Visual Signature Profile of the OASIS Digital Signature Services

Working Draft v0.1

12 May 2008

Document Identifier:

oasis-dss-1.0-profiles-ebxml-cd

Specification URIs:

This Version:

Previous Version:

Latest Version:

Latest Approved Version:

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):

Ezer Farhi , *ARX,* <ezer@arx.com>

In Memory of Uri Resnitzky, ARX who was an active member of OASIS DSS-X Committe.

Related work:

This specification is related to:

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

Abstract:

The visual signature profile enables to embed visual signature characteristics into documents as part of a digital signature operation and also validate these characteristics as part of the verify signature operation.

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” or “Latest Approved 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

1 Introduction

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

1.3 Normative References

1.4 Non Normative References

2 Overview

For many processes that incorporate a digital signature operation or a verification of a digital signature, there is a need to view displayed information that is related to the binary digital signature.
This visual display of information can include displaying the signer's identity, the time when the digital signature operation was performed, and additional information as well.
The visible information comes in addition to the actual digital signature data, and is aimed at providing end users with information that closely relates to the digital signature act. By no means does this visible information replace the important element of the digital signature.

Visible signatures are strongly associated with documents. The visible signatures will normally be displayed in the document in addition to other displayed information such as text and images.
There are several documents types and applications that already support digital signature in conjunction with visual signatures:

- Adobe Reader/Adobe Acrobat using digital signatures inside PDF documents.
- Microsoft Office 2007 using digital signatures inside OOXML documents.
- Other proprietary solutions exist that enable the use of visual signatures as well as digital signatures in other documents types such as TIFF, Office XP/2003, and other document formats.

The target of the Visual Signatures Profile is to define mechanisms that will enable clients that interact with a digital signature service, based on DSS core, to incorporate visual signatures into documents as part of a digital signature operation.
The signature operation can be applicable for any type of document and can be displayed with any tool that displays the document.
The signature verification service should be able to validate some of the displayed information as part of the signature verification operation.

Remark: It is mandatory that the proposed profile will not impose any conflict with existing document standards such as PDF or OOXML, so that it is possible to use the profile for incorporating visual signatures into these documents types.

Digital Signature Operation

There are two types of usage scenarios that involve visual signatures as part of a digital signature operation:

- Submission of a document to be signed
  In this scenario, an unsigned document is submitted to be signed by the digital signature service. As part of the submission, the client needs to provide some visual information that will be used by the signature service in order to build a visual content that relates to the digital signature.
  The visual information will also include some information for the User/CA certificates that will be extracted by the digital signature service.
  Most of this visual content will also be included in the digital signature operation, so that modifying the displayed information will invalidate the digital signature itself.
  In this type of scenario there is generally a single digital signature in the document.
- Digital Signature operations as part of a workflow
  In this scenario, the document will already contain empty locations (named "signature fields") that are uniquely identified in the document. As part of the digital signature operation, the client will need to specify which signature field should be signed.
  The signature field may already contain Meta data such as the display configuration. If this is the case, the client will not need to provide information as part of the digital signature operation.
  This scenario will normally involve several digital signatures in a given document.

The following specification is aimed to address both above scenarios. The resulting visible signature and digital signature are very similar in both above scenarios.

Visual Signature Content

The structure of the visual signature is made of components (normally strings and images) that are displayed in a certain location inside the visible signature.
The following is information that may be included as part of the visual signature. The parameters are not listed in the order of their importance.

- **Signer Information** - Information of the signer that performs the digital signature operation. The information will be extracted from the signer's certificate.
  Besides the signer's *Common Name*, additional information can be displayed from the signer's certificate such as: *serial number, role, organization*, or any other specific information that is located inside the signer's certificate.
  Multiple elements that are retrieved from the signer's certificate can be displayed in the visual signature.
- **CA Information** - Information on the certificate authority that produced the certificate for the signer. The information will be extracted from the signer's certificate or CA certificate.
  In addition to the CA's *Common Name*, additional information can also be displayed from the signer's certificate or CA Certificate, such as: *CA's country, organization,* or any other specific information that is located inside the CA's certificate.
  Multiple elements that are retrieved from the signer's certificate or CA certificate can be displayed in the visual signature.
- **Signature Time** - The date and time of the digital signature. The format of the displayed time is also required (i.e. "dd mmm yy hh:mm").
- **Signer's Related Image** - End users and organizations appreciate the ability to view personal images such as the end user's hand-written signature, as part of the visible signature. This will normally be a scanned image of the user's hand-written signature.
  In some cases, depending on the context of the signature, this field can also be used to contain an organizational logo.
- **Additional Application Info** - In certain cases, additional information should be displayed in the visual signature. For example, some applications require adding the *Reason* for the digital signature operation.
- **Digital Signature Value** - This value is a base64 encoding or other scanable representation of the binary digital signature. This value can be scanned out of the printed document and used for digital signature verification purposes. In relation to other visually displayed components, this field must not be included as part of the data to be signed.

The following information may be sent to the digital signature service as part of the digital signature information, so that the service is able to embed the visual signature into the document.

- **Document Type** - This value defines the format of the provided document so that the digital signature service can embed both a visual sSignature and a digital signature into the document, according to the document format.
- **Position** - The visual signature is visually located inside the document. Therefore, the position of the visual signature needs to be specified. This parameter is essential for the Document Submission Scenario. The position may be specified according to page number and location in a page, or any other metric that determines the exact location and size of the visual signature.
- **Signature Field Identification** - This identification can be used in both above scenarios. Through this approach, the signature service can locate the signature field that will contain both the visual signature and digital signature.
- **Visual Signature Configuration and Policy** - This parameter is optional and may direct the service how to configure the visual signature. The configuration will include which components will be

displayed inside the visual signature and what their position will be. For a given specified configuration, all visual components must be incorporated into the visual signature.

Some of the information described in the Visual Content section should be sent to the digital signature service to be embedded into the visual signature.

Digital Signature Verification Operation

Depending on the document format, some of the visual components will be included in the digital signature, and thus be verified as part of the signature verification operation.
Depending on the document type, it is possible to have additional validation operations such as comparing the signer's identity in the certificate against the displayed Identity.

[Editor Remarks:

- It is suggested to avoid including the profile signature field management operations such as signature field creation operation or clearing a signature field operation.

]

.

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.

2.1.3 Element <dss:SignatureObject>

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

2.2 Profile of Signing Protocol

2.2.1 Element <dss:SignRequest>

2.2.1.1 Element <dss:OptionalInputs>

2.2.1.1.1 New Optional Inputs

2.2.2 Element <dss:SignResponse>

2.3 Profile of Verifying Protocol

2.3.1 Element <dss:VerifyRequest>

A. Revision History

[optional; should not be included in OASIS Standards]

Rev	Date	By Whom	Content
Wd-01	13.05.2008	Ezer Farhi	Initial version