LegalXML Electronic Court Filing 3.0

XML Signature Document Signature Profile 1.0

Working Draft, [approval date]

Document Identifier:

legalxmlcourtfiling-ecf-v3.0-xmlsig-spec-wd-2.doc

OASIS Identifier:

[OASIS document number]

Location:

Persistent: http://www.oasis-open.org/apps/org/workgroup/legalxml-courtfiling/
This Version: http://www.oasis-open.org/apps/org/workgroup/legalxml-courtfiling/
Previous Version: none

Technical Committee:

OASIS LegalXML Electronic Court Filing TC

Chairs:

John Greacen, Individual Member
Thomas Clarke, National Center for State Courts

Editor:

Roger Winters, Washington Administrative Office of the Courts

Contributors:

James Cabral, MTG Management Consultants
Scott Came, Individual Member

Subject/Keywords:

Legal, Government, Court, E-Filing

OASIS Conceptual Model topic area:

Specialized Process

Related work:

- LegalXML Electronic Court Filing 3.0 specification (http://www.oasis-open.org/apps/org/workgroup/legalxml-courtfiling/)

Abstract:

This document defines a Document Signature Profile, as defined in section 6 of the LegalXML Electronic Court Filing 3.0 specification. The XML Document Signature Profile is the signature profile used to indicate documents that are signed with an XML Digital Signature.

Status:

This document is a Working Group Draft NOT yet accepted by the Working Group as reflecting its consensus; however, it will serve as the basis for discussions. As a work in progress, it should NOT be considered authoritative or final. Other subsequently issued documents will supersede this document. Technical Committee members should send their comments on this specification to the workgroup_mailer@lists.oasis-open.org list. Others should subscribe to and send comments to the mailto:legalxml-courtfiling@lists.oasis-open.org list. To subscribe, send an email message to mailto:legalxml-

courtfiling@lists.oasis-open.org?subject=Subscribe with the word “subscribe” as the body of the message.

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 President.

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 President.

Table of Contents

1 Introduction

This document defines a Document Signature Profile, as called for in section 6 of **[ECF 3.0]**. The purpose of the XML Signature Document Signature Profile is to provide a signature consisting of a digital signature encoded in the W3C XML Signature syntax specified in **[XMLSIG]**.

As with all Document Signature Profiles, the purpose of this profile is to define an allowable XML syntax for the content of the `SignatureType` structure, as defined in the `urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:DocumentType-3.0` namespace.

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 **[RFC 2119]**.

The XML Namespace prefix `xsd`, whenever it appears in this document, represents the `http://www.w3.org/2001/XMLSchema` namespace.

1.2 Normative References

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

[ECF 3.0] R. Winters, *LegalXML Electronic Court Filing 3.0*, http://www.oasis-open.org/apps/org/workgroup/legalxml-courtfiling/, OASIS, November 2005

[XMLSIG] D. Eastlake., J. Reagle, D. Solo, *XML-Signature Syntax and Processing*, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, W3C Recommendation, February 2002.

[XAdES] J. Cruellas, G. Karlinger, D. Pinkas, J. Ross, *XML Advanced Electronic Signatures,* http://www.w3.org/TR/XAdES/, ETSI TS 101 903and W3C Note, February 20, 2003

2 Profile Design

This section describes the design of the XML Document Signature Profile and identifies how it satisfies the requirements of a document signature profile listed in Section 6 of the **[ECF 3.0]** specification.

2.1 Document Signature Profile Identifier

The identifier for this Document Signature Profile is identical to the identifier for its namespace, namely:

`urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:XMLSignature-1.0`

2.2 Satisfaction of Document Signature Profile Requirements

The XML Document Signature Profile satisfies the requirements of Document Signature Profiles as defined in section 6 of **[ECF 3.0]**, as follows:

1. **Signer name assertion** – The signer's name is provided in the REQUIRED `SignerName` element. Note that if the `KeyInfo` structure included in the **[XMLSIG]** `Signature` element includes X.509 certificate information, it is possible that the signer's name would be reflected in the X.509 `SubjectName` element. However, this will not always be the case, so it is necessary to provide a separate element to store the signer's name, and to make its inclusion REQUIRED. Where X.509 certificates are employed the `SignerName` MUST be the same as the X.509 certificate `SubjectName CommonName` field.
2. **Signed date assertion** – The date of signing of the document is provided in the REQUIRED `SignedDate` element. Where the signature includes an element specifying the signing time (e.g. `SigningTime` as specified in **[XAdES])** the `SignedDate` MUST be the same as the date component of the signing time within the signature.
3. **Multiple signatures** – Multiple signatures are provided for by the unbounded upper limit on the Signature element within the `SignaturesType` structure.

The XML Document Signature Profile satisfies the optional non-functional requirements defined in section 6 of **[ECF 3.0]** as follows:

1. **Signer and date non-repudiation** – The algorithms defined by **[XMLSIG]** support non-repudiation of the signer and signing date through inclusion of a digital signature created using the signer's private key. Because the sender is the only one with access to the private key and the date is included in the signature, receivers can be reasonably assured of the signer and signing date.
2. **Document integrity** – The algorithms defined by **[XMLSIG]** support document integrity through inclusion of a public-key-based digital signature. Because the signing date and document hash are included in the signature and the entire signature is computed using the sender's private key, the receiver can easily compare the hashes to verify that the document has not been altered since it left the control of the sender on the specified date.
3. **Document signature auditing** – The `Signatures` element can be extracted from the CoreFilingMessage and persisted for later retrieval and examination.

