# MERS® eRegistry Procedures Manual

Release 16.25

Effective Date: February 10, 2020

# Contents

# Introduction

This document, the *MERS® eRegistry Procedures Manual* ("*Procedures*"), sets forth the operating procedures and Quality Assurance ("QA") Program for the *MERS® eRegistry*. The Procedures supplement the requirements specified in the *MERS® eRegistry Addendum to MERS® System Membership Agreement* ("MERS® eRegistry Addendum"). This version of the Procedures replaces and supersedes, in their entirety, any and all previously published Procedures in place up to the effective date noted on the cover page. Each *MERS® eRegistry Participant* ("Participant") is bound by the Procedures and any amendments made to it.

The MERS® eRegistry is one (1) of multiple functions utilized by Participants to satisfy the control requirement of Section 201(c) of the *E-SIGN* Act and Section 16(c) of the *UETA* with respect to a transferable record ("*eNote*"). Its role is to be the *System of Record* to identify the Participant that has *Control* of the eNote and the *Location*. Each Participant is responsible for determining that all the functions, including the MERS® eRegistry as set forth herein, utilized by the Participant and its service provider(s) constitute a system that satisfies the control requirements of Section 201(c) of the E-SIGN Act and Section 16(c) of the UETA.

## Structure

Each chapter is generally organized into the following sections:

- *Overview:* Gives a brief description of the process or function and how it relates to the MERS® eRegistry.
- *Requirements:* States what information, actions, and access are required to complete the business process.
- *Procedure:* Gives a step-by-step view of the process, including business-related steps and general MERS® eRegistry instruction.
- *Audit Information:* A full audit trail of information flowing to and from the MERS® eRegistry is captured for all changes made to an eNote Record. This section lists the information reflected in the audit trail for an eNote Record as a result of the corresponding transaction.

In addition, certain items have special formatting to allow the reader to quickly identify them:

- *Glossary Terms*: Terms defined in the glossary have the first letter of each word in the term capitalized. The first time a glossary term is used in the document, it is formatted as a dotted underline link to the Glossary entry (e.g., *Digital Signature*).
- *Configuration Options*: MERS® eRegistry configuration options are formatted in bold font (e.g., **eRegistry Participant** option).
- *Transactions, Notifications, Confirmations, eNote statuses, and Action Types*: MERS® eRegistry Transactions, *Notifications*, *Confirmations*, eNote statuses, and Action Types are formatted in italic font (e.g., *Change Status* transaction and *PaidOff*).

# Requirements for eNotes Registered on the MERS® eRegistry

MERSCORP Holdings has requirements for eNotes registered on the MERS® eRegistry.

- Each eNote must:
  - Be a *Transferable Record* as defined by E-SIGN and UETA,
  - Contain a valid, unique 18-digit MIN, and
  - Include language sufficient to definitively identify MERSCORP Holdings, Inc. as the entity maintaining the registry in which the identity of the first Controller and Location of the eNote will be recorded along with the identity of any subsequent Controller and/or Location.
- If a *Mortgage* for an eNote registered on the MERS® eRegistry is also registered on the MERS® System, the MIN on the MERS® System must match the MIN on the eNote.
- Certain types of electronic notes such as a Home Equity Line of Credit (HELOC) may not meet the definition of a Transferrable Record. Participants should consult their own legal counsel to ensure their objectives are achieved by registering specific products on the MERS® eRegistry. MERSCORP Holdings has the right to review and approve the types of loans to be registered to confirm that the products are suitable for registration on the MERS® eRegistry.

## Participants Providing eVaulting Services

The entity maintaining the *Authoritative Copy* of an eNote must have procedures in place sufficient to identify the single Authoritative Copy of the eNote it maintains from other copies of the eNote that may exist.

## Participants Named as Location

A Participant named as *Location* of an eNote must have procedures in place that ensure it has received a copy of the eNote and has validated the eNote's *Digital Signature* against the MERS® eRegistry after being named as Location in a *Registration* transaction and prior to being named in a *Transfer of Location* transaction. Likewise, each *Controller* must ensure that the Participant to be named as Location on each of its *eNote Records* has received a copy of the eNote, prior to being named as Location on the MERS® eRegistry.

## Location of Electronic Modifications, Note Addenda, Note Allonges

The terms of an eNote can be changed by electronic modification agreements, addenda, and allonges. When this occurs, these electronic documents may be vaulted with the same Location that is maintaining the Authoritative Copy of the eNote. The Controller should make the determination as to where such documents should be stored to meet the legal requirements for retaining *Control* of the modified eNote.

## Servicing-Agent Agreements

For Controllers that have elected to have another Participant perform certain MERS® eRegistry transactions on the Controller's behalf by being named in the Servicing Agent field on the eNote Record, it is expected that an agreement be in place between the Controller and the *Servicing Agent*. The agreement should specify that the Controller expressly authorizes the Servicing Agent to initiate transactions on the MERS® eRegistry on the Controller's behalf.

## Vendor Agreements

Many Participants use a *Vendor* to (1) enter data, initiate transactions, or register loans on the MERS® eRegistry on their behalf or (2) act as a technology provider enabling them to enter data, initiate transactions, or register loans on the MERS® eRegistry. In each capacity, the XML Requests submitted to the MERS® eRegistry name the Participant as the *Requesting Party*, the Vendor as the *Submitting Party*, and are signed with a *Digital Certificate* issued to the Vendor by a *Certificate Authority* approved by MERSCORP Holdings.

# eNote Record Overview

The following is an overview of how *eNote Records* are maintained on the MERS® eRegistry.

- When an *eNote* is registered, an eNote Record is created in the MERS® eRegistry database.
- While an eNote Record remains active, the appropriate *Authorized Rights Holder*:
    - Maintains the eNote Record data such that it matches the Participant's internal records.
    - Presents the eNote for *Digital Signature* validation if the SMART® Doc was not presented at *Registration*.
    - Reports any change of an Authorized Rights Holder using the appropriate *Transfer* transaction or *Change Data Update* transaction when applicable.
    - Reports any modification or assumption that occurs to the eNote.
    - May optionally record the document type and Digital Signature of another document associated with the eNote.
- Any Participant can validate the Digital Signature of a registered eNote by presenting it to the MERS® eRegistry.
- An eNote Record remains active until the eNote is paid off, charged off, transferred to another registry, or converted to a paper note at which time the eNote Record is deactivated by the appropriate Authorized Rights Holder on the MERS® eRegistry using the appropriate *Deactivation* transaction.

# Supporting Documentation

When reviewing the *Procedures*, Participants may refer to the following documents, which are available on *MERSCORP Holdings'* Member website *members.mersinc.org*:

- *MERS® eRegistry OnLine User Guide*: Provides instructions for using *MERS® eRegistry OnLine*.
- **MERS® eRegistry Integration Series**:

- *Programming Interface:* Provides the technical specifications for transacting with the MERS® eRegistry, including the XML *Digital Signature* specification.
- *Business Process Analysis:* Provides business processing information that corresponds to the information in the ***Programming Interface***, including examples of transfer scenarios.
- *MERS® eRegistry DTDs*: Transactions and *Notifications* are submitted to the MERS® eRegistry as *XML* messages (Requests and Responses) which are defined by the MERS® eRegistry *DTDs*.

# MERS® eRegistry Participation

## Overview

To become a MERS® eRegistry *Participant*, an organization must be a *MERS® System* Member ("Member") and agree to abide by the terms and conditions set forth in the *MERS® eRegistry Addendum* and *MERS® eRegistry Procedures*. Each Member that intends to become a Participant goes through an *Integration* process which includes security, *System-to-System* interface, and business considerations. MERSCORP Holdings, in its sole discretion, determines when an organization is ready to begin the Integration process.

If a Participant is already a MERS® System Member, some of these requirements may already have been met during its MERS® System Integration effort.

As defined by a contractual agreement, a Participant may grant security access to the MERS® eRegistry to one (1) or more *Vendors* to submit transactions on its behalf, to *Servicing Agents* to submit certain transactions for eNotes on which it is the *Controller*, to *Delegatee for Transfers* to register and transfer *Control* of eNotes on its behalf, to Participants to be named as *Secured Party* on its eNote Records, and to *Secured Party Delegatees* to perform certain MERS® eRegistry transactions on the Secured Party's behalf (see *Appendix A: Secured Party Terms and Conditions* for further details).

# MERS® eRegistry Integration

During Integration, a Participant or its *Vendor* will:

- Complete and submit the online *MERS® eRegistry Addendum* to *MERSCORP Holdings*.
- Secure a *Digital Certificate* from a *Certificate Authority* approved by MERSCORP Holdings for signing XML messages submitted to the MERS® eRegistry. For details, see *Transaction Security Requirements*.
- Establish and test connectivity to the MERS® eRegistry.
- Implement enhancements to its systems for originating, vaulting, selling, buying, and servicing eNotes, as applicable.
- Document revised business processes to reflect MERS® eRegistry activity.
- Test its systems enhancements internally and during the MERS® eRegistry Integration process.
- Obtain access to the *MERS® eRegistry OnLine* Integration region to learn how to view information in MERS® eRegistry OnLine.
- Identify the Participant's internal MERS® eRegistry System Administrator.
- Determine the *Member Profile* settings for the Participant's use of the MERS® eRegistry:
    - MERS® eRegistry System Addresses
    - MERS® eRegistry Notification Versions
    - Digital Certificate Information (if applicable)
    - eRegistry Relationships (See *Procedure: Maintaining Member Information* for descriptions.)

- Develop and implement a MERS® eRegistry Quality Assurance program in accordance with the requirements set forth in the *Procedures*. See MERS® eRegistry *Quality Assurance Program* for details.

# Authorized Rights Holders

*Authorized Rights Holders* are *Participants* associated with an *eNote* registered on the MERS® eRegistry and include the following:

- **Controller:** The Participant named on the MERS® eRegistry that has *Control* of the eNote and its *Authoritative Copy*.
- **Delegatee for Transfers:** The Participant named on the MERS® eRegistry that is authorized by the *Controller* to perform certain MERS® eRegistry transactions on the Controller's behalf.
- **Location:** The Participant named on the MERS® eRegistry that maintains the Authoritative Copy of the eNote.
- **Secured Party:** The Participant named on the MERS® eRegistry that has been sold, pledged, assigned, or granted a security interest in the eNote by the Controller.
- **Secured Party Delegatee:** The Participant authorized by the Secured Party to perform certain MERS® eRegistry transactions on the Secured Party's behalf.
- **Servicing Agent:** The Participant that is authorized by the Controller to perform certain MERS® eRegistry transactions on the Controller's behalf.

Each Participant named on an *eNote Record* can submit certain transactions to the MERS® eRegistry based on the Authorized Rights Holder position in which it is named. See *Authorized Rights Holder Processing Rules* for details.

## *eRegistry Relationships*

A Participant establishes one or more *eRegistry Relationships* in its Member Profile to identify its trading partners. Each *eRegistry Relationship* enables certain permissions or behaviors in the MERS® eRegistry as described in *Procedure: Maintaining Member Information*.

## *Controller Delegatee for Transfers Relationship*

The *Controller Delegatee for Transfers* relationship allows a Participant to be named as a *Delegatee for Transfers* on an eNote Record in order to perform certain transactions on behalf of the Controller (see *Authorized Rights Holder Processing Rules* for details). A Delegatee for Transfers must be any active Participant.

For a *Broker*, the Delegatee for Transfers uses the *Registration and Transfer of Control* transaction to register the eNote and immediately transfer Control to the Delegatee for Transfers. In this scenario, the Delegatee for Transfers is generally the Broker's *Investor*.

A Delegatee for Transfers can be named on an eNote Record through a *Registration* or *Data Update* transaction.

Unless removed, a Participant will continue to be named as the Delegatee for Transfers on an eNote Record if the Controller Delegatee for Transfers relationship exists with the current Controller.

A Participant is billed an annual membership fee for each Controller Delegatee for Transfers relationship it has with a Broker whose MERS® System membership is active.

## Secured Party Relationship

The *Secured Party* field may be used to indicate that the Controller of an *eNote Record* has sold, pledged, assigned, or granted an interest in the eNote to another Participant without that Participant being named in the Controller field.

A Participant can be named as a Secured Party on an eNote Record only if both of the following eRegistry relationships exist between the Controller and Secured Party:

- The Secured Party must have the **Secured Party Controller** relationship with the Controller.
- The Controller must have the **Controller Acknowledges Secured Party** relationship with the Secured Party.

A Participant named in the Secured Party field can:

- Perform transactions to its eNote Records to protect and release its secured interest.
- Access information about its eNote Records.
- Initiate any *Transfer* transaction except a stand-alone *Transfer of Servicing Agent* for one of its eNotes Records and must confirm any of these transfers that it or its *Secured Party Delegatee* did not initiate.

An eNote Record naming a Secured Party cannot be deactivated on the MERS® eRegistry unless the Secured Party permits the deactivation of its eNote Records in its Member Profile.

A Secured Party can designate a Secured Party Delegatee on its eNote Records. The following requirements apply:

- A Secured Party Delegatee can be named in a *Registration* transaction by the Controller.
- The Secured Party can add a Secured Party Delegatee post Registration.
- The Secured Party must have a **Secured Party Delegatee** relationship with the Secured Party Delegatee.

A Secured Party or Secured Party Delegatee cannot have a *Line of Business* of *Vendor* or *Broker*.

# Participant Requirements

The following requirements apply to any Participant submitting a transaction to the MERS® eRegistry as a *Requesting Party* or *Submitting Party*, any Participant being named as an *Authorized Rights Holder* on an eNote Record, and any Participant included in a *MERS® eDelivery* transaction:

- The Status of the Participant's Org ID must be 'Active' on the MERS® eRegistry.
- For MERS® eRegistry transactions, the **eRegistry Participant** indicator in the Participant's Member Profile must be enabled.
- For MERS® eDelivery transactions, the **eDelivery Participant** indicator in the Participant's Member Profile must be enabled.

In addition, for any Participant submitting a transaction to the MERS® eRegistry for an eNote Record on which it is named an Authorized Rights Holder, the MERS® eRegistry verifies that the appropriate eRegistry relationship is in place before accepting the transaction for processing. If the appropriate eRegistry relationship is not in place, the transaction is rejected. See *Procedure: Maintaining Member Information* for the list of available eRegistry relationships and *Authorized Rights Holder Processing Rules* for the list of transactions that each Authorized Rights Holder can submit to the MERS® eRegistry.

# Secured Party Certificate Form Process

The MERS® eRegistry *Secured Party Certificate Form* ("*Certificate Form*"), available on the Member website, allows an authorized representative of a Participant to request that MERSCORP Holdings name the Participant as the Secured Party on one or more eNote Records when the Controller will not take such action.

