

MISMO eMortgage Workgroup eVault Implementation Guide

Version 2.0

October 24, 2005



Copyright MISMO, 2005

eVault Implementation Guide

Revision History

Date	Version	Description	Author
1/23/05	1.0 Draft	Initial Release	Various
3/30/05	1.0 Final	Initial Release	Various
10/24/05	2.0 Final	IPR Release	Various

Table of Contents

CHAPTER 1: INTRODUCTION.....	5
1.1 PURPOSE.....	5
1.2 BACKGROUND	5
1.3 CRITICAL TERMS	7
CHAPTER 2: EXISTING LAW & LEGISLATIVE OVERVIEW	9
2.1 EXECUTIVE SUMMARY	9
2.2 COMPLIANCE WITH ESIGN AND UETA REQUIREMENTS	9
2.2.1 ESIGN.....	9
2.2.2 UETA.....	10
2.3 COMPLIANCE WITH UNDERLYING STATUTORY AND REGULATORY OBLIGATIONS	10
CHAPTER 3: GOVERNMENT SPONSORED ENTERPRISES (GSE) REQUIREMENTS.....	11
3.1 FREDDIE MAC	11
3.2 FANNIE MAE	11
3.3 GINNIE MAE	11
3.4 SUMMARY	12
CHAPTER 4: PRACTICAL CONSIDERATIONS.....	13
4.1 VALUE PROPOSITION FOR MORTGAGE PROCESSES INVOLVED WITH eVAULTS	13
4.1.1 Assumptions and Clarifications	13
4.1.2 Process Impacts that an eVault might bring to a given practice	15
4.1.3 Value Propositions.....	16
4.2 eVAULT IMPLEMENTATION SCENARIOS	19
4.2.1 ASP Scenarios.....	19
4.2.2 Non-ASP Scenarios	20
CHAPTER 5: GUIDELINES FOR eVAULT INTERFACES.....	32
5.1 eVAULT TRANSACTIONS LIST	32
5.1.1 eVault Transfer & Notification Interfaces	32
5.1.2 eVault Document Interfaces.....	33
5.1.3 MERS® eRegistry Interfaces.....	35
5.2 eVAULT TRANSACTION MODEL EXAMPLE	37
CHAPTER 6: SUGGESTED APPLICATION REQUIREMENTS.....	40
6.1 ACCESSIBILITY OF RECORDS	40
6.2 ABILITY TO HANDLE TRANSFERABLE RECORD REQUIREMENTS	41
6.3 ABILITY TO VERIFY DOCUMENT INTEGRITY	42
6.4 ABILITY TO VERIFY AND AUTHENTICATE CERTIFICATES(S).....	44
6.5 DIVISION OF ROLES WITHIN APPLICATION.....	45
6.6 FULL AUDITING CAPABILITIES	45
6.7 ABILITY TO INTERFACE WITH MERS® eREGISTRY	45
GLOSSARY OF TERMS	46
APPENDIX A.....	54
ESIGN AND UETA PROVISIONS AFFECTING ELECTRONIC RECORD RETENTION	54
ESIGN.....	54

eVault Implementation Guide

<i>UETA</i>	60
FEDERAL RESERVE BOARD (FRB)	62
FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)	62
OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)	62
OFFICE OF THRIFT SUPERVISION (OTS)	63
FREDDIE MAC PRELIMINARY SPECIFICATION ON ELECTRONIC MORTGAGE LOAN DOCUMENTATION.....	64
STANDARDS AND PROCEDURES FOR ELECTRONIC RECORDS AND SIGNATURES (SPERS).....	64
APPLICATION OF ESIGN TO EXISTING ACTS AND REGULATIONS.....	65
APPENDIX B	66
FREQUENTLY ASKED QUESTIONS (FAQ)	66

Chapter 1: Introduction

On August 11, 2005, the MBA announced it was endorsing eMortgages for its membership, and its commitment to help members “stay ahead of the curve” regarding eMortgages. Long before the announcement, however, the MBA had been leading the effort to bring together the necessary industry participants to help provide guidance and foresight on implementing the eMortgage and all its components. One of these components is eVaults.

1.1 Purpose

The purpose of this document is to provide information and guidance for evaluating, implementing, and relying on eVaults for storing electronic documents, and in particular, the eNote. The term “eVault” is typically used in the mortgage industry today to identify a system where electronic documents are stored for safekeeping. However, to date, there has been no comprehensive and authoritative source that defines requirements and responsibilities for implementing and operating an eVault on the behalf of lenders, warehouse lenders, or investors.

This is not intended to be a visionary document, but rather one that can be put to immediate use to provide guidance on finding answers to the most commonly asked questions for people interested in the requirements for storing electronic promissory notes (eNotes). The initial focus is on the eNote because the investor community has contributed considerable resources within the Mortgage Bankers Association’s Mortgage Industry Standards Maintenance Organization (MISMO) to develop a standard uniform eNote. The processing of an eNote is also less dependent on the cooperation of third parties since it is not recorded in the county land records.

The transition from paper to a completely electronic mortgage process incorporating industry standards for security instruments and other closing documents will no doubt take many years. During the transition period, custodians will be required to handle paper documents as well as electronic ones. As the eMortgage environment develops and matures, this document will be revised to reflect changes in law, technology, investor requirements and industry practices.

Since this document is produced under the auspices of MISMO, it does not define requirements for eVaults because MISMO has no authority to publish requirements on behalf of investors. After developing your requirements from a review of all available information sources, you should review your requirements with your investors to confirm that they are appropriate and comply with each investor’s requirements for delivering and storing eNotes. This document also does not address fraud concerns associated with eNotes. Please refer to the work of the MISMO Fraud Prevention Workgroup for more information on this important topic.

Note: Many key terms such as eMortgage, eVault, Authoritative Copy, and more are explained in a Glossary at the end of this document for your convenience.

1.2 Background

During the evolution of the secondary mortgage market, most investors transitioned from requiring physical delivery of the promissory note for loans they purchased or securitized to allowing mortgage lenders (seller/servicers and issuers) to maintain the promissory notes in approved custodial facilities. These facilities could exist internal to the operations of the mortgage lender (e.g. a trust department), or the lender could contract with a third party facility to hold the notes in custody for the investor.

The current role of the Document Custodian emerged from this evolution, and Fannie Mae, Freddie Mac, Ginnie Mae and the Federal Home Loan Banks have all published their respective requirements for how approved Document Custodians must operate. Consistent with all these investor requirements, the Document Custodian is contractually an agent of the mortgage lender, not the investor. Therefore, the onus is on the mortgage lender, not the investor, to ensure that their custodial solutions meet investor's requirements.

Although there are differences in secondary market investor requirements for document custodians, they all describe the following basic responsibilities:

- Physical safekeeping – Storage of documents in a secure and fire-resistant facility. This includes policies and procedures to prevent unauthorized access to documents and to maintain control over all documents received.
- Custodial control over the documents – A document tracking system to maintain ownership records and to maintain the status of all notes in a specific pool.
- Certification of information on documents and data submitted to provide assurance for the investor that the custodian possesses the signed original note and all other documents required by that investor.

In addition to these responsibilities, investors typically require that the Document Custodian meet the following eligibility requirements:

- Be a financial institution subject to supervision of the appropriate regulator (FDIC, OCC, OTS, NCUA, etc.)
- Be in good standing with its regulator
- Maintain an acceptable rating with the Rating Agencies (Fitch, Moody's, S&P, etc.)
- Comply with the investors' published requirements for document custodians
- Maintain adequate insurance
- Establish, test, and maintain a disaster recovery plan and procedures
- Establish and maintain quality assurance procedures
- Employ knowledgeable personnel

Note: For more information on the role of the Document Custodian, please see the MBA's Document Custody Conference Beginner's Workshop Manual from which this summary is quoted.

Some of today's challenges for those analyzing the business impact of storing eNotes on behalf of investors are:

- What documentation exists that provides guidance on the legal basis for storing eNotes and other electronic mortgage documents?
- What additional custody requirements have been developed by secondary market investors that purchase eNotes?
- What are some of the practical implications of holding eNotes? For instance, how do you

certify a mixed pool of paper notes and eNotes?

- How do I determine what the technical requirements should be for storing and transferring eNotes to other eVaults and for communicating with the MERS® eRegistry?

The subsequent chapters of this document are intended to help guide you through the publicly available information needed to develop well-informed answers to these questions.

1.3 Critical Terms

The enabling law and the use of new technologies in the world of electronic documents have introduced a jumble of new terms. In addition to the Glossary in this document, listed below are key terms used to describe eNotes and their paper-based equivalents.

Paper World	Electronic World
Negotiable Instrument	Transferable Record (“eNote”): An Electronic Record under E-SIGN 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 E-SIGN, relates to a loan secured by real property. A Transferable Record is also referred to as an eNote.
Possession	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 E-Sign. For example, Control can be though or as having possession of an original paper note.
Original Note	Authoritative Copy of eNote: The unique controlling reference copy of a Transferable Record (eNote), which is registered on the MERS® eRegistry
Investor/Holder	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.
Custodian	Location (eVault): 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
Endorsement and Delivery	Transfer of Control: A MERS® eRegistry transaction used to change the Controller of the eNote

eVault Implementation Guide

Holder in Due Course	Transferable Record Audit trail: The history of transactions on the MERS® eRegistry for a registered eNote
Servicer	Controller's Delegatee: A member of the MERS® eRegistry that is authorized by the Controller to perform certain MERS® eRegistry transactions on the Controller's behalf
"Wet Signature"	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.
Attachment of Physical Signature	Logically Associated Signature referenced in the eNote registration record

In addition, the following terms are unique to the electronic world so have no paper world equivalent:

Electronic Record means a record created, used or stored in a medium other than paper. Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. The term Record is intended to embrace all means of communicating or storing information except human memory.

eNote Clause or **eNote Language** means additional terms in the text of the eNote to comply with ESIGN and UETA requirements.

eNote Registration means the process of creating the initial record in the MERS® eRegistry for tracking the controller of the eNote.

As you read and apply the information in this guide, it will help to note that there is no single "best" implementation of an eVault. Chapter 4 provides examples of various implementations to show that eVault components can be provided by a variety of sources. The best implementation for you may or may not be included here.

You are encouraged to read this document in conjunction with the MISMO eMortgage Guide, which will give you an overall framework of which eVaults is a part.

Other useful documents are the MISMO eMortgage Workgroup "Lost or Destroyed Data Issues Analysis" and agency-published documents on the topic.

Finally, MISMO thanks all members of the MISMO eVaulting workgroup for their time and contributions to this document.

Chapter 2: Existing Law & Legislative Overview

2.1 Executive Summary

This Overview is designed as a starting point to assist mortgage industry participants in discussions with counsel and developers on the legal requirements for storage of electronic loan documents in residential loan transactions. All information provided in this document is for informational purposes only. **The information is provided “as-is,” and all warranties, express or implied, are disclaimed.** The information provided may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. This document should not be considered legal advice generally or on any specific facts or circumstances.

2.2 COMPLIANCE WITH ESIGN AND UETA REQUIREMENTS

2.2.1 ESIGN

The storage of electronic documents integrates with ESIGN in the context of ESIGN's grant of validity for electronic signatures and records. 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 the eVault in conjunction with the ESIGN consent process, any changes in the software or hardware requirements for accessibility are required to be disclosed to the consumer in a particular manner. These hardware or software disclosures must be accompanied by a disclosure to the consumer about the ability of the consumer to withdraw consent to the use of electronic records.

Please note that 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 existing regulatory requirements as to the accuracy and integrity of electronic records. 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 beginning an eVaulting project.

A Securities and Exchange Commission (SEC) rule on electronic storage is referenced in the legislative history of ESIGN. This rule is cited only for informational purposes because the SEC rule illustrates standards on electronic storage from another industry. The SEC rule sets out the standards for electronic storage and requires notice and collaboration with the SEC to ensure the accuracy of the stored records. Specifically, the 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.

2.2.2 UETA

The concept of retention is incorporated into several provisions in the UETA. The UETA definition of “record” incorporates a retention requirement defining a record as information that is stored in an electronic or other medium and is retrievable in perceivable form. In the comment to the definition section of the UETA, the 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.

The UETA provides that electronic records may satisfy existing record retention requirements if the electronic records are accurate and remain accessible for later reference. In the context of electronic records under the UETA, accuracy refers to data corruption and the potential that some modes of electronic storage are more susceptible to corruption than others. The continuing accessibility requirement refers to the potential 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.

UETA permits parties to convert original written records to electronic records for retention so long as the requirements of accuracy and continuing accessibility are satisfied. This provision may be applicable in a hybrid environment where scanned images of paper loan documents are stored.

The scope of information required to be stored under UETA’s retention requirements is determined by the purpose for which the information is needed. (i.e., If the addressing and pathway information regarding an eMail is relevant, then that information should also be retained. However, if it is the substance of the eMail that is relevant, only that information need be retained. Of course, wise record retention would include all such information since what information will be relevant at a later time will not be known.)

The UETA also provides that a governmental agency of the State may specify additional requirements for the retention of a record subject to the agency’s jurisdiction.

2.3 Compliance with Underlying Statutory and Regulatory Obligations

While ESIGN and the UETA provide for the use of electronic records, ESIGN and the UETA do not alter existing document retention or disclosure requirements. Therefore, electronic storage systems must comply with existing statutory or regulatory document retention requirements. In the mortgage industry, these requirements may originate under federal or state laws and regulations.

Electronic records must also be stored in a manner that ensures that these records will later be admissible in federal or state court. Standards on the admissibility of these records may vary from state to state. More complete data, the simpler manipulation of data, more routine processing, and more verifiable results are beneficial for building the case for admission.

The storage of electronic records also raises the issues of security and privacy. Electronic storage systems will need to integrate with the existing security and privacy requirements that apply to a particular institution.

See Appendix A for a list of relevant statutory and regulatory obligations.

Chapter 3: Government Sponsored Enterprises (GSE) Requirements

The objective of this section is to document, at this early stage of development of the eNote infrastructure, what is known about GSE custody requirements for eNotes. As more information becomes available, this section will be revised to refer the reader directly to publicly available documents of the corresponding GSE. It should also be noted that a specific investor's delivery requirements may be negotiated on a seller by seller basis. The reader should contact their investors directly for additional information that may not be included in these public documents.

Although Ginnie Mae and the Federal Home Loan Banks have participated in industry discussions about eMortgages, to date, only Fannie Mae and Freddie Mac have publicly published information related to originating and delivering eNotes.

3.1 Freddie Mac

In June 2001, Freddie Mac published its "Preliminary Specifications for Electronic Mortgage Loan Documentation." In general, the document includes Freddie Mac's commentary on the enabling legislation for eNotes (E-SIGN and UETA) and then defines specifications for creating, signing, delivering and storing eNotes that are sold to Freddie Mac.

Freddie Mac is currently developing a complete eMortgage Specifications and Requirements Handbook that will set forth its requirements and guidance for Sellers/Service providers that wish to create or manage mortgage loans using Electronic Records and Electronic Signatures and sell such mortgages to Freddie Mac. This effort is targeted to be complete by the end of 2005.

For additional information about Freddie Mac's Preliminary Specifications for Electronic Mortgage Loan Documentation, go to <http://www.freddiemac.com/singlefamily/elm/elmqa.html>

3.2 Fannie Mae

Fannie Mae is working with its document custodians to design processes for certification and storage of electronic documents. Their current requirements for eMortgages are available in their *Guide to Delivering eMortgages to Fannie Mae 2.0* available at <http://www.efanniemae.com>. Fannie Mae is continuing to work with this important segment of the industry to refine eMortgage processes and will update our guides as standards evolve.

3.3 Ginnie Mae

Ginnie Mae is dedicated to the development of basic standards for eMortgages and has committed to work, in conjunction with MISMO, on the technology that will revolutionize the mortgage industry. Ginnie Mae is still in the process of defining its specific requirements for eMortgages, however, some general requirements have been established.

For eMortgages securitized in Ginnie Mae pools, Ginnie Mae will require that the eNote be registered with a third party registry (for example, the MERS[®] eRegistry) that meets the technical requirements established in the original text of Uniform Electronic Transactions Act of 1999 (UETA). Ginnie Mae will be the Controller of the eNote and the Issuer will be its Delegatee so as to enable the Issuer to perform required loan administration activities. The Ginnie Mae document eCustodian will be shown in the eRegistry as the Location of the eNote, therefore the document custodian will be required to maintain an acceptable eVault. More detailed eligibility

requirements for eMortgages and eVaults are still being developed.

3.4 Summary

In addition to evaluating publicly published requirements for storing eNotes on behalf of investors, you should contact your investors directly for additional requirements that may not be available to the general public. Given the current immature state of the eMortgage infrastructure, it is likely that investor requirements will continue to evolve as they gain more experience with purchasing eNotes. If your investor has not yet integrated its eMortgage delivery systems with the MERS[®] eRegistry, you should ask them if that is their intent and when you might expect them to be ready. The business process and technical requirements for delivering eNotes to an investor's proprietary registry will change when that investor integrates with the MERS[®] eRegistry.

Finally, in lieu of any instructions to the contrary, you should expect that the provider of eVaulting services is subject to the same requirements that Ginnie Mae, Fannie Mae, Freddie Mac and other investors have stipulated for the holding of paper notes.

Chapter 4: Practical Considerations

Once we possess a clearer understanding of the strategic importance of eVaults in the eMortgage process, our thoughts naturally turn from the strategic and the technical to the tactical and operational. That transition from ideas to implementation evokes questions and/or concerns relative to the potential impact eVaulting represents to the various constituents in the mortgage industry. Simply stated, "How does this affect me and my company?" This section, Practical Considerations, seeks to provide direction in obtaining answers to that query.

In studying this section, you should understand that the information contained herein is not intended to provide the final or all-encompassing response. Every entity, whether a lender, service provider, or partner, should use these examples as guidelines for practice, and subsequently tailor any solution to the particular and unique needs of its situation. In arriving at the appropriate, solution, you will solicit input from investors, legal resources, technology providers, and business partners alike. Also, as the state of the industry is rapidly evolving with respect to technology, regulatory environment, and rate of adoption, it is vital to note that implementation considerations must evolve as the eMortgage process matures.

