Entity Seal Profile of the OASIS Digital Signature Service

Committee Draft, 24 December 2004 (Working Draft 06)

Document identifier:

oasis-dss-1.0-profiles-eseal-spec-cd-01

Location:

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

Editor:

Nick Pope, *individual* <pope@secstan.com>

Contributors:

John Messing, *American Bar Association*
Dallas Powell, *Individual*
Juan Carlos Cruellas, *Individual*
Trevor Perrin, *individual*

Abstract:

This draft defines a profile of the OASIS DSS protocol and XML signature for the purpose of creating and verifying entity seals.

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

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 profiles the core to support creation and validation of a “seal” created by a given Entity or Organization on electronic data.

The seal is a form of electronic signature which:

a) protects the integrity of the document,

b) includes the time at which the seal was applied proving that the data existed at the given time,

c) includes the identity of the entity requesting the seal,

d) may include a statement of intent for applying the seal.

This profile includes a few options that require further profiling for implementing interoperable systems.

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

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]**.
- The prefix xades: stands for the ETSI XML Advanced Electronic Signature namespace **[XAdES]**

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:eseal

2.2 Scope

This document profiles the DSS signing and verifying protocols defined in **[DSSCore]** and profiles the XML signature format for entity seals created by a given Entity or Organization on electronic data.

2.3 Relationship To Other Profiles

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

2.4 Signature Object

This profile supports the creation and verification of [XMLSig] signatures as defined in section 5.

2.5 Transport Binding

This profile is transported using the HTTP POST Transport Binding defined in **[DSSCore]**.

2.6 Security Binding

2.6.1 Security Requirements

This profile MUST use security bindings that:

- Authenticates the requester to the DSS server
- Authenticates the DSS server to the DSS client
- Protects the integrity or a request, response and the association of response to the request.
- Optionally, protects the confidentiality of a request and response

The following is recommended to meet these requirements..

2.6.2 TLS X.509 Mutual Authentication

This profile is secured using the TLS X.509 Mutual Authentication Binding defined in **[DSSCore]**.

3 Profile of Signing Protocol

3.1 Element <SignRequest>

3.1.1 Element <OptionalInputs>

The optional inputs from **[DSSCore]:**

- `<dss:ClaimedIdentity>`
- MUST be supported by the DSS server. This MAY be sent by the client to provide the claimed identity of the requester. If present the `<Name>` element of `<dss:ClaimedIdentity>` MUST be authenticated by the Security Binding.
- `<dss:SignedProperties>`

MAY be supported by the DSS server. If present this MAY be used by the client to request the CommitmentTypeIndication property. The CommitmentTypeIndication property is requested using the identifier and value as defined in [DSS-XAdES].

3.1.2 Element <InputDocuments>

At least one of the following types of InputDocuments from **[DSSCore]:**

- `<dss:DocumentHash>`
- `<dss:Document>`

MUST be supported by the DSS server. The DSS client may use either form.

If the client uses an element that is not supported by the server, the server SHOULD return `ResultMinor` set to indicate `NotSupported` and ResultMessage set to text providing further details`.`

3.2 Element <SignResponse>

3.2.1 Element <Result>

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

3.2.2 Element <OptionalOutputs>

This profile requires no optional options.

3.2.3 Element <SignatureObject>

If successful, the server MUST return a <ds:Signature> with the signature properties as defined in section 5.

4 Profile of Verifying Protocol

4.1 Element <VerifyRequest>

4.1.1 Element <OptionalInputs>

This profile places no specific requirements on the optional inputs.

4.1.2 Element <SignatureObject>

The server MUST support `<ds:Signature>`.

4.1.3 Element <InputDocuments>

The at least one of the input document element from **[DSSCore]:**

- `<dss:DocumentHash>`
- `<dss:Document>`

MUST be supported by the DSS server. The DSS client may use either form. Other elements MAY be supported.

4.2 Element <VerifyResponse>

4.2.1 Element <Result>

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

4.2.2 Element <OptionalOutputs>

This profile places no specific requirements on the optional outputs.

5 Profile of ESeal Signatures

The signature form used by the profile is an XML Signature as defined in **[XMLSig]**.

The XML signature MUST contain the element `<xades:SignedProperties>` within the element `<xades:QualifyingProperties>` as defined in **[XAdES]** within the `<ds:object>` element of the XML signature.

The following property must be present within the `<xades:SignedProperties>` element:

- `<xades:SigningTime>`

In addition, the following may be present:

- `<xades:CommitmentTypeIndication>`

The following property must be present within a `<ds:SignatureProperty>` element:

- `<dss:RequesterIdentity>`

The digest value of the `<ds:SignatureProperty>` and the `<xades:SignedProperties>` elements shall be included in the signature references.

6 Server Processing Rules

6.1 Sign

In addition to the processing rules define in **[Core-XSD]** the server MUST:

a) ensure that the requester is authorized to request an ESeal,

b) authenticate that requester is as identified in `<dss:RequesterIdentity> and,` if present, `<dss:ClaimedIdentity>`

6.2 Verify

In addition to the processing rules define in **[Core-XSD]** the server MUST:

a) ensure that the properties required in section 5 are present.

7 Editorial Issues

1) *Requirements for additional text identified by in line editorial comments.*
2) *Statement of Intent requires further work. Is this a general DSS requirement? This is similar to XAdES commitment type but does not require an OID.*

***Resolution**: Used XadES Commitment type. WD-02*

8 References

8.1 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)**

[DSS-XAdES] Juan Carlos Cruellas et al*. XAdES Profile of the OASIS Digital Signature Service*

[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.

[XAdES] XML Advanced Electronic Signatures ETSI TS 101 903, February 2002 *(shortly to be re-issued)* http://pda.etsi.org/pda/home.asp?wki_id=1UFEyx7ORuBCDGED3IiJH

[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

-

221 Appendix A. Revision History

Rev	Date	By Whom	What
wd-01	2004-03-07	Nick Pope	Initial version
wd-02	2004-03-14	Nick Pope	Filling in further details
wd-03	2004-04-12	Nick Pope	Completing details
wd-04	2004-06-13	Nick Pope	Updating technical details of carrying “`RequesterIdentity`
wd-05	2004-11-13	Nick Pope	Updating in line with comments from Trevor

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.

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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.