If the Participant has exhausted good faith efforts to resolve a dispute pertaining to use of the Secured Party field on the MERS® eRegistry, it may use the *Certificate Form* to request that MERSCORP Holdings perform the transaction(s) on the MERS® eRegistry to name the Participant in the Secured Party field, and its delegatee in the Secured Party Delegatee field, as applicable, for the eNote Records specified in the *Certificate Form*. The completed *Certificate Form* is submitted to MERSCORP Holdings using the email address *certificates@mersinc.org.*

A Secured Party Delegatee may not submit a *Certificate Form* on behalf of a Secured Party. No confirmation from the other Participant named in the Controller field or any other Authorized Rights Holder on the MERS® eRegistry for the eNote Records identified in the *Certificate Form*, shall be required in order for MERSCORP Holdings to perform the requested transaction(s) pursuant to this *Certificate Form* process. Additionally, in no event will MERSCORP Holdings be obligated to perform the transaction(s) requested in the *Certificate Form* to the extent a third-party Participant, other than the Participant with whom the **Secured Party Controller** relationship was established, is named on the MERS® eRegistry in the Controller field for the eNote record at the time the *Certificate Form* is received by MERSCORP Holdings. Please see the *Certificate Form* for additional terms and conditions.

# MERS® eRegistry Security

## Overview

The MERS® eRegistry security scheme includes safeguards for eNote transactions and online identity validation for viewing *eNote Records* on which a Participant is an *Authorized Rights Holder*.

## Transaction Security Requirements

- All XML Requests submitted by a Participant to the MERS® eRegistry must be digitally signed to apply a Tamper-Evident Digital Signature ("*Digital Signature*"). If an XML Request is not digitally signed, the MERS® eRegistry rejects it and will not process the transaction(s) in the Request.
- Only enveloped Digital Signatures are supported, not detached or enveloping Digital Signatures.
- The MERS® eRegistry applies a Digital Signature to all XML *Notifications* it sends to Participants.
- Vendors, and Participants setting up their own access to the MERS® eRegistry, must secure a *Digital Certificate* from a *Certificate Authority* approved by MERSCORP Holdings to sign the XML messages sent to the MERS® eRegistry. A "Medium Device Assurance" *PKI* signing certificate is used to digitally sign the XML messages.
- Strong security practices should be in place to ensure the integrity of the private key related to the Digital Certificate. Best practices include, but are not limited to, the following:
  - Securely protecting and controlling access to the private key
  - Securely storing the private key using a mechanism that includes encryption
  - Limiting the number of people authorized to access the private key and passphrase
  - Auditing changes made to the Digital Certificate and private key
  - Immediately revoking the Digital Certificate if the private key or certificate has been compromised.
- Additional Digital Certificate requirements:
  - The Organization Unit ('OU') attribute from the Subject field of the Digital Certificate in each XML message must match the data in the **Organization** field on the *eRegistry Certificate Information* page of the *Member Profile* of the Participant submitting the transaction. A Vendor sending a transaction on behalf of another Participant would use the Vendor's Digital Certificate, which would be compared to the Vendor's Member Profile.
  - Participants must implement adequate information security controls to ensure that only its authorized users and automated processes are able to trigger the creation and submission of XML messages to the MERS® eRegistry.
  - Participants must collect sufficient information on the transactions and users to be able to track the user or process that triggered the creation of the XML messages, and such information must be capable of being produced in a readable format and be retained.

# Authorized Rights Holder Processing Rules

The table below lists the available MERS® eRegistry transactions and indicates which *Authorized Rights Holders* are authorized to submit each transaction.

| Transaction | Controller | Location | Delegatee for Transfers | Secured Party | Secured Party Delegatee | Servicing Agent |
|---|---|---|---|---|---|---|
| Register eNote | Yes | No | Yes | No | No | No |
| Register eNote and Transfer of Control | No | No | Yes | No | No | No |
| Add Secured Party | Yes | No | No | No | No | No |
| Release Secured Party | No | No | No | Yes | Yes | No |
| Reverse Secured Party | No | No | No | Yes | Yes | No |
| Add Secured Party Delegatee | Yes | No | No | Yes | No | No |
| Change Secured Party Delegatee | No | No | No | Yes | No | No |
| Remove Secured Party Delegatee | No | No | No | Yes | Yes | No |
| Add Delegatee for Transfers | Yes | No | No | No | No | No |
| Change Delegatee for Transfers | Yes | No | No | No | No | No |
| Remove Delegatee for Transfers | Yes | No | Yes | No | No | No |
| Transfer Control (Initiate) | Yes | No | Yes | Yes | Yes | No |
| Transfer Location (Initiate) | Yes | No | No | Yes | Yes | Yes |
| Transfer Servicing Agent (Initiate) | No | No | No | No | No | Yes |
| Transfer Control and Location (Initiate) | Yes | No | Yes | Yes | Yes | No |
| Transfer Control and Servicing Agent (Initiate) | Yes | No | No | Yes | Yes | No |
| Transfer All (Initiate) | Yes | No | No | Yes | Yes | No |
| Update eNote Data | Yes | No | No | No | No | Yes |
| Present eNote | Yes | No | No | No | No | Yes |
| Add Servicing Agent | Yes | No | No | No | No | No |
| Change Servicing Agent | Yes | No | No | No | No | No |

| Transaction | Controller | Location | Delegatee for Transfers | Secured Party | Secured Party Delegatee | Servicing Agent |
|---|---|---|---|---|---|---|
| Remove Servicing Agent | Yes | No | No | No | No | No |
| Report Modification | Yes | No | No | No | No | Yes |
| Modification Reversal | Yes | No | No | No | No | Yes |
| Report Assumption | Yes | No | No | No | No | Yes |
| Assumption Reversal | Yes | No | No | No | No | Yes |
| Add Document | Yes | Yes | No | No | No | Yes |
| Add Document Reversal | Yes | Yes | No | No | No | Yes |
| Change Location | Yes | No | No | No | No | No |
| Charged Off Deactivation | Yes | No | No | No | No | Yes |
| Charged Off Deactivation Reversal | Yes | No | No | No | No | Yes |
| Converted To Paper Deactivation | Yes | No | No | No | No | Yes |
| Converted To Paper Deactivation Reversal | Yes | No | No | No | No | Yes |
| PaidOff Deactivation | Yes | No | No | No | No | Yes |
| PaidOff Deactivation Reversal | Yes | No | No | No | No | Yes |
| Transferred To Proprietary Registry Deactivation | Yes | No | No | No | No | Yes |
| Transferred To Proprietary Registry Deactivation Reversal | Yes | No | No | No | No | Yes |
| Registration Reversal | Yes | No | No | No | No | Yes |
| eNote Inquiry Request | Yes | Yes | Yes | Yes | Yes | Yes |
| Initiate eDelivery | Yes | Yes | Yes | Yes | Yes | Yes |
| Connectivity | Yes | Yes | Yes | Yes | Yes | Yes |

# MERS® eRegistry OnLine Security Requirements

There are three (3) levels of identity validation within the *MERS® eRegistry OnLine* security scheme:

- Org ID
- User ID
- User Password

Any attempt to access MERS® eRegistry OnLine is denied unless all three (3) tiers of security are provided by a user. The Org ID, which identifies a Participant, is assigned by MERSCORP Holdings when its MERS® System membership application is approved.

## MERS® eRegistry System Administrator

A Participant's internal MERS® eRegistry System Administrator is responsible for establishing and maintaining the security settings that control access to MERS® eRegistry OnLine, including the following User ID management tasks:

- Create and maintain a unique User ID for each employee that requires online access to MERS® eRegistry OnLine.
- Reset user passwords and re-enable disabled User IDs.
- Disable or delete User IDs that are no longer active.

See the *MERS® eRegistry OnLine User Guide* or *System Administrator QRG* for instructions.

# Member Information

## Overview

A *Participant* can view all the information in its *Member Profile* at any time. Some of this information is changed by a Participant through *MERS® OnLine*, and the remainder is changed by *MERSCORP Holdings*.

Member Profile changes are copied to the *MERS® eRegistry* at the start of each hour that the MERS® System is available and generally become effective once the copy is complete.

The following Member Profile configuration settings apply to both the *MERS® System* and the MERS® eRegistry:

- Password Expiration Days
- Minimum Response Length
- Minimum Password Length
- Automated Password Reset (APR)

A Participant's corporate name and *Org ID* is also shared between the two (2) applications.

## Member Information Requirements

- At least one person in the Participant's organization must have the access needed to maintain the Member Profile and be responsible for keeping that information accurate and current.
- At least monthly, a Participant is required to review and reconcile the information in its Member Profile related to the MERS® eRegistry to ensure that it is accurate and current.
- A Participant must have at least one (1) *MERS® eRegistry Contact* in its Member Profile. If a Participant has multiple eRegistry contacts, the **Title** field can be used to designate the specific role of each person (e.g. Technical, Business, or Signing Certificate Sponsor).

## Procedure: Maintaining Member Information

Refer to the *MERS® System Procedures Manual* for the list of Member Profile fields that a Participant is required to maintain that is not specific to the MERS® eRegistry. In addition, a Participant must maintain its MERS® eRegistry Contact(s) and the following eRegistry Relationships if used:

| eRegistry Relationship | Description |
|---|---|
| Auto-Confirm Transfer | The list of *Org IDs* from which a Participant will automatically accept transfers of *Control* and/or *Location* where the Org ID is named the current *Controller* of an *eNote Record*. |
| Controller Delegatee for Transfers | The list of Org IDs authorized to act as a *Delegatee for Transfers* on behalf of a Participant. See *Controller Delegatee for Transfers Relationship* for details. |

| eRegistry Relationship | Description |
|---|---|
| Vendor | The list of Org IDs authorized to act as a *Vendor* to submit transactions to the MERS® eRegistry on behalf of a Participant or that a Participant uses as a technology provider. |
| Secured Party Controller | The list of Org IDs in a *Secured Party's* Member Profile that are authorized to name the Participant the Secured Party on eNote Records where an Org ID in the list is the Controller.<br>A Controller in this list must also have the reciprocal **Controller Acknowledges Secured Party** relationship established with the Secured Party in order to name the Participant the Secured Party on its eNote Records.<br>Prior to removing a **Secured Party Controller** relationship with a Controller from its Member Profile, a Secured Party must ensure that there are no active eNote Records on the MERS® eRegistry that name the Participant the Secured Party for that Controller. |
| Controller Acknowledges Secured Party | The list of Org IDs in a Controller's Member Profile that the Participant has authorized to be named as the Secured Party on the Controller's eNote Records.<br>A Secured Party must have previously established a **Secured Party Controller** relationship with a Controller before that Controller can set up the reciprocal **Controller Acknowledges Secured Party** relationship with the Secured Party.<br>Once established, a Controller cannot remove the **Controller Acknowledges Secured Party** relationship with a Secured Party from its Member Profile until the Secured Party has removed the **Secured Party Controller** relationship with the Controller from its Member Profile. |
| Secured Party Delegatee | The list of Org IDs in a Secured Party's Member Profile authorized by the Participant to be named as the *Secured Party Delegatee* on eNote Records where the Participant is the Secured Party.<br>A Participant can be named as a Secured Party Delegatee only if the Secured Party is named on the eNote Record, and the Secured Party also has the **Secured Party Delegatee** relationship with the Secured Party Delegatee. |

# Procedure: Updating Member Information Maintained by MERSCORP Holdings

MERSCORP Holdings maintains certain information in the Member Profile related to the MERS® eRegistry as detailed in the table below. An authorized employee of the Participant must report these changes to MERSCORP Holdings using the *Change Request Form* on the Member website.

A Member Profile change made on the MERS® System may take up to two (2) business days to become effective on the MERS® eRegistry.

MERSCORP Holdings is also responsible for making changes to a Participant's corporate name on the MERS® eRegistry. Please review the *MERS® System Rules of Membership* for policies pertaining to these events. The *MERS® System Procedures Manual* contains instructions on how to submit a corporate name change request to MERSCORP Holdings.

| Member Profile Component | Field |
|---|---|
| eRegistry Certificate Information | Contains information from a Participant's Digital Certificate that is used to validate XML messages submitted to the MERS® eRegistry and MERS® eDelivery. In particular, the Organization Unit ('OU') attribute from the Subject field. |
| eRegistry Options | • *Allow Servicing Agents*: Allows a Controller to name other Participants as a *Servicing Agent* on its eNote Records to initiate transactions on the MERS® eRegistry on their behalf.<br>• **Allow eReports:** Allows a Participant to access the eReport functionality. Enabled for all Participants.<br>• **Auto-Confirm Transfer:** Allows a Participant to automatically accept transfers of Control and/or Location from the list of Controller Org IDs listed in the Auto-Confirm Transfer relationship section of its Member Profile.<br>• **Confirm All Servicing Agent Transfers:** When enabled, allows a Participant to confirm all Servicing Agent transfers that name the Participant as the new Servicing Agent.<br>• **eRegistry Participant:** Grants access to MERS® eRegistry.<br>• **Transfer Notifications:** Allows a Participant to receive *Transfer Notifications* for eNote Records on which it is named as a current or pending *Authorized Rights Holder*.<br>• **Non-Transfer Notifications:** Allows a Participant to receive Notifications for *Registration*, *Change Data*, and *Change Status* transactions for eNote Records on which it is named an Authorized Rights Holder.<br>Note: MERSCORP Holdings enables the **Non-Transfer Notifications** option for each Secured Party unless the Participant does not have an eVault to receive Notifications. |

| Member Profile Component | Field |
|---|---|
| | • **Secured Party Allows Deactivations:** The MERS® eRegistry allows eNote Records naming a Participant as Secured Party to be deactivated when this option is set to "Yes". Set to "No" by default. |
| External System Addresses | The list of URLs to which the MERS® eRegistry and MERS® eDelivery send *Notifications*. See *External System Addresses* for details. |
| eDelivery Options | eDelivery Participant: Grants access to MERS® eDelivery. |
| Notification Versions | Controls which supported DTD version the MERS® eRegistry uses to generate the XML *Notifications* that it sends to the Participant's external system address. Options are available for the following: • Registration • Change Data • Connectivity • Change Status • Transfers<br>The DTD version may be set to the current version or one version back depending on which version a Participant is able to support.<br>The **Notification Versions** settings must be configured with the DTD versions that a Participant's system supports. For Participants using a Vendor to submit transaction to the MERS® eRegistry, the **Notification Versions** settings must match the DTD versions that the Vendor's system supports. |

## External System Addresses

A Participant receives transfer and non-transfer *Notifications* based on its Member Profile configuration settings. The MERS® eRegistry and MERS® eDelivery send Notifications to a Participant using the HTTPS URL(s) listed in the External System Addresses section. A single URL may be used for one or more system addresses, or different URLs may be used for each. Each URL must point to an application that the Participant uses to interface with the MERS® eRegistry and must be available to accept Notifications.

| System Address | Used to send Notifications to an Org ID named … |
|---|---|
| Controller Address | Current or pending Controller |
| Servicing Agent Address | Current or pending Servicing Agent |
| Location Address | Current or pending Location |
| Delegatee for Transfers Address | Current Delegatee for Transfers |
| Secured Party Address | Current Secured Party |
| Secured Party Delegatee Address | Current Secured Party Delegatee |
| eDelivery | In eDelivery Notifications and Distributions |

# Mortgage Identification Number (MIN)

## Overview

The Mortgage Identification Number ("*MIN*") is an 18-digit number that uniquely identifies an eNote registered on the MERS® eRegistry. The MIN is a data point in an eNote and cannot be duplicated or reused, but it can be reactivated if it was inactivated in error. To process information on the MERS® eRegistry, the MIN associated with the eNote must be provided.