4.1 Value Proposition for Mortgage Processes Involved with eVaults

4.1.1 Assumptions and Clarifications

The purpose of this chapter is to provide a framework for considering the Value Proposition that an eVault will have on business operations. Every business scenario is unique, and impacts will vary based on the size of the institution, integration methodologies and operations. Accordingly, this is *not* intended to be an ROI (Return on Investment) study but rather a working tool that can be a starting point for further analysis. For ROI information, see the "eClosing ROI White Paper" published by MBA.

Hybrid Mortgage vs. Hybrid Operations

- Hybrid Mortgage refers to a single mortgage that is documented via both paper documents and electronic documents (eRecords).
- Hybrid Operation refers to an operation (e.g. Document Custodian) that manages both paper documents and electronic documents, thereby being qualified for (1) Paper mortgages, (2) e- Mortgages (fully electronic) and (3) Hybrid Mortgages.
- Hybrid Pool refers to a pool that has a combination of paper mortgages, electronic mortgages, or hybrid mortgages.

Possible Criteria for a practice to be a candidate for eVault benefit

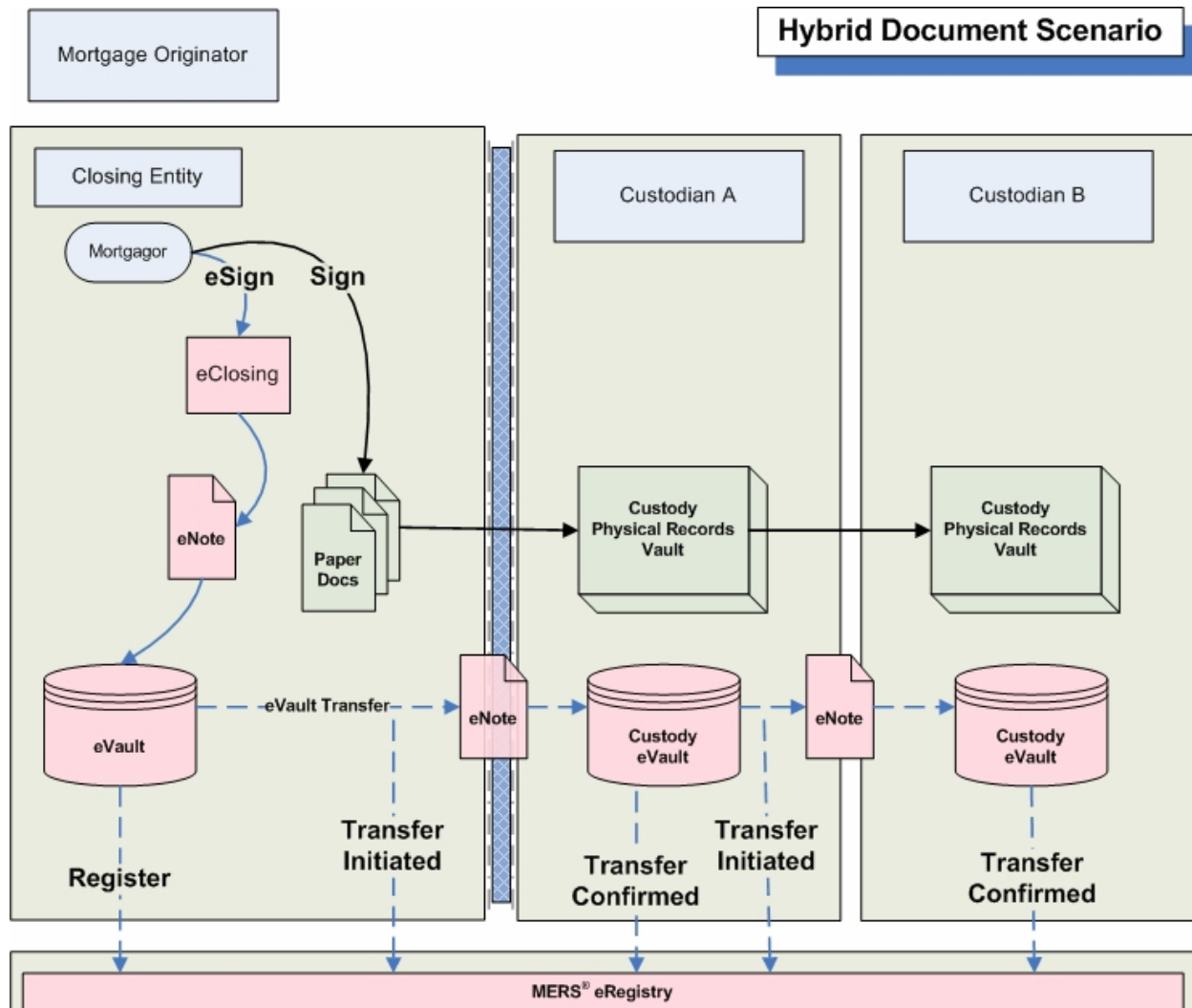
When determining the impact an eVault will have on a given practice, first consider the *types* of practices that would benefit most from eVault utilization. Then, categorize your practices using these types.

A document that benefits from utilizing an eVault for record retention will likely have the following attributes:

- It is an Electronic Record (may Require Consumer signature)
- It has been Electronically Signed
- It evidences original agreement and may need to be referenced in the future to prove enforceability
- Written Notification or Disclosure is required

- It is used in downstream transactions having financial impact

The following diagram demonstrates a sample scenario that follows the flow of a Hybrid Mortgage through a Hybrid Operations implementation. In this diagram, the eNote is initially stored in a non-custodial eVault and subsequently transferred to a Document Custodian's eVault which complements its Physical Records vault.



Source: MBMS, Incorporated

4.1.2 *Process Impacts that an eVault might bring to a given practice*

Implementing an eVault for paperless or hybrid operations impacts businesses in various ways. The following table identifies various effects an eVault might have on an operation and can serve as a starting point when considering the value proposition.

Type of Impact	Examples
Personnel Costs	<ul style="list-style-type: none"> • Retraining people to perform their jobs differently • Reduction in the number of people directly engaged in labor intensive activities • Introducing new language and concepts to an existing business model requires rethinking about how people perform their job.
Document Storage Costs	<ul style="list-style-type: none"> • Physical storage solutions (environment protection, space, shelf management, retrieval and filing) vs. Electronic storage solutions • Scalability
Technology Costs	<ul style="list-style-type: none"> • Requirements mandated by Agencies, Investors, others for holding eNotes and other electronic records • Developing capabilities to execute Electronic Document transactions with trading partners, including MERS • Requirements to upgrade appropriate systems to meet higher audit standards for transactions (record keeping, audit trails) • Higher need for standardization and integration among disparate systems
Throughput Costs	<ul style="list-style-type: none"> • Savings achieved from multiple concurrent access to authoritative information in secondary market transactions
Ownership Transfer Costs	<ul style="list-style-type: none"> • Use of MERS[®] eRegistry • Integration between eVaults and other back-end systems • Electronic vs. Physical transfers • Reduced risk of physical loss
Business Recovery Costs	<ul style="list-style-type: none"> • Loss of Physical vs. Electronic Documents • Authenticity of eVault eRecord backups as original eRecords
Transition Costs (Change Management)	<ul style="list-style-type: none"> • Costs associated with changing procedures, policies, rules in each affected process. • Costs associated with having multiple policies, procedures, rules in a hybrid environment • Duration of the transition period may affect costs. • What to do about large legacy paper world?
Regulatory Compliance /	<ul style="list-style-type: none"> • Modifying trading agreements with counterparties to enable

eVault Implementation Guide

Legal Costs	<p>new practices</p> <ul style="list-style-type: none"> • Negotiating new price points in contracts – shifts in value from those reflected in existing agreements
Risk Management Costs	<ul style="list-style-type: none"> • Impact on the existing business model from all of the above, especially the economic impact of the Hybrid world. • Uncharted territory means mistakes may be made along the way. • Incremental v. transformational change strategies of individual participants • Unknown rate of adoption of new practices in the industry will affect capital budgets (among other things)

4.1.3 Value Propositions

For the purpose of this section, consider a ‘practice’ to include the set of policies, procedures, rules, artifacts (documents) and conventions that the current set of participants employ in performing the indicated process.

With respect to current practices in the processing, closing, selling, and servicing a mortgage loan, an eVault may have a range of potential “business model ” impact points:

- 1) have no effect on an existing practice
- 2) supplement an existing practice
- 3) provide a co-existing alternative to an existing practice
- 4) substantially or completely replace an existing practice
- 5) create a new practice

The following table identifies primary mortgage Processes and Sub Processes. For each, examples describe potential business model impacts that can be used to help understand what is feasible, how new value propositions may emerge, and how existing value propositions may change.

Process	Sub Processes	Considerations / Applications of eVault	Value Propositions
Pre Closing	Processing / Underwriting	<ul style="list-style-type: none"> • Short term access to package • Multi-party / collaborative access to Package • Use of temporary eVault 	<ul style="list-style-type: none"> • Simultaneous access to records (e.g. HUD-1) improves confidence in facts. • Reduced processing times • Known file location • Improved protection of private data
	Regulatory Compliance	Long term storage of consumer acknowledgements of disclosures, and records of applications received	<ul style="list-style-type: none"> • Reduced compliance costs • Improved efficiencies in compliance auditing

eVault Implementation Guide

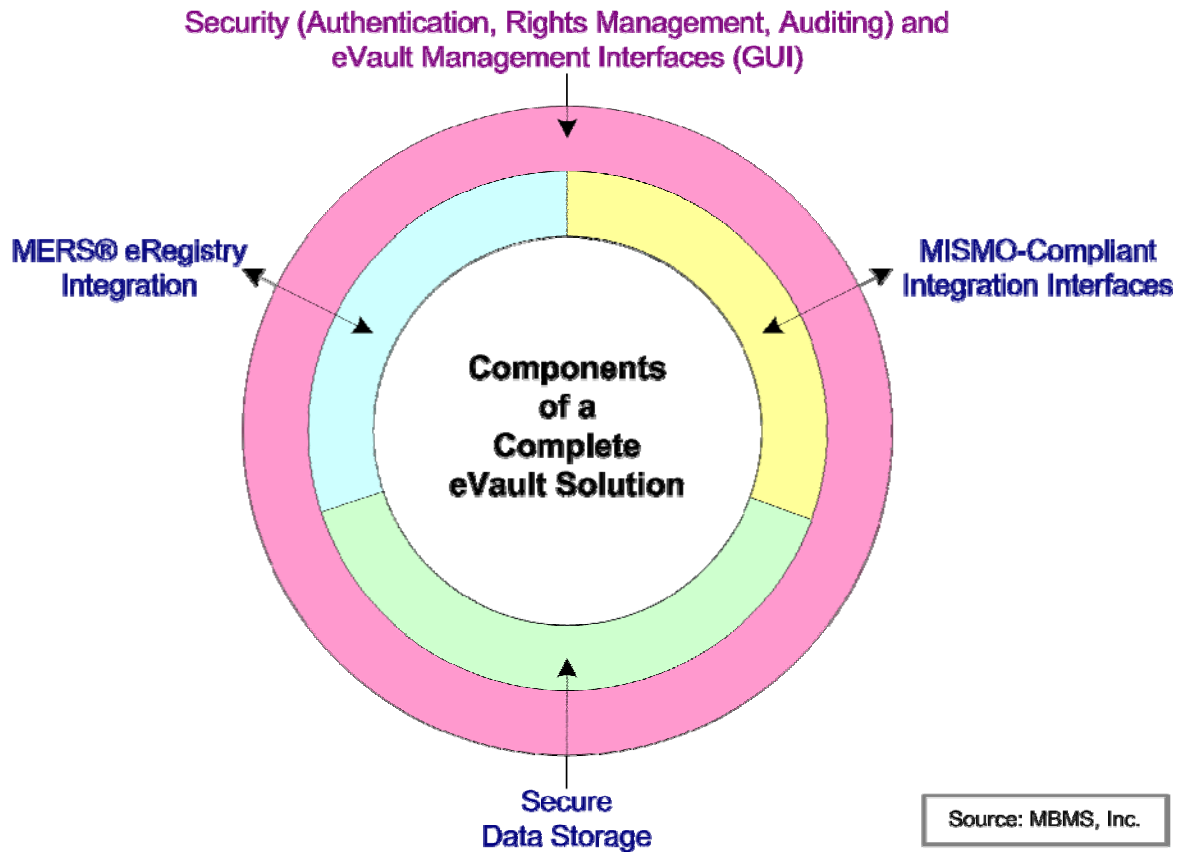
Process	Sub Processes	Considerations / Applications of eVault	Value Propositions
Closing	Document Preparation	Newly prepared documents can be safely stored in an eVault prior to closing and execution.	<ul style="list-style-type: none"> • Simultaneous access to authenticated & prepared documents • Reduced handling costs for 3rd party service providers (e.g. fund sources) • Reduced/eliminated shipping costs
	Execution of Documents	<ul style="list-style-type: none"> • Closing entities may access closing package via eVault. • Newly executed documents can be safely stored in an eVault. 	<ul style="list-style-type: none"> • Simultaneous access to authenticated, signed, prepared docs • Reduced shipping costs • Quicker time-to-vault reduces risk-point for physical loss of documents.
	Funding	Undetermined	Undetermined
Post Closing	Quality Assurance	Reconciliation of data contained in SMART™ Documents with data contained in other systems.	<ul style="list-style-type: none"> • May alter the labor content involved in post closing review, and alter the systems used • Change from system- facilitated reviews to system- generated reviews
	Commencement of Servicing	Use of data in SMART Doc™ forms as authoritative information for setup	Automated loading of SMART Doc™ forms data will reduce errors when posting to Servicing system
	Warehousing	eVault provides Warehouse Lender with security and almost instantaneous access to eNote	For applicable “wet funding” states, may reduce funding costs as nearly instantaneous access to eNote simulates dry funding.
	Document Routing	eVault provides simultaneous access to various departments/parties.	Reduced labor costs due to elimination of manual steps to physically separate, handle, and secure the Note for secondary marketing purposes
Secondary Marketing / Investor Delivery	Delivery	eVault can provide simultaneous access to authoritative information (and associated documents.)	Reduced delivery cycle times due to concurrent access and elimination of shipping
	3 rd Party Custodial Services	Simultaneous access among multiple parties in a transaction to the eNote and to authoritative information	Reduced labor costs due to concurrent activities and/or more highly automated transactions to complete the transaction
	Due Diligence	Simultaneous access among multiple parties in a transaction to the eNote and to authoritative information	Reduced storage retrieval costs and travel/living costs associated with audits
Servicing	Customer Service	Simultaneous access among multiple parties in a transaction to the eNote	Improved response times due to immediate and shared access to

eVault Implementation Guide

Process	Sub Processes	Considerations / Applications of eVault	Value Propositions
		and to authoritative information	necessary data
	Payoff / Satisfaction	eVault with MERS® eRegistry connectivity can change eNote status.	Reduced labor costs due to partially automated process

4.2 eVault Implementation Scenarios

As noted in the introduction chapter, there is not one “best” implementation of an eVault. There are, however, a few necessary components that all eVaults should provide. The illustration below shows these:



The following section provides examples of potential ASP and Non-ASP vaulting scenarios for ePackages and eNotes. These scenarios provide a high level flow of the documents and messaging required to register, transfer control, and optionally transfer location (one or more times) of an ePackage.

4.2.1 ASP Scenarios

For the purposes of this section, ASP or Application Service Provider, means an electronic closing room or full service eMortgage outsource platform. Many variations on these scenarios can be defined. Examples of variations include Lender originated eNotes through their own banking websites or web applications. Other implementation scenarios might include message origination from ASP or Third Party Custodian as the interface for the Lender and pooling of ePackages prior to transfer of control to the investor.

These scenarios complete upon transfer of control to the investor. Additional pooling and transfer of control may be accomplished by the investor.

