LegalXML eNotarization Use Cases Version 1.0

Committee Draft

08 May 2008

Specification URIs:
This Version:
http://docs.oasis-open.org/legalxml-enotary/UseCases/v1.0/cd01/UseCases-v1.0-cd01.doc
http://docs.oasis-open.org/legalxml-enotary/UseCases/v1.0/cd01/UseCases-v1.0-cd01.html
http://docs.oasis-open.org/legalxml-enotary/UseCases/v1.0/cd01/UseCases-v1.0-cd01.pdf
Previous Version:
N/A
Latest Version:
http://docs.oasis-open.org/legalxml-enotary/UseCases/v1.0/UseCases-v1.0.doc
http://docs.oasis-open.org/legalxml-enotary/UseCases/v1.0/UseCases-v1.0.html
http://docs.oasis-open.org/legalxml-enotary/UseCases/v1.0/UseCases-v1.0.pdf
Technical Committee:
OASIS LegalXML eNotarization TC

Chair(s):
Rolly Chambers
Mark Ladd

Editor(s):
Mark Ladd
Marc Aronson

Abstract:
This document outlines specific scenarios that were used by the eNotarization TC during the development of its XML schema. The Use Cases described were selected based on their ubiquity and commonality in actual use today. It is anticipated that additional use cases will be added at future dates that will expand the scope of the standard.

Status:
This document was last revised or approved by the LegalXML eNotarization 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/legalxml-enotary/.

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/legalxml-enotary/ipr.php.

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

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 name "OASIS" is a trademark 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

In order to facilitate the adoption of notarized electronic documents, it is desirable to develop data standards for electronic notarizations that can be applied across a wide variety of applications. It is the goal of this document to identify several common notarial acts that are utilized in a variety of vertical markets as a starting point for detailed analysis of data points and nomenclature that can be codified in an XML vocabulary which can then be adopted by a wide range of industries.

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 **[RFC2119]**.

1.2 Normative References

[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.

[Reference] [Full reference citation]

1.3 Non-Normative References

[Reference] [Full reference citation]

2 Foundational Assumptions Regarding Notarial Acts

During the signature event the signer binds their signature to the document content. The notary binds the signer's signature to the signer's identity through the certificate content which additionally establishes voluntariness. The notary's signature binds the certificate content to the notary's identity and wraps the entire set of document content values and bindings of signatures to identities in a tamper-evident mechanism. The notary seal (or seal information under UETA) binds the notary to the power of the commissioning state.

3 Use Case #1 – Acknowledgments

Overview:

Acknowledgments contain two essential elements. The first element is a formal declaration made by a person who signed a document indicating that the signature is genuine and that signing the document was a free will act performed for the purposes indicated in the document. This declaration is made in the presence of a notary.

It should be noted that the signing may be executed prior to appearing before the notary. The notary is taking the singer's acknowledgment that he or she did, in fact, sign the document willingly and knowingly.

The second element is the notary's certificate; a written statement that the signer did appear in person, was satisfactorily identified and made the acknowledgment. This notarial act is authorized in and follows a similar process in each of the 50 states and the District of Columbia.

Actors:

- Document Preparer/Drafter (Passively involved. They may or may not be present.)
- Document Signer(s)
- Notary Public

Precondition:

An electronic document has been generated by the parties or their agent. Included in the document preparation would be appropriate acknowledgment certificate language. The party(ies) sign the document and appear before a notary public.

Postcondition:

Signers have provided acceptable identification documents, have acknowledged that they signed a document with full understanding of the purpose of the document, indicated their intent to execute the document (and thus be bound by its terms and conditions.) The document has been electronically signed by the part(ies) acknowledging their signatures. The notary public has completed the notary certificate and affixed his or her electronic signature to the document. In states that require an electronic notarial seal, this would also be affixed to the document.

Requirements for Effective Acknowledgment:

- A statement by the signer that the signature is genuine.
- An evidence of awareness, understanding and absence of duress by the signer
- Presentation of acceptable identification documents by the signer to the notary
- The signer's signature (Application can occur anytime prior to acknowledgment)
- Completed notary certificate
- Application of notary's signature together with information required by state law (e.g., commission number, expiration date and words “Notary Public”)

Issues Related to Use Case:

- What does the notary actually notarize?
    - Document content (some of which is not necessarily visible in an electronic document) or just the signature event?
        - The notary’s role is to certify the acknowledgment event. The notary does not, in