The MERS® eRegistry validates a MIN at registration by checking for duplicate MINs, ensuring the *Check Digit* is properly calculated, that the first seven (7) digits of the MIN match an active Org ID on the MERS® System, and that the MIN was not used to register a loan on the MERS® System before the MERS® eRegistry release date.

Many loan origination and document preparation solutions can generate MINs programmatically. If a Participant is currently using such a solution to generate MINs for use on the MERS® System, that system can also be used for the MERS® eRegistry so long as the same MIN is used to register any loan registered on both the MERS® eRegistry and the MERS® System.

Participants may also develop an in-house MIN generation function.

Additional information about the MIN is available in the *MERS® System Procedures Manual*. Instructions for calculating the Check Digit are in the *MERS® System Integration Handbook*.

## MIN Requirements

- A MIN is valid on the MERS® eRegistry if it:
  - Is an 18-digit number,
  - Begins with a 7-digit Org ID that is active on the MERS® System,
  - Ends with a valid Check Digit, and
  - Is not duplicated on the MERS® eRegistry.
- If an eNote registered on the MERS® eRegistry will be registered as a *Mortgage* loan on the MERS® System, the two registrations must use the same MIN. See *MIN Mismatch with MERS® System* for details on correcting this issue.

# eNote Registration

## Overview

The *Registration* transaction is used to submit the required information to the *MERS® eRegistry* to report that an *eNote* originated with the MERS® eRegistry language exists, thereby establishing the original *Lender* named in the executed eNote as the initial *Controller* and identifying the *Location* maintaining the *Authoritative Copy* of the eNote.

The MERS® eRegistry supports two types of *Registration* transactions:

- **Data Point Registration:** The *Registration* transaction does not present the *SMART® Doc* eNote to the MERS® eRegistry for *Digital Signature* validation. The eNote is presented for Digital Signature validation post registration using the *Data Update transaction*.
- **eMortgage Package Registration:** The *Registration* transaction presents the SMART® Doc eNote for Digital Signature validation by the MERS® eRegistry.

The result of a successful *Registration* transaction is the creation of an *eNote Record* for the eNote with a status of **Active** on the MERS® eRegistry.

The MERS® eRegistry audit trail captures the *Tamperseal Date* and the Registration Date, allowing trading partners to audit the elapsed time against their requirements.

The *Registration Reversal* transaction is used to reverse a *Registration* transaction. See the *Change Status* chapter for details.

A Participant can submit a single XML Request that contains one (1) or more eNote Registration transactions to the MERS® eRegistry. See the *Programming Interface Guide* for details on creating XML Requests with multiple eNote *Registration* transactions.

## Registration Requirements

To register an eNote, the registering *Participant* must follow these requirements:

- The first Controller named on an eNote Record must be the *Lender* named on the eNote.
- If the Participant registering an eNote is not named as the Controller, it must have the **Delegatee for Transfers** Relationship with the Controller and be named the Delegatee for Transfers in the *Registration* transaction.
- The first Controller or *Delegatee for Transfers* is required to register the eNote on the MERS® eRegistry no later than one (1) business day after the final tamper sealing of the eNote.
- For a *CEMA* eNote *Registration*, the CEMA eNote must be assigned a new *MIN*.
- The eNote must have the 18-digit MIN as the unique loan identifier.
- If present, the SMART® Doc must be in the *MISMO* SMART® Doc version 1.02 format, and must be digitally signed.

- The *Registration* transaction must include the *Tamperseal Date* of the Digital Signature associated with the eNote being registered.
- The following data elements must be included for each eNote being registered (either contained within a SMART® Doc, if sent, or contained in the *Registration* for each eNote):
  - Digital Signature of the eNote
  - Borrower Type – individual or entity
  - Borrower Name(s) – first and last, or entity Name
  - *SSN* (if individual) or *TIN* (if entity)
  - Street name, city, state, county, zip code of property
  - Lien Priority Type

**Note:** If the Borrower SSN or TIN is not included in the data section of the SMART® Doc, the data point payload of the XML message must include the complete Borrower information for the eNote, including Borrower SSN or TIN, for all Borrowers on the eNote. The Borrower information in the data point payload must exactly match the Borrower information in the data section of the SMART® Doc, with the sole exception that the Borrower SSN or TIN may be blank for each Borrower in the data section of the SMART® Doc.

- The data elements must have the following characteristics. (See *Registration Request and Response Documentation* in the Programming Interface Guide for specifics.)

| Org IDs associated with the Registration | |
|---|---|
| **Data Element** | **Special Considerations** |
| Submitting Party | Conditional. Required if the *Submitting Party* is not the *Requesting Party*.<br>Submitter's *Org ID* must be the same as the Requesting Party or have a *Vendor* relationship with the Requesting Party. |
| Requesting Party | Required. Requester's Org ID must be the Controller or the Participant must have the *Controller Delegatee for Transfers* relationship with the Controller. |
| Controller | Required. |
| Location | Required. |
| Servicing Agent | Conditional. Required if a *Servicing Agent* will perform certain MERS® eRegistry transactions on the Controller's behalf.<br>The Controller must have the **Allow Servicing Agents** option enabled in its *Member Profile*. |
| Delegatee for Transfers | Conditional. Required when a *Delegatee for Transfers* registers an eNote on behalf of a *Broker*. Can be the same as Requesting Party.<br>The Delegatee for Transfers must have the Controller Delegatee for Transfers relationship with the Controller. |

| Org IDs associated with the Registration | |
|---|---|
| **Data Element** | **Special Considerations** |
| Secured Party | Optional. The field is available for a Participant that requires its *Secured Party* interest in an eNote is reflected on the MERS® eRegistry.<br>• The Secured Party must have the **Secured Party Controller** relationship with the Controller.<br>• The Controller must have the **Controller Acknowledges Secured Party** relationship with the Secured Party.<br>• A Secured Party is not permitted in a *Registration and Transfer of Control* transaction. |
| Secured Party Delegatee | Optional. The field is available for a Secured Party that intends to rely on another Participant to perform certain MERS® eRegistry transactions on its behalf.<br>A Secured Party must be named in the *Registration* transaction, and the Secured Party must have the **Secured Party Delegatee** relationship with the *Secured Party Delegatee*. |

| Registration Record Data | |
|---|---|
| **Data Element** | **Special Considerations** |
| Vault Identifier | The *Vault Identifier* provides additional information for locating the Authoritative Copy of an eNote. |
| MIN | Must be a valid MIN on the MERS® eRegistry. See *MIN Requirements* for details. |
| Digital Signature | • Must meet *W3C* specifications.<br>• If a SMART® Doc is presented at the registration, the MERS® eRegistry validates the eNote's Digital Signature. Refer to *eNote Digital Signature Generation Options* for details. |
| Tamperseal Date | • Must meet W3C specifications.<br>• Must be valid. |
| Lien Priority Type | Either *First Lien* or *Other*. |

| Borrower Information | |
|---|---|
| **Data Element** | **Special Considerations** |
| Borrower Type | Y for Entity<br>N for Individual Borrower |

| Borrower Information | |
|---|---|
| **Data Element** | **Special Considerations** |
| First and Last Name of Individual<br>OR<br>Entity Name | Required if Borrower Type = N<br><br>Required if Borrower Type = Y |
| SSN<br>OR<br>TIN | Required if Borrower Type = N<br><br>Required if Borrower Type = Y |

| Property Information | |
|---|---|
| **Data Element** | **Special Considerations** |
| City | None |
| State | Only the two character state abbreviation is stored. If a state name is provided, it is converted to the abbreviation. If the correct abbreviation cannot be determined, the submitted value is truncated to the first two characters, and a warning message is returned in the Registration Response. |
| Postal Code | Must be in 5 or 9 digit format |
| County | None |

| Parsed Street Address | |
|---|---|
| **Data Element** | **Special Considerations** |
| Apartment or Unit | Conditionally required if the property address includes an apartment or unit number. |
| Direction Prefix | Specifies additional information before the street name, such as West or NE. Conditionally required if the property address includes a direction prefix. |
| Direction Suffix | Specifies additional information after the street name, such as East or SW. Conditionally required if the property address includes a direction suffix. |
| House Number | Conditionally required if the property address includes a house number. |
| Street Name | Required |

| Parsed Street Address | |
|---|---|
| **Data Element** | **Special Considerations** |
| Street Suffix | Additional information for the street name such as Street, Road, or Avenue. Conditionally required if the property address includes a street suffix. |

## *SMART® Doc eNote Digital Signature Validation Options*

The MERS® eRegistry currently supports Digital Signature validation only for eNotes in the SMART® Doc format. A SMART® Doc eNote can be presented for Digital Signature validation at *Registration* or post-*Registration* as described below:

1. For an *eMortgage Package Registration*, the eNote is included in the *Registration* transaction for Digital Signature validation.
2. For a *Data Point Registration*:
   - The Digital Signature of the eNote is included in the XML payload of the *Registration* transaction, but the eNote is not included.
   - Post Registration, the eNote is presented to the MERS® eRegistry for Digital Signature validation using the *Data Update* transaction.

For both presentation options:

- The MERS® eRegistry calculates the Digital Signature of the eNote when it is presented.
  - For an eMortgage Package Registration, the MERS® eRegistry compares its calculated Digital Signature value to the value in the SMART® Doc eNote.
  - For a Data Point Registration, the MERS® eRegistry compares its calculated Digital Signature value to the value in the SMART® Doc eNote and the value presented at Registration.
- If the calculated Digital Signature does not match the comparison values, the MERS® eRegistry rejects the *Update* or *Registration* transaction.
- If the calculated Digital Signature matches the comparison values, the MERS® eRegistry sets the *SMART® Doc Presented* flag on the eNote Record to indicate that the Digital Signature was successfully validated.
- The MERS® eRegistry processes the SMART® Doc eNote and tracks that it was presented for Digital Signature verification but does not store the actual SMART® Doc.

# Procedure: eNote Registration

To register an eNote on the MERS® eRegistry:

1. The Requesting Party submits the *Registration* transaction once the final tamper seal has been applied to the eNote, or a Submitting Party submits the transaction on the Requesting Party’s behalf in an XML Request.

2. The MERS® eRegistry validates the XML Request before processing any of the included *Registration* transaction(s) by verifying:
    - The XML Request was generated in conformance with a supported DTD version.
    - The Requesting Party and any Submitting Party are active Participants.
    - The Requesting Party has a Vendor relationship with the Submitting Party if the Submitting Party does not match the Requesting Party.
    - The Digital Certificate in the XML Request was issued by an approved *Certificate Authority*, is not revoked based on the *Certificate Revocation List*, is not expired, has an identity assurance type of "Medium", and matches the certificate information stored in the Submitting Party's Member Profile.
    - The XML Request contains a Digital Signature and Tamperseal Date.
3. If these validations:
    - Fail: The MERS® eRegistry rejects the XML Request, stops processing it, and sends an XML Response with the corresponding error message to the Submitting Party or the Requesting Party if there is no Submitting Party.
    - Pass: The MERS® eRegistry proceeds to the next step.
4. The MERS® eRegistry verifies the Digital Signature of the XML Request by recalculating it using the Submitter's Digital Certificate and comparing the calculated value to the value included in the XML Request. If Digital Signature validation:
    - Fails: The MERS® eRegistry rejects the XML Request, stops processing it, and sends an XML Response with the corresponding error message to the Submitting Party or the Requesting Party if there is no Submitting Party.
    - Passes: The MERS® eRegistry attempts to process each *Registration* transaction in the XML Request.
5. For each *Registration* transaction, the MERS® eRegistry verifies that:
    - The Requesting Party is named as either the Controller or the Delegatee for Transfers.
    - A Controller and Location are included in the *Registration* transaction.
    - All named *Authorized Rights Holders* are active Participants.
    - The appropriate eRegistry Relationships are set up for the named Authorized Rights Holders.
    - The MIN being used to register the eNote is valid.
6. The MERS® eRegistry determines if a SMART® Doc eNote is included in the *Registration* transaction.
    - If an eNote is included, the MERS® eRegistry attempts to validate the eNote's Digital Signature. If Digital Signature validation:
        - Fails: The MERS® eRegistry rejects the *Registration* transaction but continues processing any remaining *Registration* transactions in the XML Request.
        - Passes: The MERS® eRegistry extracts the following data from the eNote to populate the eNote Record: MIN, Borrower Information, Lien Priority Type, and Property Information.

- If an eNote is not included, the MERS® eRegistry:
    - Verifies that the eNote's Digital Signature is included in the *Registration* transaction.
    - Uses the data from the *Registration* transaction to populate the eNote Record.

7. The MERS® eRegistry verifies that all required data is received and valid. The *Registration* transaction fails if any required data is missing or invalid.
8. If the MIN of the eNote being registered matches a MIN previously registered on the *MERS® System*, and the Borrower, Property Address, and Lien Type information do not match, the *Registration* transaction fails.
9. If all other system edits are successful, the MERS® eRegistry registers the eNote.
10. If a previously registered active eNote contains matching Lien Type, Zip Code, and SSN or TIN values for the eNote being registered, the MERS® eRegistry registers the eNote and returns a warning message in the XML Response and the *Success Notification*.
11. For a successful eNote registration, the MERS® eRegistry stores the following information:
    - Digital Signature and Tamperseal Date of the eNote.
    - Authorized Rights Holders, Borrower Information, Lien Priority Type, and Property Information.
12. The MERS® eRegistry communicates its processing results to the Submitting and/or Requesting Parties and each Authorized Rights Holder on the eNote Record that did not initiate the transaction as described in *After eNote Registration*.

# Procedure: eNote Registration and Transfer of Control

This procedure is the same as *Procedure: eNote Registration* except as follows:

A *Delegatee for Transfers* submits a *Registration and Transfer of Control* transaction to the MERS® eRegistry as the Requesting Party on behalf of a Broker once the final tamper seal has been applied to the eNote, or a Submitting Party submits the transaction on the Requesting Party's behalf.

When processing a *Registration and Transfer of Control* transaction, the MERS® eRegistry verifies that:

- The Requesting Party is an active Participant and is named as the Delegatee for Transfers.
- The Controller has the **Broker** Line of Business and a **Controller Delegatee for Transfers** relationship with the Delegatee for Transfers.
- There is no Secured Party or Secured Party Delegatee named in the transaction.

If the *Registration and Transfer of Control* transaction is successful, the MERS® eRegistry:

- Registers the eNote with the Broker named as the first Controller.
- Generates an automatic *Accept Confirmation* of the *Transfer of Control* to the new Controller.
- Immediately transfers Control to the Delegatee for Transfers (new Controller).

# After eNote Registration

Once the MERS® eRegistry completes processing of the eNote registration(s) in an XML Request, it sends a synchronous XML Response to the Submitting Party or the Requesting Party if there is no Submitting Party. The XML Response indicates if each eNote registration was a success, failure (an error occurred), or if a warning condition occurred.

