

**PROPOSED RULES FOR IMPLEMENTING
UNIFORM REAL PROPERTY ELECTRONIC RECORDING ACT**

**TITLE 60. OKLAHOMA ARCHIVES AND RECORDS COMMISSION
CHAPTER 15. ADMINISTRATION OF UNIFORM REAL PROPERTY**

ELECTRONIC RECORDING ACT

SUBCHAPTER 1. GENERAL PROVISIONS

60:15-1-1. Purpose

The rules of this Chapter implement the Uniform Real Property Electronic Recording Act, as adopted in Oklahoma set out in Sections 86.1 through 86.7 of Title 16 of the Oklahoma Statutes, directing the Oklahoma Archives and Records Commission to establish standards for implementation of the Act.

60:15-1-2. Definitions

In addition to the definitions in the Uniform Electronic Transactions Act, as adopted in Oklahoma set out in Sections 15-101 through 15-121 of Title 12A of the Oklahoma statutes, and the Uniform Real Property Electronic Recording Act, the following words and terms shall be applied when implementing the Act.

1. “**Act**” means the Uniform Real Property Electronic Recording Act, as adopted in Oklahoma.
2. “**Commission**” means the Oklahoma Archives and Records Commission.
3. “**E-Recording**” means electronic recording.
4. “**PRIA**” means the Property Records Industry Association.

60:15-1-3. Glossary of Terms

The following words, terms, phrases, acronyms, and abbreviations are defined in other Oklahoma Statutes and are included here for use in connection with the Act or these rules, or are words, terms, phrases, acronyms, or abbreviations that may require further explanation to assist in the understanding of the Act and these rules.

1. **ACH:** Automated Clearing House
2. **Agreement:** means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.
3. **ANSI:** American National Standards Institute
4. **Asymmetric encryption:** A method of encryption that uses two keys, a public key and a private key. Together, the keys constitute a key pair. Although the keys are mathematically related, it is not possible to deduce one from the other. The public key is published in a public repository and can be freely distributed. The private key remains secret, known only to the key holder.
5. **Authentication:** The act of tying an action or result to the person claiming to have performed the action. Authentication generally requires a password or encryption key to perform, and the process will fail if the password or key is incorrect.

6. **Automated transaction:** means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
7. **Computer program:** means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.
8. **Digitized signature or digital signature:** A representation of a handwritten signature, existing as a computerized image file. Digitized signatures are one of several types of electronic signatures, and have no relation to digital signatures.
9. **DTD: Document Type Definition.** A document created using the Standard Generalized Markup Language (SGML) that defines a unique markup language such as XHTML or XML. A DTD includes a list of tags, attributes, and rules of usage.
10. **Electronic commerce:** Also known as e-Commerce, refers to trade that occurs electronically, usually over the Internet. Electronic commerce often involves sharing information, buying or selling products, or extending both new and traditional services to customers via electronic means. Electronic commerce allows business to take advantage of e-mail, the Web, and other online innovations to improve the business process and offer consumers more ways to access products, faster information transfer and decreasing costs.
11. **Electronic record:** A record created, generated, sent, communicated, received or stored by electronic means.
12. **Electronic notary:** A notary public who provides electronic notarial acts pursuant to the provisions of section 86.3 of Title 16 of the Oklahoma Statutes.
13. **Encrypt:** To apply an encryption key to a message in order to make it unreadable without a description key in an effort to prevent unintended use of the information.
14. **E-SIGN:** Electronic Signatures in Global & National Commerce (15 U.S.C. Sections 7001 – 7006).
15. **FTP:** File Transfer Protocol
16. **Hash function:** A mathematical algorithm that takes an electronic document and creates a document fingerprint. The document fingerprint is much smaller than the original document, and does not allow the reconstitution of the original document from the fingerprint. A slightly different document, processed through the same hash function, would produce a very different document fingerprint. A hash function helps to secure data by providing a way to ensure that data is not tampered with.
17. **HTML:** HyperText Markup Language
18. **HTTP:** HyperText Transfer Protocol
19. **HTTPS:** HyperTextTransfer Protocol Secure
20. **Information:** means data, text, images, sounds, codes, computer programs, software, databases, or the like.
21. **ISO:** International Standards Organization
22. **Key pair:** A set of keys, including a private key and a public key, used in asymmetric encryption. Sometimes a key pair will be reserved for specific uses, such as creating digital signatures.
23. **Metadata:** Commonly described as "data about data." Metadata is used to locate and manage information resources by classifying those resources and by capturing information not inherent in the resource.