The following list identifies the ASP scenarios described in this section

- ASP Originated, Using ASP eVault
- ASP Originated, Lender eVault
- ASP Originated, Third Party eVault
- ASP Originated, Investor eVault

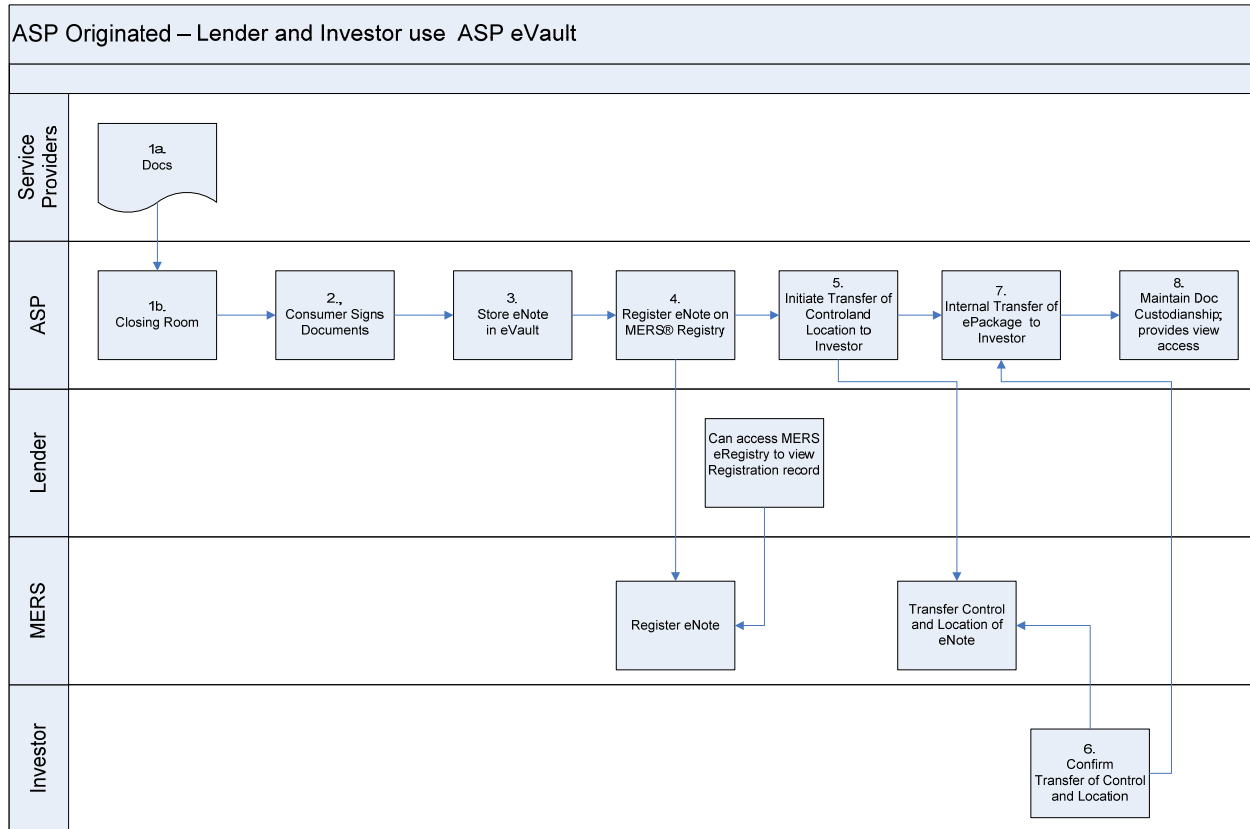
4.2.2 Non-ASP Scenarios

For the purposes of this section, Non-ASP means each party involved is providing its own technology. The following list identifies the ASP scenarios described in this section

The following list identifies the Non-ASP scenarios described in this section

- Non-ASP Retail Scenario
- Non-ASP Broker Scenario – Closing in name of Lender
- Non-ASP Broker Scenario – Closing in name of Broker
- Non-ASP Correspondent Scenario
- Non-ASP Correspondent Scenario – 3rd Party eVault
- Non-ASP Warehouse Bank Scenario – with Custodian
- Non-ASP Warehouse Bank Scenario – without Custodian

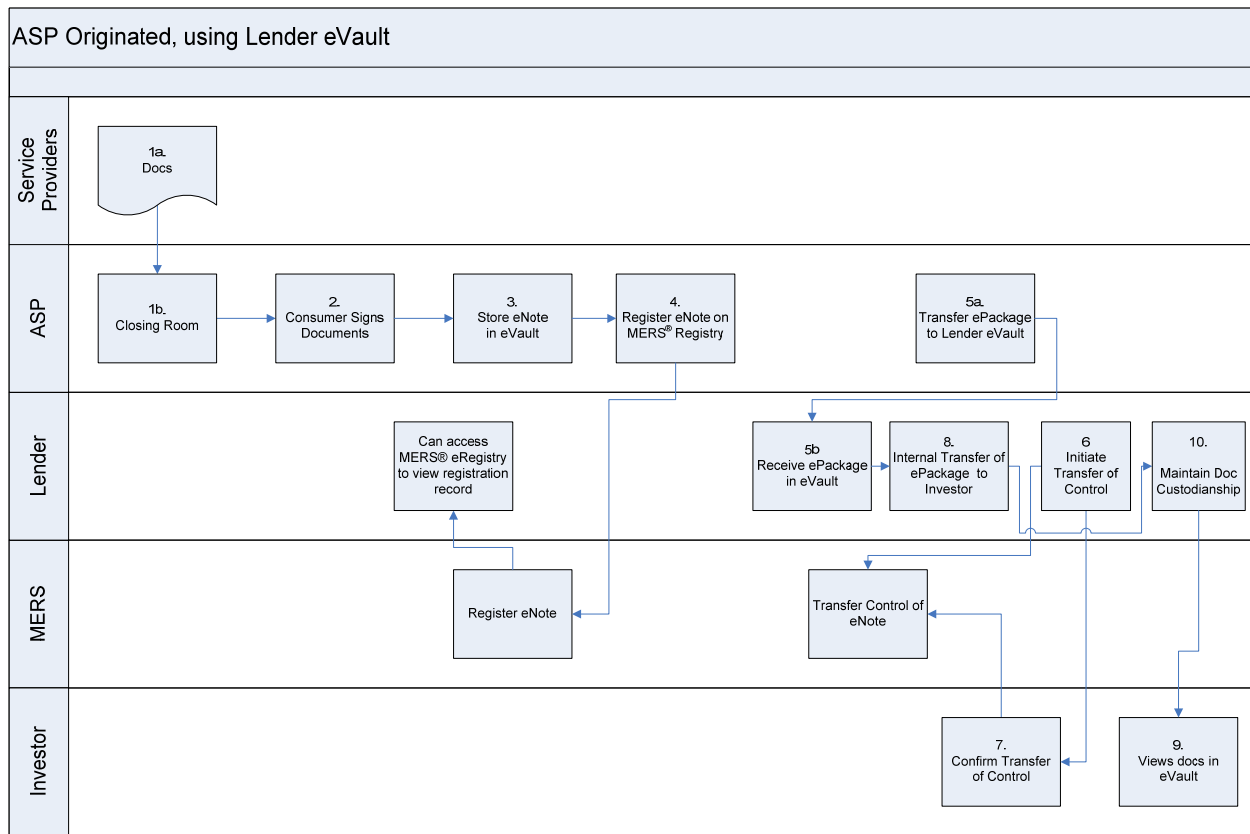
eVault Implementation Guide



Description:

1. Documents are uploaded into the closing room.
2. Consumer uses closing room to sign appropriate documents, including eNote.
3. eNote is routed to the eVault, where it is authenticated and stored.
4. ASP acting as Registrar (meaning acting on behalf of its customer) for the Lender submits initial eNote registration request to the MERS® eRegistry with Lender as Controller and Location.
5. ASP acting as Registrar for the Lender submits Transfer of Control and Location in the MERS® eRegistry.
6. Investor confirms Transfer of Control and Location with the MERS® eRegistry. (Note: some investors will require the eNote to be delivered to the Investor's eVault before the Investor will confirm a Transfer of Control)
7. ASP transfers control of ePackage within the eVault. This process includes transfer of ownership privileges, access rights, and updates internal audit trail within the eVault.
8. Investor accesses views of documents stored in the ePackage through ASP eVault user interface. eVault may retain electronic, differentiated copies of documents in the Lender's partition of the eVault for archival and audit purposes.

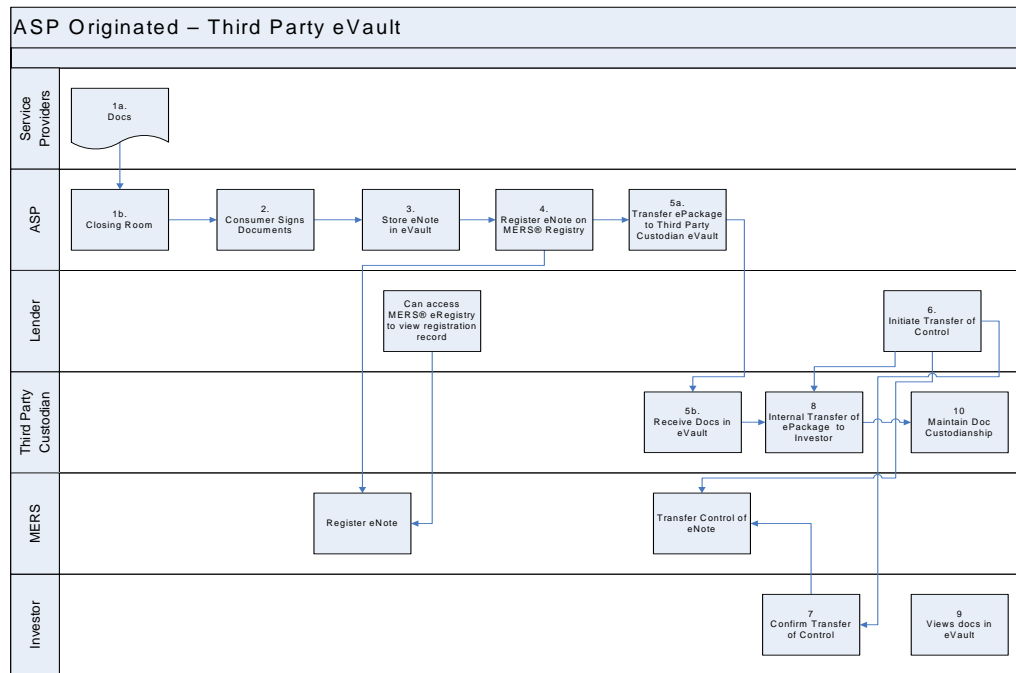
eVault Implementation Guide



Description:

1. Documents are uploaded into the closing room.
2. Consumer uses closing room to sign appropriate documents, including eNote.
3. eNote is routed to the ASP's eVault, where it is authenticated and stored.
4. ASP acting as Registrar (meaning acting on behalf of its customer) submits initial eNote registration request to the MERS® eRegistry with Lender as Controller and Location,
5. ASP transfers ePackage to Lender's eVault.
6. Lender initiates Transfer of Control with MERS® eRegistry (Lender remains as "Location" as Custodian of eNote).
7. Investor confirms Transfer of Control with the MERS® eRegistry. (Note: some investors will require the eNote to be delivered to the Investor's eVault before the Investor will confirm a Transfer of Control)
8. Lender transfers control of ePackage in the eVault. This process includes transfer of ownership privileges, access rights, and updates internal audit trail within the eVault.
9. Investor accesses views of documents stored in the ePackage through Lender eVault user interface.
10. eVault may retain electronic, differentiated copies of documents in the Lender's partition of the eVault for archival and audit purposes.

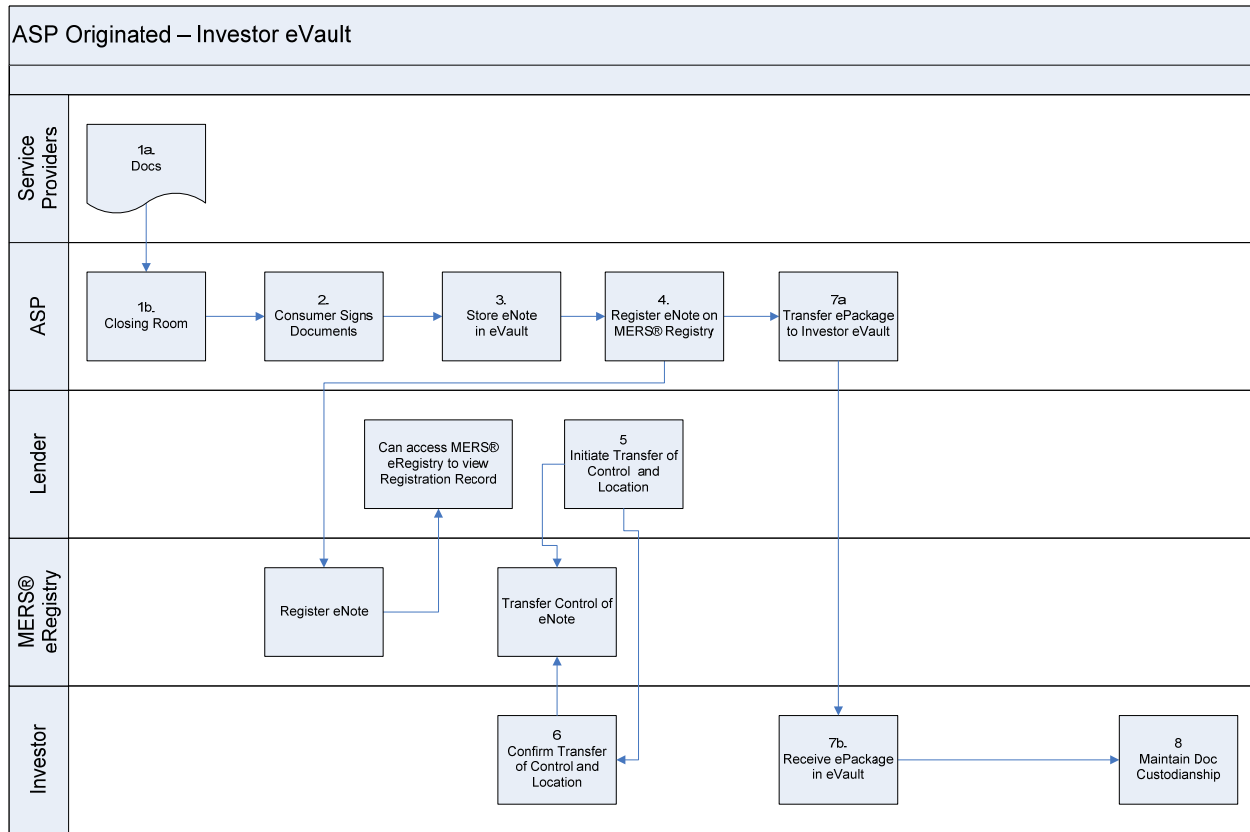
eVault Implementation Guide



Description:

1. Documents are uploaded into the closing room.
2. Consumer uses closing room to sign appropriate documents, including eNote.
3. eNote is routed to the ASP's eVault, where it is authenticated and stored.
4. ASP acting as Registrar (meaning acting on behalf of its customer) for the Lender submits initial eNote registration request to the MERS® eRegistry with Lender as Controller and 3rd Party Custodian as Location.
5. ASP transfers ePackage to Third Party Custodian eVault.
6. Lender initiates Transfer of Control to Investor with MERS® eRegistry. Notifies Third Party Custodian of pending transfer request.
7. Investor confirms Transfer of Control with the MERS® eRegistry. Notifies Third Party Custodian of transfer acceptance. (Note: some investors will require the eNote to be delivered to the Investor's eVault before the Investor will confirm a Transfer of Control.)
8. Third Party Custodian transfers control of ePackage in the eVault. This process includes transfer of ownership privileges, access rights, and updates internal audit trail within the eVault.
9. Investor accesses views of documents stored in the ePackage through Third Party eVault user interface.
10. eVault may retain electronic, differentiated copies of documents in the Lender's partition of the eVault for archival and audit purposes.

eVault Implementation Guide

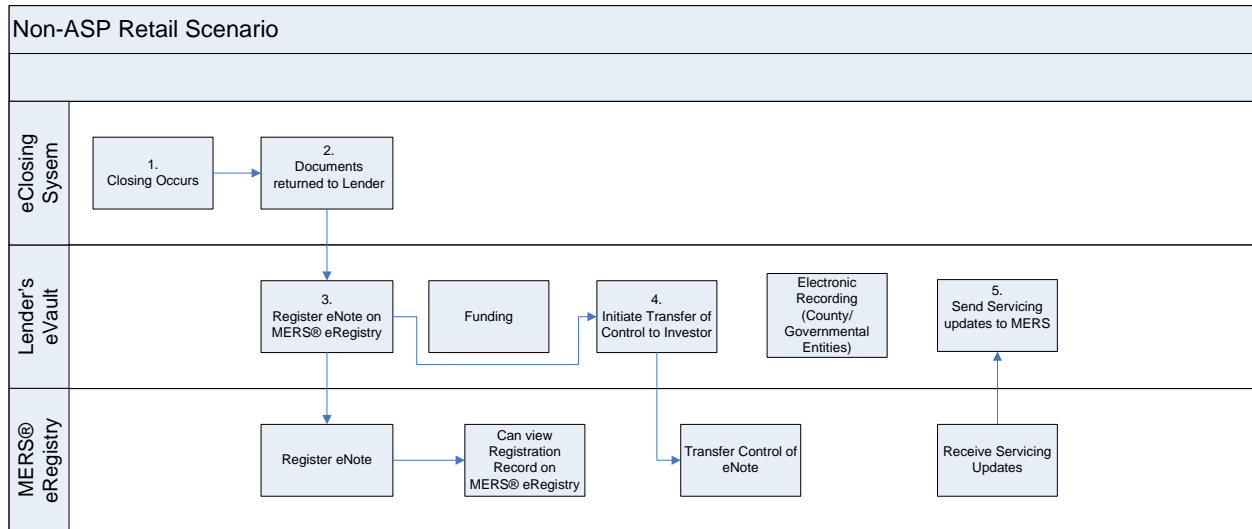


ASP Originated, Using Investor eVault

Description:

1. Documents are uploaded into the closing room.
2. Consumer uses closing room to sign appropriate documents, including eNote.
3. eNote is routed to the eVault, where it is authenticated and stored.
4. ASP acting as Registrar (meaning acting on behalf of its customer) for the Lender submits initial eNote registration request to the MERS® eRegistry with Lender as Controller and Location ..
5. Lender initiates Transfer of Control and Location to Investor with MERS® eRegistry. Notifies ASP of pending transfer request.
6. Investor confirms Transfer of Control and Location with the MERS® eRegistry. Notifies ASP of transfer acceptance. (Note: some investors will require the eNote to be delivered to the Investor’s eVault before the Investor will confirm a Transfer of Control and Location[.])
7. ASP transfers ePackage to Investor eVault. ASP eVault may retain electronic, differentiated copies of documents in the Lender’s partition of the eVault for archival and audit purposes.
8. Investor accesses views of documents stored in the ePackage through internal eVault user interface.