3 Schema

To be valid according to this profile, a CoreFilingMessage (as defined in **[ECF 3.0]**) MUST contain the element `Signatures`, as defined in the following schema, in place of the `xsd:any` wildcard appearing in the `Signature-Type` definition in the `urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:DocumentType-3.0` namespace.

```
<xsd:schema
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:xmlsig="urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:XMLSignature-1.0"
   targetNamespace="urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:XMLSignature-1.0"
   elementFormDefault="qualified" attributeFormDefault="unqualified">

   <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>

   <xsd:element name="Signatures" type="xmlsig:SignaturesType"/>
   <xsd:element name="Signature" type="xmlsig:SignatureType"/>
   <xsd:element name="SignerName" type="xsd:string"/>
   <xsd:element name="SignedDate" type="xsd:date"/>

   <xsd:complexType name="SignaturesType">
          <xsd:sequence>
                 <xsd:element ref="xmlsig:Signature" minOccurs="1" maxOccurs="unbounded"/>
          </xsd:sequence>
   </xsd:complexType>

   <xsd:complexType name="SignatureType">
          <xsd:sequence>
                 <xsd:element ref="xmlsig:SignerName" minOccurs="1" maxOccurs="1"/>
                 <xsd:element ref="xmlsig:SignedDate" minOccurs="1" maxOccurs="1"/>
                 <xsd:element ref="ds:Signature" minOccurs="1" maxOccurs="1"/>
          </xsd:sequence>
   </xsd:complexType>

</xsd:schema>
```

Appendix A. (Informative) Acknowledgments

The following individuals were members of the committee during the approval of this draft:

Participants:

Jed Alpert, Wolters Kluwer
Jim Beard, Individual Member
Donald Bergeron, Reed Elsevier
Terry Bousquin, Individual Member
James Cabral, MTG Management Consultants, LLC.
Scott Came, Individual Member
Tom Carlson, National Center for State Courts
Rolly Chambers, American Bar Association
James Bryce Clark, OASIS
Thomas Clarke, National Center for State Courts
James Cusick, Wolters Kluwer
Robert DeFilippis, Individual Member
Christopher Durham, Reed Elsevier
Scott Edson, LA County Information Systems Advisory Body
Robin Gibson, Missouri Office of State Courts Administrator
David Goodwin, Maricopa County
John Greacen, Individual Member
Jim Harris, Individual Member
Allen Jensen, Orange County Superior Court
Laurence Leff, Individual Member
Rex McElrath, Judicial Council of Georgia
John Messing, American Bar Association
Shogan Naidoo, Individual Member
Robert O'Brien, Ottawa Courts Administration Service
Catherine Plummer, Search Group, Inc.
Nick Pope, Individual Member
Dallas Powell, Individual Member
David Roth, Thomson Corporation
John Ruegg, LA County Information Systems Advisory Body
Christopher Smith, California Administrative Office of the Courts
Thomas Smith, Individual Member
Eric Tingom, Individual Member
Roger Winters, Washington Administrative Office of the Courts

Appendix B. (Informative) Revision History

Rev	Date	By Whom	What
Wd-01	2005-11-06	Scott Came James Cabral	Initial version
Wd-02	2005-11-08	James Cabral	Synchronized signer name and date with the XML digital signature. Referenced the [XAdES] specification.

Appendix C. (Informative) Example Instance

This non-normative section provides an example of the syntax of this Document Signature Profile. Note that the following is for illustrative purposes only, and due to annotations included in the sample, it is not well-formed XML.

```
<CoreFilingMessage
   xmlns="urn:oasis:names:specification:legalxml-courtfiling:schema:xsd:CoreFilingMessage-3.0"
   xmlns:xmlsig="urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:XMLSignature-1.0"
   xmlns:document="urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:DocumentType-3.0">

   ... (content removed for brevity)

   <FilingLeadDocument>

   ... (content removed for brevity)

   <document:ExtendedDocumentDescriptiveMetadata>

     ... (content removed for brevity)

     <document:DocumentSignature>
      <document:SignatureProfileIdentifier>
   urn:oasis:names:tc:legalxml-courtfiling:schema:xsd:XMLSignature-1.0
      </document:SignatureProfileIdentifier>
      <document:Signature>
       <xmlsig:Signatures>
        <xmlsig:Signature>
         <xmlsig:SignerName>jsmith</xmlsig:SignerName>
         <xmlsig:SignedDate>2005-11-07</xmlsig:SignedDate>
          <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
           <ds:SignedInfo Id="foobar">
            <ds:CanonicalizationMethod
   Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod
   Algorithm="http://www.w3.org/2001/04/xmlenc#sha256”/>
            <ds:Reference URI="#Attachment1">
             <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
             <ds:DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:DigestValue>
            </ds:Reference>
           </ds:SignedInfo>
           <ds:SignatureValue>MC0E~LE=</ds:SignatureValue>
           <ds:KeyInfo>
            <ds:X509Data>
             <ds:X509SubjectName>CN=John Smith,O=ABC Inc.,ST=Seattle,C=WA</ds:X509SubjectName>
             <ds:X509Certificate> MIID5jCCA0+gA...lVN</ds:X509Certificate>
            </ds:X509Data>
           </ds:KeyInfo>
          </ds:Signature>
        </xmlsig:Signature>
       </xmlsig:Signatures>
      </document:Signature>
     </document:DocumentSignature>
   </document:ExtendedDocumentDescriptiveMetadata>
   </FilingLeadDocument>
</CoreFilingMessage>
```