24. **Nonrepudiation:** Effectively implementing a process in such a way that the creator of a digital signature cannot deny having created it. Nonrepudiation involves supplying enough evidence about the identity of the signer and the integrity of a message so that the origin, submission, delivery, and integrity of the message cannot be denied. Protecting the private key of a user is also a critical factor in ensuring nonrepudiation. The entire Public Key Infrastructure (PKI) industry exists to create and ensure the trust necessary for nonrepudiation.
25. **Notary public:** “Notary public” and “notary” mean any individual appointed and commissioned by the Oklahoma Secretary of State pursuant to the provisions of section 1 of Title 49 of the Oklahoma Statutes who performs notarial acts pursuant to the provisions of the Uniform Law on Notarial Acts, as adopted in Oklahoma set out in Sections 111 through 22 of Title 49 of the Oklahoma Statutes.
26. **OAIS:** Open Archival Information Systems
27. **PDF: Portable Document Format.** A file format created by Adobe Systems, Inc. that uses the PostScript printer description language to create documents. PDF files capture the appearance of the original document, can store both text and images, are difficult to modify, and can be rendered with free cross-platform viewer software.
28. **Portal:** A Web site considered an entry point to other Web sites, often by being or providing access to a search engine, useful content, or by functioning as a gateway to other Web locations or both. Portals are usually provided free of charge, in the hope that users will use the site.
29. **Private Key:** A large, randomly generated prime number used in asymmetric encryption. The private key is used to encrypt a document fingerprint which is the result of processing an electronic document through a hash function in order to create a digital signature. A private key is generated by its holder at the same time a related public key is created. While the public half of a key pair is made available to anyone, the private key is only known by its owner, who must keep it confidential to maintain its integrity.
30. **Proprietary:** Indicates that software or other employed technology is owned or controlled exclusively by the vendor. These software solutions are not generally transferable to other systems without payment of license fees.
31. **Public Key:** A large, randomly generated prime number used to decrypt an electronic document that has been encrypted with a private key. A public key is generated by its holder at the same time a related private key is created. Within the Public Key Infrastructure (PKI), public keys are used to verify digital signatures. Public keys are contained in digital certificates, published and otherwise distributed by the issuing certificate authority (CA).
32. **PKI: Public Key Infrastructure.** The framework of different entities working together to create trust in electronic transactions. The PKI industry facilitates signed transactions by using asymmetric encryption to ensure security and verifiable authenticity. The PKI includes all parties, policies, agreements, and technologies applicable to a transaction. This infrastructure allows all concerned parties to trust electronic transactions created within the standards set by the PKI industry.
33. **Schema:** A method for specifying the structure and content of specific types of electronic documents which use XML.
34. **Security procedure:** means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term “security procedure” includes a

procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

35. **SSL: Secure Socket Layer.** A security technology that uses both asymmetric and symmetric cryptography to protect data transmitted over the Internet.

36. **Signature Authentication:** The process by which a digital signature is used to confirm the identity of a signer and the validity of the document.

37. **Signed Digital Document:** An electronic document that includes an embedded digital signature. The digital signature contains an encrypted document fingerprint, which allows anyone receiving the document to verify its validity using the process of signature authentication.