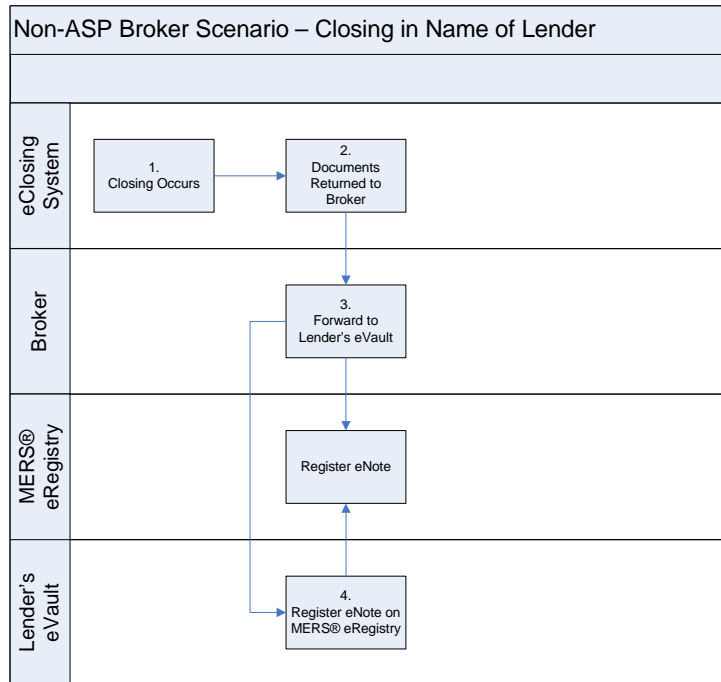
eVault Implementation Guide



Description:

1. Closing documents are executed
2. Documents are returned to the Lender
3. Lender registers eNote with the MERS® eRegistry. Lender is Controller and Location.
4. Lender Initiates Transfer of Control to Investor
5. Lender performs duties for life of loan

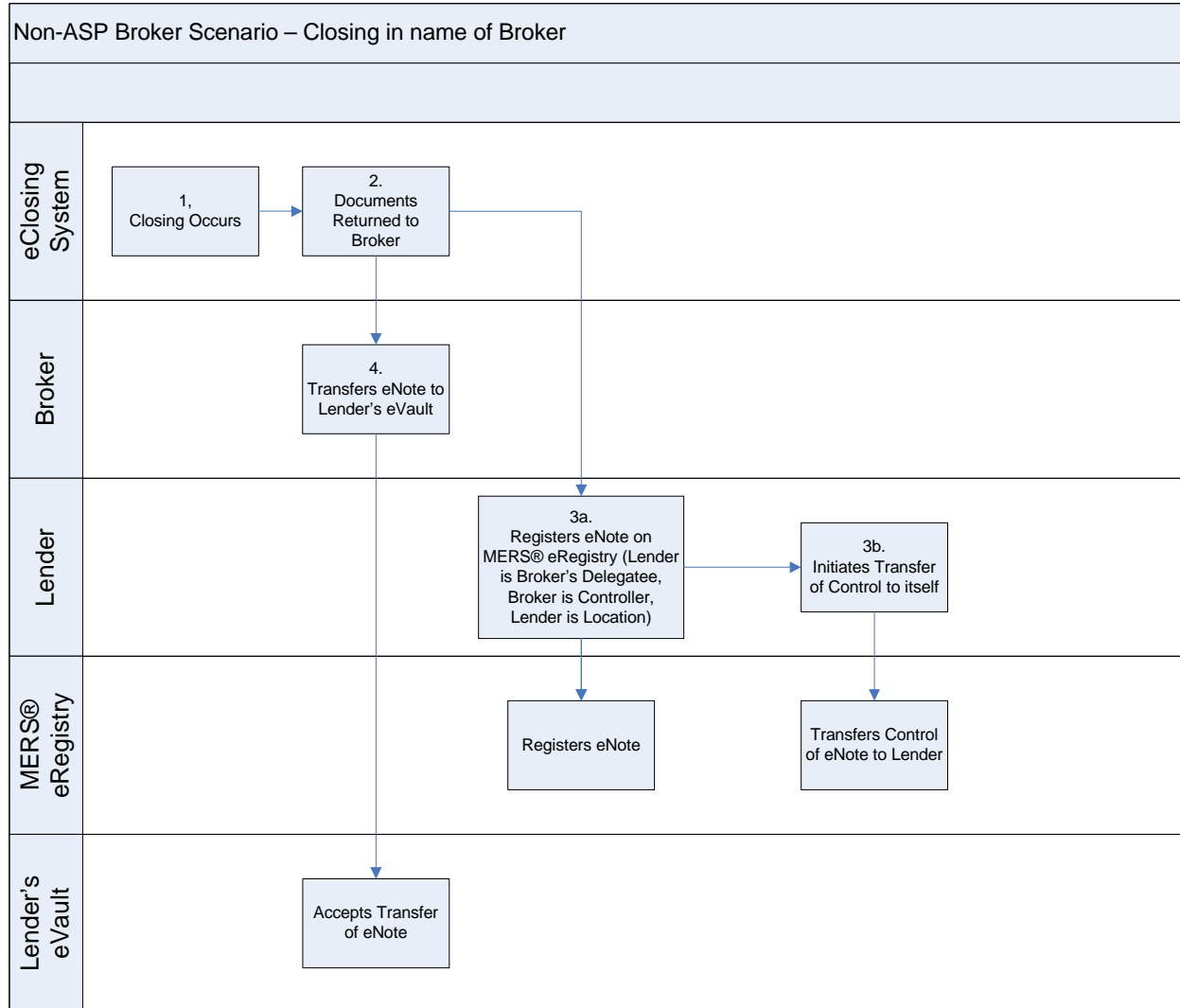
eVault Implementation Guide



Description:

1. Closing documents are executed
2. Documents are returned to the Broker
3. Broker forwards Lender's document to Lender's eVault
4. Lender registers eNote with the MERS® eRegistry. Lender is Controller and Location.

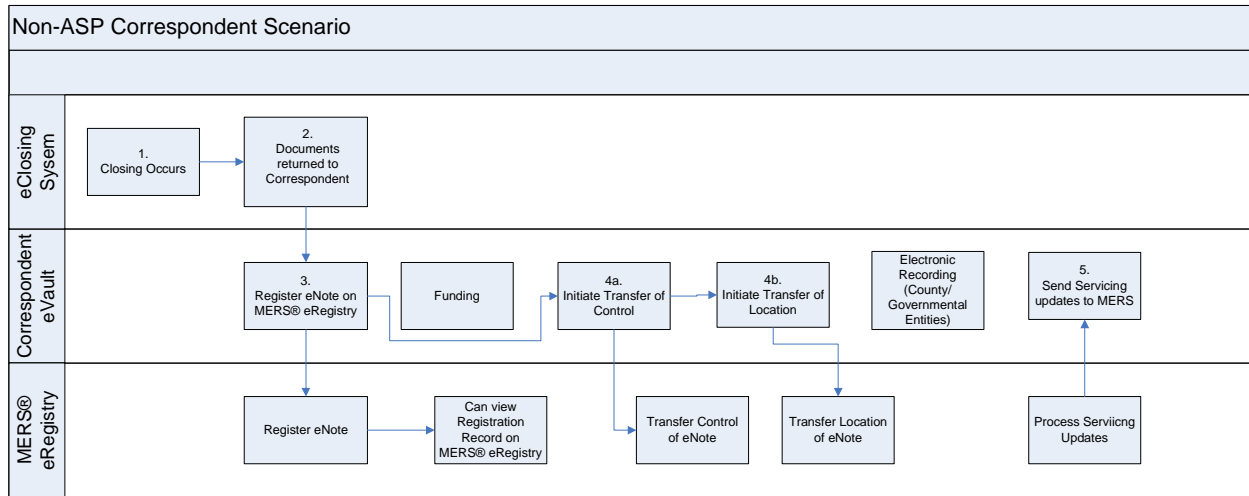
eVault Implementation Guide



Description:

1. Closing documents are executed
2. Documents are returned to the Broker
3. Lender registers eNote with the MERS® eRegistry (Lender is Broker's Delegatee. Broker is named first Controller on the eRegistry, Lender is Location.)
4. Broker transfers eNote to Lender's eVault

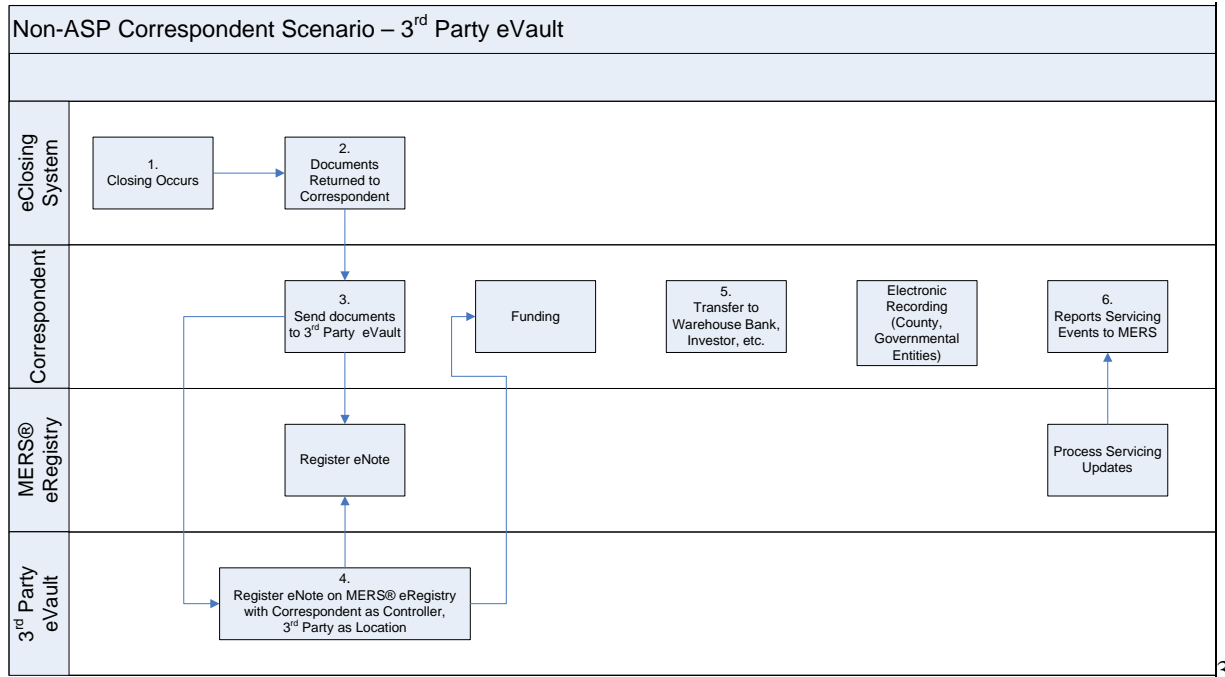
eVault Implementation Guide



Description:

1. Closing documents are executed
2. Documents are returned to the Correspondent
3. Correspondent registers eNote with the MERS® eRegistry (Correspondent is the Controller and Location)
4. Correspondent transfers Control (and possibly Location) to Warehouse Bank or Investor
5. Correspondent performs duties for life of loan

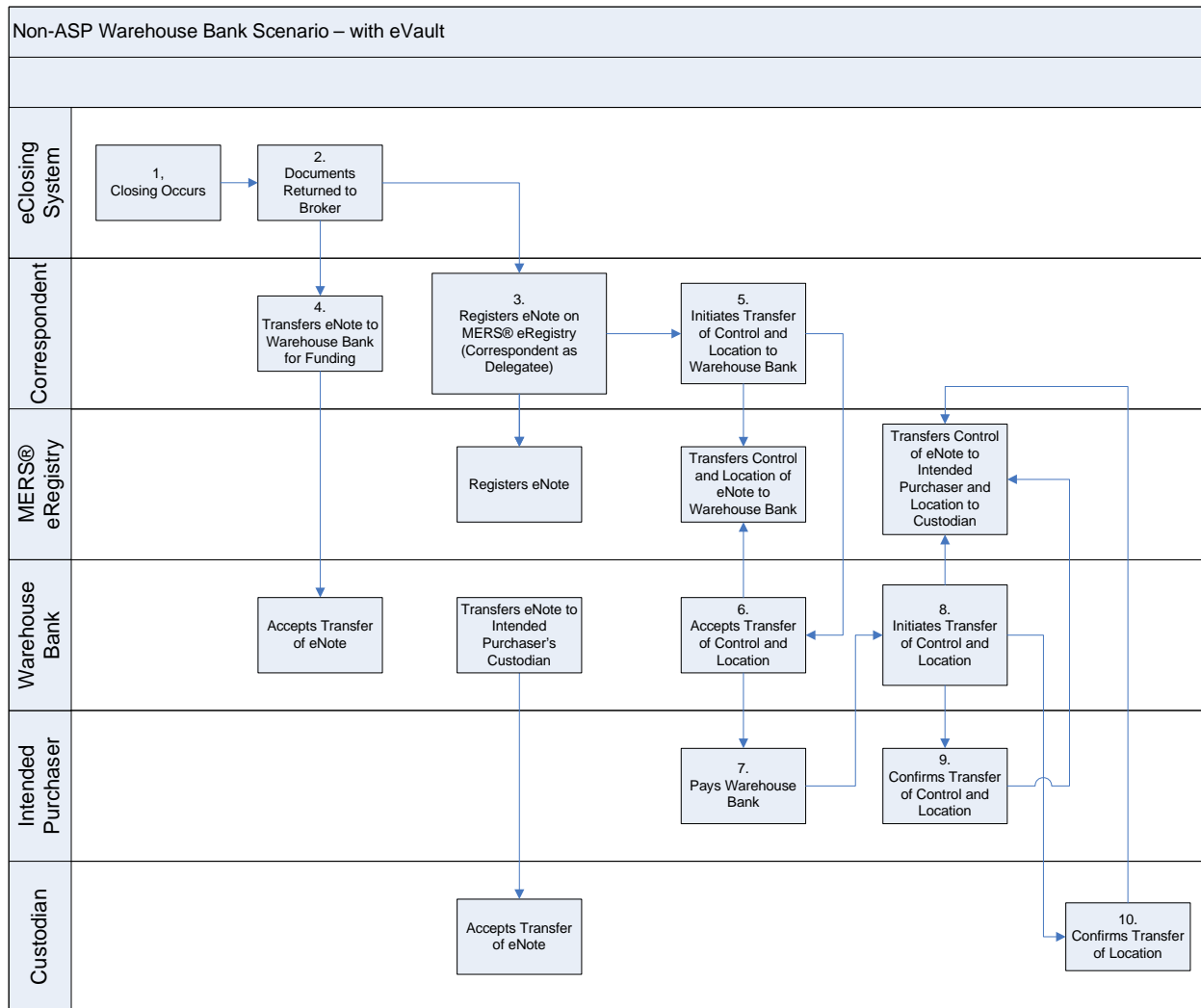
eVault Implementation Guide



Description:

1. Closing documents are executed
2. Documents are returned to the Correspondent
3. Correspondent forwards documents to Third-Party eVault
4. Correspondent registers eNote with the MERS® eRegistry through Third-Party’s eVault interface (eVault interface acts as Registrar) Correspondent is the Controller; Third-Party eVault Organization is Location
5. Correspondent transfers Control to Warehouse Bank or Investor
6. Correspondent performs duties for life of loan

eVault Implementation Guide

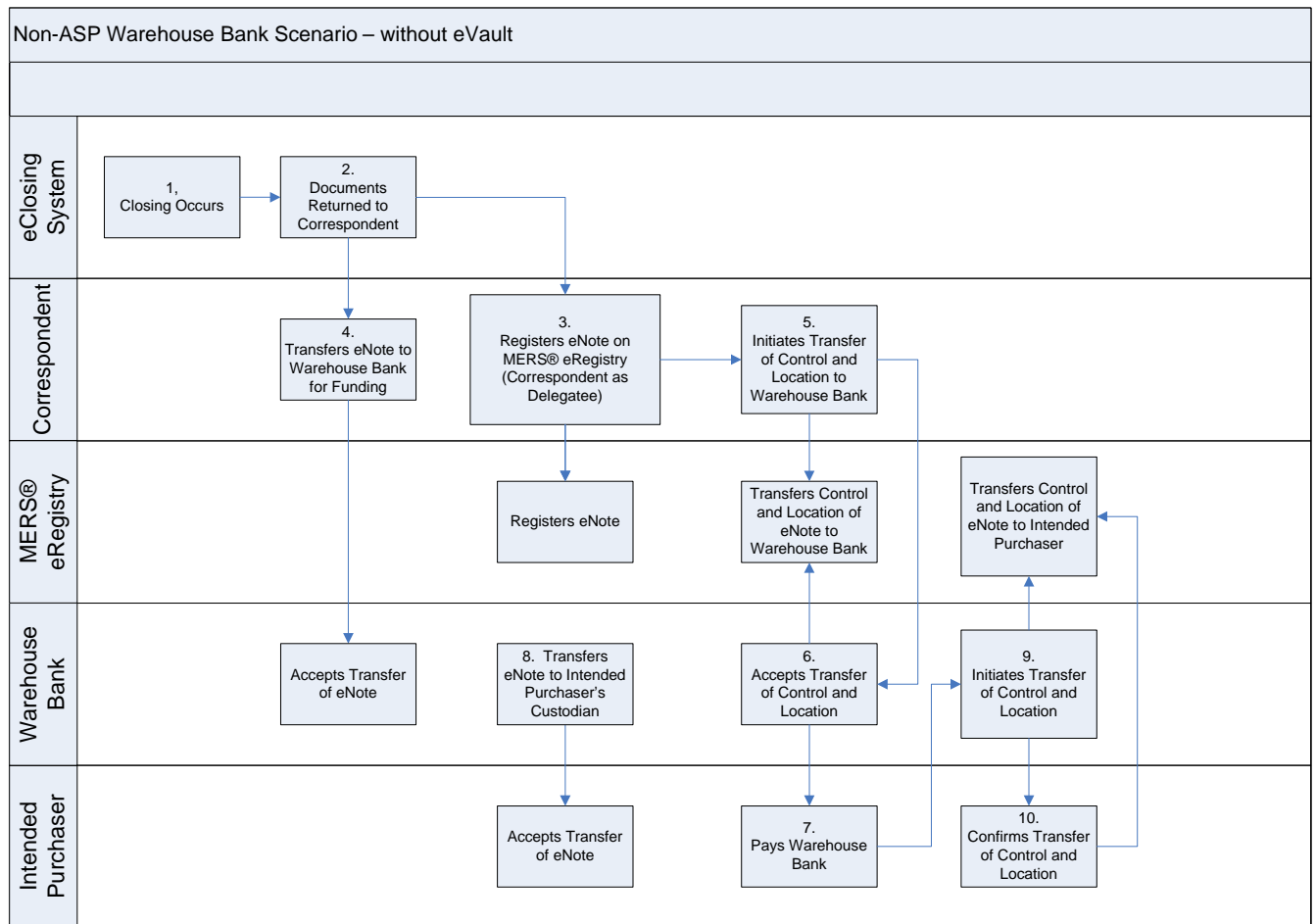


Description:

1. Closing documents are executed
2. Documents are returned to the Correspondent
3. Correspondent registers eNote with the MERS® eRegistry (Correspondent is named Controller and Location)
4. Correspondent transfers eNote to Warehouse Bank
5. Correspondent transfers Control and Location on eRegistry to Warehouse Bank.
6. Warehouse Bank accepts transfer of Control and Location
7. Intended Purchaser delivers funds to Warehouse Bank
8. Warehouse Bank transfers eNote to Custodian, and initiates Transfer of Location and Control on eRegistry (Custodian becomes the Location, Intended Purchaser becomes Controller)
9. Intended purchaser confirms transfer of control.
10. Custodian confirms transfer of location

It's important to note that this is one of many possible scenarios and is meant to merely provide an example workflow

eVault Implementation Guide



Description:

1. Closing documents are executed
2. Documents are returned to the Correspondent
3. Correspondent registers eNote with the MERS® eRegistry (Correspondent is named Controller, Location and Investor Delegatee)
4. Correspondent transfers eNote to Warehouse Bank
5. Correspondent transfers Control and Location on eRegistry to Warehouse Bank
6. Warehouse Bank accepts transfer of Control and Location
7. Intended Purchaser delivers funds to Warehouse Bank
8. Warehouse Bank transfers eNote to Intended Purchaser
9. Warehouse Bank transfers Control and Location to Intended Purchaser
10. Intended Purchaser Confirms transfer of Control and Location

It's important to note that this is one of many possible scenarios and is meant to merely provide an example workflow

Chapter 5: Guidelines for eVault Interfaces

The objective of this chapter is to identify a core set of interfaces expected from an eVault or to be provided by its 3rd party service provider. The intent is to focus on the external interfaces needed for users, other eVaults, the MERS[®] eRegistry, and other systems to interact with an eVault.

