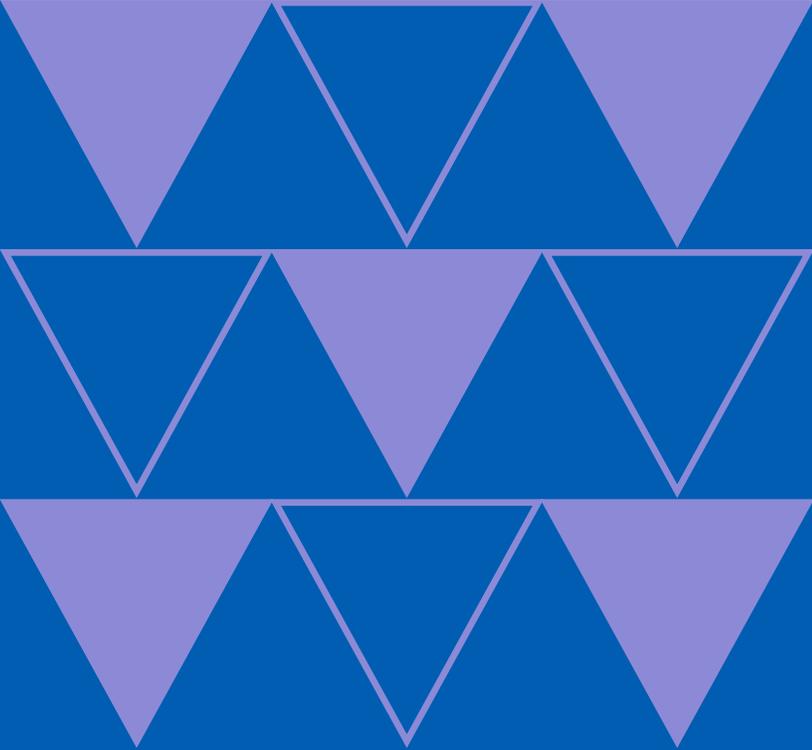


eMortgage Closing Guide



Version 1.0
Final Release
April 27, 2006

MISMO eMortgage
Workgroup



eMortgage Closing Guide: A guidance paper by the MISMO eMortgage Workgroup

Abstract

This MISMO® eMortgage Closing Guide, published by MISMO®, Inc., a wholly owned subsidiary of the Mortgage Bankers Association, is a mortgage industry reference tool, providing general guidelines for electronic closing platforms and services.

* * * The information provided is educational in nature, providing general information about legal, financial, technological and other considerations associated with eMortgages. It is not intended as legal or other professional advice. You should consult an appropriate professional with any specific questions.

© 2006 MISMO®. All rights reserved.

This work may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by an information storage and retrieval system without permission in writing from MISMO. Please contact info@mismo.org for more information.

MISMO® is a registered service mark of the Mortgage Bankers Association.

MISMO eMortgage Closing Guide

Table of contents

1	About this guide	4
1.1	Summary	4
1.2	Purpose.....	4
1.3	Scope.....	4
2	General.....	5
2.1	Executive summary.....	5
2.2	eClosing overview	6
2.3	Certification overview	10
3	Guidelines	11
3.1	Legal Considerations	11
3.2	eDoc Guidelines.....	31
3.3	eSignature Guidelines	34
3.4	eNotary Guidelines	39
3.5	Tamper-Evident Seal Guidelines	41
3.6	System Interfaces Guidelines.....	42
3.7	System Audit Trail Guidelines.....	44
3.8	Electronic Records Storage Guidelines	46
3.9	Security Guidelines	48
4	Appendix.....	52
4.1	Reference Links	52
4.2	Glossary	53
4.3	Index	57

1 About this guide

1.1 Summary

The MISMO eMortgage Closing Guide, published by the Mortgage Industry Standards Maintenance Organization, Inc. (“MISMO[®]”), a wholly owned subsidiary of the Mortgage Bankers Association, is a mortgage industry reference tool – a guide to the various aspects of electronic mortgage closing technology and business. MISMO is dedicated to developing, promoting, and maintaining, through an open process, voluntary electronic commerce procedures and standards for the commercial and residential mortgage industries.

1.2 Purpose

The MISMO eMortgage Closing Guide is intended to provide general guidelines for electronic closing platforms and/or services. This guide provides general information about the legal framework surrounding electronic closing implementation. It is educational in nature and is not intended as legal advice. Professional advice should be sought in connection with any specific efforts to implement electronic closing.

1.3 Scope

The MISMO eMortgage Closing Guide describes and explains general electronic closing concepts, definitions, and voluntary guidelines. It is not intended to be a technical implementation guide. It also does not provide information about any specific company’s internal processes, patented concepts, business logic, algorithms, or other proprietary details nor is it intended to affect the existing obligations (contractual or otherwise) between business partners. Neither does it provide legal advice. Rather, this guide provides general information about the legal framework surrounding electronic closing implementation. Professional advice should be sought in connection with any specific implementation of electronic closing.

Recommendations contained in this Guide, including those labeled “best practices,” are identified as such only as of the time of publication of this Guide. The subject matter of this Guide is subject to rapid change, as is electronic commerce generally and the legislative and regulatory rules that seek to keep up with it.

2 General

2.1 Executive summary

The mortgage industry continues to evolve into an electronic mortgage environment. Since 2001, the mortgage industry has been working cooperatively within the Mortgage Industry Standards Maintenance Organization (MISMO[®]) to define key processes, transactions, and XML data standards to exchange the mortgage data and documents electronically. This collaborative work led to the formation of a suite of eMortgage concepts and standards that may be used to move forward with eMortgages in the industry.

The closing (or settlement) is the process by which borrowers sign the documents and pay all expenses to take official ownership of their homes. This is a critical event for the borrowers, lenders, closing agents, and other parties in the mortgage transaction. Although the closing process varies from place to place, many activities are standard. One of the standard activities is to sign the documents.

In the electronic closing environment, originators, lenders and title underwriters need to make sure that this electronic transaction is enforceable after the electronic documents are electronically signed and funds are disbursed. There are a number of electronic closing solutions available today. Given the financial significance of the mortgage finance process, industry participants and borrowers will benefit from a standard way to assess whether potential solutions meet minimum compliance requirements.

This guide provides voluntary industry guidelines that may be used to evaluate the platform and/or service that comprises an eMortgage closing solution. The guidelines cover legal, process, and technical aspects of the transaction. The guide also includes supporting overview material and sample processes to connect key concepts, processes, and guidelines across the electronic closing transaction. It is not intended to be a technical implementation guide. It also does not provide information about any specific company's internal processes, patented concepts, business logic, algorithms, or other proprietary details.

Industry adoption is growing because eMortgages reduce time, cost, and risks. MISMO standards are critical to achieve eMortgage adoption across the industry. The eMortgage Closing Guide is one of the key building blocks in the evolution to the complete electronic mortgage environment.

2.2 eClosing overview

Introduction

The closing of an electronic note (eNote), security instrument (eSecurityInstrument), and other electronic closing documents requires the use of a specialized computing platform, generally known as an electronic closing or eClosing system. An electronic closing system is typically a web-based platform that allows the lender, the closing agent and the borrower to electronically review, sign, store and transfer closing documents.

Assumptions

For the purposes of this guide we assume that the closing results minimally with an eNote signed by the borrower. Other closing documents (e.g., security instruments) may or may not be electronically signed.

The electronic closing process may occur at the offices of a lender, trusted settlement agent, in the borrower's home, or at some other acceptable location. Regardless of the location, a notary or signing agent must be present to confirm the identity of the principals (e.g., borrowers, property sellers, etc.).

A title insurer may be involved in conducting the electronic closing or, at a minimum, issuing a title insurance policy. In general, a lender's title insurance policy protects a lender's security interest in the property against loss due to title defects, liens or other matters of public record. It is expected that title insurance will provide this coverage, regardless of whether the loan closing occurs electronically or in paper. Some lenders may wish to supplement title insurance with a "Closing Protection Letter" from the title insurer covering the settlement or title agent's acts or omissions in conducting an electronic closing.¹ In some cases, a title policy is not required by the lender; consequently, the lender should analyze the risks associated with executing notes and other loan documents electronically in the absence of title insurance.

The specific process used for any given electronic closing transaction will vary according to the lender, the product and the electronic closing platform on which the electronic closing is conducted. However, the following key principles apply to all electronic closings:

- A notary is present to confirm the identity of the borrower and the capacity and willingness of the borrower to sign documents.
- The process obtains the borrower's consent to sign electronically.
- The eNote and/or eSecurity Instrument and other documents if applicable are electronically signed by the borrower consistent with applicable law.
- The process properly applies a tamper evident signature to the eNote.
- The eNote is registered with the MERS® eRegistry immediately after closing.

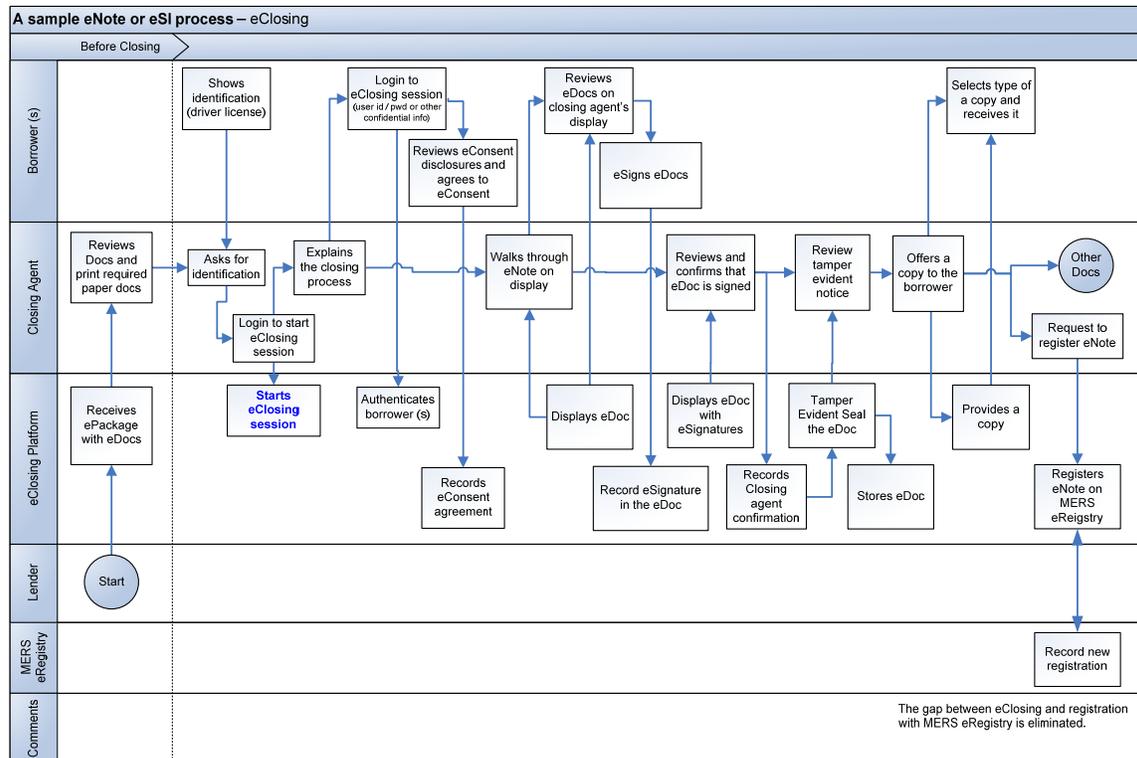
¹ Since title insurance coverage varies by policy and closing protection letters may not be available for issuance in every state, lenders should discuss this issue with their title insurers to understand the extent of title insurance and closing protection letter coverage.

eClosing overview

- The electronic closing platform maintains a permanent audit trail of all transactions.
- The electronic closing process results in an enforceable eNote.

Process summary

The processes in the mortgage industry vary based on state law, loan product type, lender requirements, investor requirements, and other requirements. The goal of this process summary is to point out common steps that may be involved in a sample electronic closing to support the proposal discussion.



Origination - Closing

- Lender
 - Generates closing docs and delivers them to the closing agent.
- Closing Agent
 - Manages the closing process by having the borrower execute the documents and delivering the recordable documents to the county recorder² for recordation.
- County Recorder
 - Records the documents and delivers them back to the lender per instruction.
- Lender

² As referenced throughout this Guide, the term “county recorder” is meant to be a generic term for the public or authorized official in the city, county, or other jurisdiction in charge of recording liens or other interests to real property. Such officials are also referred to, for example, as “county clerks,” “registrar of deeds,” and “recorder of deeds.”

eClosing overview

- Waits for the trailing recordable documents, receives them, and sends them to a servicer, other lender or investor).
 - Depending on investor requirements, the documents may go to a custodian for a final certification and safekeeping.

Key documents

Real property loans are customarily evidenced by the borrower's signing the loan obligation (the promissory note or promise to pay) and the security instrument (the trust deed or mortgage). Other documents are also required for a mortgage transaction.

