Policy-Wise Server Abstract Profile of the OASIS Digital Signature Service

Committee Draft, 24 December, 2004 (Working Draft 04)

Document identifier:

oasis-dss-1.0-profiles-pws-spec-cd-01.doc

Location:

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

Editor:

Paul Madsen, Entrust <p.madsen@entrust.com>

Contributors:

Abstract:

This draft profiles the OASIS DSS core protocols for environments where the client is either ignorant of signing/verification policy or does not have the authority to specify such policy. It is the server (or the infrastructure behind it) that maintains and specifies policy and so is 'policy-wise'. This profile is abstract as it is not expected to be directly implementable but rather is itself profiled by other implementable profiles.

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 3
1.1 Notation 3
1.2 Namespaces 3
1.3 Overview (Non-normative) 3
2 Profile Features 5
2.1 Identifier 5
2.2 Scope 5
2.3 Relationship To Other Profiles 5
2.4 Signature Object 5
2.5 Transport Binding 5
2.6 Security Binding 5
3 Profile of Signing Protocol 6
3.1 Element <SignRequest> 6
3.1.1 Element <OptionalInputs> 6
3.1.2 Element <InputDocuments> 7
3.2 Element <SignResponse> 7
3.2.1 Element <Result> 7
3.2.2 Element <OptionalOutputs> 7
3.2.3 Element <SignatureObject> 7
4 Profile of Verifying Protocol 8
4.1 Element <VerifyRequest> 8
4.1.1 Element <OptionalInputs> 8
4.1.2 Element <SignatureObject> 8
4.1.3 Element <InputDocuments> 8
4.2 Element <VerifyResponse> 8
4.2.1 Element <Result> 8
4.2.2 Element <OptionalOutputs> 8
5 Profile of Server Processing Rules 9
6 References 10
6.1 Normative 10
Appendix A. Revision History 11
Appendix B. Notices 12

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 these protocols to limit their flexibility and extend them in concrete ways. It also profiles the processing rules followed by clients and servers when using these protocols. The resulting profile is an *abstract profile*. Further profiles will build on this one to provide a basis for implementation and interoperability.

The following sections describe how to understand the rest of 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

.

This schema is associated with the following XML namespace:

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

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 `pws:` stands for the DSS code-signing namespace **[PWS-XSD]**.
- 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]**.

1.3 Overview (Non-normative)

DSS provides to clients significant flexibility in customizing the base SignRequest/VerifyRequest messages, implying that the DSS client is sufficiently aware of signing/verification policy to create appropriate requests. In many scenarios, for reasons of security and/or policy management, clients will not have this policy awareness; signing/verification policy will be instead stored and managed at (or behind) the DSS server on behalf of its clients.

Consequently, in these scenarios, the full flexibility that the base DSS profiles provide for request customization is unnecessary. The Policy-wise DSS Profile will remove this undesirable flexibility to facilitate interoperability.

105

106 • Signature creation will be based on DSS SignRequest. Currently optional request inputs for
107 Selective Signing, Signature Placement, Processing steps, Output options, etc will be
108 removed.

109 • Signature verification will be based on DSS VerifyRequest. Currently optional request inputs
110 for Selective Verification, Trust Settings etc will be removed.

2 Profile Features

2.1 Identifier

urn:oasis:names:tc:dss:1.0:profiles:pws

2.2 Scope

This document profiles 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]**. This profile is an abstract profile which is not implementable directly and must be further profiled or combined with another implementable concrete profile.

2.4 Signature Object

This profile does not specify or constrain the type of signature object.

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

3.1 Element <SignRequest>

3.1.1 Attribute profile

The profile identifier for Policy Wise Server MUST NOT be used as the value of the Profile attribute.

3.1.2 Element <OptionalInputs>

The <ServicePolicy> and <ClaimedIdentity>, optional inputs from **[DSSCore]** are supported and may be sent by the client.

Clients MUST NOT send the following optional inputs unless contained within a <SignedInput> element (defined below):

- Element <IntendedAudience>
- Element <SignatureType>
- Element <AddTimestamp>
- Element <KeySelector>
- Element <Language>
- Element <SignedReferences>
- Element <Properties>
- Element <SignaturePlacement>
- Element <EnvelopingSignature>

3.1.2.1 Element <AdditionalProfile>

The Policy Wise Server profile identifier MUST be placed in an <AdditionalProfile> element.

3.1.2.2 Element <SignedInput>

This profile introduces a new <SignedInput> element within <OptionalInputs>. The <SignedInput> element will carry signed policy statements for signing requests.

If present, the <SignedInput> element MUST contain one or more <ds:Signature> elements that envelop the policy statements.

```
<xs:element name="SignedInput">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ds:Signature" minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
```

3.1.3 Element <InputDocuments>

For requests to sign XML documents, the client MUST only send <Document> input documents - the client MUST NOT send <DocumentHash> input documents as this would require that the client know which elements of the original XML document were to be signed.

3.2 Element <SignResponse>

3.2.1 Element <Result>

This profile defines no additional <ResultMinor> codes.

3.2.2 Element <OptionalOutputs>

This profile does not specify or constrain the optional outputs returned by the server.

3.2.3 Element <SignatureObject>

This profile does not specify or constrain the type of signature object returned by the server.

4 Profile of Verifying Protocol

4.1 Element <VerifyRequest>

4.1.1 Element <OptionalInputs>

The client MUST NOT send any optional inputs unless these inputs are contained within a <pws:SignedInput> element.

4.1.2 Element <SignatureObject>

This profile does not specify or constrain the type of signature object.

4.1.3 Element <InputDocuments>

This profile does not specify or constrain the type of input documents.

4.2 Element <VerifyResponse>

4.2.1 Element <Result>

This profile defines no additional <ResultMinor> codes.

4.2.2 Element <OptionalOutputs>

This profile does not specify or constrain the optional outputs returned by the server.

5 Profile of Server Processing Rules

In addition to the basic processing steps defined in **[DSSCore]**, a DSS Server should validate any `<ds:Signature>` element contained within the `<OptionalInputs>` element according to section 3.2.2 in **[XMLSig]**.

For any such signatures, the DSS Server MUST verify that the signer is authorized to specify policy for the corresponding request.

6 References

6.1 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

•

Appendix A. Revision History

Rev	Date	By Whom	What
wd-01	2004-02-10	Paul Madsen	Initial version
wd-02	2004-03-22	Paul Madsen	To reflect template changes & feedback
wd-03	2004-04-30	Paul Madsen	Introduce <SignedInput> element
wd-04	2004-10-09	Paul Madsen	Fixed typo in <SignedInput> schema. Removed reference to normative Policy Wise Server XSD, changed allowed <OptionalInputs> on <SignRequest>. Added profile identifier

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 implementers 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.