5.1 eVault Transactions List

Program Interface Descriptions

The following sections provide high-level descriptions of examples of common programming interfaces expected from an eVault. Although the specific syntax and object models will vary from eVault to eVault, the mortgage industry will benefit from establishing a baseline set of expectations and functionality for common interactions with an eVault. This includes the interfaces required to interact with the MERS[®] eRegistry and for moving eNotes between eVaults.

5.1.1 eVault Transfer & Notification Interfaces

Transaction	Description	Parameters	Return
Transfer of Control	Transfer of control or ownership from a selling entity to a buying entity.	Requesting/Submitting Party Identifier, Selling Organization Identifier, Buyer Organization Identifier, document/ePackage identifiers.	Success or Error Code
Vault to Vault Transfer	Transfer of one or more documents or ePackages from one eVault to another. All access to documents in pending transfer will be restricted.	Requesting/Submitting Party Identifier, document(s)/ePackage(s) to be transferred, target eVault.	Success or Error Code
Activity Notifications	Notification to other integrated systems that an action or event occurred on a document.	Requesting/Submitting Party Identifier, document/ePackage identifier, action or event, result or status	Success or Error Code

5.1.2 eVault Document Interfaces

Transaction	Description	Parameters	Return
New/Revised Documents			
Add New Document(s)	<p>Add ePackage and/or document(s) to be stored in eVault with the appropriate document properties and permissions.</p> <p>Each document type and category has its own unique requirements in order to process and validate the integrity of the documents being added. An example would be the validation of an eNote's tamper evident digital signature.</p> <p>Please refer to Chapter 6 of this I-Guide for more information on suggested eVault application requirements.</p>	Requesting/Submitting Party Identifier, document(s)/ePackage being added, document properties.	<p>Success or Error Code</p> <p>Document Identifier</p>
Add New Document Version	<p>Add a revised version of a document to the repository with the appropriate document properties.</p> <p>Each document type and category has its own unique requirements in order to process and validate the integrity of the documents being added. An example would be the validation of an eNote's tamper evident digital signature.</p> <p>Please refer to Chapter 6 of this I-Guide for more information on suggested eVault application requirements.</p>	Requesting/Submitting Party Identifier, document identifier, new version of document(s)/ePackage, document properties.	<p>Success or Error Code</p> <p>Document Identifier</p>
Update Document Record			
Update Document Status	Update status (Paid Off, Charged Off, etc.) of a document.	Requesting/Submitting Party Identifier, document identifier, status.	Success or Error Code

eVault Implementation Guide

Update Document Location	Update document record with current Location Organization Identifier.	Requesting/Submitting Party Identifier, document identifier, Location Organization Identifier.	Success or Error Code
Update Document Controller	Update document record with Controller Organization Identifier.	Requesting/Submitting Party Identifier, document identifier, Controller Organization Identifier.	Success or Error Code
Document Review/Certification (View)			
eNote Tamper Evident Digital Signature Comparison	Compare tamper evident digital signature of eNote with tamper evident digital signature registered with MERS® eRegistry	ePackage or SMART™ Document, signature value of eNote registered in MERS® eRegistry	Success or Error Code
Search Document or ePackage	Get a list of all the documents or ePackages that satisfy specified search criteria (i.e. interest rate, closing date, etc.)	Requesting/Submitting party identifier, ePackage/document identifier, search criteria	Success or Error Code Search results
Get Document Versions	Retrieve a list of all versions associated with a document identifier.	Organization identifier, user identifier, document identifier.	Success or Error Code Document version list
Get Document and/or ePackage	Retrieve document(s) or ePackage(s) for viewing.	Requesting/Submitting Party Identifier, user identifier, document/ePackage identifier, document version	Success or Error Code Document or ePackage

eVault Implementation Guide

<p>Get Document Information</p>	<p>Retrieve requested metadata, status, properties, and/or summary information from Document.</p> <p>Retrieve the VIEW section from the SMART Doc™ file</p> <p>Retrieve the DATA section from the SMART Doc™ file</p> <p>Retrieve the Tamper Evident Digital Signature from the SMART Doc™ file</p> <p>Retrieve Document Status</p> <p>Retrieve Document Summary</p> <p>Retrieve Document Properties, such as indexing details</p> <p>Retrieve all relevant document information</p>	<p>Requesting/Submitting Party Identifier, user identifier, request type, document/ePackage identifier, request criteria,</p>	<p>Success or Error Code</p> <p>Document View</p> <p>Document Data</p> <p>Digital Signature</p> <p>Document Status</p> <p>Summary Information</p> <p>Document Properties</p> <p>All Document Information</p>
<p>Get Document Activity</p>	<p>Allow external systems to retrieve activities or events that occurred on a document</p>	<p>Requesting/Submitting Party Identifier, user identifier, document identifier, request criteria</p>	<p>Success or Error Code</p> <p>Activity Details</p>

5.1.3 MERS® eRegistry Interfaces

Transaction	Description	Parameters	Return
<p>Transfer Confirmation</p>	<p>eVault sends a Transfer Confirmation Request to the MERS® eRegistry rejecting or accepting a pending Transfer of Location for an eNote where the eVault Organization Identifier is named as the new Location on the pending transfer.</p>	<p>Requesting/Submitting Party Identifier, MIN, Tamper evident digital signature of eNote, Confirmation Type.</p>	<p>Success or Error Code</p>

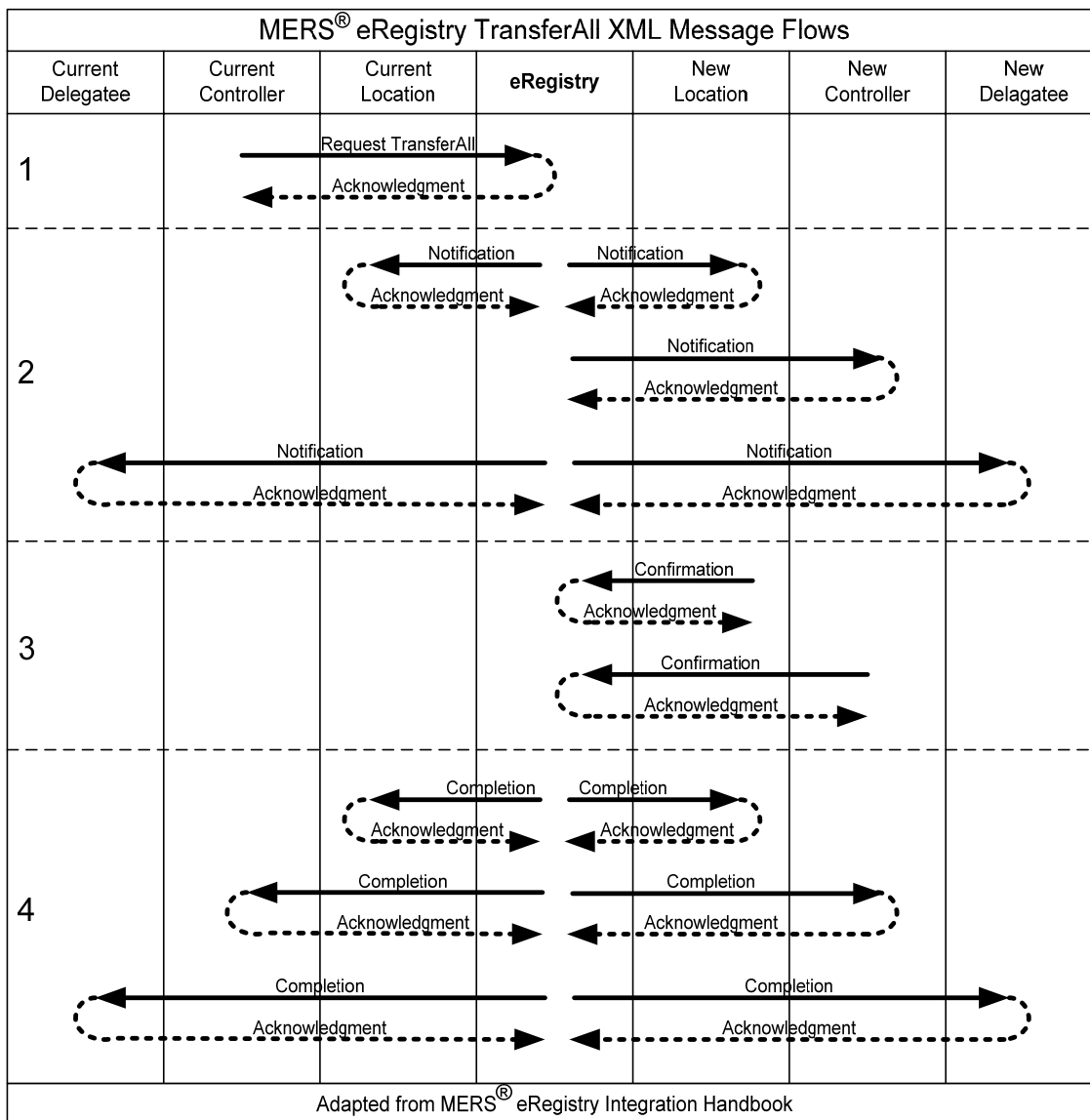
eVault Implementation Guide

eNote Information Inquiry	<p>eVault sends an eNote Information Inquiry request to MERS® eRegistry.</p> <p>The MERS® eRegistry will determine the appropriate eNote status and summary information to return based on the request type and whether the requesting organization identifier is currently or has previous been named on the eNote.</p>	Requesting/Subsubmitting Party Identifier, MIN, Tamper evident digital signature of eNote, Inquiry type.	<p>Success or Error Code</p> <p>eNote registration status and/or eNote summary information of eNote</p>
Pending Transfer Notification	<p>eVault receives a notification of a new pending transfer from the MERS® eRegistry.</p> <p>Pending notification requests are sent by the MERS® eRegistry to the current and new Controller, Location, and/or Delegatee organization ID's to notify them that an eNote is in a pending Transfer of Control, Location, and/or Delegate.</p>	Requesting/Subsubmitting Party Identifier, MIN, Request Type, Transfer Type, Transfer Status, Action Effective Date, and Controller, Location, and/or Delegatee Organization Identifier eNote is being transferred to.	Success or Error Code
Transfer Completion Notification	<p>eVault receives a notification of a completed (processed) eNote transfer from the MERS® eRegistry.</p> <p>Transfer Completion Notification requests are sent by the MERS® eRegistry to the old and new Controller, Location, and/or Delegatee organization Id's to notify them that an eNote was successfully or unsuccessfully transferred to a new Controller, Location, and/or Delegatee.</p>	Requesting/Subsubmitting Party Identifier, MIN, Request Type, Transfer Type, Success/Failure of transfer completion, Action Effective Date, and Controller, Location, and/or Delegatee Organization Identifier named in original transfer initiation request.	Success Code or Error Code

5.2 eVault Transaction Model Example

MERS eNote Transfer including Transfer of Location

The MERS[®] eRegistry tracks the Controller (owner), Delagatee (authorized representative), and Location (electronic document custodian) of eNotes but does not store or provide access to the eNotes themselves. It has processes that enforce the MERS[®] eRegistry business rules to allow any or all of them to be changed via transfer requests by authorized parties. One of the more complex eVault transactions envisioned involves the transfer of an eNote from one eVault to another coordinated with a complete transfer of all three roles in the MERS[®] eRegistry.



A request to the MERS[®] eRegistry to TransferAll:

1. is initiated by the current Controller (or its Delegatee),
2. creates a pending transfer in the eRegistry which sends a set of pending Notifications to all the other affected parties,
3. requires Confirmation by the New Location and the New Controller accepting (or rejecting) the request,
4. and creates a set of Completion notifications (either success or failure) to all the affected parties including the original requestor.

Transfer requests involving transfer of location send a pending Notification to both the current location and the new location. The new location **MUST** send a Confirmation accepting the change for successful Completion of the transaction although other Confirmations may still cause a failure, e.g. the current Controller may cancel the request or the new Controller may reject it. MERS does not address when nor how the eNote is moved from one location to another.

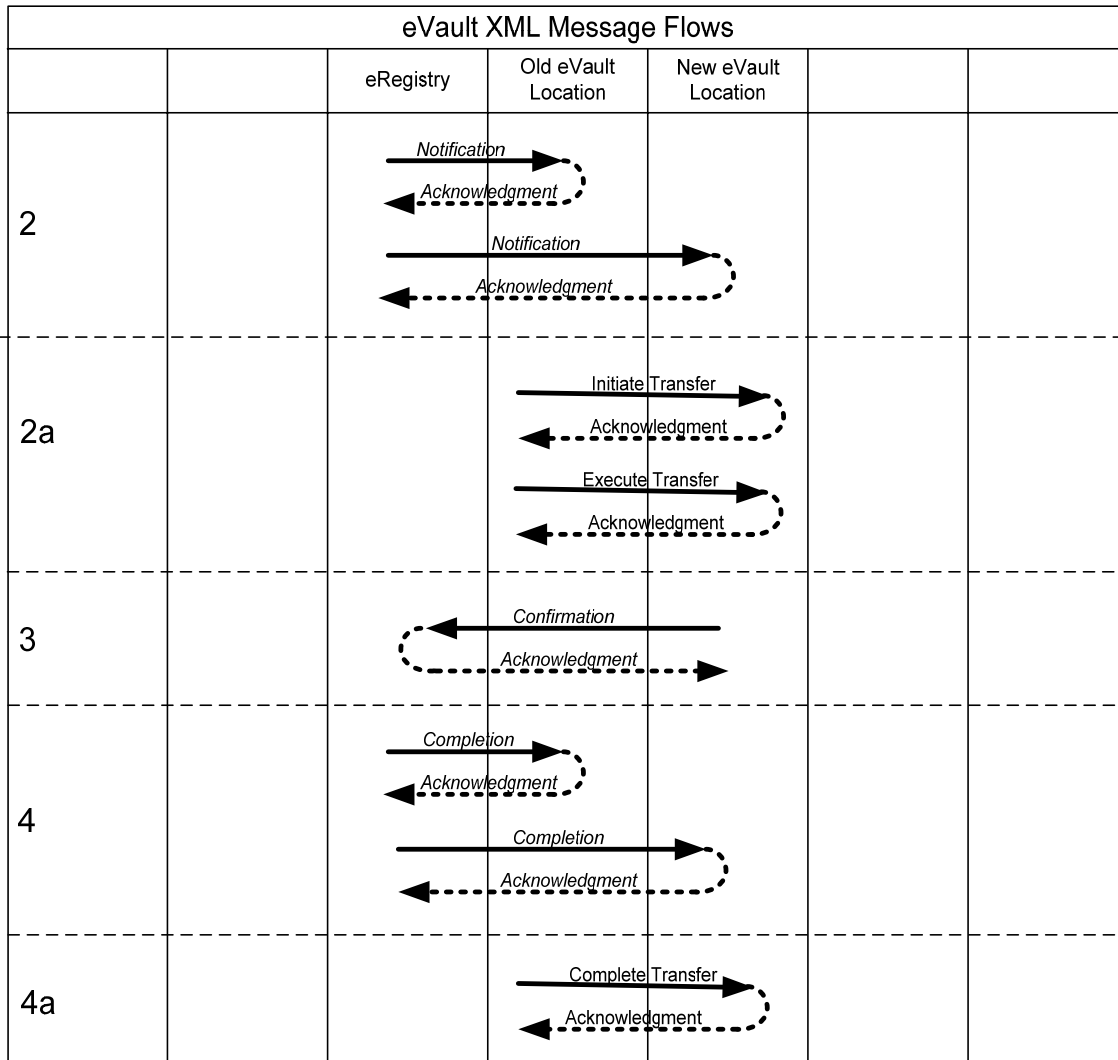
eVault eNote Transfer of Location

When MERS notifies the current location and pending new location of the pending transfer, it includes relevant information about the transaction including:

1. the unique Mortgage Identification Number (MIN) of the eNote,
2. the MERS OrgIDs of the proposed new controller, delegatee, and location,
3. the signature value of the tamper evident digital signature of the eNote.