71 the case of an acknowledgment, certify that the signature was made. The notary
72 only certifies that the signer personally appeared and acknowledged that the
73 signature is genuine and was purposefully made.
74 ▪ Regarding electronic content that is not seen or understood by the notary, this
75 document relies on an analogy drawn from a current practice with paper
76 documents; specifically foreign language documents. While a notary may not be
77 able to decipher the content of a document drafted in another language, the
78 notary can take an acknowledgment.
79 ▪ The assumption of this document is that document content (displayed and
80 metadata) are the responsibility of the document signer, not the notary.
81 • Uniformity in certificate language
82 o Since certificate language varies by jurisdiction, what is the best way to publish and track
83 changes to certificate languages?
84 ▪ Include a generic XML container element for certificate language
85 ▪ Specific certificate language is outside the scope of this standard
86 ▪ Supporting documentation could provide sample references
87 • Is it appropriate for a notary to append a notarial certificate to an electronic document if a
88 certificate is not provided within the document itself?
89 o Numerous business cases were noted wherein this would be necessary and appropriate.

4 Use Case #2 – Affidavits

Overview:

An affidavit is a voluntary written statement of fact, sworn to or affirmed by the person making it before a notary (or other person authorized by law to administer oaths and affirmations) and officially certified by the notary under his or her seal of office.

An affidavit is valid only when signed in the presence of the notary who administers an oath or affirmation. The affiant must swear to the statement contained in the affidavit, and the fact of his or her swearing or affirming must be certified by the notary.

Actors:

- Document Preparer/Drafter (Passively involved. They may or may not be present.)
- Affiant(s)
- Notary Public

Precondition:

An electronic affidavit has been generated by the parties or their agent. Included in the document preparation would be appropriate oath or affirmation language.

The notary and affiant must be present together for the oath or affirmation. It is not necessary that the oath or affirmation administered be formal, nor is it necessary that any exact words or specific ceremony be used to constitute a valid administration of an oath or affirmation. There must be concurrent action on the part of the affiant and the notary by which the affiant consciously, solemnly takes upon him or herself to be bound by the obligation of an oath or affirmation.

An affidavit must contain a statement of facts based on the personal knowledge of the affiant. An affidavit must also contain a statement indicating that the person who made it was under oath or affirmation.

Postcondition:

Signers have provided acceptable identification documents and have sworn to the statement contained in the affidavit. The document has been electronically signed by the part(ies) thusly swearing. The notary public has completed a jurat and affixed his or her electronic signature to the document. In states that require an electronic notarial seal, this would also be affixed to the document.

Generally, an affidavit must be signed by the affiant, in order to constitute a formal affidavit. (However, courts have ruled an affidavit valid which was not signed by the affiant, but in which appeared the name of the affiant indicating the person who took an oath or made an affirmation.) The affiant's signature need not be at the end, if it appears in any part and is obviously applicable to the affidavit.

A jurat is generally defined as a certificate added to an affidavit stating when, before whom, and where an oath was taken or affirmation made. A jurat certifies the administration of an oath or affirmation associated with an affidavit, but it is not a required part of an affidavit. The jurat provides one type of evidence that an affidavit was sworn to or affirmed properly, that is, in the presence of someone authorized to administer oaths and affirmations.

Requirements for Effective Affidavits:

- Personal Appearance before a notary
- Documented statement by affiant

- Oath or affirmation made by affiant
- Affiant's signature
- Completed jurat
- Application of notary's signature together with information required by state law (e.g., commission number, expiration date and words “Notary Public”).

Issues Related to Use Case:

- Is there an electronic equivalent or substitute for personal appearance?
    - At this time, we see no acceptable alternative for personal appearance.
- Can/should uniform language be developed for the oath?

5 Use Case #3 – Personal Credentialing for System Access

Overview:

In this scenario a trusted person identifies another individual to a computer network which issues a credential to the second individual based upon criteria on behalf of an actual or potential relying party. The second individual then logs on to the computer network. All activities performed while logged-in are presumed to be the actions of the second individual.

Actors:

- Individual with need for authorizing credentials
  - User name and password (shared secret)
  - Digital certificate
  - Security Token
- Trusted Person (Notary Public or other agent)

Precondition:

The system recognizes the trusted person. The individual requesting access has presented to the trusted person identity credentials that satisfy relying party requirements. The system being accessed has sufficient capacity to record the identity of the individual, issue the credential, logically associate the two, and securely store the information. The individual is “in the presence” of the trusted person when initially requesting the identity credentials.

Postcondition:

The identity of the individual has been authenticated and a credential issued. The relationship between identity and issued credentials has been recorded and stored, such that actions taken on the basis of the credential are presumed to be those of the individual.

Requirements for Effective Personal Credentialing for System Access:

- Trusted person with system access
- Relying party requirements including:
  - Suitable Identification
  - System access, storage and security requirements

Issues Related to Use Case:

- Must trusted person be a notary?
- Duration of credential?
- Legal effect?