Once executed by a borrower, a promissory note represents the legal obligation of the borrower to repay the debt secured by the mortgage. A promissory note that meets certain conditions under Article 3 of the Uniform Commercial Code would be considered negotiable. This allows the mortgage lender to assign the loan upon sale into the secondary mortgage market. The promissory note is the key instrument in the mortgage loan transaction, and if there are conflicts in the provisions of the note and trust deed, the terms of the note are generally controlling. The note is not a recordable instrument.

A security instrument secures the note and evidences the mortgage lender's security interest in the real property. A security instrument may be a "mortgage" or a "deed of trust" or "security trust deed." The security instrument gives a complete legal description of the property securing the loan and provides for foreclosure or conveyance of the property from the borrower (mortgagor) to the lender (mortgagee) in the case of default under the note. A "mortgage" typically requires judicial foreclosure. In general, the security instrument must be properly and timely recorded to protect the priority of the lender's lien on the property.

Other key documents involved in a loan closing may include the following:

- A warranty deed, which conveys title to a property from a seller (grantor) to a buyer (grantee);
- A settlement statement, which provides an itemized listing of the costs and charges that are payable at closing. Items that appear on the statement include real estate commissions, loan fees, points, and initial escrow amounts. HUD provides standard settlement statement forms (e.g., HUD-1 and HUD-1A). The settlement statement is also commonly known as a "closing statement" or "settlement sheet";
- Various disclosures, which are required by federal and state law (e.g. RESPA, TILA, E-SIGN, etc.)
- A power of attorney, which authorizes one individual to act on behalf of another individual (e.g., the borrower).

Conclusion

As discussed above, the electronic closing process shares virtually all the characteristics of a paper-based closing with the exception that key documents can be signed and

eClosing overview

retained electronically. However, the enforceability and transferability of the eNote, and the legality of other electronically signed documents depend on whether the closing process and/or system used to create, execute, and store the electronic documents complies with applicable federal and state legal requirements. Additionally, the purchase or investment by secondary market participants in such electronically-created mortgage loans will also depend on whether the closing process and/or system comply with requirements set by the investors.

2.3 Certification overview

Introduction

This eMortgage Closing Guide may be used by interested parties (e.g., auditors, investors, lenders, vendors, etc.) to develop a certification checklist for evaluating eMortgage closing systems or processes. Such a checklist might include the elements required to create, execute, store, and communicate legally enforceable closing package documents (e.g., electronic note, security instrument, etc.). Ideally, the certification checklist would be technology-neutral in order to be a useful tool in evaluating a variety of electronic closing processes and systems.

Process

The certification process used will depend on the requirements of the lender, title insurer and/or the lender's investor. One or more of the following approaches to certifying an electronic closing system or process may be permitted or required:

Level 1 - A self-certification process by a electronic closing system vendor using a certification checklist based on industry guidelines (e.g., information from this Guide, investor requirements, etc.). Completion of the self-certification process could result in a report signed and certified by a senior compliance officer of the eMortgage closing system provider.

Level 2 - An independent and accredited audit and/or qualified law firm certification process using a certification checklist based on industry or other required guidelines. The independent audit would result in a report certified by the audit firm and/or a legal opinion issued by the law firm.

Level 3 - A separate originator, lender, or title underwriter certification process that leverages Level 1 and Level 2 certifications.

Conclusion

The closing package includes the promissory note, security instrument, and other critical mortgage documents. A certification process designed around a certification checklist would provide a consistent way to measure and communicate compliance with legal requirements across the mortgage industry, while still allowing for the protection of proprietary information and the creation of compliant electronic closing systems and processes.

3 Guidelines

3.1 Legal Considerations

Section Outline

- I. Introduction
- II. General Laws Applicable to Loan Closings
- III. Uniform Electronic Transactions Act Summary
- IV. ESIGN Summary
- V. Authentication (Verification of Identity)
- VI. Electronic Signatures and Attribution
- VII. Consent Requirements under ESIGN and UETA
- VIII. Electronic Format and Delivery of Consumer Disclosures
- IX. Summary of the Board of Governors of the Federal Reserve System's (FRB) Interim Final Rules
- X. Establishing Control of a Transferable Record
- XI. eNotarization
- XII. eRecording
- XIII. Evidentiary Importance of an Audit Trail
- XIV. Data Security
- XV. Title Insurance Coverage for eMortgages
- XVI. Compliance with ESIGN and UETA Document Retention Requirements
- XVII. Conclusion

I. Introduction

This Section of the eMortgage Closing Guide provides a high-level overview of the legal issues associated with the electronic closing of a residential mortgage loan. It both reviews the legal foundation for using electronic documents in mortgage transactions, and highlights some of the key issues that must be addressed for an effective electronic loan closing.

The materials in this chapter are drawn from a number of sources. Readers seeking additional or more detailed information on legal issues related to the use of electronic records and signatures are encouraged to consult the Standards and Procedures for electronic Records and Signatures ("SPeRS"). Portions of this Section are based on the information from SPeRS.

This Section of the eMortgage Closing Guide is published for purposes of education and discussion. It is intended to be informational only and does not constitute legal advice regarding any specific situation, product or service. The use of this Guide is completely voluntary; the Guide's existence does not in any respect preclude anyone, whether that person has approved of the Guide or not, from manufacturing, marketing, purchasing, or using products, processes or procedures not conforming to this Guide. Any person using

Legal Considerations

this Guide should consult their own legal counsel and/or compliance personnel concerning their particular situation.

II. General Laws Applicable to Loan Closings

There are a multitude of federal and state laws, regulations, and cases that govern and/or influence a typical loan closing event. Although this list is not exhaustive, some examples of loan closing laws include the federal Real Estate Settlement and Procedures Act (RESPA), which provides instructions on how to prepare a HUD-1 settlement statement, the federal Truth in Lending Act, state “wet” or “good funds” laws, state notary laws and witness requirements, and state and local requirements governing real estate document recording. In general, these laws would apply to loan closings, whether conducted with paper documents and ink signatures or electronic documents and signatures. While these loan closing laws provide a baseline to conduct a compliant electronic loan closing, originators, lenders and title insurers will also need to comply with electronic commerce laws that enable an electronic loan closing and, further, the creation of an enforceable electronic mortgage loan transaction.

III. Uniform Electronic Transactions Act Summary

The National Conference of Commissioners on Uniform Laws (NCCUSL)³ promulgated the Uniform Electronic Transactions Act (UETA) in 1999 as a model act for adoption by the states. UETA represents the first effort at providing uniform rules to govern transactions in electronic commerce. Since UETA’s introduction, almost every state, including the District of Columbia, has adopted some version of UETA although some states have included non-uniform provisions.⁴ The objective of UETA is to ensure that transactions in the electronic marketplace are as enforceable as transactions memorialized on paper with manual signatures. In general, UETA does not change any of the substantive rules of law that apply to covered transactions. It also does not impose specific technology requirements for verification of identity or the integrity of the document itself.⁵ Note that UETA applies only to a transaction in which each party has agreed by some means to conduct electronically.

The basic rules for electronic transactions are found in Section 7 of UETA (Legal Recognition of Electronic Records and Electronic Signatures). To summarize, the fundamental rules are as follows:

- A record or signature may not be denied legal effect or enforceability under state law solely because it is in electronic form;
- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation;
- Any law that requires “a writing” will be satisfied by an electronic record.
- Any signature requirement in the law will be met if there is an electronic signature.

³ NCCUSL’s model acts can be viewed on their website at www.nccusl.org.

⁴ The extent to which these non-uniform provisions are effective is limited by the federal ESIGN Act (see summary below). A detailed discussion of the various state non-uniform provisions and the limitations placed on them by the ESIGN act is beyond the scope of this Guide.

⁵ As discussed below, UETA does make some substantive changes to the law concerning the transfer of negotiable debt instruments in an electronic environment.

Legal Considerations

UETA establishes the concept of “transferable records” in Section 16. An electronic record that would otherwise be a negotiable promissory note under Article 3 (Negotiable Instruments) of the Uniform Commercial Code (UCC) may be a “transferable record” under UETA if agreed by the parties. The “transferable record” concept is significant because the residential mortgage industry relies heavily on negotiable promissory notes to preserve the liquidity of mortgage loans. For a negotiable promissory note executed in paper, the ability to negotiate or transfer the note depends in part upon possession of the original promissory note itself as evidence of the noteholder’s exclusive right to enforce and collect the underlying debt. Since it is impossible, in an electronic environment, to “possess” an “original” document, Section 16 of UETA establishes an alternative structure for preserving negotiability.

In general, under Section 16 a person has “control” of a transferable record, meaning the exclusive right to enforce or transfer ownership of the underlying debt obligation (i.e., a “holder” under the UCC), if “a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.” Nothing more is required. However, Section 16 also establishes a “safe harbor” for determining that a system for transferring interests in the transferable record is adequate. Under the safe harbor, a transferable record exists when there is a single authoritative copy of that record existing and unalterable in the “control” of a person. For more information on the safe harbor, see the Establishing Control of a Transferable Record Section below.

If a state has enacted UETA, it will be the governing law in the state regarding the enforceability of electronic transactions. Because states may amend UETA as they deem appropriate, state enactment of UETA by itself has not resulted in a national standard for real estate finance professionals to follow. However, the federal Electronic Signatures in Global and National Commerce Act (ESIGN) limits the effectiveness of state amendments to UETA. See the following section for a discussion of how UETA relates to the federal ESIGN legislation.

IV. ESIGN Summary

On June 30, 2000, Congress enacted ESIGN to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically. This congressional action reflected concerns over the pace of state enactment of UETA coupled with the ongoing enactment by states of laws either modifying UETA or establishing new regulatory regimes, conditions which prevented the establishment of a uniform national standard. For states that have enacted a uniform version of UETA, the provisions of ESIGN may be superseded in whole or in part. However, non-uniform amendments to UETA that conflict with the main provisions of ESIGN are preempted, for the most part. Also, state regulations that conflict with the requirements of ESIGN are preempted, whether or not the state has enacted UETA.⁶ Most of the provisions in ESIGN mirror provisions contained in UETA. However, in order to preserve the underlying consumer protection laws governing consumers’ rights

⁶ The federal ESIGN Act permits a state to supersede Section 101 of ESIGN with a conforming UETA enactment. Section 104 of ESIGN, which governs state regulation, is not affected by a state’s UETA enactment.

Legal Considerations

to receive certain information in writing, ESIGN imposes special requirements on parties that want to use electronic records. For more information on these requirements, see the Consent Requirements section below.

V. Authentication (Verification of Identity)

“Authentication” is the process used to confirm an individual’s identity as a party to a transaction.⁷ To ensure enforceability of a mortgage transaction, as well as to minimize the risk of fraud, a lender should ensure that its customers are who they purport to be. In addition, lenders may also be subject to laws requiring authentication of any individual or entity obtaining a loan. For example, the USA Patriot Act and its implementing regulations, which were passed to combat terrorism and money-laundering, require certain financial institutions to verify the identity of any person seeking to open an account and to maintain a record of the information used to verify such person’s identity. Further, certain categories of financial institutions, such as national banks, are required by the Patriot Act to adopt written customer identification programs (“CIPs”), which require collection of a customer’s name, date of birth, residential or work address for individuals or physical location for legal entities, and a tax identification number (TIN) before the customer can open a deposit or loan account. The information gathered pursuant to the CIP must be verified to the extent reasonable and practicable.

In a traditional loan closing situation, an example of authentication occurs when a signing agent or notary asks to see a person’s drivers license or passport to confirm that the person is who he or she purports to be. Generally speaking, authentication of identity in an electronic transaction may occur in two contexts:

- When the relationship between the parties is first created.
- When a transaction occurs in the course of an existing relationship.

In a residential mortgage transaction, authenticating identity when a relationship is first created usually requires reference to some kind of outside source for validation, be it a government-issued ID or verification of ID from another trusted source (e.g., credit bureau, etc.). Authenticating the borrower thereafter over the course of the transaction may rely primarily on a credential issued to the borrower, such as a user ID and password.⁸ However, where state law requires applicable mortgage-related documents to be notarized, authentication at the time of notarization in accordance with notarial law will be required.

It is important not to confuse authentication (including notarization) with the act of signing. Authentication involves accurately identifying the parties to a transaction. A signature does not have to provide evidence of the signer’s identity, although some types

⁷ In this subsection, we are primarily concerned with “authentication” in the context of verifying identity; it should not be confused with other types of authentication, such as authentication of a security agreement in the UCC Revised Article 9 context, “document authentication” performed by a notary to help ensure that documents can be trusted in government or commercial dealings, or the authentication procedure used in litigation for the purposes of admitting certain records into evidence.

⁸ The FFIEC has recently advised that certain remote consumer transactions require the use of a two-part authentication process, employing both a password and some other information that is in the consumer’s possession, such as a random number generator. At this time, it is not clear that a residential mortgage lending transaction is the type of high risk remote consumer transaction contemplated by the FFIEC guidance.

Legal Considerations

of signatures may help identify the signer. An authentication process also does not necessarily provide signature attribution or protect an electronic record from alteration, although, once again, some types of authentication will associate a signer with his or her signature and protect a record's integrity. See Subsection VI for a general discussion on Electronic Signatures and Attribution and Subsection XI for a discussion on eNotarization and its relationship to authentication.