The current Controller or its Delegatee has the necessary MIN and OrgIDs to start a transfer of Location transaction. The new location has the necessary OrgIDs and would have received the tamper evident digital signature from the current location to accept the transfer. Only the new location can send the MERS[®] eRegistry a Confirmation accepting the transfer; it also controls when in the process it sends the Confirmation based on its business rules, but it must be prior to the expiration of the transfer request. Both locations can act on the MERS Completion notification as well as their own completion transaction to update the final status of the transferred eNote in their own systems.

eVault Implementation Guide



eVaults need to add transactions between each other to the process flow of the MERS[®] eRegistry:

- 2a. The eVaults must move a verifiable duplicate of the eNote from the old location to the new location.
- 4a. The eVaults must track the status of their duplicate as the authoritative copy and may exchange information about the completion of the transfer.

The transaction definitions between eVaults or between users and eVaults may support both synchronous and asynchronous interactions using push or pull exchanges as appropriate to the business processes and relationships.

Chapter 6: Suggested Solution Requirements

The purpose of this chapter is to provide an outline of possible eVault features. These features are not intended to be a benchmark, but rather suggestions for eVault functionality. Refer to MISMO's "Lost or Destroyed Data Issues Analysis" which contains recommendations for offline storage, data and system backups, data archiving, and Security procedures.

This chapter is divided into the following seven sections:

- 6.1. Accessibility of Records
- 6.2. Ability to handle Transferable Record Requirements
- 6.3. Ability to verify document integrity
- 6.4. Ability to verify and authenticate certificates(s)
- 6.5. Division of roles within Application
- 6.6. Full auditing capabilities
- 6.7. Ability to interface with MERS® eRegistry.

6.1 Accessibility of Records

- Controller of record should have access – the eNote's designated controller will be required to verify information and status contained within the record and to be the final arbiter of the record's authenticity.
- Transaction Participants
 - Should have ability to control access – any eVault system should be able to control access to different transaction participants.
 - View of record – the human-readable XHTML portion of the eNote.
 - Signature info – Allow certain individuals to view the information associated with the electronic and digital signature
 - Audit trail – Track who can access the audit trail information.
 - Registration data – System should be able to protect information regarding the MERS registration data from unauthorized individuals.
 - Most likely need ability to retain or access copy of record after transfer – after transferring an eNote between eVaults, the sending system should maintain a copy of the transaction records for legal and archival purposes.
 - Borrower may need ability to view document(s) – borrowers may need to view the eNote to prove authenticity and enforceability. See Chapter 2 for more information on legal issues.
- Auditors and Regulators may need to be given access – See Chapter 2 for more information on legal issues.

- System should address technology obsolescence and record conversion. Systems and technologies will change over time and systems should provide a path into those new technologies. Systems should provide a conversion model or models between technologies.
 - May include ability to convert to/from varying file formats as W3C standards change
- Ability to handle records for applicable time period – Systems may be authorized to handle records only for certain periods of time.
- Retainability (of copy) - transaction Participants may need to retain a copy
 - May provide access and/or electronic record at agreed-upon location (e.g. website) – Borrowers (and others) may be given access to the record through a web site.
 - May provide opportunity to print or download the electronic record – At certain points, closing for example, Borrower (and others) may be given opportunity to request a printed or electronic copy of record(s).
 - May provide participant a paper or electronic copy of electronic record - Borrowers (and others) may be given a copy of the electronic record on electronic media or paper.
 - If record is provided to the participant an acknowledgement may be prudent – Recipients of electronic records should be required to execute some type of acknowledgement when receiving the records.
 - Transaction Participant may retain record in different format than Owner of Record – Borrowers may desire a record in a format they are comfortable with, which may differ from the “internal” SMART Doc™ file format stored in the eVault. Here are some initial guidelines on providing documents in alternate formats:
 - Conversion of Record to alternate format should not change or obscure relevant information
 - Conversion process should be preserved so it can be reproduced
 - Copy of converted file should be maintained so that it can be compared against the unconverted record

6.2 Ability to handle Transferable Record Requirements

- Ability to identify and track authoritative record in eVault in conjunction with MERS® eRegistry
 - The eVault should keep track of all the parties to the eNote (location, controller, and delegatee).
 - The eVault should have the ability to keep track of the location of the eNote. The location entity should have the authoritative copy.
- Ability to distinguish authoritative record from copies
 - If your eVault is not the current location of the eNote, then you do not have the authoritative copy. If you are the current location, then you have the authoritative copy.
- Ability to transfer authoritative record
 - eVault should have the capability to confirm transfers of location with the MERS®

eVault Implementation Guide

eRegistry for the purposes of transferring storage location, ownership, and administrative duties of the eNote.

- Ability to identify controlling party
 - The eVault should keep track of all the parties to the eNote (location, controller, and delegatee).
- Log MERS communication and status
 - The eVault should keep track of all communication initiated and received from MERS[®] eRegistry transactions. This will provide an audit record of past events.
- Convert an eNote to Paper. If a Note is no longer to exist in electronic form:
 - The Servicer must print a new Note, and get the borrower to sign the new Note.
 - The MERS[®] eRegistry must be updated to change the status of the eNote to Inactive for reason of converting to paper
 - The eVault must update its records to show the eNote has been converted to paper.

6.3 Ability to Verify Document Integrity

- Ability to detect alterations by checking tamper evident digital signature on demand or in batch mode
 - The eVault should have the ability to verify the XML-DSig digital signature (NOTE: is “XML-DSig digital signature” the same thing as “tamper evident digital signature” ? If so, use the same term) contained within a document and report the validity of the signature. It should also have the ability to automate tamper evident digital signature checking on a regular basis, to verify that no alterations have been made to the existing documents.
 - The eVault should be able to reconcile the Tamper Evident Digital Signatures of the eNotes it holds against those registered on the MERS[®] eRegistry. This option for the eRegistry will be available with Release 2.0.
- Ability to track document access
 - Access to documents should be restricted to only authorized parties. This access should be controlled by an administrative party.
 - Document access should be logged for audit purposes.
- Ability to track completeness of signing / audit trail
 - The eVault should have the ability to verify that the documents that can be signed are fully signed (optional), and that the tamper evident digital signature has been applied to the eNote if it is to be registered with the MERS[®] eRegistry. It should also have

the ability to verify that a tamper evident digital signature has been applied to documents with a tamper evident digital signature signer.

- Ability to preserve clarity of view (readability)
 - The documents should remain human-readable throughout the process, from creation and signing through vaulting. Formatting should be preserved.
- Encryption/Decryption of document
 - The eVault should provide a means of encrypting documents for storage. This should include a means of decryption as well.
- Reporting tamper evident digital signatures to auditors
 - The eVault should provide a way to validate the tamper evident digital signature on command for audit purposes. This may also be an automated batch process.
- Printing – Certified Originals / Watermarked Copies
 - Printing the eNote should be limited to watermarked copies, unless the document is being converted to paper. If the eNote is to be converted to paper, allow the document to be printed once, and then return to printing watermarked copies. If the printing fails, administrative access should be required on some level to allow re-printing and to verify that only one original copy exists.
- Should check upon submission to eVault
 - Upon submission, the eVault should have the ability to verify document integrity including but not limited to: compliance with DTDs, tamper evident digital signature validity, document signing status, and completeness of package.
- May check at periodic points with transaction
 - The eVault should have the ability to automate checking of integrity at certain schedulable intervals.
- Should handle if invalid tamper evident digital signatures
 - Recover uncorrupted from backup
 - The eVault should have the ability to recover untainted data from backup devices if the current data is determined to be invalid.
 - Tamper evident digital signature found invalid
 - The eVault should have the ability to lock down the system, requiring administrative access to restore system to a valid state. This will provide a timely notification of corruption/intrusion/etc and allow for system integrity to be restored.
 - Optionally notify controller or controllers' system
 - If the tamper evident digital signature is determined to be invalid, you can notify the controller of the document's validity status. This could provide an outside means of determining a compromised system.

- Get clean from backup
 - If the tamper evident digital signature is determined to be invalid, the eVault system should provide a way to restore a known-good backup to restore system integrity.
- Log of event
 - The eVault should record the tamper evident digital signature validation in an event log for audit purposes.

6.4 Ability to Verify and Authenticate Certificates(s)

- Validate Certificate used for tamper evident digital signature
 - Should check CRL
Certificate Revocation List (CRL) must be checked for revoked certificates.
 - Must update CRL per SISAC guidelines
CRL list on eVault machine should be periodically updated in order to get new updated lists from major providers.
 - May check OCSP
Online certificate status protocol (OCSP) may be used to validate certificates in real-time (live connection to OCSP service needed)
 - Should verify SISAC-approved issuer.
Root certificates for certificates; tamper evident digital signature should be issued by SISAC-approved providers
 - Hash digest comparison with the MERS[®] eRegistry (optional feature)
May compare hash of eNote in incoming package with hash of same eNote from the MERS[®] eRegistry (if eNote has been registered before). (This option will be available with Release 2.0 of the MERS[®] eRegistry)
 - Validate entire certificate chain
 - On Vault-to-Vault transfer – should check tamper evident digital signature - on transfers between vaults it may be enough to check only the last certificate in the chain, or seal only the last certificate in the chain (because certificates may be outdated or revoked already, but were valid at time seal was made)
 - On initial registration – should check entire certificate chain.
In order to accept new package in eVault, entire certificate chain should be checked in addition to tamper evident digital signature itself.
- Electronic Signatures – may be tamper-evident sealed using HSM.
Hardware security module (HSM) may be used to provide additional security to key, used in tamper evident digital signature
- May require to register eNote

eVault may require to register eNote on the MERS[®] eRegistry from new package automatically after receiving, if the eVault is acting as a Registrar on the MERS[®] eRegistry for the Lender.

6.5 Division of Roles Within Application

- Vault administration – roles and groups
In order to provide different levels of access eVault needs definitions of roles/groups and utility to manage it
- Tiered Access & Permissions within application
Detailed (function and/or record based permissions) access system should be used in order to have flexible control over user permissions level
- Management reporting
Should provide mechanism to create and customize reports where any information from stored documents can be used

6.6 Full Auditing Capabilities

- Track document access
Should log any event in which user gains access to any specific package
- Track document or document meta-data properties alteration
Should record changes in document/package with optional storage of full old version of document/package
- Track document receipt and processing
Should log receiving and processing events for specific package, include receipts and communication packages between eVault and the MERS[®] eRegistry
- Track document transfers
Should track Vault-to-Vault transfer events for specific package

6.7 Ability to Interface With MERS[®] eRegistry

- Inter-vault transfers/messaging
Should transfer to eVault in another organization's network with changes to location, controller or delegatee
- Intra-vault transfers
Should support intra-vault transfers (inside organization network) without changing location, controller or delegatee. Must have the ability to identify authoritative copy of eNote within organization vaults.
- MERS[®] eRegistry messaging
Should support MERS[®] eRegistry protocol for confirmations of transfers, and receipt of transfer pending and complete notices.

Glossary of Terms

Term	Definition	Examples/Comments
AIA	Accredited Issuing Authority. An organization approved by SISAC to sell digital certificates	
Alteration	A change to the terms or conditions of a document, or change in the variable information added to the document, after it is signed, or if it is not required to be signed, after it is delivered to the intended recipient.	
API	An Abbreviation for application program interface; a set of routines, protocols and tools for building software applications	
ASP	Application Service Provider	
Authentication	The process of validating credentials presented by an individual or organization.	
Authoritative Copy	The unique controlling reference copy of the Transferable Record (eNote), which is registered on the MERS® eRegistry	
Borrower	A mortgagor who receives funds in the form of a loan with the obligation of repaying the loan with interest (if applicable), and in addition, any person purchasing (aka purchaser) the real property securing the loan, executing the promissory note, executing a guaranty of the debt evidenced by the promissory note, or signing a security instrument in connection with a loan.	
Broker Delegatee	Lender authorized to submit registrations on behalf of a Broker who does not have access to the MERS® eRegistry	
Certificate Authority	A trusted Third party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. This role guarantees the individuals involved in an electronic legally enforceable transaction are who they claim to be	
Click-through Signature	Electronic signature in which a consumer assents to a contract with a simple mouse click after viewing the applicable terms and conditions.	The terms of the contract must be "commercially reasonable," consumers must have an opportunity to reject them, and an affirmative act of assent is required.

eVault Implementation Guide

Term	Definition	Examples/Comments
Consumer	<p>A person defined as a consumer under the federal E-SIGN Act.</p> <p>NOTE: eCommerce definition is different</p>	<p>In the mortgage finance industry this party has historically been known as the borrower. However, E-SIGN legislation referring to the term “consumer” actually references any non-commercial party to the transaction, which could include Borrowers and sellers for the purpose of consent and disclosure</p>
Control	<p>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 E-SIGN. For example, Control can be thought of as having possession of an original paper note.</p>	
Controller	<p>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.</p>	
Controller’s Delegatee	<p>A member of the MERS® eRegistry that is authorized by the Controller to perform certain MERS® eRegistry transactions on the Controller’s behalf.</p>	
CRL	<p>Certificate Revocation List. A periodically (or exigently) issued list, digitally signed by an Issuing Authority, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer’s name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates’ serial numbers, and the specific times and reasons for revocation.</p>	
DES	<p>An abbreviation for Data Encryption Standard and may include 56-key or 128 key symmetric and asymmetric encryption methods</p>	
Digital Certificate	<p>A public key (or digital) certificate is a certificate which 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.</p>	

eVault Implementation Guide

Term	Definition	Examples/Comments
Digital Signature or Encryption Key	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.	
eClosing	The act of closing a mortgage 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.	
eCustodian	The holder (not beneficiary owner or entity that maintains the holder in due course rights) of the authoritative copy of the electronic promissory note. This is not the data storage provider, but the entity whose role it is to ensure the safe and accurate storage and archival of these critical loan documents.	
eDelivery	Providing for the transfer of data and documents created electronically to another entity	
eDocument	Any document that has been converted (created?) and executed in electronic form.	
Electronic Record	A record created, generated, sent, communicated, received, or stored digitally.	
Electronic Signature	an electronic symbol or process attached to or logically associated with an electronic record and signed or adopted by a person with the intent to sign the record	

eVault Implementation Guide

Term	Definition	Examples/Comments
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. Parts of the transaction that precede the actual closing may occur on paper initially, but are ultimately converted to electronic form prior to Closing.	
Encryption	The manipulation of a packet's data in order to prevent any but the intended recipient from reading the data.	Encrypted data is often referred to as cipher data
eNote	An electronic record that would be a promissory note if it were issued in paper, and that the Borrower has agreed to issue as a transferable record.	
eNote Clause	Also known as “eNote Language” means additional terms in the text of the eNote to comply with ESIGN and UETA requirements.	
eNote Registration	The process of creating the initial record in the MERS [®] eRegistry for identifying the controller of the eNote	
ePackage	(Short for eMortgage Package.) An XML specification that provides a flexible yet simple mechanism to collect one or more SMART Doc [™] forms, image files, Word Documents, PDF file, and other related and/or encoded embedded files in a single 'electronic file' for exchange between two trading partners.	
eRecord	A record created, generated, sent, communicated, received, or stored digitally.	
eRecording	The act of recording the security instrument electronically with the county recorder or similar jurisdictional authority	
eServicing	The servicing of an electronic mortgage. To date the implications of servicing electronic mortgages seem minimal on a performing loan. The nuances of pursuing foreclosure using electronic mortgage documentation need to still be addressed.	
eUnderwriting	The act of underwriting a loan through electronic means. Today, automated underwriting tools allow the credit package of a loan to be underwritten and electronically scored. The future of electronic mortgages expands this opportunity to obtaining income documentation and validation through electronic interface, asset validation through electronic interface and collateral assessments through electronic documentation and interface. All these factors will ultimately comprise what will be known as e-underwriting	

eVault Implementation Guide

Term	Definition	Examples/Comments
eVault	A transferable records management solution that meets E-SIGN, UETA, and other compliance requirements. The concept is similar to a paper vault run by the document custodian industry today. In addition to the transferable records, the solution may support other types of eDocuments.	Because there will be multiple eVaults, there is a need for national registry service (MERS® eRegistry) to manage the authoritativeness of records.
Frame Relay Circuit	Type of interface that supports data encryption between two systems	
GIF	Graphics Interchange File Format	
HSM	Hardware Security Module used to store and manage Organizational-level digital certificates	
HTML	HyperText Markup Language – the <i>lingua franca</i> for publishing hypertext on the World Wide Web. It is a nonproprietary format based upon SGML, and can be created and processed by a wide range of tools, from simple text editors to sophisticated WYSIWYG authoring tools. HTML uses tags to structure text into headings, paragraphs, lists, hypertext links, etc. These tags determine the size, shape, coloring, and placement of text, graphics and sound on the web page, and can integrate the static page with dynamic content such as Java applets.	
Hybrid Mortgage	An electronic mortgage and a paper-based mortgage together. Specifically this means that parts of the transaction were conducted electronically (the borrower closing, generation of the promissory note and security instrument), but some part of it (other than the promissory note) is converted to paper (i.e. printing the security instrument for filing with the county recording office)	
Hybrid Operations	An operation that manages both paper and electronic documents.	
Image	A digitized presentation of a document or other text form. The image is only viewable, and data from within the image is only text.	PDF, JPEG, TIF
Investor Delegatee	MERS® eRegistry Members (typically Servicers) allowed to initiate certain transactions on eNote registration records on behalf of the Controller.	
JPEG or JPG	A graphics file format. The name comes from a standards body, the Joint Photographic Experts Group, because JPEG is an image compression standard for photographs.	
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.	
Logically Associated	The electronic equivalent of the attachment of a physical signature in the paper world.	