- For a *Registration* transaction, the Success Response acknowledges each successfully registered eNote included in the XML Request.
- For a *Registration and Transfer of Control* transaction, the *Success* Response acknowledges each successfully registered and transferred eNote in the XML Request.
- Each Response can contain multiple error and or warning messages for a single eNote registration. Error messages are detailed in the Programming Interface Guide.

For successfully registered eNotes, the MERS® eRegistry also sends a *Notification* to each Authorized Rights Holder that did not initiate the transaction if that Participant has the **Non-Transfer Notifications** option selected in its Member Profile.

Once an eNote is registered on the MERS® eRegistry, the status of the eNote Record is *Active*. While an eNote Record is in an *Active* status, the data on the MERS® eRegistry must match the corresponding data in the Participant's internal records. To view the list of transactions that each Authorized Rights Holder is authorized to submit to the MERS® eRegistry, see *Authorized Rights Holder Processing Rules*.

# Matching Another eNote Record

If the newly registered eNote Record contains the same borrower, property, and lien type as another active eNote Record, a warning will be returned in the registration response indicating the MIN and Servicing Agent Org ID and Name (if one is named for the eNote – otherwise the Location) of the matching eNote Record.

Additionally, both MINs will be reflected on the *Duplicate eNote Records Reports (EH and EI)* available on the MERS® System, which are distributed to all Authorized Rights Holders on the matching eNote Records. Refer to the MERS® System Reports Handbook for details on these reports.

# Data Mismatch with MERS® System

If the MIN for an eNote record matches a MIN subsequently registered on the MERS® System, and the borrower and property address information do not match, the MIN will be reflected on the *Mismatched MINs/eNote Records (EJ)* report generated by the MERS® System and is distributed to all Authorized Rights Holders for the MIN on the MERS® System and MERS® eRegistry (see the MERS® System Reports Handbook for details). Because the MERS® eRegistry is the *System of Record*, the Member associated with the MIN on the MERS® System must correct the information there.

# MIN Mismatch with MERS® System

If an eNote registered on the MERS® eRegistry is registered as a *Mortgage* loan on the MERS® System using a different MIN, the registration on the MERS® System must be corrected to use the MIN associated with the eNote. This would require correcting the MIN on any documents recorded in the county land records, as well as reversing the registration and re-registering the loan on the MERS® System with the correct MIN. This is necessary because the MERS® eRegistry is the System of Record.

# Audit Information

Audit information stored for all *Registration* transactions includes:

- The Requesting and Submitting Party Org IDs of the *Registration* transaction.
- Transaction Time/Date Stamp.
- Registration Date and Time
- Registering Participant
- All Authorized Rights Holders

Additional Audit information stored for the automated *Transfer of Control* in a *Registration and Transfer of Control* transaction includes:

- Transfer Date
- First and new Controllers
- Automatic Confirmation of the transfer by the new Controller

A Participant can view Audit information for each eNote Record to which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions on accessing this information.

# Transfers

## Overview

To change an *Authorized Rights Holder* of an *eNote* registered on the *MERS® eRegistry*, the appropriate Authorized Rights Holder (depending on the type of transfer) initiates a *Transfer* transaction from its external system. There are six (6) types of *Transfer transactions*:

| Transfer Transaction | Description |
|---|---|
| *Transfer of Control* | Used to change the current *Controller* of an eNote on the MERS® eRegistry to another *Participant*. |
| *Transfer of Location* | Used to report that the Participant named as the current *Location* of the *Authoritative Copy* of an eNote has changed to another Participant.<br>A new *Vault Identifier* may be specified as part of the transfer. The Vault Identifier is not validated by the MERS® eRegistry.<br>Note: A Controller may be able to update the Location field using the *Data Update* transaction if certain conditions are met. See the *eNote Record Data* chapter for details. |
| *Transfer of Servicing Agent* | Used to change the current *Servicing Agent* of an eNote on the MERS® eRegistry to another Participant. |
| *Transfer of Control and Servicing Agent* | Used to change the current Controller and Servicing Agent of an eNote on the MERS® eRegistry to another Participant or Participants.<br>The *Transfer Effective Date* is the same for both transfers.<br>A Transfer of Control and Servicing Agent is accepted or rejected in full. For example, the *Transfer of Control* cannot be accepted while the *Transfer of Servicing Agent* is rejected. |
| *Transfer of Control and Location* | Used to change the current Controller and Location of an eNote on the MERS® eRegistry to another Participant or Participants.<br>The Transfer Effective Date is the same for both transfers.<br>A new Vault Identifier may be specified as part of the transfer. The Vault Identifier is not validated by the MERS® eRegistry.<br>A *Transfer of Control and Location* is accepted or rejected in full. |
| *Transfer All* | Used to change the current Controller, Location, and Servicing Agent of an eNote on the MERS® eRegistry to another Participant or Participants.<br>The *Transfer Effective Date* is the same for all three (3) transfers.<br>A new Vault Identifier may be specified as part of the transfer. The Vault Identifier is not validated by the MERS® eRegistry.<br>A *Transfer All* is accepted or rejected in full. |

Four different XML Requests are used to complete a *Transfer* transaction:

| XML Message | Description |
|---|---|
| *Initiation Request* | Sent by the *Requesting Party* to the MERS® eRegistry to create a pending *Transfer*. |
| *Pending Notification* | Sent by the MERS® eRegistry to the current and pending Authorized Rights Holders named in the *Initiation Request*, but not the Requesting Party, to inform them that a pending *Transfer* is awaiting confirmation.<br>*Pending Notifications* are sent to a Participant only if the **Transfer Notifications** eRegistry option is enabled in its *Member Profile*. |
| *Transfer Confirmation* | Sent by each Authorized Rights Holder that is required to confirm a pending *Transfer*. There are three (3) types of *Transfer Confirmations*:<br>• *Accept Confirmation*: The Participant accepts the pending *Transfer*.<br>• *Reject Confirmation*: The Participant rejects the pending *Transfer*.<br>• *Reset Confirmation*: The Participant rescinds its previously submitted *Accept* or *Reject* confirmation and must confirm the *Transfer* again. |
| *Completion Notification* | Sent by the MERS® eRegistry to the current and pending Authorized Rights Holders to inform them that the processing of a *Transfer* is complete. There are three (3) types of *Transfer Completion Notifications*:<br>• *Transfer Success Notification*: The Transfer completed successfully.<br>• *Transfer Reject Notification*: One current or pending Authorized Rights Holder rejected the *Transfer*.<br>• *Transfer Expired Notification*: One or more current or pending Authorized Rights Holders did not send its *Transfer Confirmation* by the *Transfer Effective Date*, so the pending *Transfer* expired.<br>*Completion Notifications* are sent to a Participant only if the **Transfer Notifications** eRegistry option is enabled in its Member Profile. |

# Transfer Requirements

Requirements for *Transfer* transactions differ according to the type of transfer, but the following apply to **all** types of *Transfer* transactions:

Any *Transfer*—including a Transfer of Control—cannot be reversed. If a *Transfer*—including a Transfer of Control—is submitted in error, any Participant involved in the transfer can send a *Reject Confirmation*, or let it expire without accepting it. If an erroneous transfer is accepted, the new Controller (or *Delegatee for Transfers*) must initiate a new *Transfer* to transfer the *eNote Record* back to the correct Authorized Rights Holder.

## *Transfer Initiation Requirements*

- The Transfer Effective Date is typically the same day on which the *Transfer* is submitted, but it can be future-dated within 30 calendar days of the date the MERS® eRegistry accepted the pending *Transfer*. The Transfer Effective Date cannot be retroactive.

- The initiating Participant must be a current Authorized Rights Holder on the *eNote Record* authorized to initiate the *Transfer* transaction per the *Authorized Rights Holder Processing Rules*.
- The *Transfer Initiation Request* must include:
    - The correct Transfer Request Type of *Initiation*.
    - The appropriate Action Type for the particular *Transfer* transaction.
    - The pending Authorized Rights Holder(s) that will need to approve the *Transfer*.
    - The *MIN* and *Digital Signature* of each eNote to be included in the pending *Transfer*.
    - The Transfer Effective Date for the pending *Transfer*.
- The *Transfer Initiation Request* may optionally include:
    - New *Vault Identifier*
    - *Registry Transaction Identifier*
    - *Counterparty Org ID*
- Each pending Authorized Rights Holder, and any Counterparty Org ID, must be an active Participant.
- Each eNote Record in the *Initiation Request* must be active on the MERS® eRegistry and must not be in another pending *Transfer* transaction.
- The Digital Signature of each eNote in the *Initiation Request* must match the value stored on the MERS® eRegistry.
- If a new Servicing Agent is named as part of a *Transfer* transaction, the Participant that will be the Controller once the *Transfer* is processed must have the **Allow Servicing Agents** option enabled in its Member Profile.
- A Delegatee for Transfers can submit a *Transfer of Control* to itself or another Participant.
- If a *Secured Party* is named on an eNote Record, it can initiate any T*ransfer* transaction except a *Transfer of Servicing Agent*.
    - The Secured Party must have the **Secured Party Controller** relationship with the Controller.
    - The Controller must have the **Controller Acknowledges Secured Party** relationship with the Secured Party.
- A *Secured Party Delegatee* may initiate a *Transfer* transaction on behalf of the *Secured Party*.
- If the Secured Party Delegatee submits a *Transfer* transaction on behalf of the Secured Party:
    - The Secured Party must have the:
        - **Secured Party Delegatee** relationship with the Secured Party Delegatee.
        - **Secured Party Controller** relationship with the Controller.
    - The Controller must have the **Controller Acknowledges Secured Party** relationship with the Secured Party.
- Only the last eNote Record in a *CEMAs* chain can be transferred. To transfer an earlier eNote in the chain, any subsequent CEMA modification must be reversed first.

## Pending Transfer Notification Requirements

- The Requesting Party is not sent a *Pending Notification* unless the *Transfer* is future dated.
- No *Pending Notifications* are sent if a *Transfer* is initiated on the Transfer Effective Date and all *Confirmations* are automatically generated.
- When generated, a *Pending Transfer Notification* includes:
  - The type of *Transfer* transaction.
  - The Transfer Effective Date.
  - The current Controller, Secured Party, and Secured Party Delegatee.
  - The pending Authorized Rights Holder(s).
  - The *Transfer Identifier* assigned by the MERS® eRegistry.
  - The MIN and Digital Signature of each eNote in the pending *Transfer*.
  - The *SMART® Doc Presented* flag for the eNote Record and the *SMART® Doc* version if the eNote was presented to the MERS® eRegistry for Digital Signature validation.
- The *Transfer Pending Notification* includes the following if a *Modification* was reported:
  - Modification type (paper, electronic, CEMA).
  - Digital Signature of any electronic modification.
  - For a CEMA eNote Record: MIN and Digital Signature of the consolidated eNote.
- The *Pending Transfer Notification* includes the following if provided in the *Initiation Request*:
  - New Vault Identifier.
  - Registry Transaction Identifier.
  - Counterparty Org ID.

## Transfer Confirmation Requirements

- For all *Transfer* transactions except a *Transfer of Servicing Agent* to occur, the following Authorized Rights Holders must confirm the pending *Transfer* by sending an *Accept* or *Reject Confirmation* to the MERS® eRegistry on or before the Transfer Effective Date:

| Approving Participant | Requirements |
|---|---|
| Current Controller | • If the current Controller initiates a *Transfer*, its *Confirmation* is automatic.<br>• If a *Transfer* is initiated by the current Secured Party or Secured Party Delegatee, the current Controller's Confirmation is automatic because of the Controller Acknowledges Secured Party relationship.<br>• When a Delegatee for Transfers initiates a *Transfer of Control* from a *Broker* named as Controller to itself or another Participant, no *Confirmation* is required from the current Controller. On the Transfer Effective Date, the Delegatee for |

| Approving Participant | Requirements |
|---|---|
| | Transfers becomes Controller and remains in the Delegatee for Transfers field. |
| Current Secured Party | • The current Secured Party's *Accept Confirmation* is automatic if:<br>  ○ It initiates a *Transfer* transaction.<br>  ○ The current Secured Party Delegatee initiates a *Transfer* transaction on behalf of the Secured Party.<br>  ○ It has an Auto-*Confirm Transfer* relationship set up with the current Controller.<br>• Otherwise, the current Secured Party must confirm the *Transfer,* including the scenario where the Delegatee for Transfers initiates the *Transfer*.<br>• The Secured Party Delegatee can confirm the *Transfer* on behalf of the Secured Party only if the Secured Party has the **Secured Party Delegatee** relationship with the Secured Party Delegatee. |
| Each pending Authorized Rights Holder, except Servicing Agent | • The pending Authorized Rights Holder's *Confirmation* is automatic if has an *Auto-Confirm Transfer* relationship with the current Controller.<br>• Otherwise, the pending Authorized Rights Holder must confirm the *Transfer*. |
| Pending Servicing Agent | • A pending Servicing Agent's *Confirmation* is automatic for all *Transfers* except a *Transfer of Control and Servicing Agent* and *Transfer All* if the **Confirm All Servicing Agent Transfers** option is not enabled in its Member Profile. In this configuration:<br>  ○ The MERS® eRegistry automatically updates the eNote Record to show the new Servicing Agent at the end of the Transfer Effective Date.<br>  ○ The pending Servicing Agent can send a *Reject Confirmation* to reject the automatic confirmation any time before the MERS® eRegistry processes the *Transfer*.<br>  ○ A pending Servicing Agent cannot confirm (Accept or Reject) a *Transfer of Control and Servicing Agent* or *Transfer All* irrespective of the setting it has for the **Confirm All Servicing Agent Transfers** option in its Member Profile.<br>• If the **Confirm All Servicing Agent Transfers** option is enabled, a pending Servicing Agent must confirm the *Transfer* even when it has an *Auto-Confirm Transfer* relationship set up with the current Controller. |

- The *Transfer Confirmation* must contain:
  - The MIN of the eNote Record.
  - The Transfer Identifier assigned by the MERS® eRegistry.
  - The Digital Signature of the eNote. Two *Confirmations* are exempt from this rule:

    - *Reject Confirmations*.
    - *Accept Confirmations* for a *Transfer of Control* from the pending Controller.
  - The Digital Signature of the eNote which must match the value on the MERS® eRegistry.
  - The Action Type of the *Transfer* transaction.
  - The Confirmation Type: Accept, Reject, or Reset.

  Note: A Reject Code and Description may be optionally included in a *Reject Confirmation*. These values are defined by Participants and not the MERS® eRegistry. Contact the Participant that rejected the transfer if further explanation is required.