The Federal Financial Institutions Examination Council (FFIEC) has published Frequently Asked Questions about the Patriot Act and CIP obligations, as well as a guidance document on "Authentication in an Internet Banking Environment" which is available at www.ffiec.gov. Given these obligations, a lender or originator should ensure that its electronic closing process accommodates the particular customer identification requirements applicable to it. Such an authentication process can occur either technologically within an electronic closing system or through methods traditionally used in paper-based closings. See SPeRS for a general discussion on how an authentication process may be designed to provide evidence of identity and protect a record's integrity.

VI. Electronic Signatures and Attribution

Both ESIGN and UETA similarly define an "electronic signature" as any sound, symbol or process, attached to or logically associated with an electronic record and executed or adopted with the intent to sign the electronic record. Both ESIGN and UETA are intentionally neutral with regard to specifying which electronic signatures would be acceptable in a particular situation. However, lenders should check with their investors for specific guidance on the types of electronic signatures that would be acceptable for use in eMortgages intended to be sold to the such investors. For some examples of different electronic signature types, see Section 3.3 of this Guide.

A Attachment or Logical Association

In a paper-based transaction, the association of a signature to a document is generally shown by such signature being physically affixed to a particular document. However, depending on the circumstances, an electronic signature may be considered valid under ESIGN and UETA even though the signature is not physically viewable on the electronic record itself. For example, a click-through signature process may be a valid electronic signature if designed in such a way that the system logically associates the click signature to a particular electronic record.

B Intent

The validity of an electronic signature requires the intent by the signer to sign and be bound to a particular record. Similar to a paper-based transaction, evidence of intent can be found within the document itself and/or the surrounding circumstances in which the document was signed.

C Attribution of a Signature and Record to a Person

Although ESIGN and UETA provide that electronic signatures are legally equivalent to "wet" ink signatures, attribution remains an issue. Attribution is the process of connecting a particular person to his or her signature on a particular document. For ink signatures, attribution may be done through a handwriting comparison or, in certain

Legal Considerations

circumstances, through a notary witnessing a person signing a document and acknowledging such act. With the exception of when a notary is present during the signature process, attribution of other electronic signatures may be more complex. UETA provides guidance in this area by stating that an electronic record or electronic signature is attributable to a person if it was the act of the person. An act of a person includes an act done by the agent of a person, as well as an act done by an electronic agent (i.e., computer, signing pad) of a person.

The UETA commentary provides some examples of electronic acts in which the record and signature would be attributable to a person, as follows:

- The person types his/her name as part of an e-mail purchase order;
- The person's employee, pursuant to authority, types the person's name as part of the e-mail purchase order;
- The person's computer, programmed to order goods upon receipt of inventory information within particular parameters, issues a purchase order which includes the person's name, or other identifying information as part of the order.

The act of the person may be shown in any manner, including showing the efficacy of any security procedure applied (i.e., access controls, password and PIN, etc.) to determine the person to which the electronic record or electronic signature was attributable. Furthermore, UETA provides that the effect of an attributed electronic record or signature can be determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise provided by law. This means that even if proper attribution occurs, the legal enforceability of such record and signature may still be dependent on other factors (i.e., intent, legal age, capacity, proper authority, etc.).

VII. Consent Requirements under ESIGN and UETA

A. Under ESIGN and UETA, a party must agree to use electronic records and/or signatures with respect to a specific transaction or group of transactions.

Nothing in ESIGN or UETA requires a party to use electronic records and/or electronic signatures in a transaction. In general, the agreement to use electronic records and/or signatures may be either express or implied, and an express agreement may be oral or in writing. However, before a party can electronically provide information to a consumer otherwise required by law to be delivered "in writing", the provisions of ESIGN (and in some cases, the state UETA) require the party to provide specific ESIGN consent disclosures to the consumer, and require the consumer to affirmatively consent to receive the information electronically.

ESIGN requires businesses to obtain from consumers electronic consent or confirmation to receive information electronically that the law requires to be delivered in writing (e.g., Truth in Lending disclosures). Before consent can be given, the consumer must receive a disclosure regarding:

- any right or option the customer has to receive disclosures in paper form;

Legal Considerations

- whether the consent applies only to a particular transaction or to categories of records that may be provided during the course of the parties' relationship;
- the right to withdraw consent to have records provided electronically, including any conditions, consequences, or fees associated with doing so. The institution must describe the procedures for withdrawing consent and for updating information needed to contact the consumer electronically;
- how, after the consent, the consumer may obtain a paper copy of a record upon request; and
- the hardware and software requirements for access to and retention of the electronic information.

ESIGN requires that consumers express their consent electronically, or confirm their consent electronically, in a manner that reasonably demonstrates that the consumer will be able to access required notices or disclosures electronically. If, after consent is provided, a change is made in the hardware or software requirements needed to access or retain the electronic disclosures and the change creates a material risk that the consumer will not be able to access or retain an electronic disclosure that was the subject of the prior consent, the consumer must be provided with an appropriate notice of the change and must re-consent electronically in a manner that reasonably demonstrates the consumer's ability to access the electronic notice or disclosure within the changed hardware or software environment.

B. Under ESIGN and UETA, an issuer (borrower) must expressly agree to treat an electronic record as a transferable record.

An electronic form of promissory note qualifies as a "transferable record" under ESIGN or UETA only with the express agreement of the borrower. This express agreement can be obtained separately from the transferable record or be contained within the transferable record itself. For example, Fannie Mae and Freddie Mac have developed an eNote clause that must be included in any eNote intended to be sold to Fannie Mae or Freddie Mac. The eNote clause articulates the borrower's specific agreement to treat the eNote as a transferable record.

VIII. Electronic Format and Delivery of Consumer Disclosures

The delivery of required consumer disclosures in an electronic mortgage lending environment presents a unique challenge. Not only do some disclosures require an ESIGN consent before they may be provided electronically, lenders will still need to keep in mind that neither ESIGN nor UETA affect any statutory or regulatory requirement regarding the content, proximity or format of any warning, notice, disclosure or other record required to be posted, displayed or publicly affixed. For example, if a required notice must appear immediately above the consumer's signature line in a writing, that requirement must also be met in an electronic environment (e.g., the notice may appear immediately above the portion of the screen where the consumer places her electronic signature, or the notice may be placed in a dialog box that is presented to the consumer just before her signature is added to the record).⁹ Additionally, lenders will need to

⁹ The electronic medium offers a variety of ways to address proximity and timing requirements in an innovative manner. See Section 3 of SPeRS for more ideas on innovative display of disclosures.

Legal Considerations

determine that the method they choose for providing electronic disclosures will meet any requirements related to communication, timing, verification or acknowledgment of receipt, storage and retention.

ESIGN contains a few additional limitations on providing disclosures electronically. For example, for disclosures that require an ESIGN consent to be delivered electronically, oral communication of such disclosures to a consumer would not qualify as electronic delivery unless otherwise provided under applicable law. Additionally, ESIGN does not allow the consumer to consent to receive in electronic form any notice of acceleration, repossession, foreclosure, eviction, or right to cure relating to a credit contract secured by the consumer's primary residence.

For compliance guidance on the electronic delivery and retention of consumer disclosures, mortgage lenders should look to federal agency issuances, such as the interim final rules (although they are not mandatory) amending Regulation B and Regulation Z (as discussed below) and advisory letters issued by the Comptroller of the Currency on Electronic Consumer Disclosures and Notices (AL 2004-11) and Electronic Record Keeping (AL 2004-9). Mortgage lenders should also consult SPeRS for additional guidance on effectively obtaining consumer consent and delivering disclosures.

IX. Summary of the Board of Governors of the Federal Reserve System's (FRB) Interim Final Rules

In order to establish uniform standards for the electronic delivery of disclosures required under Regulation Z (Truth in Lending) and Regulation B (Equal Credit Opportunity Act), the FRB released Interim Final Rules in 2001. Since then, the FRB has withdrawn the mandatory compliance date on the Interim Final Rules, but has subsequently advised that compliance with the Interim Final Rules will satisfy the statutory requirements for consumer disclosures under ESIGN. Therefore, the Interim Final Rules provide both a handy reference for issues to address when designing electronic disclosures and insight into the approach regulators are likely to take when evaluating the effectiveness of electronic delivery.

For these reasons, this Section includes a summary of some of the provisions in the Interim Final Rules that may provide guidance for electronic delivery of disclosures in a mortgage lending transaction. However, bear in mind that the Interim Final Rules are not mandatory – an approach to presenting and delivering electronic records in a mortgage transaction that does not comply with the Interim Final Rules may still be sufficient under ESIGN and the UETA.

A Electronic Delivery Provisions in Regulation Z and Regulation B

1. Requirements for Electronic Communication

Regulation Z and Regulation B define "Electronic Communication" as a message transmitted electronically between a creditor and consumer in a format that allows visual text to be displayed on equipment (e.g. a personal computer monitor). Generally, a creditor may provide, by electronic communication, any disclosure required by Regulation Z or Regulation B to be in writing. Before a creditor can provide such

Legal Considerations

disclosures electronically, a creditor is usually required to obtain a consumer's affirmative consent to receive such disclosures electronically pursuant to ESIGN.¹⁰

For purposes of either Regulation Z or Regulation B, a consumer's electronic address is an e-mail address that is not limited to receiving communications transmitted solely by a creditor. For consumer disclosures that require an ESIGN affirmative consent, a creditor shall either (1) send the disclosure to consumer's electronic address; or (2) make the disclosure available at another location (i.e., Internet Web site) and alert the consumer of the availability of the disclosure through a notice sent to the consumer's electronic address. In either situation, the creditor is required to make the disclosure available for at least 90 days from the date disclosure becomes available or from the date of the consumer notice, whichever is later.¹¹

If an electronic disclosure is returned to creditor undelivered, the creditor is required to take reasonable steps to redeliver the disclosure using information from its files. If the regulation requires a consumer to sign or initial a particular disclosure, then an electronic signature, as defined by ESIGN, would satisfy this requirement.

For disclosures provided on a creditor's equipment (i.e., a computer terminal in creditor's lobby, ATM at a public kiosk, etc.), the creditor must ensure the equipment satisfies requirements to provide timely disclosures in a clear and conspicuous format that consumer may keep. For example, if disclosures are required at time of the on-line transaction, the disclosures must be sent to consumer's e-mail address or be made available on an Internet Web site, unless the creditor provides a printer that automatically prints the disclosures.

B. Applicability to Delivery of Regulation Z Disclosures

1. ESIGN Consent Required for Transaction-Specific Regulation Z Disclosures

Regulation Z makes a distinction between disclosures specific to a loan transaction and those disclosures that are not (i.e., early shopping disclosures, advertisements, etc.) with respect to the need to obtain a consumer's ESIGN consent. For transaction-specific disclosures required to be in writing (i.e., rescission notices), an affirmative ESIGN consent is required from the consumer before the creditor can deliver such disclosures electronically. On the other hand, disclosures that are not transaction-specific (i.e., early adjustable rate mortgage (ARM) disclosures, early home equity disclosures, credit advertisements, etc.) are permitted to be provided electronically without the consumer's affirmative ESIGN consent.¹²

2. Early Home Equity and Early ARM Disclosures

¹⁰ The Interim Rules articulate a few exceptions to the ESIGN consent rules. See discussion below under "Applicability to Delivery of Regulation Z Disclosures."

¹¹ The staff of the Federal Reserve Board has referred to this informally as the "kitchen table rule." Disclosures that are provided in writing are not always read immediately – instead, they may be "thrown on the kitchen table" for later review.

¹² Although ESIGN preserves federal rulemaking authority to interpret ESIGN's consumer consent provisions, some commentators to the FRB's Interim Rules have asserted that ESIGN does not actually authorize these exceptions.

Legal Considerations

With respect to early disclosures required by Regulation Z, a consumer must be able to access the disclosures (including FRB's home equity brochure, if applicable) at the time the blank loan application or reply form is made available by electronic communication, such as on a creditor's Internet Web site. With respect to early home equity disclosures, a creditor can provide these on a Web site using a link to prevent the applicant from bypassing the disclosures before submitting the application. If a link is not used, the application or reply form must clearly and conspicuously refer the consumer to the fact that rate, fee, and other cost information either precedes or follows the application or reply form. As an alternative to a link, a creditor can provide the early home equity disclosures by ensuring that the disclosures automatically appear on the computer screen when the application or reply form appears. A creditor is not required to confirm that the consumer has read the disclosures or the home equity brochure.

3. Notice of Right to Rescind

In any paper-based transaction subject to rescission under Regulation Z, creditors must deliver two copies of the notice of right to rescind to each consumer entitled to rescind. However, if electronic communication (i.e., e-mail) is used for delivery, the Interim Final Rules permit a creditor to comply by sending one notice to each consumer entitled to rescind. However, each consumer must have consented to receive electronic disclosures and each must have designated an electronic address for receiving the disclosure.¹³

C. Applicability to Delivery of Regulation B Disclosures

1. Regulation B Disclosures Given At Time of Application

With respect to Regulation B, if certain disclosures are provided on or with the loan application, the Interim Final Rules suggest that those disclosures are not subject to the affirmative consent requirement under E-SIGN. Regulation B disclosures that may be provided on or with the electronic loan application without affirmative consumer consent are the notice of right to receive a copy of the appraisal and the information requested for monitoring purposes.