eVault Implementation Guide

Term	Definition	Examples/Comments
MERS® eRegistry	The system of record that identifies the owner (Controller) and custodian (Location) for registered eNotes.	
Metadata	Information about information. DTDs and markup tags of XML docs are metadata. Metadata is critical to support search and navigation capabilities.	
MIN	Mortgage Identification Number. The 18-digit number used to identify a loan on the MERS® System and the MERS® eRegistry.	
MISMO	The Mortgage Industry Standards Maintenance Organization, whose mission is to develop, promote, and maintain voluntary electronic commerce standards for the mortgage industry.	
Mortgage File	The promissory note, security instrument, consumer disclosures, title insurance policy, hazard insurance binder or certificate, flood zone certificate, appraisal or home valuation information, and other documents associated with a real-estate secured loan and/or customarily included in the loan documentation file created by the originating lender.	
Non-repudiation	A process to make sure customers cannot deny having been party to and accepting the terms of an online transaction, after the transaction has been conducted.	
Note holder	The person to whom the note was issued as original obligee or, if the note has been transferred, the current transferee entitled to enforce the note	
PDF	Portable Document Format	
Person	An individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government agency, public corporation, or any other legal or commercial entity	
Procedure or Process	Means the series of actions or steps necessary to perform a particular task or meet a particular requirement of these specifications. Except where applicable law or the context requires otherwise, a procedure may be deployed through electronic means, or involve steps or actions which are non-electronic, or a combination of the two.	
Protocol	Rules governing transmitting and receiving of Data	
Public Key Encryption	An encryption method requiring two unique software keys for decrypting data, one public and one private. Data is encrypted using the published public keys, and the unpublished private keys are used to decrypt the data.	
Record	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form	

eVault Implementation Guide

Term	Definition	Examples/Comments
Registry	A file, database, digital signature process or other electronic method for tracking information concerning use, access to and alteration of electronic records, including tracking the transfer of ownership of promissory notes and servicing among note holders and servicers, which is logically associated with the related electronic records.	
Scalability	Refers to how much a system can be expanded. The term by itself implies a positive capability. For example, "the device is known for its scalability" means that it can be made to serve a larger number of users without breaking down or requiring major changes in procedure.	
SISAC	Secure Identity Services Accreditation Corporation, responsible for accrediting digital identity credential issuers for the mortgage industry. SISAC is owned by the Mortgage Bankers Association.	
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.	
SSL	Secure Sockets Layer - a leading security protocol on the Internet. Developed by Netscape, it provides a secure link between a Web server and its communicating browser	
Tamper Evident Digital Signature	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.	Sometimes referred to as a "Tamper Evident Seal" or "Tamper Seal"
TIFF	Tagged Image File Format.	
Transfer to Paper	To convert an electronic document into paper format by printing it out. May imply converting the e-document permanently to paper, but not always.	
Transferable Record	An Electronic Record under E-SIGN 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 E-SIGN, relates to a loan secured by real property. A Transferable Record is also referred to as an eNote.	
Trusted Third Party	A person other than the note holder or servicer who is in the business of providing services intended to enhance (i) the trustworthiness of the process for signing electronic records using an electronic signature, or (ii) the integrity and reliability of the signed electronic records.	

eVault Implementation Guide

Term	Definition	Examples/Comments
VPN	Virtual Private Network – a secure connection over the Internet that supports data encryption between two systems	
Wrapping Wrapper?	To use an Encryption Key to authenticate the combination of an electronic record and existing electronic signatures associated with that electronic record, or to detect alterations to the combination of the electronic record and the prior electronic signatures, or to authenticate or detect alterations in a package of multiple electronic records	

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 is a simple, very flexible text format derived from SGML It is essentially a set of rules or convention for putting structured data in a text file. It is platform independent and therefore allows the computer to generate or read files easily. XML uses tags to delimit pieces of data, but leaves the interpretation of the data up to the application (hence the need for standardized DTDs in our industry if we are going to seamlessly exchange quality financial data).	
XML Schemas	XML Schemas express shared vocabularies and support rules based application processing. They provide a means for defining the structure, content and semantics of XML documents	

Appendix A

ESIGN and UETA Provisions Affecting Electronic Record Retention

ESIGN

- **ESIGN 101(e)¹ Accuracy and Ability to Retain Contracts and Other Records**—Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or ***enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.***
- **ESIGN 101(d) Retention of Contracts and Records: Accuracy and Accessibility**—If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that— ***(A) accurately reflects the information set forth in the contract or other record; and (B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.***
 - (2) EXCEPTION.—A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.
- **ESIGN 104(b)(3)(A) Performance Standards:** a Federal regulatory agency or State regulatory agency may interpret section 101(d) to specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained.
 - **ESIGN 104(b)(3)(B) Paper or Printed Form:** a Federal regulatory agency or State regulatory agency may interpret section 101(d) to require retention of a record in a tangible printed or paper form
- **ESIGN 101(c)(1)(D) Change in Hardware Software Requirements:** if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and (ii) again complies with subparagraph (C) [Hardware/Software Consent Disclosures].

¹ According to OCC, not necessarily a long-term retention issue.

- Legislative History
 - 106 H Rept 341
 - 105(c) describes the rules regarding retention of records in an electronic format. It states that when a law requires that a contract be in writing, that requirement is satisfied by an electronic record of the information in the record provided to the parties which: 1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and 2) remains capable of retention in a form that can be accessed for later reference and used to prove the terms of the agreement. This section provides that when a contract may be provided electronically, it shall be provided to each party to the contract in a manner in which it can be retained and used at a later time to prove the terms of the contract.
 - The exception contained in section 105(b) is apparently intending to prevent parties' agreements from overriding important consumer and other laws. However, the Amendment to H.R. 1714 as reported from the Subcommittee on Courts and Intellectual Property merely allowed electronic records and signatures to substitute for the pen and ink equivalents. All other legal requirements such as that notices or disclosures be "made," "delivered" or "actually received," that consumers be able to "retain" those notices or disclosures, or that particular statements be "clear and conspicuous" would be retained, unchanged. The obligation of businesses to demonstrate that they have satisfied those requirements would continue. It also would not change any of the substantive requirements of any consumer disclosure statute. These statutes require "reasonable notice." This could not be satisfied by sending notices and disclosures to a location where the consumer is not. A business could not claim that it satisfied the law by sending a notice to a physical address where the consumer does not reside. Similarly, a business could not satisfy "reasonable notice" requirements by sending an electronic notice to an email address that the consumer does not have.
 - 145 Cong Rec S 14881
 - Further, accurate copies of contracts must be delivered to consumers. The Abraham-Leahy substitute amendment therefore provides that if a law requires a contract to be in writing, an electronic record of the contract will not satisfy such law unless it is delivered to all parties in a form that can be retained for later reference and used to prove the terms of the agreement. This important provision is intended to protect consumers who execute contracts online, by ensuring that contracts are provided in a tamperproof, or "read-only" format. The delivery of any other type of electronic record would make it useless to prove its terms in court.
 - The basic rules of good faith and fair dealing apply to electronic commerce, and this Act should not be the basis upon which parties to a contract can be asked to agree to terms and conditions for using electronic signatures and electronic contracts which are unreasonable based on the circumstances surrounding the transaction. For example, when the parties have conducted a transaction entirely in person, the fine print of a form contract should not include an agreement that the contract can be provided electronically rather than on paper. In addition, companies must deliver to consumers electronic records of the contract in a form they can receive, retain, and use to prove the terms of an agreement. Such an electronic record would have to be provided in a "locked," or tamper proof, format.

- 146 Cong Rec H 4346
 - There is concern that S. 761 may actually create a new basis for denying legal effect to electronic records if they are not in a form that could be retained and accurately reproduced for later reference by any parties who are entitled to retain them. It is my hope, Mr. Speaker, that Congress will be able to respond effectively to these and other challenges that would be brought on by the rapidly changing nature of the Internet economy.
 - Retention of Contracts and Records.--Section 101(d)(1) and Section 104(b)(3). The Conferees added provisions that state: "if a statute, regulation, and other rule requires that a contract or other record relating to a transaction... be retained," the requirement is met by retaining an electronic record of the information that "accurately reflects the information" and "remains accessible" to all who are entitled to it "in a form that is capable of being accurately reproduced for later reference...." Moreover, Federal or State regulatory agencies may interpret this requirement to specify performance standards to "assure accuracy, record integrity, and accessibility of records that are required to be retained." Moreover, these performance standards can be specified in a manner that does not conform to the technology neutrality provisions, provided that the requirement serves, and is substantially related to the achievement of, an important governmental objective. These record retention provisions are essential to the capacity of federal and State regulatory and law enforcement agencies to ensure compliance with laws. For example, the only way in which a Government agency can determine if participants in large Government programs are complying with financial and other requirements of those programs may be to require that records be retained in a form that can be readily accessible to government auditors. Similarly, agencies must be able to require that companies implement anti-tampering protections to ensure that electronic records cannot be altered easily by money launderers or embezzlers or others seeking to hide their illegal activity. Without the ability of these agencies to ascertain program compliance through electronic record retention, taxpayers could be exposed to far greater risk of fraud and abuse. Similarly, bank and other financial regulators need to require that records be retained in order that their examiners can insure the safety and soundness of the institutions and their compliance with all relevant regulatory requirements. The standards set forth in the SEC's existing electronic recordkeeping rule, Rule 17a-4(f), such as the requirement that an electronic recordkeeping system preserve records in a non-rewritable and non-erasable manner, are essential to the SEC's investor protection mission and are consistent with the provisions of the conference report. The Conferees also expect the SEC to work with the securities self-regulatory organizations (SROs) to the extent necessary to ensure that accuracy, accessibility, and integrity standards also cover SRO recordkeeping requirements in an electronic environment.
- SEC Rule 17a-4(f) Excerpt
 - The records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.

eVault Implementation Guide

- For purposes of this section:
 - The term micrographic media means microfilm or microfiche, or any similar medium; and
 - The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and (f)(1)(ii) of this section, that meets the applicable conditions set forth in this paragraph (f).
- If electronic storage media is used by a member, broker, or dealer, it shall comply with the following requirements:
- The member, broker, or dealer must notify its examining authority designated pursuant to Section 17(d) of the Act prior to employing electronic storage media. If employing any electronic storage media other than optical disk technology (including CD-ROM), the member, broker, or dealer must notify its designated examining authority at least 90 days prior to employing such storage media. In either case, the member, broker, or dealer must provide its own representation or one from the storage medium vendor or other third party with appropriate expertise that the selected storage media meets the conditions set forth in this paragraph (f)(2).
- The electronic storage media must:
 - Preserve the records exclusively in a non-rewriteable, non-erasable format;
 - Verify automatically the quality and accuracy of the storage media recording process;
 - 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
 - Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.
- If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:
 - At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.
 - Be ready at all times to provide, and immediately provide, any facsimile enlargement which the Commission or its representatives may request.
 - Store separately from the original, a duplicate copy of the record stored on any medium acceptable under Rule 17a-4 for the time required.
 - Organize and index accurately all information maintained on both original and any duplicate storage media.

eVault Implementation Guide

- At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
 - Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.
 - Original and duplicate indexes must be preserved for the time required for the indexed records.
- The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.
 - At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
 - The audit results must be preserved for the time required for the audited records.
- The member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media; or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.
- Section 101(e) addresses statutory and regulatory requirements that certain records, including contracts, be in writing. The statute of frauds writing requirement exemplifies one such legal requirement. The section states that an electronic record or contract may be denied legal effect and enforceability under section 101(a) of this Act, if such an electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties entitled to retain that contract or record. This provision is intended to reach two qualities of "a writing" in the non-electronic world. The first such quality of "a writing" is that it can be retained, e.g., a contract can be filed. The second such quality of "a writing" is that it can be reproduced, e.g., a contract can be copied.
- Section 101(d) addresses statutory and regulatory record retention requirements. It states that when a statute, regulation, or other rule of law requires that a record, including a contract, be retained that requirement is satisfied by the retention of an electronic record, if two criteria are met. First, the electronic record must accurately reflect the information set forth in the contract or record required to be retained. Second, that electronic record must remain accessible to all parties who by law are entitled to access the record for the period set out in that law. Moreover, the electronic record must be in a form capable of accurate reproduction for later reference. ***The reproduction may be by way of transmission, printing or any other method of reproducing records.*** [Emphasis Added]
- 146 Cong Rec S 5281

- The subsection merely requires that if a statute requires a contract to be in writing, then the contract should be capable of being retained and accurately reproduced for later reference by those entitled to retain it. Thus if a customer enters into an electronic contract which was capable of being retained or reproduced, but the customer chooses to use a device such as a Palm Pilot or cellular phone that does not have a printer or a disk drive allowing the customer to make a copy of the contract at that particular time, this section is not invoked. The record was in a form that was capable of being retained and reproduced by the customer had it chosen to use a device allowing retention and reproduction.
- the records must, however, be capable of being accurately reproduced at the time that reference to them is required by law
- 146 Cong Rec S 5215
 - Most importantly, the conference report preserves substantial authority for Federal and State regulators with respect to record-keeping requirements. In a letter dated May 23, 2000, the Department of Justice expressed concern that an early draft of the conference report, produced by certain Republican conferees, would "seriously undermine the government's ability to investigate, try and convict criminals who alter or hide required records in programs such as Medicare, Medicaid, and federal environmental laws." The Department explained:
 - Record Retention. As presently drafted, the bill leaves the public at risk for serious waste, fraud, and abuse. For example, under the current bill, there is nothing to prevent a Medicare contractor from retaining its financial records on a spreadsheet (such as Excel or Quattro Pro). However, because those programs generally contain no security features to monitor changes to the files they create, anyone could change one number on a spreadsheet, which would then change all other numbers affected by the impermissible entry, reflecting a financial picture different from the reality. The government could have its hands tied in seeking to establish rules to ensure that such records could not be altered.
 - The Department's concerns regarding the Federal Government were shared by the States, whose regulators need and deserve the same flexibility as Federal regulators. This is particularly true in areas where the States are the primary regulators, as they are with respect to insurance and State-chartered banks. Having pressed this point throughout the conference, I am pleased that the final report treats Federal and State regulators with equal respect, and that it has won the support of the National Conference of State Legislatures.
 - Under earlier drafts of this conference report, as in H.R. 1714 as passed by the House, a requirement that a record be retained could be met by retaining an electronic record that accurately reflected the information set forth in the record "after it was first generated in its final form as an electronic record." By striking that final phrase, we made clear that agencies, through their interpretive authority, can ensure that electronic records remain accurate throughout the period that they are required by law to be retained. For additional certainty, we expressly authorized agencies to set performance standards to assure the accuracy, integrity, and accessibility of records that are required to be retained and, if necessary, to require retention of a record in paper form. We also delayed the effective date of the Act with respect to record retention requirements, to give agencies time to put in place appropriate regulations designed to assure effective and sustainable record retention, and to prevent companies from retaining

materials in any easily alterable form that they chose until regulations are forthcoming. Together, these changes will avoid facilitating lax record-keeping practices that could impede the enforcement of program requirements, anti-fraud statutes, environmental laws, and many other laws and regulations.

- Accuracy and Ability to Retain Contracts and Other Records, 101(e). The Conferees added new language in section (e) of 101 to establish that a contract or record which is required under other law to be in writing loses its legal validity unless it is provided electronically to each party in a manner which allows each party to retain and use it at a later time to prove the terms of the record.

UETA

- “Record.” This is a standard definition designed to embrace all means of communicating or storing information except human memory. It includes any method for storing or communicating information, including “writings.” **A record need not be indestructible or permanent, but the term does not include oral or other communications which are not stored or preserved by some means.** Information that has not been retained other than through human memory does not qualify as a record. As in the case of the terms “writing” or “written,” the term “record” does not establish the purposes, permitted uses or legal effect which a record may have under any particular provision of substantive law. ABA Report on Use of the Term “Record,” October 1, 1996. [Emphasis Added]
- Retention of Electronic Records; Originals. (a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which: (1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and (2) remains accessible for later reference. (b) A requirement to retain a record in accordance with subsection (a) does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received. (c) A person may satisfy subsection (a) by using the services of another person if the requirements of that subsection are satisfied. (d) If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection (a). (e) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (a). (f) A record retained as an electronic record in accordance with subsection (a) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this [Act] specifically prohibits the use of an electronic record for the specified purpose. (g) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of a record subject to the agency’s jurisdiction. Source: UNCITRAL Model Law On Electronic Commerce Articles 8 and 10.
- Comment 3 to UETA Section 12
 - Subsection (a) requires accuracy and the ability to access at a later time. The requirement of accuracy is derived from the Uniform and Federal Rules of Evidence. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems. It is not unlikely that within the span of 5-10 years (a period during which retention of much information is required) a corporation may evolve through one or more generations of technology. More to the point, this technology may be incompatible with each other necessitating the reconversion of information from one system to the other.
 - For example, certain operating systems from the early 1980’s, e.g., memory typewriters, became obsolete with the development of personal computers. The information originally

stored on the memory typewriter would need to be converted to the personal computer system in a way meeting the standards for accuracy contemplated by this section. It is also possible that the medium on which the information is stored is less stable. For example, information stored on floppy discs is generally less stable, and subject to a greater threat of disintegration, than information stored on a computer hard drive. In either case, the continuing accessibility issue must be satisfied to validate information stored by electronic means under this section.