# Procedure: Transfer Initiation

To change one (1) or more Authorized Rights Holders on an eNote Record on the MERS® eRegistry:

1. The appropriate *Transfer* transaction is initiated by an Authorized Rights Holder permitted to do so as specified by the *Authorized Rights Holder Processing Rules*.
2. The cutoff for *Transfer Initiation Request*s is 00:00 *UTC*, Tuesday – Sunday. *Transfer Initiation Request*s received after the cutoff are processed the next day. As a best practice, *Transfer Initiation Request*s with a Transfer Effective Date equal to the date that the MERS® eRegistry receives the *Initiation Request* should be submitted by 11:50 PM UTC.
3. The MERS® eRegistry validates the XML Request before processing any of the included *Transfer* transactions. See steps 2-4 of *Procedure: eNote Registration* for details. If those validations:
    - Fail: The MERS® eRegistry rejects the XML Request, stops processing it, and sends an XML Response with the corresponding error message to the Submitting Party or the Requesting Party if there is no Submitting Party.
    - Pass: The MERS® eRegistry attempts to process each *Transfer* transaction in the XML Request.
4. For each *Transfer* transaction, the MERS® eRegistry verifies that:
    - The corresponding *Transfer Initiation Requirements* are satisfied.
    - All required data is received and valid.
5. If any requirement is not satisfied or the required data is incomplete or invalid, the *Transfer* transaction fails. The MERS® eRegistry continues to process any other *Transfer* transactions in the XML Request.
6. If all requirements are satisfied and the required data is received and valid, the MERS® eRegistry processes the *Transfer* transaction. The MERS® eRegistry:
    - Creates a transfer batch for the eNote Record(s) in each REQUEST container of the *Transfer Initiation Request* with a Status of *Pending*.
    - Assigns a unique Transfer Identifier to the pending *Transfer* which is returned in the XML Response sent to the transfer initiator and all Notifications regarding the *Transfer*.
    - Generates automatic *Accept Confirmations* for the current Controller and Secured Party and pending Authorized Rights Holders as specified in *Transfer Confirmation Requirements*.

- Communicates the results of the *Transfer Initiation* process to the current and pending Authorized Rights Holders: The MERS® eRegistry sends:
  - An XML Response to the Requesting Party to indicate acceptance of the *Transfer* transaction and identify which MIN(s) were accepted in the transfer batch and which were rejected due to an error.
  - *A Transfer Pending Notification* to all other current and pending Authorized Rights Holders that have the **Transfer Notifications** eRegistry option enabled in their Member Profile except as noted in *Pending Transfer Notification Requirements*.
- Only current Authorized Rights Holders can see the pending *Transfer* on *MERS® eRegistry Online*.

# Procedure: Transfer Confirmation

1. Any current or pending Authorized Rights Holder required to confirm the *Transfer* transaction that did not have an automatic *Accept Confirmation* generated by the MERS® eRegistry must submit a *Transfer Confirmation* (Accept or Reject) no later than the *Transfer Effective Date*. See *Transfer Confirmation Requirements* for details.
2. If the last (or only) required *Accept Confirmation* is received on the Transfer Effective Date, the MERS® eRegistry processes the *Transfer* immediately.

Note: Because most *Transfers* are submitted to the MERS® eRegistry on the Transfer Effective Date, they are usually processed immediately upon receipt of the last *Accept Confirmation*.

3. If all required *Accept Confirmations* are received before the Transfer Effective Date, the MERS® eRegistry processes the *Transfer* once the Transfer Effective Date has ended (00:01 UTC next day).

Note: When the Transfer Effective Date is future dated, the current Controller can reject or reset its automatic *Accept Confirmation* any time before the MERS® eRegistry receives the last required *Transfer Confirmation* from any Authorized Rights Holder except a pending Servicing Agent.

4. When the MERS® eRegistry processes a *Transfer* transaction for an eNote Record, it:
   - Makes any pending Authorized Rights Holder a current Authorized Rights Holder.
   - Makes any replaced Authorized Rights Holder a previous Authorized Rights Holder.
   - Removes any Delegatee for Transfers if the new Controller does not have the **Controller Delegatee for Transfers** relationship with the Delegatee for Transfers.
   - Removes any Secured Party or Secured Party Delegatee if the *Transfer* transaction included a *Transfer of Control*.
   - Sends a *Transfer Complete Notification* to the previous, new, and any unchanged Authorized Rights Holders.
5. A pending Authorized Rights Holder, or the current Secured Party, can reset or reject its previously submitted *Accept Confirmation* any time before the MERS® eRegistry processes the *Transfer*. Resetting puts the *Transfer* back to its initial status of requiring an *Accept* or *Reject Confirmation* from that Participant.

6. If a current or pending Authorized Rights Holder sends a *Reject Confirmation* before the Transfer Effective Date, the MERS® eRegistry:
   - Immediately cancels the pending *Transfer* without changing any Authorized Rights Holders.
   - Sends a *Transfer Reject Notification* to all current and pending Authorized Rights Holders.
   - The *Reject Confirmation* may include an optional reject reason to explain why it was rejected.
7. If all required *Accept Confirmations* are not received, or a pending *Transfer* is not rejected, prior to the end of the Transfer Effective Date, the MERS® eRegistry:
   - Expires the pending *Transfer* without changing any Authorized Rights Holders.
   - Sends a *Transfer Completion Notification* to all current and pending Authorized Rights Holders to indicate that the pending *Transfer* has expired.
8. For *Seasoned Transfers* of *Control* (with or without *Transfer of Location* or *Servicing Agent*), the requesting Participant is billed the Seasoned *Transfer of Control* fee.

# Deactivations for eNote Records in Pending Transfers

If a *Deactivation* transaction is received for an eNote Record in a pending *Transfer*, the MERS® eRegistry determines if a *Secured Party* is named on the eNote Record:

- If a Secured Party is not found, the eNote Record is deactivated. When the MERS® eRegistry processes the *Transfer*, it rejects the *Transfer* because the eNote Record's Status is *Inactive*.
- If a Secured Party is found and its Member Profile is configured to:
  - Allow its eNote Records to be deactivated, the MERS® eRegistry processes the *Deactivation* and rejects the *Transfer* when it is processed because the eNote Record's Status is *Inactive*.
  - Prevent the deactivation of its eNote Records, the MERS® eRegistry rejects the *Deactivation* transaction and *Transfer* processing continues.

# Transfers Due to a Repurchase or Registration Error

If an Investor requires a Participant to repurchase an eNote, the Investor (as the Current Controller) must initiate a *Transfer of Control* back to the appropriate Controller

If an eNote was registered naming an incorrect initial Controller, a *Transfer of Control* must be submitted back to the registering Participant by the incorrect Controller. The registering Participant must then reverse the incorrect Registration and re-register the eNote with the correct Controller.

In either case, the eNote Record must not be included in another pending *Transfer* transaction, or the MERS® eRegistry will reject that MIN in the *Transfer of Control* Initiation Request.

# Audit Information

The Audit trail captures all data for *Transfer* transactions, including:

- The Requesting and Submitting Party Org IDs of the *Transfer* transaction.
- Transaction Time/Date Stamp.
- Org IDs of the previous and current Authorized Rights Holders.
- Type of transfer.
- Confirmation type (including automatic Confirmations).
- Initiation, Confirmation, and Transfer Effective Dates.
- Value changes.
- Counterparty Org ID, if included in the *Transfer Initiation Request.*
- Vault Identifier, if included in the *Transfer Initiation Request*.

# Change Data - eNote Record Data Update

## Overview

The *Data Update* transaction is used to update an *eNote Record* when changes occur to loan data, *Vault Identifier*, *Location*, *Delegatee for Transfers*, *Servicing Agent*, or *Secured Party Delegatee*. The *Data Update* transaction is also used to present a *SMART® Doc eNote* to the *MERS® eRegistry* for *Digital Signature* validation if it was not presented in the *Registration* transaction. The *Data Update* transaction is defined by the *Change Data* *DTDs*.

Refer to *Authorized Rights Holder Processing Rules* for the list of *Data Update* transactions that each *Authorized Rights Holder* can submit to the MERS® eRegistry.

The *Data Update* transaction cannot be used to change the *MIN*, Digital Signature, or *Controller* of an eNote Record.

- If the MIN or Digital Signature is incorrect, the eNote Record must be reversed and re-registered with the correct values.
- If the Controller is incorrect, the incorrect Controller must initiate a *Transfer of Control* to the Registering Org ID, and that Participant must reverse the Registration.

Once a *CEMA* has been reported, the Vault Identifier field can be updated on the eNote Record associated with either the consolidated eNote or the CEMA eNote. The Vault Identifier field can also be updated on an eNote Record after the SMART® Doc has been presented for Digital Signature validation.

The *Data Update* transaction should be sent no later than one (1) business day after discovering an error in the eNote Record information.

## eNote Data Update Requirements

The following requirements apply to all *Data Update* transactions:

- The *Requesting Party* must be an Authorized Rights Holder on the eNote Record authorized to initiate the *Data Update* transaction per the *Authorized Rights Holder Processing Rules*.
- The *Change Data Request* must indicate that it is a *Data Update* transaction with the Action Type of *Update*.
- The *Data Update* transaction must include:
  - The MIN of the eNote Record.
  - The Digital Signature of the eNote.
  - The eNote data or *Org ID* to be updated on the eNote Record.
- The eNote Record must be active on the MERS® eRegistry.
- The eNote Record must not be in a pending *Transfer* transaction.
- The submitted Digital Signature of the eNote must match the value on the MERS® eRegistry.

## Requirements for Updating Loan Data or Vault Identifier, or for Presenting SMART® Docs after Registration

The following requirements apply to *Data Update* transactions other than changes to Location, Delegatee for Transfers, Servicing Agent, or Secured Party Delegatee:

- A SMART® Doc can be presented to the MERS® eRegistry if it has not been previously presented. When a SMART® Doc is presented, the MERS® eRegistry calculates the Digital Signature and compares it to the value provided at Registration. If the values:
  - Do not match, the MERS® eRegistry rejects the *Data Update* transaction.
  - Match, the MERS® eRegistry extracts the data from the eNote and overrides the values in the *eNote Record* previously presented in the *Data Point Registration*.
- Loan data may be updated to correct certain fields so that they agree with the equivalent information on the eNote.
  - If a SMART® Doc eNote has not been presented to the MERS® eRegistry, any loan data can be updated on the eNote Record. If Property Information needs to updated:
    - The entire set of Property Information fields do not need to be submitted in the *Data Update* transaction, just the field(s) that need to be updated.
    - To delete a value from a field, the literal "DELETE" must be included in the *Data Update* transaction for that field.
  - Once a SMART® Doc is presented, only the following fields on an eNote Record can be updated using a *Data Update* transaction:
    - Vault Identifier
    - Location Org ID
    - Borrower SSN or TIN
    - Servicing Agent Org ID
    - Delegatee for Transfers Org ID
    - Secured Party Delegatee Org ID

## Requirements for Updating Location, Delegatee for Transfers, Servicing Agent, or Secured Party Delegatee

The following requirements apply to *Data Update* transactions that change the Location, Delegatee for Transfers, Servicing Agent, or Secured Party Delegatee:

- After a CEMA modification, updates to Location, Delegatee for Transfers, Servicing Agent, and Secured Party Delegatee can be performed only on the last eNote record in the CEMA chain.
- The Controller is able to update the Location field using the *Data Update* transaction if its Org ID is the *Primary Member* of the current and new Location Org IDs. If the Controller is not the Primary Member of both Org IDs, the Controller must initiate a *Transfer of Location* transaction to make the change to the eNote Record.
- The Controller can add a Secured Party Delegatee to one of its eNote Records only if:
  - There is not another Secured Party Delegatee already named,
  - There is a Secured Party named, and

  - The Secured Party has the **Secured Party Delegatee** relationship set up with the Secured Party Delegatee.
- The Secured Party can add, change, or remove a Secured Party Delegatee only if the Secured Party has the **Secured Party Delegatee** relationship set up with the Secured Party Delegatee included in the *Data Update* transaction.
- The Delegatee for Transfers and Secured Party Delegatee may submit a *Data Update* transaction only to remove itself from an eNote Record.
  - The Delegatee for Transfers can remove itself from any eNote Record on which it is named.
  - The Secured Party Delegatee can remove itself from any eNote Record on which it is named.
- When a Location, Servicing Agent, or Secured Party Delegatee is added to an eNote Record, it is considered an Authorized Rights Holder and when removed is considered a previous Authorized Rights Holder.

# Procedure: eNote Record Data Update

To process a data update on an eNote Record on the MERS® eRegistry:

1. The Requesting Party submits the *Data Update* transaction, or a Submitting Party submits the transaction on the Requesting Party's behalf, in an XML Request.
2. The MERS® eRegistry validates the XML Request before processing any of the included *Data Update* transaction(s). See steps 2-4 of *Procedure: eNote Registration* for details. If those validations:
   - Fail: The MERS® eRegistry rejects the XML Request, stops processing it, and sends an XML Response with the corresponding error message to the Submitting Party or the Requesting Party if there is no Submitting Party.
   - Pass: The MERS® eRegistry attempts to process each *Data Update* transaction in the XML Request.
3. For each *Data Update* transaction, the MERS® eRegistry verifies that:
   - The corresponding requirements are satisfied.
   - All required data is received and valid.
4. If any requirement is not satisfied or the required data is incomplete or invalid, the *Data Update* transaction fails. The MERS® eRegistry continues to process any other transactions in the XML Request.
5. If all requirements are satisfied and the required data is received and valid, the MERS® eRegistry processes the *Data Update* transaction.
6. Once the MERS® eRegistry completes processing of the *Data Update* transaction(s) in an XML Request, it sends a synchronous XML Response to the Submitting Party or the Requesting Party if there is no Submitting Party. The XML Response indicates if each update was a success, failure (an error occurred), or if a warning condition occurred.
7. For successfully processed *Data Update* transactions, the MERS® eRegistry sends a *Notification* to each current and previous Authorized Rights Holder, including the current Controller that did not

initiate the transaction if that *Participant* has the **Non-Transfer Notifications** option enabled in its *Member Profile*.

# Audit Information

For Audit purposes, the following data is captured and stored:

- The Requesting and Submitting Party Org IDs of the *Data Update* transaction.
- Transaction Time/Date Stamp.
- Type of *Data Update* transaction.
- Before and After values associated with the *Data Update* transaction.

A Participant can view certain Audit information for each eNote Record for which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions.

# Change Data - Secured Party

## Overview

The *Secured Party Update* transaction is used to update an active *eNote Record* when changes occur to the *Secured Party* associated with the *eNote*. A Secured Party can be added, released, or reversed. The *Secured Party Update* transaction is defined by the *Change Data* *DTDs*.

- *Add Secured Party* is used to add a Secured Party to an eNote Record after it has been registered.
- *Release Secured Party* is used by a Secured Party or the Secured Party Delegatee to remove a Secured Party from an eNote Record when it no longer has an interest in the eNote.
- *Reverse Secured Party* is used by a Secured Party or the Secured Party Delegatee to reverse the erroneous addition of a Secured Party to an eNote Record.

When a Secured Party is added to an eNote Record, it is considered an *Authorized Rights Holder*. When a Secured Party is removed from an eNote Record, it is considered a previous Authorized Rights Holder.

The *Data Update* transaction is used to update an eNote Record when changes occur to the *Secured Party Delegatee* associated with the eNote. See the *eNote Record Data Update* chapter for details.