If the creditor allows an applicant to apply on-line, the applicant must be required to access any disclosure required at application before the consumer is able to submit the application. For example, a creditor can utilize a link to prevent the applicant from bypassing the disclosures before submitting the application or a creditor can have the disclosures appear automatically on the computer screen. In either case, the creditor is not required to confirm that the applicant has read the disclosures.

2. Appraisals and Adverse Action

The commentary to Regulation B provides that disclosures provided by e-mail are timely based on when the disclosures are sent. With respect to disclosures posted at an Internet Web site, such as adverse action notices or copies of appraisals, disclosures are timely when the creditor has (1) made the disclosures available on the Web site and (2) sent a notice alerting the applicant that the disclosures have been posted. For example, under 12 C.F.R. § 202.9, a creditor must provide a notice of action taken within 30 days of

¹³ The Rescission Notice is, perhaps, the only disclosure given under Regulation Z that is not constructively delivered to all co-applicants when it is delivered to one of them. Delivering the rescission notices electronically therefore requires special care and attention to detail.

Legal Considerations

receiving a completed application. For an adverse action notice posted on the Internet, a creditor must post the adverse action notice and notify the applicant of its availability within 30 days of receiving the applicant's completed application.

X. Establishing Control of a Transferable Record

A key aspect of the secondary mortgage market is the mortgage industry's ability to sell mortgage notes. As mentioned above, ESIGN and UETA create a parallel structure for the transfer and negotiability of an electronic promissory note to a third party so that a third party transferee has the rights and defenses analogous to those held by a "holder," or a "holder in due course," under the UCC. The key to the transferability of an electronic record under ESIGN and UETA is "control," which can be thought of as the equivalent of "possession plus delivery and endorsement" in the paper context. ESIGN and UETA provide that a person has "control" of a transferable record if the system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

While this standard stands on its own, UETA and ESIGN offer a "safe harbor" for meeting the control requirement.¹⁴ Control exists if the system for maintaining control meets the list of safe harbor requirements under Section 16(c) of UETA and Section 201(c) of ESIGN, as described below.

A. A single authoritative copy of the record exists that is unique, identifiable, and unalterable without detection.

To qualify as an authoritative copy, an electronic promissory note must be unique, identifiable and unalterable without detection. An electronic promissory note can be unique by having a specific characteristic that distinguishes it from other copies. The characteristic can be provided by technology, by process, or by agreement. For the electronic promissory note to be identifiable, the system being used or the agreement between the parties needs to specify or describe the unique feature that identifies the authoritative copy and how that unique feature can be accessed or confirmed. The electronic record must be protected or monitored so that alterations can be identified as authorized or unauthorized.¹⁵

B. The authoritative copy identifies the person asserting control as either the person to whom the transferable record was issued or the person to whom the transferable record was most recently transferred.

The authoritative copy must be tied to a system or process for identifying the current party in control of the record. This can be accomplished either (1) through information logically associated with the authoritative copy, or (2) through the use of a trusted third party registry, which is referenced in the authoritative copy of the record.¹⁶ For example,

¹⁴Neither UETA nor ESIGN expressly requires that the safe harbor requirements be met in order to establish control. A system that meets the safe harbor will establish control – however, it is both conceivable and probable that many systems not meeting the safe harbor's requirements would also establish control.

¹⁵ UETA and ESIGN leave to other law the question of who can authorize alterations to the transferable record. In general, except as otherwise agreed, only the issuer of a negotiable promissory note can authorize alterations (other than the addition of endorsements by the holders).

¹⁶ The use of a registry system that is cross-referenced in the authoritative copy, rather than an addition to the record itself, is discussed in the commentary to the UETA.

Legal Considerations

the MERS® eRegistry was designed as an industry utility serving as the central location to identify the current person in control and the location of the authoritative copy of the electronic promissory note. Language, such as Fannie Mae and Freddie Mac's eNote clause, is included in the electronic promissory note referencing the MERS® eRegistry or another trusted third party registry, as the system for identifying the person in control of the electronic promissory note.

C. The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian.

The person asserting control of the authoritative copy or her designated custodian would be equivalent to the person who is authorized to possess the physical promissory note in a paper environment. As a result, the person asserting control or his or her custodian must have access to the authoritative copy and be able to maintain the authoritative copy without the ability for others to duplicate or acquire the authoritative copy without their permission.

D. Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control. ESIGN and UETA permit an authoritative copy to be revised in order to add or change its identified assignee, but only with the consent of the person asserting control.

E. Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy.

All copies of the authoritative copy of the electronic promissory note need to be readily identifiable as such. This can be accomplished, for example, by inserting language into the electronic promissory note that gives third parties notice that they may not be viewing the authoritative copy of the note and that they would need to check a designated third party registry (i.e., the MERS® eRegistry) in order to determine the actual location of the authoritative copy. Fannie Mae and Freddie Mac drafted the eNote clause for their Uniform Instruments to meet this requirement.

F. Any revision of the authoritative copy is readily identifiable as an authorized or unauthorized revision.

Revisions to an authoritative copy, such as modifications to an electronic promissory note, must be identifiable as authorized or unauthorized. This can be accomplished using a trusted third party registry, such as the MERS® eRegistry. Whenever a modification is created and agreed upon by the person in control and the obligor(s) to the electronic promissory note, the modification can be registered on the third party registry in such a way that it is associated with the original electronic promissory note. Any persons that

The control requirements may be satisfied through the use of a trusted third party registry system. Such systems are currently in place with regard to the transfer of securities entitlements under Article 8 of the Uniform Commercial Code, and in the transfer of cotton warehouse receipts under the program sponsored by the United States Department of Agriculture. This Act would recognize the use of such a system so long as the standards of subsection (c) were satisfied. In addition, a technological system which met such exacting standards would also be permitted under Section 16.

Legal Considerations

check the registry will be put on notice that a modification to the electronic promissory note exists.

XI. eNotarization

Notarization plays an important role in a real estate transaction because, for example, documents to be recorded in a land record system are generally required to be notarized. The essential components of notarization are (1) personal appearance of the signer before the notary, (2) proof of identity of the signer, (3) acknowledgment by the signer that he or she intends to create a binding agreement, (4) observation by the notary that the signer does not appear to be acting under threat or duress, and (5) observation by the notary that the signer appears to be aware of the document signing. These steps assist in detecting attempted fraud or deterring fraud in a loan closing and create evidence of the validity of the transaction. To achieve these goals, an electronic loan closing system should implement electronic notarization in a way that meets applicable legal requirements and provides evidence of notarization of a document sought to be enforced in court.

A. Notarization under UETA and ESIGN

Notaries in the United States entered a new era in 1999 when UETA was published. UETA specifically allows for the use of electronic signatures by notaries:

Section 11. Notarization and Acknowledgment. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

Additionally, ESIGN closely tracks UETA, including the provision on use of electronic signatures by notaries:

Subsection 101(g). Notarization and Acknowledgment. If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

The legislative history of ESIGN indicates that 101(g) is intended to remove any requirement of a stamp, seal, or similar embossing device, as applicable, for electronic notarizations. This notation recognizes that the notary's seal may be represented simply as "information" (textual or otherwise) on an electronic document, as long as that data conforms to existing state laws concerning the information that must be conveyed by the notary's seal. However, the fact that ESIGN itself does not directly address the removal of the seal requirement specifically raises interpretative issues that many real estate and legal professionals would like to see clarified by statute.

B. State Laws and Regulations Enabling eNotarization

Legal Considerations

States have adopted or are currently working on adopting legislation to support electronic notarization, including clarification of the status of seals. NCCUSL's draft of the Uniform Real Property Electronic Recording Act (URPERA) [Sec. 3(c)], which some states have already adopted, effectively duplicates the UETA and ESIGN language regarding the use of electronic signatures by notaries and adds a provision that the notary's seal need not be displayed as a physical or visual image on an electronic document being recorded.

Notarial law varies widely from state to state, and must be taken into account in addition to ESIGN, UETA, and URPERA when contemplating the use of electronic notarization. The Model Notary Act was updated in 2002 to provide a comprehensive system of authorization and regulation of electronic notarization. The electronic notarization provisions of this Act have been adopted in their entirety in North Carolina and are under consideration in other states. In addition, the Act's requirement that notaries specially register with the state commissioning official before performing electronic notarizations has been adopted in Alaska, Colorado, Kansas and Pennsylvania. Requirements for affixing and securing the notary's electronic signature and seal on electronic documents also have been adopted in Arizona and California and are under consideration in other states. For example, some states may require or recommend that electronic notarization be implemented using document integrity measures that help establish that the notary's electronic signature is associated with the document that the notary signed and that the document is genuine and unaltered at the time of signing.

These legislative efforts will bring clarity to the legal effect of electronically notarized documents and will establish the rules, procedures, and guidelines that govern notary practice in the electronic age. Parties interested in eNotarization should determine whether their state has, or will implement laws or regulations governing eNotarization. Additional guidance can also be found through state or national notary professional organizations.

XII. eRecording

Implementation of electronic recording (eRecording) necessarily implies that the real estate document being submitted for filing in the public land records is a valid electronic document and that the receiving body is authorized and willing to accept the electronic record for recording. Fortunately, the broad nature of ESIGN and UETA permits real estate documents to be in electronic format, to contain electronic signatures, and to be accepted for filing in the event county recorders choose to do so. However, there has been a lot of discussion as to whether ESIGN or UETA, without additional state law, provide county recorders with the authority to engage in electronic recordation. URPERA also addresses the recordation of electronic records in the public land records.

ESIGN and UETA's general rules of validity similarly provide that, with respect to a "transaction," a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. Both ESIGN and UETA define a "transaction" as an action or set of actions relating to the conduct of business, consumer, commercial affairs between two or more persons, and in the case of UETA, the definition of "transaction" additionally covers governmental activities. In addition, ESIGN's definition of

Legal Considerations

“transaction” specifically includes the sale, lease, exchange, or other disposition of any interest in real property. Real estate documents, such as deeds of trusts and mortgages, often have to be notarized or acknowledged under applicable state law. ESIGN and UETA provide that this requirement can be met if the electronic signature of the notary or other authorized person is attached to or logically associated with the electronic real estate document. Therefore, ESIGN or UETA do not specifically preclude real estate documents from being in an electronic format or having electronic signatures.

A. ESIGN and UETA, as applicable, may be written broadly enough to allow a county recorder the choice of accepting electronic real estate documents for recording. ESIGN and UETA do not mandate that county recorders accept electronic real estate documents for recording. However, since ESIGN and UETA provide that electronic records and electronic signatures are legally equivalent to paper records and ink signatures, a county recorder can choose to accept electronic real estate documents for recording, subject to any record standards or format requirements issued by a federal or state regulatory agency or self-regulatory organization.

State attorneys general and the Property Records Industry Association (PRIA) have differing opinions on whether ESIGN and UETA give county recorders sufficient authority to accept electronic real estate documents, including scanned documents, for recording. Several state attorneys general (“AGs”), including those in California and New York, have issued opinions in recent years maintaining that ESIGN and UETA, without additional state law, do not require a county recorder to accept electronic documents, including documents with electronic signatures, for recording. The AGs’ opinions stipulate that electronic real estate documents are legal and enforceable between the parties to a particular transaction. However, the opinions point out the difference between enforcing the underlying real estate document between parties and the distinct activity, under state statutes that require the filing of paper documents with “live” signatures, of accepting an electronic document for recording in the public land records to give third parties notice of rights in a parcel of real property. There is also controversy regarding whether scanned documents (i.e., paper documents converted to electronic form) meet state requirements that an “original” document or document containing an “original signature” be presented for recording. California, New York and Texas attorneys general have asserted that scanned documents and/or scanned signatures are only copies of original documents or signatures.

PRIA and the Electronic Financial Services Council (EFSC) have taken the position that ESIGN and UETA do provide a clear basis for recordation of electronic real estate documents. With regard to scanned images, PRIA and EFSC maintain that the definition of “electronic” includes a scanned image. This opinion is supported by the UETA commentary which makes it clear that “electronic data interchange, electronic mail, voice mail, facsimile, telex, telecopying, scanning and similar technologies” would qualify as electronic.

As a result of these differing views, mortgage lenders should consult with the particular counties and the state attorney generals’ offices in the states in which they wish to submit

Legal Considerations

electronic or scanned documents for recording to determine whether such states or counties recognize the validity of electronic real estate document filings.

B. URPERA and other state laws clarify the authority of county recorders to accept electronic real estate documents for recording.