- This section permits parties to convert original written records to electronic records for retention so long as the requirements of subsection (a) are satisfied. Accordingly, in the absence of specific requirements to retain written records, written records may be destroyed once saved as electronic records satisfying the requirements of this section.
 - The subsection refers to the information contained in an electronic record, rather than relying on the term electronic record, as a matter of clarity that the critical aspect in retention is the information itself. What information must be retained is determined by the purpose for which the information is needed. If the addressing and pathway information regarding an e-mail is relevant, then that information should also be retained. However if it is the substance of the e-mail that is relevant, only that information need be retained. Of course, wise record retention would include all such information since what information will be relevant at a later time will not be known.
- Comment 3 to UETA Section 8
 - The policies underlying laws requiring the provision of information in writing warrant the imposition of an additional burden on the sender to make the information available in a manner which will permit subsequent reference.
 - It is left for the courts to determine whether the sender has complied with this subsection if evidence demonstrates that it is something peculiar to the recipient's system which precludes subsequent reference to the information.
 - Comment 1 to UETA Section 16
 - The importance of facilitating the development of systems which will permit electronic equivalents is a function of cost, efficiency and safety for the records. The storage cost and space needed for the billions of paper notes and documents is phenomenal. Further, natural disasters can wreak havoc on the ability to meet legal requirements for retaining, retrieving and delivering paper instruments. The development of electronic systems meeting the rigorous standards of this section will permit retention of copies which reflect the same integrity as the original. As a result storage, transmission and other costs will be reduced, while security and the ability to satisfy legal requirements governing such paper records will be enhanced.

Federal Reserve Board (FRB)

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, Appendix D-2 (State Member Banks), 12 CFR Part 208
- FRB Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Edge or agreement corporation), 12 CFR 211.5 N/A
- FRB Interagency Guidelines Establishing Standards for Safeguarding Customer Information (uninsured state-licensed branch or agency of a foreign bank), 12 CFR 211.24 N/A
- Interagency Guidelines Establishing Standards for Safeguarding Customer Information (bank holding companies and their non-bank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), 12 CFR Part 225 Appendix F
- Standards for Safeguarding Customer Information, SR Letter 01–15

Federal Deposit Insurance Corporation (FDIC)

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 CFR Part 364 Appendix B
- Electronic Banking Examination Procedures, FIL–14–97
- Electronic Commerce and Consumer Privacy, FIL–86–98
- Electronic Financial Services and Consumer Compliance, FIL–79–98
- Electronic Signatures in Global and National Commerce Act, FIL–72–2000
- Weblinking, FIL-30-2003

Office of the Comptroller of the Currency (OCC)

- Electronic Activities, 12 CFR Part 7, Subpart E
- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 CFR Part 30, Appendix B
- Authentication in an Electronic Banking Environment, OCC Advisory Letter 2001–8
- Network Security Vulnerabilities, OCC Alert 2001–04
- OCC Advisory Letter 2004-11: Electronic Consumer Disclosures and Notices
 - Determine whether E-SIGN consent provisions apply to specified disclosures, and comply when appropriate
 - Develop effective notice for non-E-SIGN consent disclosures
 - Ensure electronic disclosures comply with the timing, format, content, and recordkeeping requirements of the underlying substantive rule
 - Factors for Evaluating Technology
 - Reasonably be expected to reliably deliver disclosures to consumers
 - Maintain the security of sensitive customer information
 - Limit or prevent fraudulent and other illegal activities
 - Provide disclosures in a form that consumers can retain
- OCC Advisory Letter 2004-9: Electronic Record Keeping

- Electronic Record Retention Systems
 - Potential use in litigation support
 - It is an unsafe and unsound practice if the bank fails to maintain loan documentation that, among other things, ensures that the bank's claims against its borrowers are legally enforceable
 - Records must be sufficient to ensure admissibility in relevant courts
 - Standards for admissibility of electronic records can vary from state to state
- Internal and external audits and controls
- Bank supervision
- Compliance with regulatory requirements
 - Inadequate record retention systems may result in compliance violations
- Security
 - The failure to properly secure and protect bank electronic record retention systems that contain confidential customer information will violate the minimum security standards imposed under section 501(b) of the Gramm-Leach-Bliley Act (GLBA).

Office of Thrift Supervision (OTS)

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 CFR Part 570 Appendix B
- Electronic Operations, 12 CFR Part 555
- Privacy of Consumer Financial Information, 12 CFR Part 573
- Security Procedures Under the Bank Protection Act, 12 CFR Part 568
- Suspicious Activity Reports and Other Reports and Statements, 12 CFR 563.180
- Identity Theft and Pretext Calling, CEO Ltr 139
- Interagency Guidance on Authentication in an Electronic Banking Environment (transmits FFIEC document, Authentication in an Electronic Banking Environment), CEO Ltr 143
- Interagency Guidance: Privacy of Consumer Financial Information, CEO Ltr 155
- Interagency Statement on Branch Names, CEO Ltr 86
- Policy Statement on Privacy and Accuracy of Personal Customer Information and Interagency Pretext Phone Calling Memorandum, CEO Ltr 97
- Statement on On-Line Personal Computer Banking, CEO Ltr 70
 - Transactional Web Sites, CEO Ltr 109

Freddie Mac Preliminary Specification on Electronic Mortgage Loan Documentation

- The System must maintain a high degree of security relative to both the physical environment and the protection of data. Guiding principles relevant to sound practices and System compliance must meet, or exceed, examination guidelines defined in the **Federal Financial Institutions Examination Council's (FFIEC) Information Systems Examination Handbook**, found in but not limited to, Chapters 13, 14 and 15. Additional resource material published by the **Federal Deposit Insurance Corporation's Division of Supervision regarding Electronic Banking Safety and Soundness Examination Procedures** is also useful resource material.
- The highest level of physical security in definition and practice addressing access control, surveillance, fire suppression, water detection, etc. for Transferable Records
- The Seller is responsible for providing appropriate cross references from the written Mortgage File to the associated Electronic Records, and from the Electronic Records to the written Mortgage File
- The System must be designed to control access to the Electronic Records. The System and file formats should be designed to insure that the data may be effectively stored on multiple types of media, including magnetic hard drives, CDs and DVDs, as well as mass storage devices anticipated at the time the System is developed. File formats should be designed so that the data may be converted and viewed across multiple operating System platforms. Software and System licenses should include the obligation to support conversion of existing data if existing software is upgraded or new versions are released.

Standards and Procedures for Electronic Records and Signatures (SPeRS)

SPeRS (Standards and Procedures for Electronic Records and Signatures) is a cross-industry initiative to establish commonly understood "rules of the road" or guidelines for using and accepting electronic records and signatures.

With the statutory framework in place for the enforceability of electronic records and signatures firmly established by the Federal E-sign Legislation (ESIGN) and the rapid adoption of the Uniform Electronic Transactions Act (UETA), businesses must now invest significant time, effort and manpower in answering the questions of how to handle the practical, routine aspects of electronic transactions.

The SPeRS guidelines provide concrete, practical, technology-neutral advice and strategies for understanding the legislation, recognizing the pitfalls, and answering the questions that might not be readily apparent in issues such as:

- Understanding the risks and liabilities associate with accepting and using a PIN or password.
- Obtaining a consumer's consent to use electronic records and signatures.
- Selecting a signature process that is appropriate for the transaction.
- Establishing the intent to sign an electronic record.
- Effectively delivering information in an electronic environment.
- Using hyperlinks and other devices used in referencing, displaying, and drawing attention to information and disclosures.

- Describing and offering the option to download or print out documents the transaction participant is entitled to retain.

Application of ESIGN to Existing Acts and Regulations

- *Application of the Electronic Signatures in Global and National Commerce Act to Record Retention Requirements Pertaining to Issuers Under the Securities Act of 1933, Securities Exchange Act of 1934 and Regulation S-T, SEC, June 14, 2001*

Appendix B

Frequently Asked Questions (FAQ)

Can the MERS® eRegistry be used to hold eNotes?

No, the MERS® eRegistry is the system of record to identify the Controller and Location of an eNote. An eNote is stored in an eVault owned by the Controller of the asset or the managed through a third-party relationship such as document custodian.

What is “Location” on the MERS® eRegistry?

“Location” identifies the organization that stores the Authoritative Copy of the eNote. That organization is identified by the 7-digit MERS-assigned Org ID. The Controller of the Authoritative Copy may choose to specify its own Org ID as the Location, or a designated Custodian.

What is an eVault?

eVault is a transferable records (aka “eNotes”) and/or electronic records management solution that meets E-SIGN , 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 eVaults, there is a need for a national registry service (MERS® eRegistry) to manage the authoritativeness of the eNote. In addition to the transferable records, the solution may support other types of eDocuments.

How can you transfer an eNote in the eMortgage world?

There are three types of transfers in the eMortgage world: inter-vault transfers without ownership change, intra-vault ownership change transfers, and inter-vault transfers with ownership change. The transfer of an eNote is reported to the MERS® eRegistry through a Transfer of Location transaction. A transfer of Location transaction is initiated by the Controller or its Delegatee on the MERS® eRegistry. The receiving eVault must confirm the transfer.

Please refer to Chapter 5 of this guide to learn more about transfer activities or interactions between two eVaults.

How does a document custodian interact with the MERS® eRegistry?

A document custodian will only interact with the MERS® eRegistry for the following reasons: confirm Transfer of Location into the eVault, and receive of Transfer of Control. The document custodian's eVault (the pending Location) will receive a notification from the MERS® eRegistry of a Transfer of Location transaction which is initiated by the Controller or its Delegatee; send the MERS® eRegistry an accept or reject confirmation, and physically transfer or receive the eNotes on the effective transfer date in the eVault. At the effective date, all rights holders will receive a notification of transfer completion from the MERS® eRegistry. The eVault may contract with a 3rd party to perform their transactions.

What technology does the eVault need to interact with the MERS® eRegistry system?

The following technology is needed in an eVault to conduct business with the MERS® eRegistry:

1. The entity interacting with the MERS® eRegistry must establish either a VPN or Frame Relay connection.
2. All transactions with the MERS® eRegistry must be signed with an Individual (medium or high assurance level) or an Organizational (medium assurance level) digital certificate issued by a SISAC-accredited Issuing Authority.
3. The eVault must be able to send and receive transaction messages in XML format that contains DTDs that illustrate and identify each transaction request.

For more information on how to interact with the MERS® eRegistry system visit MERS' web site (www.mersinc.org).

What is a digital certificate?

A *digital certificate* is an electronic file that establishes your credentials for web transactions. Digital "certs" are issued by a Certification Authority (CA) and contain reference information to allow verification of the certificates' validity.

How can I obtain a digital certificate for an eVault?

Digital certificates are sold through an Accredited Issuing Authority (AIA). SISAC issues accreditations based on specified requirements developed through the organization. The only accredited issuer for a digital certificate today is VeriSign.

For more information on digital certificates and how to obtain them, visit the SISAC web site (www.sisac.org).

What is the intrinsic value of an eDocument? Will the Authoritative Copy of the eNote be required by investors?

A document in an electronic form reduces the amount of data errors between systems by eliminating the need for manual data entry. An eNote can reduce the amount of lost notes, therefore reducing lost note affidavits and lost note bonds. An eNote can reduce fraud. For example, with only one authoritative copy of an eNote defined by the tamper evident digital signature, hash value and the MERS® eRegistry system, copying of an eNote is less likely than a paper note and double pledging will not occur. Funding will be more efficient because the closing, transfer, review, and certification can occur in the same day. A same day process can collapse the current business practice of wet funding. Processes with an eNote and other eDocuments can increase the efficiency of a business therefore increasing profit.

How does an eNote reduce fraud?

Electronic documents in an electronic closing environment cannot fully prevent fraud from a title company or from the eClosing service company. The MERS® eRegistry system can help reduce fraudulent claims on eNotes by pointing to the only authoritative copy of the eNote. At an eClosing an eMortgage must be tamper-evident sealed and the eNote registered almost immediately after being electronically signed. The tamper-evident digital signature only provides evidence of changes to the eNote, therefore an eNote will not necessarily reduce fraud without the tamper-evident digital signature.

What if there is a discrepancy between the eVault and MERS® eRegistry?

There should not be a discrepancy between the two systems. However, if a discrepancy occurs, the MERS® eRegistry is the legal system of recording the Controller and Location of the authoritative copy of the eNote.

What are the different forms a mortgage will look like in the future?

Currently, the industry is willing to accept eNotes. Standards and guidelines for other specific electronic documents have not been established. There are three types of mortgages in the future: loans with all eDocuments, a hybrid loan with an eNote and paper documents, and a loan with all paper documents. Hybrid loans will be accepted during the transition period in the industry where eNotes are currently recognized in the industry as documents are developed electronically.

While the eNote is in a SMART Doc™ format, how will businesses accommodate trailing paper documents?

The trailing paper documents can continue to be processed the same way they are today. A system will continue to be needed to track and report paper trailing documents in the same manner they are today.

How are reviews and certifications of eDocuments managed in an eVault?

Electronic documents and certifications will continue to be completed according to investor guidelines and agreements between the document custodian and investor. An eVault should have the ability to track transactions, validate data and report on eDocuments or communicate with a system that can.

How are exceptions handled with eDocuments?

Exceptions for eDocuments will continue to be based on investor guidelines. Assuming loans will be hybrid for the next several years, exceptions should be tracked on the eVault or document tracking system and reported in the same fashion they are today.

How can an eNote be viewed from an eVault?

Authorized parties will be able to view eNotes per agreements between interested parties. A request can be made to see the eNote. An official copy of the authoritative copy of the eNote is produced for the requestor to view in an electronic format.

Can you view an eNote from the MERS® eRegistry?

No. The MERS® eRegistry does not store copies of eNotes.

Can an eVault store imaged documents?

The technology of an eVault will typically allow imaged documents to be stored. It is the controlling party of the asset's decision to store imaged documents in an eVault. This decision is likely to be based on investor requirements. For example, in a private security, investors typically only accept original documents and the paper document would still need to be stored in a physical vault. Existing agreements would need to be updated to allow an imaged document to replace an original paper document.

In today's model, if the note is determined to be incorrect, the paper note is destroyed and a corrected copy produced to replace it. In an eNote environment, how is this procedure managed?

The process to correct the authoritative copy of the eNote is dependent on if the eNote has already been registered on the MERS® eRegistry.

If an eNote has not yet been registered, the Lender will create a corrected SMART Doc™ eNote and go through the signing event again. The corrected eNote will then get registered.

If an eNote has been registered, a "Change Status" request can be made to the MERS® eRegistry from the Controller or its Delegatee with the action type of registration reversal. The Controller will create a corrected SMART Doc™ eNote and it will then be re-registered (assuming the same MIN will be used).

Who is responsible for converting an eNote to paper?

The Controller or its Delegatee is responsible for converting an eNote to paper. The Controller or its Delegatee initiates a "Change Status" request to the MERS® eRegistry. The submitting party receives a confirmation back from the MERS® eRegistry. For guidance on the legal aspects of converting an eNote to paper, see your legal counsel.

How does a bailee letter apply to the eMortgage world?

The value of a bailee letter is the legal language designed to obligate various parties to adhere to the statements made in the letter. Bailee letters may still apply to private investors in the eMortgage world. The issue of bailee letters will depend on each individual company's practice with an investor. Freddie Mac, for example does not embrace bailee letters. For more information on Freddie Mac's practices on bailee letters please review Chapter 19 of their Single-Family Seller/Servicer Guide, Volume 1.

Currently, MERS is considering including rules and procedures analogous to bailee letter information in the MERS® eRegistry.

What happens when an eDocument is missing from an eVault?

If an eDocument is missing from an eVault, the eVault operator would first check the backup data, archives, and transaction activity. Such data or electronic recovery practices and policies need to be fully documented and tested through business continuity and technology risk management per company and regulatory guidelines. If applicable, a lost note affidavit or lost note bond can still be created.

What existing laws apply to an eVault?

Types of laws include eCommerce laws (ESIGN, UETA), as well as privacy, security, record retention, and rules of admissibility. See Chapter 2 for more complete information.

How do ESIGN and UETA differ?

ESIGN was enacted in 2000 to facilitate the use of electronic records and signatures in e-Commerce. ESIGN adopts the most significant provisions of UETA, provides consumer consent standards by legitimizing electronic disclosures for purposes of federal disclosure requirements, and sets boundaries for regulatory authority. UETA is currently enacted in 47 states and was initially approved by the National Conference of Commissioners on Uniform State Laws in 1999. UETA is adopted at a state level and authorizes electronic signatures and replacing writings with electronic records. ESIGN allows the state to modify, limit, or supersede UETA, or adopt a state alternative that is consistent with ESIGN.

For more information on ESIGN and UETA, please refer to Chapter 2 and Appendix A of this I-Guide.

What regulatory bodies will oversee a document custodian who offers eVault services?

The same regulatory bodies that oversee document custodians in a paper world will continue to regulate document custodians in an eMortgage world.

What legal guidelines have been provided for electronic record keeping?

Aside from the provisions of ESIGN and UETA, the Office of the Comptroller of the Currency (OCC) has developed an advisory letter on electronic record keeping. The advisory provides a basic overview of considerations a company should make when retaining electronic documents.

SPeRS (Standards and Procedures for Electronic Records and Signatures) was formed by the Electronic Financial Services Council to develop guidelines for implementing electronic signatures, consumer disclosure and consent, records retention, printing, delivery, and presentation of information. The SPeRS manual can be ordered at www.spers.org.

In 2001, the Federal Reserve Board issued an interim rule to establish standards for electronic disclosures to consumers for lenders to comply with ESIGN. These interim rules have never been finalized but remain a good source for compliance advice.

For a copy of the advisory letter from the OCC visit www.occ.gov. For a copy of the SPeRS manual or to learn more about SPeRS visit www.spers.org. For more information on the Federal Reserve Board visit www.federalreserve.gov.

Are there any document custody guidelines available today for an eMortgage from investors?

There have been no specific document custody requirements acknowledged in the industry today. Preliminary document custodian guidelines have been addressed by Freddie Mac and Fannie Mae. No investor from a whole loan perspective has publicly developed document custody requirements.

To see an overview of the GSE guidelines please refer to Chapter 3 of this I-Guide.