## Add Secured Party Requirements

The following requirements apply to the *Add Secured Party* transaction:

- Only the current *Controller* can add a Secured Party to one of its eNote Records.
- The *Change Data Request* must:
    - Indicate that it is an *Add Secured Party* transaction with the Action Type of *AddSecuredParty.*
    - Include the *Org ID* of the Controller in the *Requesting Party* field.
- The *Add Secured Party* transaction must include:
    - The *MIN* of the eNote Record.
    - The *Digital Signature* of the eNote.
    - The Org ID of the Secured Party.
- The eNote Record must be active on the MERS® eRegistry.
- The eNote Record must not be in a pending *Transfer* transaction.
- The submitted Digital Signature of the eNote must match the value on the MERS® eRegistry.
- The eNote Record must not have an existing Secured Party named.
- The Secured Party being named must be an active *Participant*.
- The Secured Party must have the **Secured Party Controller** relationship with the Controller.

- The Controller must have the **Controller Acknowledges Secured Party** relationship with the Secured Party.
- No other data updates that are available under the *Change Data Request DTD* can be included in the *Add Secured Party* transaction.
- The *Add Secured Party* transaction must only be submitted on the last eNote Record in a *CEMA* chain.

# Release Secured Party Requirements

The following requirements apply to the *Release Secured Party* transaction:

- Only the current Secured Party or Secured Party Delegatee can release a Secured Party from an eNote Record.
- The *Change Data Request* must:
  - Indicate that it is a *Release Secured Party* transaction with the Action Type of ReleaseSecuredParty.
  - Include the Org ID of the Secured Party or Secured Party Delegatee in the Requesting Party field.
- The *Release Secured Party* transaction must include:
  - The MIN of the eNote Record.
  - The Digital Signature of the eNote.
- The eNote Record must be active on the MERS® eRegistry.
- The eNote Record must not be in a pending *Transfer* transaction.
- The submitted Digital Signature of the eNote must match the value on the MERS® eRegistry.
- The eNote Record must have a Secured Party named.
- If the Secured Party Delegatee submits the *Release Secured Party* transaction, the Secured Party must have the *Secured Party Delegatee* eRegistry relationship with the Secured Party Delegatee.
- When a Secured Party is removed from an eNote Record, any associated Secured Party Delegatee is also removed as part of the transaction.
- No other data updates that are available under the *Change Data Request DTD* can be included in the *Release Secured Party* transaction.
- The *Release Secured Party* transaction must only be submitted on the last eNote Record in a CEMA chain.

# Reverse Secured Party Requirements

The following requirements apply to the *Reverse Secured Party* transaction:

- Only the current Secured Party or Secured Party Delegatee can reverse a Secured Party on an eNote Record.

- The *Change Data Request* must:
  - Indicate that it is a *Reverse Secured Party* transaction with the Action Type of ReverseSecuredParty.
  - Include the Org ID of the Secured Party or Secured Party Delegatee in the Requesting Party field.
- The *Reverse Secured Party* transaction must include the MIN of the eNote Record.
  - The MIN must be active on the MERS® eRegistry.
  - The MIN must not be in a pending *Transfer* transaction.
- The Digital Signature of the eNote is optional on a *Reverse Secured Party* transaction. If provided, it must match the value stored on the MERS® eRegistry.
- The eNote Record must have a Secured Party named.
- No other data updates that are available under the *Change Data Request DTD* can be included in the *Reverse Secured Party* transaction.
- If the Secured Party Delegatee submits the *Reverse Secured Party* transaction, the Secured Party must have the *Secured Party Delegatee* eRegistry relationship with the Secured Party Delegatee.
- When a Secured Party is reversed on an eNote Record, any associated Secured Party Delegatee is also reversed as part of the transaction.
- The *Reverse Secured Party* transaction must only be submitted on the last eNote Record in a CEMA chain.

# Procedure: Secured Party Updates

To process a *Secured Party Update* transaction on the MERS® eRegistry:

1. The Requesting Party submits the *Secured Party Update* transaction, or a Submitting Party submits the transaction on the Requesting Party's behalf, in an XML Request.
2. The MERS® eRegistry validates the XML Request before processing any of the included *Secured Party Update* transaction(s). See steps 2-4 of *Procedure: eNote Registration* for details. If those validations:
   - Fail: The MERS® eRegistry rejects the XML Request, stops processing it, and sends an XML Response with the corresponding error message to the Submitting Party or the Requesting Party if there is no Submitting Party.
   - Pass: The MERS® eRegistry attempts to process each *Secured Party Update* transaction in the XML Request.
3. For each *Secured Party Update* transaction, the MERS® eRegistry verifies that:
   - The corresponding requirements are satisfied.
   - All required data is received and valid.
4. If any requirement is not satisfied or the required data is incomplete or invalid, the *Secured Party Update* transaction fails. The MERS® eRegistry continues to process any other transactions in the XML Request.

5. If the required data is received and valid and all requirements are satisfied, the MERS® eRegistry processes the *Secured Party Update* transaction.
6. Once the MERS® eRegistry completes processing of the *Secured Party Update* transaction(s) in an XML Request, it sends a synchronous XML Response to the Submitting Party or the Requesting Party if there is no Submitting Party. The XML Response indicates if each update was a success, failure (an error occurred), or if a warning condition occurred.
7. For successfully processed *Secured Party Update* transaction(s), the MERS® eRegistry also sends a *Notification* to:
   - The current Controller if it is not the Requesting Party of the *Secured Party Update* transaction.
   - Each previous and new Authorized Rights Holder that did not initiate the transaction if that Participant has the **Non-Transfer Notifications** option selected in its Member Profile.

# Audit Information

For Audit purposes, the following data is captured and stored:

- The Requesting and Submitting Party Org IDs of the *Secured Party Update* transaction.
- Transaction Time/Date Stamp
- Type of *Secured Party Update*
- Before and After values of the Secured Party and Secured Party Delegatee fields.

A Participant can view certain Audit information for each eNote Record for which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions.

# Change Data - Modification

## Overview

The *Modification* transaction is used to report a modification of an *eNote's* terms to the *MERS® eRegistry*.

Once a modification to an eNote has been reported to the MERS® eRegistry, any *Transfer Pending* and *Transfer Completion Notifications* for that eNote will include information about the modification.

## Requirements

The following requirements apply to all types of modifications: paper, electronic, and CEMAs.

- The *Modification* transaction must indicate it is a *Change Data Request* with the Action Type of *Modification*.
- Only the current *Controller* or *Servicing Agent* can submit a *Modification*.

### *Paper Modification Requirements*

- A paper modification must be reported to the MERS® eRegistry no later than three (3) business days after the date on which the *Paper Modification* was fully executed.
- The *MIN* on the paper modification must match the MIN on the MERS® eRegistry.
- The *Modification* transaction must have a Loan Modification Type of "Paper".
- If an eNote is consolidated into a paper note as part of a *CEMA*, used in many loan refinances in New York State, the eNote Record must be deactivated using the *Converted to Paper* transaction.

### *Electronic Modification Requirements*

- An electronic modification must be reported to the MERS® eRegistry no later than one (1) business day after the final tamper sealing of the modification agreement.
- The *Modification* transaction must have a Loan Modification Type of "Electronic".
- The Modification transaction must contain the MIN and *Digital Signature* of both the eNote and the electronic modification agreement.
- The values for the electronic modification agreement may be included in the *Modification* transaction either in a Base64 encoded SMART® Doc or as data points in the XML message (if both are included, the data point values are ignored).
- The electronic modification agreement must contain the same MIN as the eNote being modified.
- The Digital Signature of the modification agreement is added to the *eNote Record*.
- The Controller determines whether the electronic modification agreement is vaulted with the same *Location* that is maintaining the *Authoritative Copy* of the eNote.

## *CEMA Modification Requirements*

- The CEMA eNote must be registered on the MERS® eRegistry prior to submitting the *CEMA Modification* transaction.
- The Controller or Servicing Agent on the CEMA eNote Record must match the Controller or Servicing Agent on the eNote Record associated with the eNote that was modified by the CEMA.
- The CEMA eNote must be identified with a new MIN.
- The *CEMA Modification* must be reported on the eNote Record that was modified by the CEMA eNote on the same business day that the CEMA eNote was registered.
- The *CEMA Modification* transaction must have a Loan Modification Type of "CEMA", and contain the new MIN and Digital Signature of the CEMA eNote.
- Once the *CEMA Modification* transaction is processed:
  - The consolidated eNote Record remains in an *Active* status on the MERS® eRegistry.
  - The Modification flag on the consolidated eNote Record is updated to indicate that the eNote was modified by a CEMA.
  - The MIN of the consolidated eNote Record is cross-referenced on the CEMA eNote Record.
  - The MIN of the CEMA eNote Record is cross-referenced on the consolidated eNote Record.
  - Only Borrower Information, Property Address, Vault Identifier, and Lien Type can be updated on the consolidated eNote Record.
  - Certain data updates (e.g., Borrower Information or Property Address) may need to be performed on both eNote Records.
  - Subsequent transactions are validated against the MIN and Digital Signature of each eNote Record.
  - No further modifications can be processed on the consolidated eNote Record.
  - The registration of the consolidated eNote Record cannot be reversed unless the CEMA Modification is first reversed.
  - The consolidated eNote Record cannot be deactivated unless the CEMA Modification is first reversed.
  - When the CEMA eNote Record is deactivated, the consolidated eNote Record is also deactivated using the same reason.

# Procedure: Change Data - Modification

1. The current Controller or Servicing Agent can initiate a *Change Data* (Modification) Request.
2. The MERS® eRegistry validates the MIN and Digital Signature of the eNote, that the Requesting Party and Submitting Party are active Participants with the appropriate authority to submit the Request, and performs any other validations needed for the particular *Modification* transaction.
3. If the validations do not pass, the MERS® eRegistry sends a synchronous XML Response containing an error message to the Requesting Party.

4. If the validations pass, the MERS® eRegistry sends a synchronous XML Response to the Requesting Party indicating the Modification was successfully processed.
5. The MERS® eRegistry also sends a Notification to any other Authorized Rights Holder named on the eNote Record that has the **Non-Transfer Notifications Member** option selected.

# Audit Information

For Audit purposes, the following data is captured and stored:

- The Requesting and Submitting Party Org IDs of the *Modification* transaction.
- Transaction Time/Date Stamp.
- Type of Change Data Request (Modification).
- Type of Loan Modification (paper or electronic)
- Before and After values associated with the *Modification* transaction.
- For CEMA modifications, both MINs

A Participant can view certain Audit information for each eNote Record for which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions.

# Change Data - Assumption

## Overview

The *Assumption* transaction is used to report a change to the borrowers named on an *eNote* when:

- A new borrower assumes the outstanding *Mortgage* debt,
- A new borrower is added to the existing loan obligation, or
- An existing borrower is removed from the loan obligation.

## Requirements

The following requirements apply to Assumptions:

- The *Controller* or *Servicing Agent* must report an assumption to the *MERS® eRegistry* no later than three (3) business days after the date on which the Assumption document was fully executed.
- After a *CEMA* modification, an Assumption can only be reported on the last *eNote Record* in the CEMA chain.
- The *Assumption* transaction must indicate it is a *Change Data* Request, with the Action Type of *Assumption*.
- The *Assumption* transaction must contain the *MIN* and complete list of Borrower name(s) and SSN(s) or TIN(s). The Borrower information provided must be either all Personal or Non-Personal and replaces the Current Borrower information on the eNote Record.
- No *SMART® Doc* is presented to report an *Assumption*.
- The MIN and *Digital Signature* of the eNote in the *Assumption* transaction are compared to the values on the MERS® eRegistry.
- If this is the first reported Assumption, the MERS® eRegistry moves the existing Borrower Information to the *Original Borrower* fields.
- For subsequent *Assumptions*, the Original Borrowers fields do not change. The new Borrowers become the Current Borrowers, and all Previous Borrower Information is retained as part of the eNote Record.
- The eNote Record is flagged to indicate an Assumption occurred.

## Procedure: Change Data - Assumption

The following outlines the procedures:

1. The current Controller or Servicing Agent initiate a *Change Data* (Assumption) Request.

2. The MERS® eRegistry validates the MIN and Digital Signature of the eNote, that the Requesting Party and Submitting Party are active Participants with the appropriate authority to submit the Request, and performs any other validations needed for the *Assumption* transaction.
3. If the validations do not pass, the MERS® eRegistry sends a synchronous XML Response containing an error message to the Requesting Party.
4. If the validations pass, the MERS® eRegistry sends a synchronous XML Response to the Requesting Party indicating the Assumption was successfully processed.
5. The MERS® eRegistry also sends a *Notification* to any other *Authorized Rights Holder* named on the eNote Record that has the **Non-Transfer Notifications Member** option selected.

# Audit Information

For Audit purposes, the following data is captured and stored:

- The Requesting and Submitting Party Org IDs of the *Assumption* transaction.
- Transaction Time/Date Stamp.
- Type of Change Data Request (Assumption).
- Before and After values for the Assumption transaction, including Borrower Information.

A *Participant* can view certain Audit information for each eNote Record for which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions.

# Change Data – Add Document

## Overview

The *Add Document* transaction is used to record the document type and *Digital Signature* of a document associated with an *eNote* (e.g. appraisal, title policy, etc.) on its *eNote Record*. See *Appendix B – Document Types* of the *Programming Interface Guide* for the list of supported documents. Use of the *Add Document* transaction is optional.

Documents can be added to any eNote in a *CEMA* chain.

## Requirements

The following requirements apply to all *Add Document* transactions for all document types:

- Only the current *Controller* or *Servicing Agent* can submit an *Add Document* request.
- The *Add Document* transaction must indicate it is a *Change Data* Request, with the Action Type of *AddDocument* and a valid Document Type.
- The *Add Document* transaction must contain the *Digital Signature* of both the eNote and the document being added.
- The Digital Signature of the document being added cannot match the Digital Signature of any other document of the same type for the eNote Record.
- The document type and Digital Signature of the document is added to the eNote Record.

## Procedure: Change Data – Add Document

1. The current Controller or Servicing Agent can initiate a *Change Data* (Add Document) Request.
2. The MERS® eRegistry validates the Digital Signature of the eNote, the Digital Signature, and Document Type of the document being added, and performs any other validations needed for the particular *Change Data* (Add Document) Request.
3. If the validations do not pass, the MERS® eRegistry sends a synchronous XML Response containing an error message to the Requesting Party.
4. If the validations pass, the MERS® eRegistry sends a synchronous XML Response to the Requesting Party indicating the document was successfully added.
5. The MERS® eRegistry also sends a Notification to any other Authorized Rights Holder named on the eNote Record that has the Non-Transfer Notifications Member option selected.
6. The added document is listed on the *Document Information* page for that eNote record.

# Audit Information

For Audit purposes, the following data is captured and stored:

- The Requesting and Submitting Party Org IDs associated with the *Add Document* transaction.
- Transaction Time/Date Stamp.
- Type of Request (Add Document).
- Type of document added.
- Digital Signature of the added document.

A Participant can view certain Audit information for each eNote Record for which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions.