38. **SSL:** Secure Socket Layer

39. **Submitting Party:** The entity that originates an electronic document. This is usually a bank, title company, attorney, or anyone that either inputs data into a specific template or associates an image or both, and wishes to send the documentation for electronic recordation to the county clerk.

40. **TIFF: Tagged Information File Format.** An image file format commonly used for photographs, scanned documents, or other graphics. TIFF images are graphics that are made up of individual dots or pixels. Files in the TIFF format are distinguished by a “.tif” filename extension. Group 4 TIFF (Tagged Image File Format) images are commonly used, because this format preserves the image in the most accurate and legible form.

41. **TBP:** Trusted Business Partner.

42. **Third party vendor:** Entity that may act as an intermediary in an electronic transaction. The vendor will usually add value to the transaction, such as verifying accuracy and completeness of index entries, authentication of the submitting party, or any other specific requirement of the county clerk.

43. **Transaction:** means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

44. **UETA: Uniform Electronic Transactions Act.** The uniform act on which the Uniform Electronic Transactions Act as adopted in Oklahoma set out at Sections 15-101 through 15-121 of Title 12A of the Oklahoma Statutes was based authorizing electronic documents and digital signatures to stand as equals with their paper counterparts.

45. **URPERA: Uniform Real Property Electronic Recording Act.** The uniform act on which the Uniform Real Property Electronic Recording Act as adopted in Oklahoma set out in Sections 86.1 through 86.7 of Title 16 of the Oklahoma Statutes, was based authorizing county clerks to accept electronic documents for recording in accordance with established standards.

46. **VPN:** Virtual Private Network

47. **Wet signature:** An original handwritten signature applied to a document.

48. **XHTML:** Extensible HyperText Markup Language

49. **XML Extensible Markup Language (XML):** A computer language used to create markup languages. XML allows developers to specify a document type definition (DTD) or schema in order to devise new markup languages for general or specific uses.

60:15-1-4. Authority, interpretation, and severability of rules

These rules are adopted pursuant to the provisions of the Uniform Real Property Electronic Recording Act, Sections 86.1 through 86.7 of Title 16 of the Oklahoma Statutes and the Administrative Procedures Act. Should a court of competent jurisdiction or the Attorney

General of Oklahoma find any part of these rules to be inconsistent with the provisions of law as they presently exist or are hereafter amended, they shall be interpreted to comply with the statutes as they presently exist or are hereafter amended. The partial or total invalidity of any section of the Chapter shall not affect the valid sections.

SUBCHAPTER 2. ELECTRONIC RECORDING STANDARDS

60:15-3-1. Data and document standards

(a) The data and document standards and guidelines promulgated by PRIA Version 2 as follows and found at www.pria.us (date of search November 10, 2009):

- (1) E-Recording Business Requirements dated March 12, 2008,
- (2) Document Version 2.4.1 dated October 2007,
- (3) Notary Version 2.4.1 dated October 2007,
- (4) PRIA Request Version 2.4.2 dated August 2007,
- (5) PRIA Response Version 2.4.2 dated August 2007, and
- (6) Updated e Recording iGuide dated May 2007,

are hereby adopted by the Commission pursuant to the authority of Section 86.5 (a) and (b)(2) of Title 16 of the Oklahoma Statutes.

(b) Upon any change in the data and document standards and guidelines or the models of submission the Commission will amend this section to reflect the amendment.

60:15-3-2. Web portals standards.

(a) The World Wide Web is the most common delivery medium used for electronic documents, and use of web portals enables these transactions.

- (1) Web portals can take on a variety of forms, from simple single entry sites used by an individual county clerk to support their own efforts, or by a collection of county clerks where the site provides both content and document routing.
- (2) Web portals can be created by anyone, so long as the site supports all three PRIA models and complies with security requirements.
- (3) The Commission shall not create or promote a mandatory Web portal.
- (4) Each county clerk shall decide the portal used in their county.

