complexType name="PolicySignaturePairsType">
   <xs:sequence>
          <xs:element ref="PolicySignaturePair" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>

<xs:element name="PolicySignaturePair" type="PolicySignaturePairType" />
<xs:complexType name="PolicySignaturePairType">
   <xs:sequence>
          <xs:element ref="SignatureIdentifier" />
            <xs:element ref="SignaturePolicy" />
   </xs:sequence>
</xs:complexType>
<xs:element name="SignaturePolicy" type="SignaturePolicyDetailsType" />
<xs:element name="SignatureIdentifier" type="vr:SignatureIdentifierType" />
```

Optional element `<DefaultPolicy>` specifies a default policy that the server should use for verifying any found signature that: does not have any explicit indication of signature policy and that it is not referenced within the `<ExplicitPolicies>` element.

Optional element `<ExplicitPolicies>` is a list of [signature , signature policy] pairs, each one instructing the server to verify the referenced signature of the pair with the signature policy indicated in the pair. Should the referenced signature contain an explicit indication of a different signature policy, the server will use this last one and will issue a warning reporting this situation.

2.3.2 Element <dss:VerifyResponse>

2.3.2.1 Element <dss:OptionalOutputs>

This profile does not impose any restrictions on any optional output specified in the [DSSCore] or other profiles other than those explicitly mentioned in the clauses below.

This profile defines new Optional Outputs as indicated below.

2.3.2.1.1 New Optional Outputs

2.3.2.1.1.1 Optional Input <VerifiedUnderSignaturePolicy>

This optional output will be returned by the server to indicate under what signature policy a certain signature has been verified.

```
<xs:element name="VerifiedUnderSignaturePolicy"
type="VerifiedUnderSignaturePolicyType"/>

<xs:complexType name="VerifiedUnderSignaturePolicyType">
   <xs:sequence>
          <xs:element ref="SignaturePolicy" />
          <xs:element ref="SignatureIdentifier" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>
```

Mandatory <SignaturePolicy> will identify the signature policy used.

Optional <SignatureIdentifier> references the signature that was verified under such a signature policy.

Should this optional output be present within the <vr:IndividualSignatureReport> then <VerifiedUnderSignaturePolicy> will not contain the <SignatureIdentifier> optional element (as this element will actually appear as child of <vr:IndividualSignatureReport>).

Should this optional output not be present within the <vr:IndividualSignatureReport> and <SignatureIdentifier> not present, this optional output will report that all the signatures found have been verified with the same signature policy indicated in <SignaturePolicy> element.

3 Conformance

The present profile defines two conformance levels. These two levels are defined in the clauses below.

3.1 Conformance Level 1

Any implementation of this profile is conformant with this specification if:

1. It fully supports the signing protocol, satisfying the the MUST or REQUIRED level requirements defined in this specification for the aforementioned protocol.
2. It only supports `<VerifyUnderSignaturePolicy>`'s `<DefaultPolicy>` child in the `<dss:VerificationRequest>` element.
3. It only supports `<VerifiedUnderSignaturePolicy>`'s `<SignaturePolicy>` child in the `<dss:VerificationResponse>` element.
4. It satisfies the MUST or REQUIRED level requirements defined in this specification except those that affect the not supported elements of the verification protocol (namely `<VerifyUnderSignaturePolicy>`'s `<SignatureIdentifier>` child and `<VerifiedUnderSignaturePolicy>`'s `<SignatureIdentifier>` child).

3.2 Conformance Level 2

Any implementation of this profile is conformant with this specification if:

1. It fully supports the signing protocol, satisfying the the MUST or REQUIRED level requirements defined in this specification.
2. It fully supports the verification protocol, satisfies the MUST or REQUIRED level requirements defined in this specification for the aforementioned protocol.

A. Revision History

[optional; should not be included in OASIS Standards]

Revision	Date	Editor	Changes Made
0.1	2008-04-25	Juan Carlos Cruellas	Initial Draft. No profile for verification protocol.
0.2	2008-06-09	Juan Carlos Cruellas	Addition of verification protocol and two conformance levels.