# Change Status

## Overview

The *Change Status DTD* defines several status-related *MERS® eRegistry* transactions:

- Deactivations: Used to deactivate an active *eNote Record*.
- Deactivation Reversal: Used to reverse the deactivation of a previously deactivated eNote Record.
- Registration Reversal: Used to reverse an eNote registration.
- Change Data Reversals: Used to reverse the following transactions defined in the *Change Data DTD*:
  - Assumption Reversal: Used to reverse a previously submitted Assumption transaction.
  - Modifications Reversal: Used to reverse a previously submitted Modification transaction.
  - Add Document Reversal: Used to reverse a previously added Document.

### *Deactivations*

Once an eNote is successfully registered, its eNote Record status is *Active*. The appropriate Participant must submit a *Deactivation* transaction to report when any of the following events happens to an eNote in *Active* status, changing the status to *Inactive*:

| Deactivation Transaction | Description |
|---|---|
| *Paid Off* | Used to deactivate an eNote Record when a payoff of an eNote has occurred. |
| *Charged Off* | Used to deactivate an eNote Record when a charge-off of an eNote has occurred because the borrower is no longer obligated to make payments or satisfy any other terms or conditions required by the eNote. The status change of an eNote to Charged Off on the MERS® eRegistry will not occur contemporaneously with the *Participant's* write off of the debt on its balance sheet. |
| *Transferred to Proprietary Registry* | Used to deactivate an eNote Record when an eNote has been transferred out of the MERS® eRegistry to another registry. |
| *Converted to Paper* | Used to deactivate an eNote Record when an eNote has been converted to a paper note. |

When the MERS® eRegistry processes a *Deactivation* transaction, the eNote Record's Status changes to "Inactive" with a description of the *Deactivation* transaction used to deactivate the eNote Record (e.g., "Inactive - Paid Off").

An eNote Record naming a *Secured Party* cannot be deactivated unless the **Secured Party Allows Deactivations** option is enabled in Secured Party's Member Profile.

## Deactivation Reversals

A deactivated eNote Record can be changed back to an *Active* status without re-registering the eNote by submitting the appropriate *Deactivation Reversal* transaction:

- Paid Off Reversal
- Charged Off Reversal
- Transferred to Proprietary Registry Reversal
- Converted to Paper Reversal

## Registration Reversal

The *Registration Reversal* transaction is used to reverse an eNote *Registration* on the MERS® eRegistry. A *Registration Reversal* transaction is used when:

- An eNote was registered on the MERS® eRegistry but the loan:
  - Never closed,
  - Rescinded, or
  - Was registered with an incorrect MIN, Digital Signature, or initial Controller.

    For these errors, the eNote must be re-registered after reversal with the correct values.
- Errors are identified in an eNote Record for Borrower Information (except SSN or TIN), Lien Priority, or Property Information after an eNote was presented to the MERS® eRegistry.

An eNote *Registration* can be reversed regardless of any previous transfers that occurred. The *Registration Reversal* must be initiated by the current Controller or Servicing Agent.

Once the *Registration R*eversal is complete, the eNote Record's Status is *Inactive*. The eNote can be re-registered using the same *MIN* as needed.

## Assumption, Modification, and Document Reversals

*An Assumption*, *Modification*, or *Add Document* transaction is reversed on the MERS® eRegistry using the corresponding reversal transaction:

- Assumption Reversal
- Modification Reversal
- Document Reversal

# Change Status Requirements

The following requirements apply to all transaction defined by the *Change Status DTDs:*

- *Change Status* transactions must be initiated by the current Controller or Servicing Agent.
- *A Change Status* transaction must be submitted to the MERS® eRegistry no later than five (5) business days after the date upon which the Participant's internal records show that the status change occurred on the eNote.

- If a *Change Status* transaction for an eNote Record is submitted in error, the appropriate *Reversal* transaction must be submitted to the MERS® eRegistry no later than seven (7) business days after the incorrect status is discovered.
- *Change Status* transactions must:
    - Indicate it is a *Change Status* transaction with the appropriate Action Type (*Paid Off*, *Reversal of Paid Off, Registration Reversal*, etc.).
    - Contain the MIN of the eNote Record to be deactivated or reversed (must match the MIN on the eNote Record).
    - Contain the eNote's Digital Signature (must match the value stored on the eNote Record).
    - *Change Status* transactions are performed on the last eNote Record in a CEMA chain and are cascaded to all earlier eNote Records in the chain. If a *Change Status* transaction is submitted for another MIN in the chain, it is rejected. The CEMA modification that created the chain may also need to be reversed.

## Deactivation Requirements

The following requirements apply to all eNote Deactivations:

- The eNote Record must have an *Active* status for the MERS® eRegistry to process the *Deactivation* transaction.
- If a *Deactivation* transaction is submitted in error, the appropriate *Reversal* transaction must be submitted to the MERS® eRegistry to place the eNote Record back in an *Active* status.

## Registration Reversal Requirements

The following requirements apply to *Registration Reversal* transactions:

- The eNote Record must have an *Active* status for the MERS® eRegistry to process the *Registration Reversal* transaction.
- If a *Registration Reversal* transaction is submitted in error, the eNote must be re-registered on the MERS® eRegistry to revert the eNote Record's Status to *Active*.
- Once a consolidated eNote Record has been modified by a CEMA:
    - The *Registration* of the CEMA eNote cannot be reversed until the *Modification* reported on the consolidated eNote Record is reversed.
    - The *Registration* of the consolidated eNote cannot be reversed until:
        - The *Modification* reported on the consolidated eNote Record is reversed, and
        - The *Registration* of the CEMA eNote is reversed, if applicable.

## Assumption Reversal Requirements

- The eNote Record must have a status of *Active* and an indicator of *Assumed*.
- After a CEMA modification, an *Assumption Reversal* can only be submitted on the last eNote Record in the CEMA chain.

- An *Assumption Reversal* only reverses the last reported assumption. If multiple assumptions were reported, more than one *Assumption Reversal* may need to be submitted to restore the correct borrowers.
- When an *Assumption Reversal* is processed, the most recent Assumed Indicator is removed from the eNote Record. If multiple Assumptions were reported, the Assumed Indicator remains until all assumptions are reversed.

### *Modification Reversal Requirements*

- The eNote Record must have a status of *Active* and an indicator of *Modified*.
- A *Modification Reversal* only reverses the last reported modification. If multiple modifications were reported, more than one *Modification Reversal* may need to be submitted to restore the correct modification.
- When a *Modification Reversal* is processed, the most recent Modified Indicator is removed from the eNote Record. If multiple modifications were reported, the Modified Indicator remains until all modifications are reversed.
- For CEMA Modification Reversals:
    - The original eNote Record must have a status of *Active* and an indicator of *Modified*.
    - Both MINs and their Digital Signatures must be included in the *Modification Reversal*.
    - The MERS® eRegistry removes the cross references between the original eNote Record and the CEMA eNote Record.
    - After the modification is reversed, the appropriate Participant must reverse the CEMA *Registration* as applicable.

### *Document Reversal Requirements*

- The eNote Record must be in a status of *Active*.
- A *Document Reversal* transaction for a specific document type removes the last added document of that type from an eNote Record. If multiple documents of the same type were added, more than one *Document Reversal* may need to be submitted to restore the correct number of documents for that type.
- Reversed documents do not show on MERS® eRegistry OnLine *Document Information* page.

## Procedure: Change Status (Active to Inactive / Inactive to Active)

The status of an eNote Record must be changed to reflect certain events that can happen to an eNote. These events are *Paid Off*, *Charged Off*, *Transferred to a Proprietary Registry*, and *Converted to Paper*. If such an event is reported in error, the appropriate Participant uses a *Reversal* transaction to correct it. Change Status is also used to correct a Registration done in error.

The following outlines the procedure:

1. The current Controller or Servicing Agent initiates a *Change Status* transaction, which must include the appropriate Action Type.
2. The MERS® eRegistry validates the MIN and Digital Signature, that all named Org IDs are active and have appropriate authority for the transaction, and performs any other validations needed for the particular *Change Status* transaction.
3. If a *Deactivation* transaction is received for an eNote Record, the MERS® eRegistry determines if a Secured Party is named on the eNote Record:
   - If a Secured Party is not found, the eNote Record is deactivated.
   - If a Secured Party is found and its Member Profile is configured to:
     - Allow its eNote Records to be deactivated, the MERS® eRegistry processes the *Deactivation*.
     - Prevent the deactivation of its eNote Records, the MERS® eRegistry rejects the *Deactivation*.
4. If the validations do not pass, the MERS® eRegistry sends a synchronous XML Response containing an error message to the Requesting Party.
5. If the validations pass, the MERS® eRegistry:
   - Sends a synchronous XML Response to the Requesting Party indicating the *Change Status* transaction was successfully processed.
   - Changes the status on the eNote Record.
   - If the *Change Status* transaction is for the last eNote Record in a CEMA chain, cascades the status change to all earlier eNote Records in the chain.
   - Sends a Notification to any Authorized Rights Holder on the MIN who did not initiate the transaction and has the **Non-Transfer Notifications** option selected.

# Procedure: Assumption, Modification and Document Reversal

If a *Modification*, *Assumption*, or *Add Document* transaction was sent in error, use a *Reversal* transaction to correct it. The *Reversal* transaction should be sent as soon as the error is discovered.

The following outlines the procedure:

1. The current Controller or Servicing Agent initiates a Modification, Assumption, or Document Reversal.
2. The MERS® eRegistry validates the MIN and Digital Signature, that all named Org IDs are active and have appropriate authority for the *Reversal* transaction, and performs any other validations need for the particular transaction.
3. If the validations do not pass, the MERS® eRegistry sends a synchronous XML Response containing an error message to the Requesting Party.
4. If the validations pass, the MERS® eRegistry sends a synchronous XML Response to the Requesting Party indicating the Reversal was successfully processed.

5. The MERS® eRegistry also sends a Notification to any other Authorized Rights Holder named on the eNote Record that has the **Non-Transfer Notifications Member** option selected.
   - For Modification Reversals, only the most recent modification is reversed. If it is the only modification, the MERS® eRegistry removes the Modification Indicator from the eNote Record.
   - For an Assumption Reversal, the MERS® eRegistry removes the Assumption Indicator only if the reversal restores the original borrowers as the current borrowers.
   - For Document Reversals:
     - Only the document of the specified type added most recently is reversed. To reverse a document of that type sent earlier, all subsequent documents of that type must be reversed first.
     - Reversed documents do not appear on the *Document Information* page.
   - For CEMA Modification Reversals: After the modification is reversed, the appropriate Participant must reverse the registration for the CEMA eNote as applicable.

# Audit Information

For Audit purposes, the following data is captured and stored:

- The Requesting and Submitting Party Org IDs associated with the *Change Status* transaction.
- Transaction Time/Date Stamp.
- Type of *Change Status* transaction.
- Before and After values associated with the *Change Status* transaction.

A Participant can view certain Audit information for each eNote Record for which it is an Authorized Rights Holder. See the *MERS® eRegistry OnLine User Guide* for instructions.

# eNote Information

## Overview

Information about *eNotes* registered on the *MERS® eRegistry* is available in *MERS® eRegistry OnLine*, and via the *Inquiry* transaction.

MERS® eRegistry OnLine includes three (3) options for finding eNote information:

- **Find eNote Registration:** Used to display summary information about *eNote Records* on which a *Participant* is an *Authorized Rights Holder*.
- **eReports:** Used to request an extract of information for the eNotes Records on which a Participant is an Authorized Rights Holder.
- **eNote Record Controller History:** Used to retrieve a list of the past and current *Controllers* or Controllers and *Locations* for a specific registered eNote.

The *Delegatee for Transfers* is not considered an Authorized Rights Holder when searching for eNote Records using the *Find eNote Registration* feature, the *Inquiry* transaction, or the *eNote Record Controller History* feature.

# Find eNote Registration

The *Find eNote Registration* option in MERS® eRegistry OnLine displays summary information for eNote Records on which a Participant is a current or previous Authorized Rights Holder, or the *Vendor* that was the *Submitting Party* on the *Registration* transaction. Current Authorized Rights Holders can access all information about the eNote Record, previous Authorized Rights Holders all information up to and including the transaction that removed them as an Authorized Rights Holder, and Vendors that are the *Submitting Party* on the *Registration* transaction all information up to and including the first *Transfer of Control*.

Search can be performed by *MIN*, or by any or all of the following criteria:

**Borrower Information:**

- Name
- Social Security Number (SSN)
- Tax ID Number (TIN)

**Property Information:**

- Address
- County

**eNote Information:**

- Authorized Rights Holders:
  - Controller
  - Servicing Agent
  - Location
  - Delegatee for Transfers
  - Secured Party
  - Secured Party Delegatee

- Registering Org ID
- Vault Identifier
- Status

For more information about the *Find eNote Registration* option, see the MERS® eRegistry OnLine User Guide.

# eReports

The eReports option in MERS® eRegistry OnLine allows a Participant to request an extract of information for the eNote Records on which it is an Authorized Rights Holder. When an extract is complete, a confirmation email is sent to the address the user specified when submitting the extract request. A Participant can then download and manipulate the text file using its internal systems.

For more information about the eReports option, see the MERS® eRegistry OnLine User Guide.

# eNote Record Controller History

The **eNote Record Controller History** option allows all Authorized Rights Holders except a Delegatee for Transfers to retrieve the chronological list of current and past Controllers or Controllers and Locations for an eNote since its registration date. The MIN associated with the eNote is used to retrieve the list which can then be printed for use in legal affidavits and other official documents. The list includes the following fields for each current and past Controller and Location:

| Field | Description |
|---|---|
| Date | The date that the Participant was named as the Controller or Location on the eNote Record in *UTC* format. |
| Rightsholder | The Authorized Rights Holder position (Controller or Location) that the Participant currently holds or previously held. |
| Organization ID | The *Org ID* of the Participant. |
| Organization Name | The corporate name of the Participant from its *Member Profile*. |

# Inquiry Transaction

The *Inquiry* transaction allows a Participant to retrieve status or summary information about an eNote Record for a particular MIN and/or borrower SSN or TIN. The Inquiry Response from the MERS® eRegistry contains the eNote Record information outlined in the table below:

Note: In the table below, the abbreviation “ARH" stands for Authorized Rights Holder.

| Returned Data | Summary Request | | | Status Request |
|---|---|---|---|---|
| | Current ARH | Previous ARH | Non ARH | |
| MIN | Y | Y | Y | Y |
| eNote Status | Y | Y | Y | Y |

| Returned Data | Summary Request | | | Status Request |
|---|---|---|---|---|
| | Current ARH | Previous ARH | Non ARH | |
| Inactive eNote Status Reason | Y | - | - | - |
| Controller Org ID and Name | Y | - | - | - |
| Location Org ID and Name | Y | - | - | - |
| Servicing Agent Org ID and Name | Y | Y | Y | Y |
| Delegatee for Transfers Org ID and Name | Y | - | - | - |
| Secured Party Org ID and Name | Y | - | - | - |
| Secured Party Indicator | - | Y | Y | - |
| Secured Party Delegatee Org ID & Name | Y | - | - | - |
| Borrower Identifier | Y | Y | - | - |
| Borrower Name | Y | Y | - | - |
| Non-Person Indicator | Y | Y | - | - |
| Corporate Name | Y | Y | - | - |
| SSN (or TIN) | Y | | - | - |
| Property Address | Y | Y | - | - |
| Property County | Y | Y | - | - |
| Registration Date | Y | Y | Y | - |
| Lien Type | Y | - | - | - |
| eVault Identifier | Y | - | - | - |
| SMART® Doc Presented Flag & Version | Y | - | - | - |
| Modification Indicator and Type | Y | - | - | - |
| Assumption Indicator | Y | - | - | - |
| Registering Member Org ID and Name | Y | - | - | - |
| eNote Tamperseal Date/Time | Y | - | - | - |
| Transfer Identifier | Y | - | - | - |
| Transfer Effective Date | Y | - | - | - |
| Signature Validation Indicator | Y | Y | Y | - |
| Document Type | Y | Y | Y | - |

Within either a status or summary *Inquiry* transaction, and regardless of whether a Participant is an Authorized Rights Holder on the eNote Record, the *Digital Signature* of an eNote, electronic modification agreement, or other document type added to the eNote Record can be validated, using the Digital Signature, document type, and MIN.