To clear up confusion as to whether electronic real estate documents (including scanned documents) may be accepted for recording and to establish electronic recording standards for county recorders to follow, NCCUSL published URPERA in August 2004. If adopted by a state, URPERA will give county clerks and recorders the legal authority to prepare for and develop systems to accept electronic recording of real property instruments. Similar to ESIGN and UETA, URPERA reiterates that electronic documents and electronic signatures will satisfy any state recording laws that require a document to be an “original” or “in writing,” and to contain original or written signatures, notarizations and acknowledgments. URPERA also provides that any state electronic recording commission or agency responsible for setting electronic recording standards must consider the standards and practices of other jurisdictions and the standards promulgated by national standard-setting bodies (e.g., PRIA), in addition to considering the needs of its counties and views of interested persons. Several states have already adopted URPERA while other states have bills on URPERA pending.

Additionally, states such as California and Colorado, have adopted separate statutes that provide for the acceptance of electronic real estate documents, including, in some cases, digitized images of electronic real estate documents, for recording.

XIII. Evidentiary Importance of an Audit Trail

One of the advantages of migrating from a traditional loan closing process to an electronic loan one is the opportunity for an electronic loan closing system to capture and retain a reliable and trustworthy audit trail. Such an audit trail can be used to capture data or information that represents each of the critical events in an electronic loan closing. For example, the audit trail data could include information such as the date and time a person electronically signed a particular document and the contents of that document at the moment the person’s signature was captured.

In examining the usefulness of an audit trail feature in an electronic closing system, an originator, lender, or title insurer should keep in mind federal and state rules of evidence governing the admissibility of computer records, such as an audit trail. For example, under Rule 901 of the Federal Rules of Evidence, computer records generally are not admissible unless the person presenting the computer records provides “evidence describing the process or system used to produce a result and showing that the process or system produces an accurate result.” This evidence may be provided by a person’s testimony or documentation that describes in detail how the audit trail function works and what features preserve the accuracy and integrity of the audit trail data.

XIV. Data Security

Since an electronic mortgage transaction invariably handles sensitive customer information, compliance with applicable privacy and data security laws and regulations are critical, especially from a business and reputational risk management perspective. On

Legal Considerations

the federal level, the Gramm-Leach-Bliley Act (“GLB”) sets forth requirements for protecting the privacy of a person’s financial information held by financial institutions (e.g., banks, thrifts, credit unions, insurance companies, finance companies, other non-bank entities offering financial products, etc.). The GLB Act provides federal regulatory agencies¹⁷ with the authority to issue and enforce regulations regarding the collection and disclosure of customer information, and the establishment of safeguards to protect customer information from access by unauthorized persons. For the purposes of this Guide, we will focus on the GLB Act’s requirement that financial institutions ensure the privacy and security of customer information.

Pursuant to the GLB Act, the federal regulatory agencies have issued guidelines establishing standards for safeguarding customer information from unauthorized access (known as the “Safeguards Rule” for FTC-regulated institutions and the “Security Guidelines” for depository institutions). Generally, the Security Guidelines set forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to: (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. The Security Guidelines require financial institutions to have reasonable policies and procedures in place to safeguard the security and confidentiality of customer information and to ensure proper disposal of customer information.¹⁸ The Guidelines require financial institutions to implement a written information security program that is appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. Among other requirements, a financial institution’s information security program needs to require service providers, by written contract, to protect and properly dispose of a customer’s personal information. For more guidance on how to comply with the Security Guidelines, mortgage lenders should review the Interagency Guidelines Establishing Information Security Standards: Small Entity Compliance Guide.¹⁹

In addition to the Security Guidelines, several states have passed or are considering the passage of laws and regulations requiring companies to safeguard customer information that they maintain and to notify consumers of security breaches involving consumers’ personal information. For example, the California security breach notification law (SB 1386), which applies to all organizations who maintain “personal information” on California residents, to notify such residents in the event their unencrypted personal

¹⁷ The federal regulatory agencies with supervision over financial institutions usually involved in mortgage lending are the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve, the National Credit Union Association, and the Federal Trade Commission.

¹⁸ Section 216 of the Fair and Accurate Credit Transactions Act of 2003 requires entities to properly dispose of consumer information derived from credit reports. The federal bank and thrift regulatory agencies incorporated guidance on how to comply with this requirement within its Security Guidelines. For institutions regulated by the FTC, the disposal guidance is contained within the FTC’s Disposal Rule which is available at <http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf>.

¹⁹ The Small Entity Compliance Guide was published on December 15, 2005 and is available at <http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/attachment.pdf>.

Legal Considerations

information is compromised. Under California's law, "personal information" includes an individual's first name or first initial and last name in combination with one or more of the following: (1) a social security number, (2) drivers license or California identification card number, (3) account number, and/or credit or debit card information including numbers and passwords, personal identification numbers (PINs) and access codes. Some states, notably New York and New Jersey, require notification to state law enforcement and/or regulatory agencies, in addition to notice to affected consumers. As a result, lenders should ensure that closing systems that handle this type of information have appropriate access controls, encryption, and policies regarding secure communication to mitigate the risk of security breach.

As a result of these data security compliance concerns, mortgage lenders should ensure that any electronic loan closing process and system is designed to safeguard and handle customer information appropriately. Since identity theft and security breach risks continue to be a concern among legislators, regulators, and consumers, mortgage lenders should expect more federal and state laws, regulations and guidance in the data privacy and security area.

XV. Title Insurance Coverage for eMortgages

Title insurance typically provides insurance coverage for the validity and enforceability of an insured mortgage as against insured land. In the past, both the note evidencing debt and the mortgage which secures performance of the note by creating a security interest in land were created by hand-made signatures on paper documents. Currently, there is a small, but growing, number of lenders originating mortgage loans in which the note is signed and created electronically while the accompanying mortgage or deed of trust is ink-signed and created on paper. In the future, it is expected that both the note and mortgage may be signed and created electronically. Whether the execution of the note or mortgage occurs with an ink or electronic signature, it is expected that the traditional coverage of the loan policy of title insurance will remain unchanged for real estate transactions in which title insurance is obtained.

The American Land Title Association recognizes the legal and technological advances that support the creation of enforceable electronic mortgage transactions. With this recognition, the Association is anticipating the approval of a new loan policy form by July 1, 2006 that explicitly includes insurance against the invalidity or unenforceability of the lien of the insured mortgage because of "failure to perform those acts necessary to create a document by electronic means authorized by law." It is widely agreed that this coverage will insure against invalidity of the insured mortgage because of failure of the promissory note or mortgage to be created in accordance with applicable electronic transactions laws. Notwithstanding publication of the new loan policy form, the 1992 ALTA Loan Policy provides the same insurance by insuring provision 5, which insures against "The invalidity or unenforceability of the lien of the insured mortgage upon the title."

XVI. Compliance with ESIGN and UETA Document Retention Requirements

A. ESIGN Requirements for Retention

Legal Considerations

Since an electronic closing system will store electronic documents before, during and after the loan closing event, the system would need to be designed in compliance with applicable federal and state document retention requirements. For example, ESIGN generally provides that electronic signatures and records may not be denied legal effect solely because the records are electronic. However, if electronic signatures and records are not stored in an accessible and accurate manner, these records and signatures may be denied legal effect.

This integration of accessibility, accuracy, and validity raises the issue of technology obsolescence. Regular testing, monitoring, and conversion procedures are essential for ESIGN compliance. If consumers are accessing an electronic vault or other electronic document storage repository in conjunction with the ESIGN consent process, any changes to the software or hardware requirements for electronic vault accessibility must be disclosed to the consumer in a particular manner. The hardware or software disclosures must be accompanied by a notice to the consumer about the consumer's ability to withdraw consent to the use of electronic records.

ESIGN permits a federal or state regulatory agency to specify performance standards to assure accuracy, record integrity, and accessibility of electronic records. Therefore, special care should be taken to ensure that any storage system complies with applicable regulatory requirements as. ESIGN also permits a federal or state regulatory agency to require the retention of a record in a tangible printed or paper form. Therefore, consultation with qualified counsel and appropriate regulatory agencies is advisable before developing an electronic vault or other electronic document storage repository.

The legislative history of ESIGN references the Securities and Exchange Commission's (SEC) rule on electronic storage for information purposes. Specifically, the SEC rule requires that the electronic storage media (i) preserve the records exclusively in a non-rewriteable, non-erasable format; (ii) verify automatically the quality and accuracy of the storage media recording process; (iii) serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and (iv) have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable as required. To ensure compliance with the SEC rule, entities must have an audit system in place that provides for accountability regarding the entry of records that must be maintained and preserved by the storage system. All of the procedures in the rule are instructive for structuring an electronic record storage system for the mortgage industry.

B. UETA Requirements for Retention

The concept of retention is incorporated into several provisions in the UETA. UETA's definition of "record" incorporates a retention requirement, stating that a record is information that is stored in an electronic or other medium and is retrievable in perceivable form. In the comments, the UETA drafters note that "[i]nformation that has not been retained other than through human memory does not qualify as a record." Therefore, retention is a key element for compliance with the UETA.

Legal Considerations

UETA provides that retention of electronic records may satisfy existing record retention requirements if such records are accurate and remain accessible for later reference. The requirement of accuracy, in the electronic records context, addresses the issue that some modes of electronic storage may be more prone to data corruption than others. The continuing accessibility requirement addresses the issue of potential technological obsolescence of storage technology. As storage technology becomes obsolete, conversion of the data into new formats is required to maintain compliance with this accessibility requirement.

The scope of information in an electronic record required to be stored under UETA's retention requirements is determined by the purpose for which the information is needed. However, wise record retention would retain as much information as possible in an electronic record since it may not be known at the time the record is placed in storage what information will later be relevant.

C. Compliance with Underlying Statutory and Regulatory Obligations

While ESIGN and UETA provide for the use of electronic records, ESIGN and UETA do not affect the requirement to comply with existing statutory or regulatory document retention requirements. Such requirements may originate under federal or state laws and regulations. For example, UETA provides that a governmental agency of the State may specify additional requirements for the retention of a record subject to the agency's jurisdiction. Electronic records must also be stored in a manner that ensures that these records will later be admissible in federal or state court. Rules on the admissibility of these records into evidence may vary from state to state. Electronic storage systems must also be developed in a manner that complies with security and privacy laws regarding customer information applicable to a particular institution.

XVII. Conclusion

A legal infrastructure exists for developing processes for an electronic loan closing, and in turn, creating valid and enforceable electronic loan obligations. An electronic loan closing must take into account traditional loan closing laws, as well as other laws applicable to any type of electronic commerce transaction. While this summary does not cover every legal topic raised by an electronic loan closing, it provides a preliminary overview for institutions selecting or developing an electronic loan closing process or system.

3.2 eDoc Guidelines

Introduction

An electronic document (eDoc) is intended to provide an equivalent to a paper document without a need for printing. The desire for a paperless environment has been a key driver in the evolution of the eDoc formats from imaging to electronic records. Legislatively, ESIGN and UETA similarly define an electronic record as a record "created, generated, sent, communicated, received, or stored by electronic means." Although electronic records are the legal equivalent of paper records, proving the enforceability of such records may rely on evidence within a particular document and the circumstances surrounding the creation, execution, maintenance, and storage of such document. This Section is a general discussion on how an electronic document format used within an electronic closing system can be designed to create evidentiary support for proving enforceability.

Key Points

The MISMO eMortgage Guidelines and Specifications include electronic document format guidelines that support the industry's evolutionary progress from imaging to electronic records and assist the industry in achieving incremental benefits along the way. The guidelines describe five key document characteristics which are **Securable**, **Manageable**, **Archivable**, **Retrievable**, and **Transferable**, thus creating a SMART™ electronic document. The guidelines also provide guidance on the following document format requirements:

- Information describing the document.
- Visual representation of the document.
- Data embedded in the document.
- Transparent linking of the data and visual representation.
- Electronic signatures in the document.
- Tamper-evident security in the document.
- Audit trail of changes in the document.

General requirements

An electronically signed document should contain all the information necessary to reproduce the entire electronic document and all associated signatures in a form that permits the person viewing or printing the entire electronic document to verify:

- (a) The contents of the electronic document;
- (b) The method used to sign the electronic record, if applicable; and
- (c) The person or persons signing the electronic document.

Since some electronic mortgage documents will need to be retained for the life of the loan plus 7 years, rendering of an electronically signed document should be reliant solely upon a single file containing the necessary components – data, view, mapping, signatures, and any additional files – in a single electronic document file, without requiring external

eDoc Guidelines

files or attachments. Additionally, in order to ensure accuracy of the electronic document during the documents' retention period, subsequent renderings of the document should be consistent, without alterations or changes, in order to preserve the original unique customer experience.

During the closing session, the borrower(s) must have the ability to view the entire document that they will be required to view, acknowledge, and/or sign. If this ability is restricted or limited by the electronic closing system used, a borrower might assert that the electronic closing transaction was conducted unfairly or deceptively, and might bring an action under applicable state law governing unfair and deceptive acts and practices. Certain laws may require that the information be presented in a particular format (i.e., 12-point font, clear and conspicuous requirements, etc.). The closing system must display such documents in any legally-required format.

An electronically signed document should support electronic signatures from multiple parties and all required signatures must be affixed to the document. The supported type(s) of electronic signature(s) must comply with all applicable electronic signature laws and regulations (e.g., E-SIGN and UETA).