(b) A document delivered over the Web shall provide a minimum amount of information in the electronic documents delivered which is sufficient to identify and authenticate the sender to the county clerk and an itemization of the contents of the package.

(c) Payment processing capabilities shall be determined by the county clerk with advice of a portal provider.

- (1) Web portals may provide payment processing functionality.
- (2) Payment processing, if supplied at the portal, shall comply with industry standards and any rules that may be promulgated by the Commission.
- (3) Each county clerk is authorized to decide on approved methods of payment which could include but not be limited to debit or credit cards, ACH, and prepaid fee accounts.

60:15-3-3. Business rules

(a) Electronic Recording participants shall abide by the Business Rules of the county clerk.

- (b) County clerks shall establish and publish Business Rules that govern the procedure for electronic recording.
- (c) County clerks may modify their Business Rules as they deem necessary.
- (d) The Business Rules may be in electronic or hard copy format and may appear on a portal or the website of the county clerk. Electronic acknowledgment of acceptance of the terms of the Business Rules is acceptable.
- (e) The Business Rules shall include but not be limited to the following items:
 - 1) Defined technical specifications;
 - 2) Document and indexing specifications;
 - 3) Hours of operations and processing schedules;
 - 4) Payment options;
 - 5) Termination terms;
 - 6) Document Rejection rights;
 - 7) Process for publishing amendment to Business Rules; and
 - 8) Identification of the venue of any litigation arising between the parties.

60:15-3-4. Security

Participants of electronic recording shall develop security standards and policies based on industry-accepted security practices and protocols as approved by the Commission.

(1) Transactional security. All electronic documents shall be secured in such a way that both the transmitting and receiving parties are reasonably assured of the identity of each party and that no unauthorized party can view or alter the electronic document during transmission, processing, and delivery.

(2) Organizational security. Each county clerk, who elects to accept electronic documents for recording, shall implement reasonable measures to assure that each electronic document accepted for recording is protected from alteration and unauthorized access.

60:15 -3-5. Electronic signatures

County clerks are only required to accept electronic signatures that they have the technology to support. County clerks shall have no responsibility to authenticate electronic signatures embedded within the body of the document.

60:15-3-6. Notary acknowledgment

County clerks shall have no responsibility for verifying or authenticating notary signatures and acknowledgments. Notarization and acknowledgment shall be subject to the provisions of section 86.3(c) of Title 16 of the Oklahoma Statutes, and Title 49 of the Oklahoma Statutes.

60:15-3-7. File formats for electronic recording

(a) Electronic recordings may be converted by the county clerk to and preserved as a Tagged Image File Format (TIFF) or Portable Document Format (PDF) files along with their associated metadata.

(b) Model 3 submissions shall be converted to TIFF or PDF until the viability of preserving these electronic recordings in their native format, such as Extensible Markup Language (XML) or Extensible HyperText Markup Language (XHTML) has been demonstrated.

60:15-3-8. Processing electronic recordings

County clerks shall process electronic recordings in accordance with the provisions of Section 298.1 of Title 19 of the Oklahoma Statutes, the Uniform Electronic Transaction Act as adopted in Oklahoma and the Act regarding accepting electronic documents for filing.

60: 15-3-9. Records retention and preservation

(a) County clerks shall retain all records in their custody in accordance with sections 284 and 286 of Title 19, sections 15-112 and 15-117 of Title 12A, and sections 301 and 302 of Title 67 of the Oklahoma Statutes.

(b) The registrar of deeds records in the custody of the county clerk shall be permanently preserved. Producing security microfilm that is created within the guidelines of the American National Standards Institute (ANSI) and properly stored and handled is recommended. The Commission rules for microfilm can be found at: <http://www.odl.state.ok.us/oar/docs/oar-rules.pdf>, the Oklahoma Department of Libraries website.

60:15-3-10. Payment of recording fees

(a) Electronic payment of recording fees shall be collected by the county clerk as prescribed in accordance with Section 32.3 of Title 28 of the Oklahoma Statutes and accepted reasonable industry standards.