6 Use Case #4 – Unsworn Declarations

Overview:

A signer of a document declares that the signature is executed under penalty of perjury. No other individual is involved.

Actor:

- Declarant

Precondition:

Document must declare that it is signed under penalty of perjury.

Postcondition:

Document was signed, dated and include a statement regarding location of declaration by the declarant.

Requirements for an effective Unsworn Declaration:

- Document containing appropriate declaration

Issues Related to Use Case:

- Applicable authorizing law

7 Use Case #5 – Apostilles

Overview:

An apostille is the certificate of an authorized government officer who has verified the signature and seal/stamp of a notary public or other public signatory. An apostille certifies the authenticity of the signature, the capacity in which the person signing the document has acted, and when appropriate, the identity of the seal or stamp which the document bears. An apostille does not, however, authenticate or verify the content of the public document to which it is attached.

Actors:

- Notary Public or other public signatory
- Party Requesting Apostille
- Regulatory Agency Officer

Precondition:

A document has been officially witnessed by a notary public or other public signatory in another jurisdiction (usually a foreign country). The regulatory body with oversight of notaries public or other public signatories in that jurisdiction verifies the notary or other public signatory was properly commissioned at the time of the event, and the signature and seal that appear on the document are those of the official witness.

Postcondition:

If the officer determines that the commission, signature, and seal on the document match those on file, then the officer attaches a certificate, conforming to Article Four of Convention 12 of The Hague Conference on Private International Law, to the document. A registry entry regarding each Apostille issued is also required to be maintained by the issuing agency according to The Hague rules.

Requirements for Effective Apostille:

- Uniform format and content for Apostilles are prescribed by Article Four of Convention 12 of The Hague Conference on Private International Law.
    - Language: The certificate may be written in the official language of the designated authority issuing it. The standard terms appearing therein may be in a second language also.
    - Title: The title "Apostille (Convention de La Haye du 5 octobre 1961)" must appear centered at the top of the certificate and must be written in French.
    - Certificate: The certificate may appear on the public document itself or be attached on a separate piece of paper at least 9 centimeters square (3.543 inches). The content of an apostille is strictly prescribed by the Convention to certify the following:
        - Authenticity of the signature and the capacity in which the person signing a public document has acted
        - Identity of the seal or stamp on the document (if applicable)
        - Place and date the certification took place
        - Name, title, and seal/stamp of officer issuing certificate
    - Specific Words: The form and specific wording is also mandated by Article Four of Convention 12:
        - "Apostille (Convention de La Haye du 5 octobre 1961)"
        - “1. Country: _____ ”
        - “This public document”
        - “2. has been signed by _____ ”
        - “3. acting in the capacity of _____ ”

        - "4. bears the seal/stamp of _____ "
        - "Certified"
        - "5. at _____ "
        - "6. the _____ "
        - "7. by _____ "
        - "8. No _____ "
        - "9. Seal/stamp: _____"
        - "10. Signature: _____"
- Register Entry: Article 7 of Convention 12 requires that each Apostille issued be recorded in a register or card index. Each register entry must include the following information:
    - The number and date of the certificate
    - The name of the person signing the public document and the capacity in which he has acted, or in the case of unsigned documents, the name of the authority which has affixed the seal or stamp.

Issues Related to Use Case:

- What training do officials receive for making their comparisons?
    - Upon surveying notary administrators, it appears that most of the training focuses on the mechanics of the process, not on the technical aspects of handwriting comparisons. In this regard, electronic signatures should prove to be no more difficult to verify and in some cases may be easier to verify.
- How will this translate to eApostille?
    - Since little, if any, emphasis is currently given to the "forensic" aspect of signature comparison, we may find that cryptography and biometrics will provide a higher level of assurance in this area by comparison to wet-ink signatures.
- How will electronic signatures be registered with regulatory agencies?
    - Typed signatures
    - Click-through signatures
    - Image based signatures
    - Holographic signatures
    - Digital certificates
    - Biometric signatures
- What infrastructure will be required for regulatory agencies to affix an eApostille to an electronic document?
- What work has The Hague already done regarding eApostille?
- For the purpose of this document we are deferring consideration of languages other than English at this time.

A. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Rolly Chambers, Taylor, Penry, Rash, Riemann, PLLC
Mark Ladd, Property Records Industry Association
Marc Aronson, United States Notary Association
David Ewan, New Jersey Land Title Company
John Jones, Arion Zoe Corp
Harry Gardner, Mortgage Industry Standards Maintenance Organization
John Messing, American Bar Association

B. Revision History

[optional; should not be included in OASIS Standards]

Revision	Date	Editor	Changes Made
[Rev number]	[Rev Date]	[Modified By]	[Summary of Changes]