To assist in proving attribution of an electronic signature, each signature block on the document should contain the signature symbol of the signer (e.g., handwritten signature, certificate information, etc.) and the date and time of when the signature was applied by the signer. See Section 3.1 for more discussion on Electronic Signatures and Attribution.

To preserve the evidence that a document was signed by a borrower, it may be helpful for the electronic document to contain an audit trail that can capture information on each electronic signing event along with other revisions to the document. Systems storing and managing electronic documents should protect any existing recorded audit trail events from being altered or deleted.

To preserve the integrity of the electronically signed document, an electronic document should be tamper-evident sealed using W3C compliant digital signature algorithms and utilizing X.509 certificates issued by a SISAC-accredited issuing authority. The tamper-evident seal digital signature value must be included in the document and accessible to validate that the electronic document has not been altered after it was electronically signed.

For additional format specific requirements, please refer to the MISMO® eMortgage guidelines and specifications available at www.mismo.org.

References:

1. U.S. Courts - Electronic Case Files
http://www.uscourts.gov/cmecf/cmecf_about.html
<http://pacer.psc.uscourts.gov/cmecf/developer/bkforms/DEfaq.pdf>
2. The Government Paperwork Elimination Act
<http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html>
3. The National Archives - Permanent Electronic Records
<http://www.archives.gov/records-mgmt/initiatives/pdf-records.html>

eDoc Guidelines

4. The United Nations – eDoc Standards
http://www.unece.org/etrades/unedocs/referenceimpl_ac.htm

3.3 eSignature Guidelines

Introduction

An electronic loan closing system and/or process needs to be designed to create valid and enforceable electronic signatures. Regardless of the chosen technology or implementation method, originators, lenders, and title insurers should ensure that a closing system or process produces electronically-signed documents and disclosures in such a way that (1) the signer's intent to sign such documents; (2) the authenticity of the signature; and (3) the integrity of the document are demonstrable in a court of law.

For a general legal discussion on electronic signatures and attribution of such signatures, see Section 3.1. In general, an electronic signature is intended to provide an equivalent to the "wet signature" used to sign paper documents. An electronic signature is broadly defined as an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

Key Points

ESIGN and UETA do not specify what an electronic signature should look like or what technology to use. However, the ESIGN and UETA electronic signature definitions are focused on three signature types: process, symbol, and sound. From a technical point of view, all electronic signatures require some type of "process" in order to result in an electronic symbol or sound that is attached to or logically associated with the electronic record. This remains true regardless of whether the signature is digital, electronically handwritten, "click-through," or results from some other procedure.

In addition, while the authentication of the identity of a signer need not be part of the signature itself, it is important to remember that electronic signatures will usually need to be associated, in some way, with a process that establishes the identity of the signer. An electronic signature method could be designed to include a stronger or weaker authentication process depending upon practical considerations and the nature of the underlying transaction. Digital certificates or user IDs for "click-through", as an example, can be issued with varying levels of data and verification of credentials based on the type and value of the transaction, regulatory requirements, and the company's risk tolerance levels.

This Section of the Guide will provide some common examples of electronic signatures used by the mortgage industry today. This is not intended to suggest that other types of electronic signatures are less effectual or should be avoided. In addition, this Section will provide some issues to be considered in designing and selecting an electronic signature process within an electronic closing system.

Electronic Signature Types

Click-through Signature and Password

Description: Click on an "I agree" button or other similar process resulting in an electronic signature or symbol.

eSignature Guidelines

Depending on the particular document, a click-through signature, by itself, may not be desirable without additional processes. For example, some websites provide a license agreement that requires a user to click-sign an “I agree” button to the terms and conditions before the software can be accessed and/or downloaded. Typically, the website is programmed to store two records: (1) a generic copy of the license agreement and (2) a separate record of the user’s click signature rather than an independent record of a signed license agreement. Since there may be a risk of the two records being disassociated, this type of process may not be sufficient for certain electronic mortgage documents (i.e., an eNote) that are necessary to prove the enforceability of the mortgage transaction and must be retained for the life of the loan plus seven years. For such critical documents, it may be desirable to have all signature information included within the electronic document, rather than having to reference the signature information from an external source. In addition, copies of certain documents required to be provided to the borrower should reflect the documents as they appeared when actually signed by the borrower, preferably with a visual symbol of his or her signature on the electronic document along with the date and time of signature.

As a result, an originator or lender may want to combine a click-through signature method with processes that (1) result in a signature symbol appearing on the electronic document; (2) attribute the signer with his or her signature on the electronic document; and (3) verify a signer’s intent to sign. This may be done through a variety of means. One way to incorporate such authentication and attribution processes into a click-through signature method would be to require the signatory to use a single-use password to access the electronic closing session. This password would be issued to an individual whose identity had been confirmed by other means (i.e., verification of identity by a notary, etc.) via mail or other secure method prior to the signing transaction.. See Section 3.1 for more information regarding the legal issues surrounding verification of identity. If a password is used, it should be accompanied by instructions describing how this password will be used along with the click-through signature process, to effect a person’s electronic signature on the electronic records.

The closing system should be designed to ensure that the password is not accessible to any other party in the closing process in order to prevent misuse. The usage of a password may provide additional evidence to assist in demonstrating the intent of the signer to be bound to the terms and conditions of the electronic document and may provide additional verification that a closing document was signed by a particular individual.

Handwritten Electronic Signature (also known as Digitized Signature):

Description: Recording of a handwritten signature captured from either a signature capture device or a tablet PC.

A digitized signature is represented as an image of a handwritten signature for display within the electronic document with which it is associated. This signature method has the advantage of being intuitive to the average user and is culturally acceptable in an environment that has traditionally used handwritten signatures to memorialize one’s assent to be bound to a written agreement. It also has the benefit of being comparable to

eSignature Guidelines

the handwritten wet ink signature of the signer, thus providing one method, but not necessarily the only method, of associating the signer with his or her signature on the electronic document.

Prior to the execution of a digitized, or handwritten, electronic signature, the signature procedure should be explained to the signer. Handwritten electronic signatures are typically captured using a tablet computer (PC) or a special-purpose computer peripheral.

Digital Signature

Description: The application of cryptography, i.e., using public and private keys, to a document to authenticate and validate the signer's identity, ensure document integrity, and prevent signer repudiation of his or her signature on the document.

Digital signature technology is used in many IT security, e-business and e-commerce transactions conducted today. It is based on public/private key cryptography, and is used in secure messaging, public key infrastructure (PKI), virtual private networks (VPN), web standards for secure transactions, and electronic signatures. These algorithms can be found in the Public Key Cryptography Standards (PKCS) maintained by RSA Security.

When digital signature technology is used to authenticate a particular individual, the individual's public key is digitally signed with the issuer's private key to verify the signer's identity. This process produces a managed digital certificate – the most common format used today is called X.509 V3. See the ITU standard X.509 for technical details of digital certificates.

The entire process of issuing, verifying and managing digital certificates and keys as a secure process is known as PKI. The standards for managing a digital certificate infrastructure are beyond the scope of this document. Please refer to the IETF workgroup X.509 (pkix) for further details on implementing PKI infrastructure.

While the public and private key pairs used in a digital signature are unique and can authenticate data for a very simple process, signing ceremonies are not typically simple. Therefore, developers of electronic closing platforms, if looking to leverage PKI and digital signatures and certificates, should review the guidelines from the American Bar Association to ensure proper implementation of this technology available at http://www.abanet.org/scitech/ec/isc/pagv30d5_d8.pdf.

Some Best Practice Guidelines

Regardless of what type of signature method is used, a company choosing an electronic closing system design may want to ensure that the system allows for an electronic signature to be associated with the specific electronic document or section of the electronic document to which the signature is applied. For example, the system could enable a message box to appear prior to signing that states, "By [description of electronic signature process (i.e., clicking on the "I agree" button)], you are creating an electronic signature that reflects your understanding of the terms and conditions of the XYZ

eSignature Guidelines

document and your agreement to be legally bound by such terms and conditions.” This message should be tailored based on the type of signature process and the signing purpose; consult your legal counsel or compliance officer for further guidance on specific verbiage. See SPeRS for additional guidance in designing an electronic signature process.

An electronic closing platform should also apply a final, official signature (e.g., tamper-evident digital signature) to the document to protect the document from subsequent alterations after all required participant signatures have been captured. In addition, prior to embedding the official signature in the electronic document, it may be desirable that the closing system request a final confirmation of the signer’s intent. This can be done by programmatic means or by requiring a manual review of appropriate content in the document, preferably located immediately above the signing section. See Section 3.5 for more guidance on the use of tamper-evident digital signatures.

Other Considerations

Originators and lenders should evaluate what types of signature processes are appropriate for the particular transactions to be conducted electronically. Regardless of what signature method is used, the key to the enforceability of an electronically signed document is having the related evidentiary support necessary to prove that a signature belongs to a particular person (attribution and signer authentication), that the person intended and was authorized to sign the document (intent and authority), and that the document signed is the same document that was presented to the signer (document authentication). If appropriate, an electronic signature process may be designed to provide such evidentiary support. This Section outlines some issues that an originator, lender or title insurer may want consider in conducting due diligence on the electronic signature functionality in an electronic closing system or process. SPeRS provides more in-depth guidance on all of these topics.

Authentication & Authority

One of the key elements to enforceability of any contract is providing verification of the identity of the signer(s) and a determination that the signer had the legal authority to sign. Identity and authority may be established as part of the signature process, or established separately either before or after the signature is created. As a simple example, consider a notarized signature by an individual – the notary observes the signature being created and associated to a record by the individual (or observes the individual acknowledging the signature after creation), confirms in some accepted manner the individual’s identity, and affirms the authenticity of the individual’s signature.

Providing Information on the Signing Process

Since electronic signatures are a relatively new phenomenon for the typical consumer, it may be prudent to provide an explanation of how the electronic signing process will occur. The explanation should include, at a minimum:

- A description and explanation of the procedure used to create the electronic signature; and
- A description of the sequence of events that will result in the signature becoming final and effective.

eSignature Guidelines

Establishing the Intent to Sign

The process used to create an electronic signature may be designed so that:

- It is clear that the signer intended to create a signature; and
- When not reasonably apparent under the circumstances, the signer is advised that the signature fulfills one or more purposes:
 - Affirms the accuracy of information in the record;
 - Affirms assent or agreement with the information in the record;
 - Affirms the signer's opportunity to become familiar with information in the record;
 - Affirms the source of the information in the record; or
 - Other specified purposes.

Associating an Electronic Signature with a Record

A process for signing records may be designed so that:

- The record is presented for signature before the signature is applied;
- The signature is attached to, embedded or logically associated with, the record presented; and
- The process used to attach, embed or associate the signature ensures that the signature is verifiable.

Attributing a Signature

A process for signing the records may be designed so that either:

- The signature itself provides evidence of the signer's identity:
 - i.e. Handwritten electronic signature, digitized signature or digital certificate text; or
- The process surrounding the creation or affirmation of the signature:
 - Provides evidence of the signer's identity; and
 - Is in some manner preserved or capable of recall or re-creation during the applicable life of the transaction.

Conclusion

Although UETA and E-SIGN provide basic requirements for a valid electronic signature, there may be other business and practical considerations that will help lenders determine which electronic signature process is appropriate for the particular type of electronic closing transaction.

3.4 eNotary Guidelines

Introduction

An electronic loan closing system should be designed to accommodate the participation of a person authorized to perform notarial acts (e.g., state-commissioned notary) during the closing transaction. A closing transaction typically requires one or more documents to be notarized, particularly documents that need to be recorded by a county recorder. The participation of a notary in an electronic closing transaction would assist in detecting attempted fraud or deterring fraud in a loan closing and would establish presumptive evidence of the document signer's intent to authenticate the document by enabling the notary to: (1) attest to the signer's voluntary execution and understanding of the nature of the document; and (2) verify the identity of the document signer.

For additional information, please reference the work of the American Bar Association (ABA) eTrust subcommittee on eNotarization.

Key Documents

In a typical real estate loan closing transaction, the following are commonly notarized documents: deeds, security instruments, affidavits, powers of attorney, assignments, subordination agreements, reconveyances, lien releases, mortgage satisfactions, and identity verifications.

Guiding Principles

More information about the general legal principles concerning electronic signatures and notarizations is discussed in Section 3.1 of this Guide. In addition, the reader should consult applicable state laws, regulations, and official directives for specific information about notary practices and procedures.

In general, the traditional procedures for paper notarizations are the standards for electronic notarizations. Existing legal requirements for paper-based notarial acts, in other words, must be satisfied in the electronic realm as well. These procedures generally include, but are not limited to:

- *Signer appearance:* In all 50 states, the document signer must appear in person before a notary.
- *Signer screening:* A notary verifies a signer's identity, willingness to sign, and basic understanding of the nature of the document being signed (awareness/capacity).
- *Signer declaration:* A notary takes the document signer's acknowledgment (or witnesses the document signer's signature) or sworn oath (or affirmation).
- *Notary certification:* A notary completes and signs the appropriate certificate according to state law.