(b) Payments are a prerequisite to all methods of recording as required by section 292 of Title 19 of the Oklahoma Statutes.

(c) Each county clerk may collect electronic recording fees in a manner compatible with their internal software and financial practices.

60:15-3-11. E-Recording Models

Electronic recordings, whether as pilot projects or live production initiatives, have occurred in many states. From these efforts, three distinct models have emerged. The models are referred to as Models 1, 2, and 3. Each has distinctive characteristics. Each also brings certain benefits to the submitters.

Over time the improvements in delivery methods and document formats have improved the processes as well. From scanned paper documents, to electronically signed images of the documents wrapped with XML data and securely signed, to completely electronic, XML-integrated documents using electronic and digital signatures, these models bring continuing benefits to participating county clerks and document submitters. Ongoing progress with increasing value from added benefits are expected as mortgage, legal, and recording industry standards are implemented.

(1) Model 1 Description

This model is an extension of the paper-based closing or payoff processes.

Documents are prepared and printed. The parties sign and notarize the paper documents with ink signatures. When complete, the signed and notarized paper documents are scanned and electronically sent to the county clerk. Transmission is done by the submitting parties logging on to the computer system of the county clerk over a secure network after first identifying, or authenticating, themselves to the computer of the county clerk. The county clerk makes the same

determination of recordability as with paper documents, visually inspecting them for such things as signatures and acknowledgments as well as determining the recording fees.

Once the county clerk accepts the documents for recording, the scanned image is permanently affixed with the recording information, including recording date and time as well as the unique recording reference number, such as book and page number or instrument number. Indexing is performed by the indexing staff of the office of the county clerk, as with paper documents. A copy of the recorded images is returned to the submitter, together with the recording endorsement data and receipt.

(2) Model 2 Description

Model 2 recordings may be paper or electronic based. A document image whether from a scanned paper document signed and notarized by ‘wet ink’ signatures or from an electronic document electronically signed and notarized, is wrapped in an XML wrapper containing the data necessary for processing, indexing, and returning the document. In the case of a scanned paper document, Model 2 further extends Model 1 by adding data that improves the process, specifically the indexing process in the office of the county clerk. In the case of an electronic document, the process begins to improve for the settlement agent, lender, or loan servicer submitting the document.

The model may support one or more of a number of graphics formats. The recordable electronic documents are generally delivered to the office of the county clerk by whatever means agreed to by the parties as specified in the Business Rules.

Once imported into the system of the county clerk, the legacy system handles the recording functions. In this case the system imports the data from an XML wrapper, including index data.

The recording process is partially automated, but the image may be visually inspected to determine that it meets recording requirements as well as possibly to validate against the data in the XML wrapper. The indexing data in the embedded image is not linked to the index data in the XML, so the county clerk has no automated means to verify that it is the same.

If a document meets the requirements of the county clerk, it is recorded.

(3) Model 3 Description

Under Model 3, documents are generated on a Trusted Business Partner’s document preparation system according to the PRIA standards. The document preparation person logs on to the system and enters the information necessary to complete the generation of the document. Once the document has been generated, it is signed by an individual with the authority to sign. Secure access is required for all parties that must sign the document because signing is done by electronic signature.

Once the documents are electronically prepared, they are released for recording. The document preparation system compares each document against recording rules to ensure its recordability, and then calculates recording fees. Documents are submitted to the office of the county clerk

pursuant to the terms of the Business Rules of the county clerk.

Documents received at the office of the county clerk are re-checked against the rules to determine whether or not they may be recorded. If not, they are returned to the submitter. Otherwise they are accepted for recording and the data for recording is extracted from the documents and passed to the legacy recording system. The endorsement data is received from the legacy system and entered onto the respective documents in XML format. If required, the XHTML is transformed to images for the archives of the county clerk and the documents with the recording endorsements are returned to the submitter.