Electronic Notary Signature Recommendations

In selecting or building an electronic loan closing system, interested parties (e.g., originators, lenders, title insurers, etc.) need to understand how state laws and rules may affect a notary's use of electronic signatures during a loan closing transaction. Generally,

eNotary Guidelines

unless a law or rule directs otherwise, notaries may use any technology to affix or logically associate an electronic signature to notarize a particular document. However, state laws or rules may require that a notary register his or her electronic signature with a notary commissioning official and may prescribe procedures governing its use and security for the purpose of notarial acts. For a general discussion regarding the implementation of electronic signatures, see Section 3.3 of this Guide.

To achieve the basic evidentiary purposes of signatures, a notary's electronic signature should have the following attributes: (1) the name of the notary who signed the document; (2) the notary's commission expiration date; and (3) if applicable, the notary's commission number.

Electronic Notary Seal Information Recommendations

Applicable law or regulation may require or recommend that a notary seal or seal information is attached to or logically associated with an electronic document. Such seal or seal information may be represented as an image or textual information. Closing systems should take into account that this information should be reasonably protected from alterations or misuse.

Electronic Notary Certificate Recommendations

State laws govern the appropriate content of a notary certificate for the various notarial acts. The certificate content may also vary depending on the state where the notarization is occurring. An electronic loan closing system should allow notaries to replace, edit and/or complete the text of the notary certificate for compliance with applicable law.

The Property Records Industry Association (PRIA) has published an XML DTD that defines basic data points generally utilized within notary certificates. Such data points combined with state-specific certificate text provide a "container" for electronic notary certificate data.

Conclusion

An electronic loan closing system must be designed to obtain a valid electronic signature of the notary in accordance with the requirements of ESIGN, UETA, URPERA and state notary laws or regulation.

References:

- American Bar Association (ABA) eTrust subcommittee on eNotarization
<https://www.abanet.org/dch/committee.cfm?com=ST231005&edit=1&CFID=9185943&CFTOKEN=66569594&jsessionid=f030a6a83456131777a5>

Tamper-Evident Seal Guidelines

3.5 Tamper-Evident Seal Guidelines

In order to preserve the integrity of an electronic document, one of the most common and reliable methods used today is the Tamper-Evident Seal (Digital Signature). It is the process of digitally signing a document with a valid certificate such that if a document is modified, the modification can be easily detected. In cases where the certificate references an individual or business entity, these digital signatures also provide proof of the identity of the signing party.

An eMortgage closing platform needs to ensure that:

1. A Tamper-Evident Seal Digital Signature is applied to a document after all other required signatures (electronic or digital) have been collected.
2. The certificate used to implement a Tamper-Evident Seal Digital Signature should be an organizational certificate obtained from a SISAC-accredited certificate issuer.
3. The date and time the signature was applied should be part of the signature.
4. The Tamper-Evident Seal Digital Signature should be part of the electronic document.

Applying a Tamper-Evident Seal Digital Signature to an electronic document consists of three steps. Steps 1 and 2 are performed by the creator/signer of the document. Step 3 is performed by the recipient of the electronic document.

1. Creating a hash value based upon the contents of the document using a mathematical function.
2. Encrypting this value with the private key which is a part of the certificate.
3. Creating a hash value based upon the contents of the document using the same mathematical function used in Step 1 and then comparing this value with the encrypted value after decrypting it using a public key provided by the creator/signer.

Electronic mortgage processes have the potential to be more secure than the paper processes because of mortgage industry standards such as the Tamper-Evident Seal. The seal is also a critical part of the MERS[®] eRegistry processes.

3.6 System Interfaces Guidelines

Introduction

In the paper-based closing environment, documents are sent to the settlement agent in a variety of formats that have evolved over time. Many lenders still ship the physical documents to the settlement agent using a courier, an overnight delivery servicer, or more recently electronically using web based interfaces. For those documents sent electronically, the settlement agent simply opens the document using a standard viewer (usually PDF) and prints them to a local printer. Aside from the minimal requirements of an appropriately configured personal computer and web access, the paper-based closing process imposes little technical expertise on the part of the lender or the settlement agent.

In this early stage of eMortgage adoption, existing electronic closing systems typically deploy proprietary interfaces for both document and data transmission to and from the settlement agent. This requires that the lender and the settlement agent have agreed on the specific technology solution to be used for a specific closing. This is manageable when the volumes of electronic closings between a lender and a settlement agent remain low. However, as volumes grow and as the number of lenders originating eNotes with multiple settlement agents grow, the propriety interface requirements become inefficient and difficult to manage.

It is critical for broad eMortgage adoption that lenders, settlement agents, and ultimately county recorders migrate to a common set of data interchange and document delivery standards such as those MISMO is providing.

To or From the Electronic Closing

Use of MISMO's data standards will enable document preparation vendors, loan origination system providers, electronic closing system platforms and title companies to exchange data before during and after the closing without having to re-key data or maintain multiple proprietary interfaces. As a best practice, the systems that send and receive these business critical messages, should store the messages for back up and recovery and dispute resolution purposes. These standards are being developed through the MISMO eMortgage Closing Interface Transactions (eMCIT) sub group.

MERS[®] eRegistry

This set of data standards was developed using the MISMO request/response message format so that lenders, electronic vaults, investors and servicers can register, transfer and service eNotes on the MERS eRegistry. For detailed information on these standards, visit www.mersinc.org and click on the MERS[®] eRegistry tab.

eDocument Delivery

These standards will reuse and modify the Transfer Request and Response messages and the MISMO Envelope & Packaging Specification currently used by the MERS[®] eRegistry for registration of eNotes and for transfers of Control, Location and Delegatee. For more information on these standards, see the MISMO eMortgage Guide.

System Interfaces Guidelines

eRecording

PRIA's eRecording and state and local eGovernment standards provide XML DTDs for standardized data exchange in the growing electronic recording and electronic notarization business processes. For more information on these standards, visit www.pria.us.

Conclusion

As eMortgage volumes grow and the number of trading partners multiply, standard, non proprietary interfaces for data transmission and eDocument delivery becomes essential for a secure, cost effective and efficient eMortgage infrastructure.

3.7 System Audit Trail Guidelines

Introduction

A closing system audit trail is an integral part of an electronic closing process or system. This type of audit trail is not a replacement for a traditional closing file containing either paper or electronic copies of receipts, disbursements, title policies, settlement statements and other documents that would need to be retained by a closing agent or the title company. Rather, a system audit trail would supplement the traditional closing file by capturing important events that occurred during an electronic loan closing session which may, from an evidentiary standpoint, be useful if the mortgage loan were subject to legal action. See section 3.1 of this Guide for a general legal discussion surrounding the evidentiary importance of an audit trail.

In a paper loan closing scenario, parties rely heavily on documentary evidence (i.e., the closing file, mortgage loan file checklists, closing instructions, written participant dates and signatures, etc.) and on participant recollection to re-create what occurred during a particular paper closing transaction. Participant recollection may not always be reliable especially when there is a large time gap between the loan closing and when participant recollection is required. In an electronic loan closing scenario, a system audit trail should be able provide a more reliable, less subjective record of events than participant recollection alone. This section describes some of the events that an electronic closing system audit trail should capture.

System Audit Trail Information

In general, an audit trail can be designed to answer “who, what, where, and when” types of questions. Information of this type that may be useful to record during an electronic closing includes:

- Uploading of documents to the electronic loan closing system, including date and time of upload.
- User log-in information to the electronic closing system, including date and time.
- Duration of loan closing session.
- Sign-out information, including date and time.
- Which documents in the electronic loan closing system were accessed, including date and time of access.
- How a particular document was handled within the loan closing system, including date and time of action:
 - Viewing;
 - Editing;
 - Initialing and signing;
 - Notarization;
 - Tamper-evident sealing;
 - Transferring document out of closing system; and
 - Time and date information for the above events.
- Who accessed and performed the above document handling events.

System Audit Trail Guidelines

Preserving System Audit Trail Information

The system audit trail is only useful if the information can be accessed and retained by the party who actually needs to rely on this information. Therefore, lenders should consider ways in which they can access this information from the electronic loan closing system particularly in the situation where the system audit trail is controlled by a third-party vendor.

Conclusion

From an evidentiary standpoint, a system audit trail can provide valuable information as to what occurred during an electronic loan closing. Lenders need to keep in mind that audit trail information is only as good as the system that creates it. Before audit trail information can be relied upon, the lender must ensure that the information captured is the information that would be useful if needed and that the information is accessible for as long as a cause of action or claim may be brought with respect to the particular loan closed.

3.8 Electronic Records Storage Guidelines

Introduction

An eMortgage loan closing platform must be able to accept the delivery of electronic documents for execution during loan closing, securely store such documents, and return the documents electronically to the lender or other parties after execution and/or to the county recorder for recordation. This Section will focus on the safekeeping of electronic documents within an electronic loan closing platform using compliant records management policies, processes and procedures.

Guidelines

The eMortgage closing platform should be designed to follow compliant electronic records management policies, processes and procedures. Compliance policies, processes and procedures may be dictated by law, including ESIGN, UETA, federal and state laws and regulations on data security and record retention, and by lender, investor or title company requirements. See Section 3.1 of this Guide for a general legal discussion surrounding data security and record retention. Policies and procedures for secure storage of electronic records within a closing platform should be documented and adhered to during day-to-day operations. Such documentation may be requested by an independent auditor or law firm in the case of a Level 2 eMortgage closing system certification as described in Section 2.3. Such documentation may also be requested by an originator, lender, or title company to assist such parties with their due diligence review of an eMortgage closing platform. The following are general areas of electronic records management that should be part of the documentation:

1. Records declaration
 - a. Records identifiers
 - b. Associated metadata
2. Records capture
 - a. Electronically delivered records
 - b. Electronically signed records
 - c. Imaged records
3. Records organization
 - a. Relationship to a closing transaction
 - b. Relationship to other records
 - c. Versioning of the records
 - d. Status tracking of the records
 - i. Ex: Signed, recorded, other.
 - e. Source of the records
 - i. Ex: Lender, closing agent, title company, borrower, other.
4. Records security
5. Records retrieval
 - a. Search
 - b. Access
 - i. Ex: View, print, copy, other.
6. Records preservation

Electronic Records Storage Guidelines

- a. Integrity of the records
- b. Back up of the records
7. Audit trail
8. Final records disposition
 - a. Destruction of the records
 - b. Transfer of the records

Conclusion

Since an eMortgage closing platform handles and stores electronic records that contain sensitive consumer information, a platform should be designed to ensure the security and proper disposal of such information in accordance with any applicable laws. For companies involved in developing or selecting an eMortgage closing platform, they should develop or obtain documentation of a platform's electronic records management policies and procedures. Such documentation is also a requirement for all eMortgage closing platform certification levels.

References:

- The National Archives – Electronic Records Guidance
<http://www.archives.gov/records-mgmt/policy/prod6b.html>

3.9 Security Guidelines

Introduction

An eMortgage closing system is a component of the overall mortgage process, and like all other components, it is required to comply with similar security policies, procedures, and controls applied to other components of the mortgage process. For example, the Gramm-Leach-Bliley Act (“GLB”) requires the Financial Regulatory Agencies (“the Agencies”) – including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, the Securities and Exchange Commission, the Commodity Futures Trading Commission and the Federal Trade Commission - to establish standards, relating to safeguards, for the financial institutions subject to their jurisdiction. The safeguards are to ensure the security and confidentiality of customer records and information, and to protect against any anticipated threats or hazards to the security or integrity of those records. The safeguards are also to protect against unauthorized access to, or use of the records or information, that could result in harm to the customer. The Agencies have issued guidelines that establish standards for safeguarding customer information and are authorized to enforce these guidelines with respect to the financial institutions that fall under their jurisdiction.

Steps Your Organization Can Take

Organizations should take steps to protect their electronic closing environment. The biggest step your organization can take is acknowledging that data (both physical and logical) can be a critical asset, and that it needs to be managed and secured like any other critical asset within your organization. Next, every organization needs to understand that a solution for securing sensitive information (i.e., critical information assets) is not solely a technical solution, but one that involves people and processes as well. The MISMO Information Security Work Group (ISWG) has been promoting a general five-step security method in all of its security activities. This same five-step method, which is consistent with ISO 17799, can be used by any mortgage institution to identify, assess and safeguard information. This method is also useful in performing activities required to comply with industry regulations such as the Federal Trade Commission (FTC) Safeguards Rule as well as the various State legislations addressing notification requirements for security breaches involving disclosure of personal information.

In summary, this method involves:

- *Business and Risk Description* – Simply stated, the risk is not protecting sensitive information and the ramifications for not protecting that information are legislative and regulatory compliance. Business descriptions are use cases specific to your organization where sensitive information is handled. The ISWG has generally described these use cases as collecting, processing, transferring, storing and disposing sensitive information. Mortgage companies should use these general use cases to identify in more detail the use cases that are specific to their environment, where environment is defined as the physical environment (e.g.,

Security Guidelines

buildings, offices), the logical environment (e.g., networks), and the legal environment (e.g., security breach notification laws, consumer protection laws, required security audits). The result of this activity is a detailed understanding of where sensitive information exists and how it should be handled accordingly within your company.

- *Policy and Architecture* – This is the foundation for protecting sensitive information within your organization. The policy defines the high level requirements for securely managing information and in the case where a breach occurs, for providing incident response notification. The architecture is the framework for implementing specific technical and procedural solutions in support of your company’s policy (e.g., segregation of responsibilities and infrastructure, interconnectivity).
- *People, Processes and Technology* – These are the detailed specifications for your organization to comply with your policy and to be implemented in accordance with your architecture. People need to be informed and trained on requirements for handling sensitive information; processes need to be put in place to ensure every individual and computer operates correctly with respect to the handling of sensitive information; and technology needs to be selected and implemented that provides the appropriate level of security (e.g., encryption, access control, auditing, intrusion detection, anti-virus, regulatory compliance).
- *Support Plan* – Information theft and the monitoring and notification of security breaches is an evolving landscape. Your organization should identify individuals who have a responsibility to keep up with this changing landscape (e.g., new laws, new information theft tactics, new security technologies and best practices). By keeping up with the changing landscape, your organization can adapt quickly and implement new solutions (or enhance existing solutions) for protecting your critical information assets. Business Continuity Plan/Disaster Recovery (BCP/DR), and maintenance plans (including change control) are elements of a Support Plan.
- *Education* – Education and awareness may be the single most important program your organization performs regarding the protection of sensitive information. The more your management, employees, contractors, etc. understand the importance for protecting sensitive information and the reputation benefits that can be gained by being an advocator of protected sensitive information, the more successful your organization will be in implementing information security solutions.

If your company needs consultation services, there are many organizations (large and small) that can assist your company through the 5-step method above. Companies with expertise in or offering ISO 17799 compliance services are good candidates. It is highly recommended that you clearly define your initiative as protecting sensitive information and you should ensure that any consultants you hire are able to tailor their services appropriately.

Security Guidelines

Top 10 Electronic Closing Considerations

1. *If you don't have an information security program for your eMortgage Closing system, then one should be established.* If you have an existing program, then review and update the policies and procedures where appropriate to ensure they are adequately addressing the protection of your eMortgage Closing information assets. Information Technology (IT) personnel, Business Analysts, and Closing Agents, should all be involved in the review process. In addition, your human resources personnel may handle eMortgage Closing information as they perform their job functions, and the scope of those actions should be known to those reviewing your information security program. Finally, engage your Senior Management, as their involvement indicates high-level support for your information security program, which is critical to its success.
2. *Review the regulatory environment.* Regardless of whether you are regulated by the FTC, financial agencies (FRB, FDIC, etc.), SEC or some other body, there is an abundance of documentation available. Consult with your regulators, attorneys and auditors for compliance recommendations.
3. *Define sensitive information within your eMortgage Closing system.* Not all of the information processed is sensitive, either to your organization, your partner organizations, or to the individuals involved in the eMortgage process. Identify the sensitive data and the systems that process those information assets. A comprehensive understanding of the data, systems where the data traverses across, people and processes will enable your organization to establish appropriate security controls.
4. *Once sensitive information has been identified, assess the risk associated with an unauthorized disclosure of that information by exploring the likelihood and severity of unauthorized disclosure.* A risk assessment includes the examination of threats and vulnerabilities that could lead to the compromise of sensitive data.
5. *The primary concern of legislation and regulatory requirements is unauthorized access to sensitive or personal information.* Hence, access controls (e.g. user IDs, passwords, etc.) are critical aspects of a security program. Authentication procedures, privileges, and monitoring of users and systems (both production and test) are mandated requirements. Your organization should determine its authentication and access control requirements upon careful examination of your information assets and the risks associated with those information assets.
6. *Test, retest, and assess your eMortgage Closing system, as the environment surrounding your eMortgage Closing system is a dynamic one (e.g., changing regulatory requirements, technology requirements).* Good test plans include penetration testing as well as examining results when outages occur within certain critical components. For example, is the environment sufficiently layered to handle a situation when the firewall may fail? Organizations should also continuously perform maintenance (software patches, etc.) and monitor their

Security Guidelines

systems for security related events.

7. *Develop and maintain a security incident response plan.* Murphy's Law predicts that anything that can go wrong, will. It is recommended that the plan should minimally include monitoring, impact assessment, internal and external notification procedures, and a follow-up assessment.
8. *Understand the relationships with your business partners and third party service providers.* Any sensitive information collected, processed, stored, transferred, or disposed may legally be your responsibility. Verify that the minimum standards (policies and procedures) your organization places on information security are also mirrored by your partners. This may involve a contractual mechanism and assurance of a third party audit (e.g., SAS 70, ISO 17799 compliance).
9. *Encrypt sensitive data when appropriate.* If sensitive information is being transferred or stored, the data should be encrypted.
10. *Establish a comprehensive awareness program for all employees.* Even with all the appropriate technology in place, it often comes down to an individual employee to safeguard the sensitive information. As with system maintenance, education of information security is a never-ending activity. Roles, procedures, and resources change over time, and therefore organizations should schedule training at least annually.

Conclusion

Strong security is crucial to the operations of the electronic mortgage closing systems. Business partners are requiring third party assertion of regulatory compliance. Organizations will benefit from a SAS 70 or Trust Services audit or certification. There are a number of open sources that can be leveraged to aid in the establishment of a security program. Two such examples are the MISMO ISWG white paper on Identifying and Safeguarding Personal Information, which can be found at <http://www.mismo.org> and the MBA Board of Directors Technology Steering Committee white paper on Protecting Personal Information, which can be found at <http://www.mortgagebankers.org>.

4 Appendix

4.1 Reference Links

MBA	Mortgage Bankers Association www.mortgagebankers.org
MISMO	Mortgage Industry Standards Maintenance Organization www.mismo.org
MERS	Mortgage Electronic Registration System Inc. www.mersinc.org
PRIA	Property Records Industry Association. www.pria.us
SISAC	Secure Identity Services Accreditation Corporation. www.sisac.org
SPERS	Standards and Procedures for Electronic Records and Signatures. www.spers.org
NNA	National Notary Association www.nationalnotary.org
USNA	United States Notary Association www.enotary.org

Appendix - Glossary

4.2 Glossary

Authentication	A process of identifying an individual, either in connection with the creation of a relationship or in connection with the individual's participation in a transaction.
Authoritative Copy (AC)	The unique controlling reference copy of the Transferable Record (eNote), which is registered on the MERS eRegistry.
Certificate	A computer-based record or electronic file that, at least, states name or identifies the issuing Certificate, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the Issuing Authority.
Control	A Person has control of a Transferable Record if a system employed for evidencing the transfer of interests in the Transferable Record reliably establishes that Person as the Person to which the Transferable Record was issued or transferred pursuant to Section 16 of UETA and Section 201 of ESIGN. For example, Control can be thought of as having possession of an original paper note.
Controller	The Person named on the MERS eRegistry that has Control of the eNote and its Authoritative Copy. For example, the Controller can be thought of as the "holder," "holder in due course," and/or "purchaser" of an original paper note as defined under the Uniform Commercial Code.
Delegatee	A member of the MERS eRegistry that is authorized by the Controller to perform certain MERS eRegistry transactions on the Controller's behalf.
Digital Certificate	A public key (or digital) certificate is a certificate that uses a digital signature to bind together a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual or an organization.
Digital Signature	A cryptographic method of authenticating the identity of the sender of a message or the signer of a document that can also be used to ensure that the original content of the message or document has not been changed. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message was received means that the sender cannot easily repudiate it later.
Digitized signature	A handwritten signature that is converted upon execution into an electronic form. This is usually performed with a pen and a graphics drawing tablet used for sketching new images or tracing old ones. The user makes contact with the tablet with a pen or puck (mistakenly called a mouse) that is either wireless or connected to the tablet by a wire. For sketching, the user draws with the pen or puck and the screen cursor "draws" a corresponding image. This technology alone will not encrypt a document once signed.
DTD	Document Type Definition. A file that defines the "markup language" that will be used to describe the data. It defines and names the elements that can be used in the document, the order in which the elements can appear, the element attributes that can be used, and other document features.

Appendix - Glossary

Electronic Record	A record created, generated, sent, communicated, received, or stored by electronic means.
Electronic Signature	An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
eClosing	The act of closing a mortgage loan electronically. This occurs through a secure electronic environment where all closing docs are accessed and executed via the web. This is also known as the “execution” phase of creating an electronic mortgage loan.
eMortgage	A mortgage where the critical loan documentation – specifically the promissory note, assignments and security instrument, are created electronically, executed electronically, transferred electronically and ultimately stored electronically. AKA – the paperless mortgage.
eNote	A Transferable Record as defined by ESIGN or UETA, whichever is applicable.
eRecording	An act of registering the security instrument and other recordable documents electronically with the county recorder or similar jurisdictional authority”.
eSecurity Instrument	An electronic security instrument such as a mortgage or deed of trust evidencing the pledge of real estate as collateral for the loan
Electronic Vault	An Electronic Vault is a transferable records management solution that meets ESIGN, UETA, and other compliance requirements. The concept is similar to a paper vault run by the document custodian industry today. Because there will be multiple Electronic Vaults, there is a need for national registry service (MERS [®] eRegistry) to manage the authoritativeness of records. In addition to the transferable records, the solution may support other types of eDocuments.
GSE	Government sponsored enterprise: Private organizations with government charters and backing. Examples are Freddie Mac and Fannie Mae.
HUD-1	Uniform settlement statement. Same as a closing statement.
Hybrid Transaction	A transaction in which the documents associated with the transaction are a combination of electronic records and paper-based documents.
Location (as it pertains to Transfer of Location)	The Person named on the MERS eRegistry that maintains the Authoritative Copy of the eNote either as Controller or as a custodian on behalf of the Controller.
LOS	Loan origination system.
MERS	Mortgage Electronic Registration Systems, Inc.
MERS[®] eRegistry	The MERS [®] eRegistry serves as the System of Record to identify the current Controller and Location of the Authoritative Copy of an eNote.

Appendix - Glossary

MIN	MERS Mortgage Identification Number. The MIN is an 18-digit number composed of a seven digit Organization ID, 10-digit sequence number, and check digit.
MISMO	Mortgage Industry Standards Maintenance Organization. The Mortgage Bankers Association (MBA) created the Organization in October 1999. The Mortgage Industry Standards Maintenance Organization's mission is to develop, promote, and maintain voluntary electronic commerce standards for the mortgage industry.
MOM	MERS as the Original Mortgagee. Language written into security instruments that establishes MERS as the Original Mortgagee and nominee for the Lender, its successors and assigns.
Person	An individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.
PKI	Public Key Infrastructure. A system that provides the basis for establishing and maintaining a trustworthy networking environment through the generation and distribution of keys and certificates. This is also the foundation technology for providing enhanced Internet security.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection
SISAC	Secure Identity Services Accreditation Corporation. SISAC is responsible for accrediting digital identity credential issuers for the mortgage industry. SISAC is owned by the MBA.
SMART™ Document	An electronic document created to conform to a specification standardized by MISMO. A SMART Document locks together data and presentation in such a way that it can be system-validated to guarantee the integrity of the document.
System of Record	Authoritative System recognized to establish ownership and location of the Authoritative Copy of the eNote.
Tamper-evident seal	A "seal" wrapping an electronic document that is created by a digital signature. The seal can be verified to ensure that no changes have been made to the document since the seal was put in place.
Transferable Record	An Electronic Record under ESIGN and UETA that (1) would be a note under the Uniform Commercial Code if the Electronic Record were in writing; (2) the issuer of the Electronic Record expressly has agreed is a Transferable Record; and (3) for purposes of ESIGN, relates to a loan secured by real property. A Transferable Record is also referred to as an eNote.
UCC	Uniform Commercial Code.
UTC	Universal Time Coordinated. UTC is also referred to as GMT (Greenwich Mean Time) and is the global standard for time. All dates used by the MERS eRegistry will use UTC format.

Appendix - Glossary

W3C	World Wide Web Consortium. The World Wide Web Consortium was created to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability.
X509	A standard for defining a Digital Certificate. It is the signing system used for SSL.
XHTML	Extensible Hypertext Markup Language. A family of current and future document types and modules that reproduce, subset, and extend HTML 4. XHTML family document types are XML based, and ultimately are designed to work in conjunction with XML-based user agents.
XML	Extensible Markup Language. XML is a markup language designed specifically for delivering information over the World Wide Web. In creating an XML document, the user creates and assigns the element names.

Index

4.3 Index

A	E	S
Authentication, 53	eMortgage, 54	SISAC, 55
Authoritative Copy, 53	eVault, 54	System of Record, 55
C	G	T
Click-through signature, 34	GSE, 54	Tamper-evident seal, 55
Control, 53		Transferable Record, 55
Controller, 53	M	U
D	MERS® eRegistry, 54	UCC, 55
Delegatee, 53	MIN, 55	X
Digital Certificate, 53	MISMO, 55	XHTML, 56
Digital signature, 36	P	XML, 56
Digital Signature, 53	Person, 55	
Digitized signature, 35, 53	PKI, 55	
DTD, 53		

MISMO eMortgage Closing Guide

For notes and comments