For more information about the *Inquiry* transaction, see the Programming Interface Guide.

# Verify Connectivity

## Overview

To verify connectivity after system maintenance or a system outage, a *Participant* may submit a *Connectivity* transaction, and the *MERS® eRegistry* will respond with both a synchronous XML Response and a *Notification*.

The *Connectivity* transaction is intended to be used for single requests to verify connectivity after maintenance or outage, and not for persistent requests to the MERS® eRegistry; *MERSCORP Holdings* will disable this transaction for any Participant who overuses it.

The *Connectivity* transaction must be signed with a *Digital Certificate* issued by a Certificate Authority approved by MERSCORP Holdings. The Notification from the MERS® eRegistry also will be digitally signed.

## Procedure: Verify Connectivity

1. The *Connectivity* transaction must contain:
    - Request Type of Initiation
    - System Address to which *Notification* is to be sent; either:
        - eRegistry System Address
          (Notification will be sent to the Controller System Address) or
        - eDelivery System Address
    - Optional: *Registry Transaction Identifier*
2. The MERS® eRegistry validates that the *Connectivity* transaction contains all required elements, and all elements are valid.
    - The requesting and submitting *Org IDs* are active and have appropriate authority for the *Connectivity* transaction.
3. If the validations do not pass:
    - The MERS® eRegistry sends a synchronous XML Response to the Requesting Party to indicate receipt and rejection of the *Connectivity* transaction.
    - If a Registry Transaction Identifier was included in the *Connectivity* transaction, it is included in the Response
4. If the validations pass:
    - The MERS® eRegistry sends a synchronous XML Response to the Requesting Party to indicate receipt, validation, and acceptance of the *Connectivity* transaction.
    - The MERS® eRegistry sends a *Connectivity Notification* to the external system address of the Requesting Party in the Participant's Member Profile.

If a Registry Transaction Identifier was included in the *Connectivity* transaction, it is included in both the Response and *Notification*.

# MERS® eDelivery

## Overview

*MERS® eDelivery* provides a method for distributing eMortgage packages from one (1) Participant to another, using the existing MERS® eRegistry infrastructure and transaction security requirements. Transactions use the same standard MISMO request/response envelope messaging and eMortgage Packaging standards and specifications currently used by the MERS® eRegistry. Only Participants that are activated for participation in MERS® eDelivery can use this function.

A Participant will deliver one (1) or more eMortgage packages using an *eDelivery Initiation Request* with a list of Participants who should receive each eMortgage package. Each recipient may accept or reject distribution. If any recipient accepts distribution, the initiating Participant is billed for the transaction.

After accepting distribution, each recipient may use an *eDelivery Approval* to indicate to the sender their approval, disapproval, or conditional approval of the distribution. User defined reason codes and descriptions may be included for each MIN.

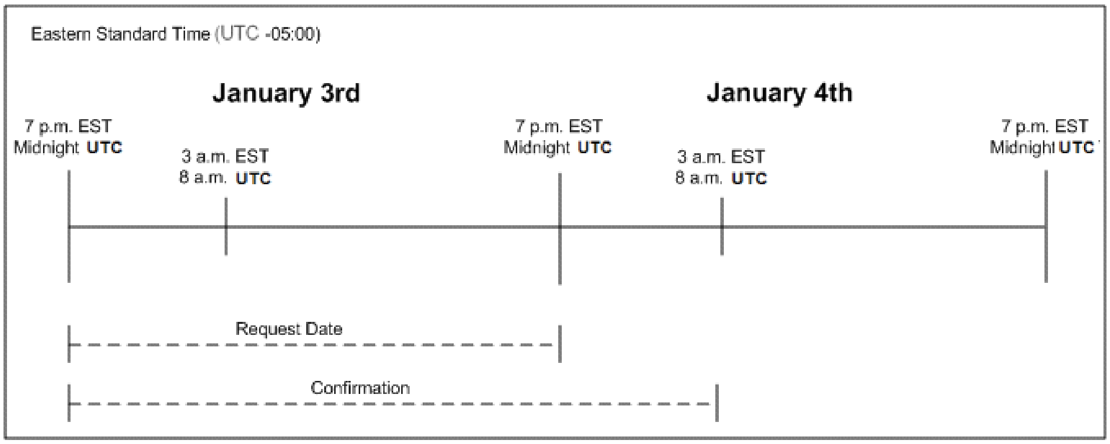
## Data Requirements

- There is a pre-defined size limit of 5MB for each *eDelivery Initiation Request*.
- Each eMortgage package must be identified by a MIN.
- The MIN must be registered on the MERS® eRegistry, or must have been reserved or registered on the MERS® System at least one (1) hour before submitting the *eDelivery Initiation Request*.
- Up to ten recipients may be named in each *eDelivery Initiation Request.*
    - Recipients must be MERS® eDelivery participants
    - Initiator may include itself as a recipient
- The *eDelivery Initiation Request* must contain:
    - Requestor Org ID
    - Recipient Org ID(s)
    - MIN(s)
    - Base64 encoded eMortgage Package(s)
- The *Distribution Approval* must contain:
    - Recipient Org ID
    - *Tracking Number*
    - Approval Type: (Approve, Disapprove, or Conditional)

## Data Options

- The *eDelivery Initiation Request* may contain a destination value.

- A Participant can submit a single XML *eDelivery* message that contains one (1) or more eMortgage packages for delivery. See the *Programming Interface Guide* for details on creating XML messages with multiple eMortgage packages.
- The *eDelivery Approval* may optionally contain:
  - MIN
  - Reason Code (up to 10 alphanumeric characters)
  - Reason Description (up to 100 alphanumeric characters)




# Procedure: MERS® eDelivery

1. A Participant submits an *eDelivery Initiation Request* to MERS® eDelivery.
   - The MERS® eDelivery checks the Org IDs presented in the *eDelivery Initiation Request* to ensure they are active MERS® eDelivery Participants.
   - If a Submitting Party is named, the Requesting Party must have an existing Vendor relationship with the Submitting Party in its Member Profile.
   - Each MIN must be reserved on the MERS® System or registered on the MERS® System and/or the MERS® eRegistry.
   - If at least one (1) valid recipient and at least one (1) valid MIN are included in the *eDelivery Initiation Request*, MERS® eDelivery processes the data in the *Request*.
   - The MERS® eRegistry processes *eDelivery Initiation Requests* when received. *eDelivery Initiation Requests* confirmed by 8:00 AM UTC are processed the next calendar day.
2. MERS® eDelivery sends a synchronous XML Response indicating success or failure for each record in the *eDelivery Initiation Request* to the Requesting Party.
   - If the *eDelivery Initiation Request* is unsuccessful, MERS® eDelivery returns a fail response with the error conditions and any warnings, and no further processing occurs.

     Each response can contain multiple error messages for one (1) eDelivery package. Error messages are detailed in the Programming Interface Guide.
   - If the request is successful, MERS® eDelivery returns a successful response containing the unique Tracking Number associated with the delivery. If multiple requests are sent in one (1)

message, each request will be identified by a separate Tracking Number.

3. MERS® eDelivery sends an *eDelivery Pending Notification* to the eDelivery Address of each named recipient Org ID. This Notification notifies the recipient that a pending eDelivery exists, and contains:
    - Requestor Org ID
    - Tracking Number
    - MIN(s)
    - Destination value, if provided by the requestor
4. The Recipient sends an *eDelivery Confirmation* to accept or reject distribution of the eMortgage package(s) by the Tracking Number.
    - *eDelivery Confirmations* must be completed prior to 8:00 AM UTC for a pending *Initiation Request* received from the previous day.
    - If multiple MINs are included in the same Tracking Number, the recipient must accept or reject for the entire Tracking Number.
5. If the *eDelivery Confirmation* request from the recipient Org ID is reject, the MERS® eDelivery creates an *eDelivery Completion Notification* to indicate the recipient Org ID has rejected the distribution and sends it to the Requesting Party.
    - An optional reason code and description may be included in the *Reject Confirmation,* and will be included in the *eDelivery Completion Notification* sent to the requestor.

    **Note:** These codes and descriptions are not defined by MERS® eDelivery, but by the eDelivery participant. Contact the recipient that supplied the code and/or description for further explanation.

    - Once a reject has been sent, the recipient Org ID cannot send an *eDelivery Confirmation* to accept distribution.
6. If the *eDelivery* Confirmation from the recipient Org ID is to accept distribution, the MERS® eDelivery sends an *eDelivery Distribution* Request to the recipient Org ID, containing the eMortgage package(s), and sends an *eDelivery Completion Notification* to the Requesting Party indicating the recipient Org ID has accepted distribution.
7. The requestor may send an *eDelivery Confirmation* with a type of cancel for the Tracking Number any time before distribution is complete
    - Any *eDelivery Confirmations* for that Tracking Number received after cancellation will be rejected with an error message that the requestor canceled the Tracking Number.
    - Recipients that have already accepted are not impacted as they have already received distribution.
8. At 8:00 AM UTC any pending *eDelivery Requests* from the previous day will expire.
    - The previous day activity is defined from 00:00:00 to 23:59:59 UTC.
    - Any recipient Org ID that did not send an *eDelivery Confirmation* will receive an *eDelivery Completion Notification* indicating expiration.

- The Requesting Party will receive an *eDelivery Completion Notification* indicating expiration for each recipient Org ID that did not send an *eDelivery Confirmation*.

9. If any recipient accepts a MERS® eDelivery distribution, the requestor is billed for each eMortgage package within the Tracking Number.
   - The billing appears on the MERS® System.
   - The *Billing Reconciliation Report* (LB) and *Monthly Billing Transaction Report* (LD) will contain the billing code for MERS® eDelivery transactions along with the MINs.
10. Within 30 days of the original distribution, any recipient who has accepted the distribution may send a *Distribution Approval Request* to MERS® eDelivery.
    - Approval Type applies to the entire Tracking Number and may be:
      - Approve
      - Disapprove
      - Conditional

    **Note:** These Types are not defined by MERS® eDelivery, but by the eDelivery participant. Contact the recipient that supplied the approval for further explanation.

    - Reason Code(s) and/or Description(s) may be included for each MIN, and will be included in the *eDelivery Approval Notification* sent to the requestor.
      - Each MIN in the request must be included in that Tracking Number
      - Any MIN included must have one (1) or more Reason Code(s) and/or Description(s)
      - Any Reason code and/or Description included must be associated with a MIN

    **Note:** These codes and descriptions are not defined by MERS® eDelivery, but by the eDelivery participant. Contact the recipient that supplied the code for further explanation.

    - The MERS® eDelivery checks to ensure the Org ID sending the Request is a Recipient for the Tracking Number included.
    - If a Submitting Party is named, the Requesting Party must have an existing Vendor relationship with the Submitting Party established in its Member Profile.
11. MERS® eDelivery sends a synchronous XML Response indicating success or failure of the Distribution Approval Request.
    - If the request is unsuccessful, MERS® eDelivery returns a fail response to the Requesting Party with the error conditions and any warnings, and no further processing occurs.
    - If the request is successful, MERS® eDelivery returns a success response to the Requesting Party.
12. MERS® eDelivery sends an *eDelivery Approval Notification* to the eDelivery Address of the Requestor Org ID for that Tracking Number. This Notification contains:
    - Recipient Org ID
    - Tracking Number
    - Approval Code
    - MIN(s), Reason Code(s) and Description(s), if included in the Distribution Approval Request

# Audit Information

- Audit information stored for MERS® eDelivery includes:
- Requestor
- Recipients
- MIN(s)
- All Confirmations
- Completion status
- Recipient Approval Information
- A Participant can view certain the information for each eDelivery made by or to it. See the MERS® eRegistry OnLine User Guide for instructions.

# MERSCORP Holdings Help Desk

## Overview

The MERSCORP Holdings *Help Desk* serves as a point of contact for MERS® eRegistry Participants regarding the use of the *MERS®* products and services, including:

- Distribution of corporate communications from MERSCORP Holdings.

  Participants should whitelist *MERS-Broadcast@mersinc.org* and *helpdesk@mersinc.org* to ensure that they receive communications sent from these email addresses.
- Functional and procedural questions about the MERS® eRegistry and MERS® eDelivery.
- Technical support, including MERS® eRegistry and MERS® eDelivery connectivity.

Other highlights of the MERSCORP Holdings Help Desk include:

- After-hours technical support for emergency technical issues.

## Contacting the MERSCORP Holdings Help Desk

- A Participant contacts the MERSCORP Holdings Help Desk by phone at 1-888-680-MERS (6377) from 8 a.m. to 8 p.m. ET, Monday through Friday or by email at *helpdesk@mersinc.org*.
- Once the Participant provides its Org ID to the Help Desk representative, a Case Number is assigned to track the inquiry and ensure a timely resolution.
- The Case is worked and a response is provided to the Member.
- The Help Desk confirms with the Participant that it has received the response.

# MERS® eRegistry Quality Assurance Program

In addition to the requirements that each Participant is required to adhere to as a MERS® System Member, each Participant is required to have policies and procedures in place to ensure compliance with all of the requirements set forth in the *Procedures* and the *MERS® eRegistry Addendum to the MERS® System Membership Agreement* ("*Addendum*") and integrate these requirements into its business processes.

Key components of the MERS® eRegistry QA Program include the following:

- **MERS® eRegistry *QA Plan*:** Confirms that a Participant has reviewed and is in compliance with the requirements set forth in the *Procedures* and *Addendum*. For details, refer to *MERS® eRegistry QA Plan*.
- **Data Reconciliation:** A Participant must reconcile all required records on the MERS® eRegistry against its internal records on a quarterly basis. For details, refer to *Data Reconciliation*.

## Requirements: MERS® eRegistry QA Program

- Each Participant is required to have policies and procedures in place to ensure compliance with the requirements set forth in the *Procedures* and *Addendum* and integrate these requirements into its business practices.
- When a Participant identifies a data mismatch between its internal records and the MERS® eRegistry, the mismatch must be corrected no later than 30 business days after discovering the mismatch.

## MERS® eRegistry QA Plan

Each Participant with the ability to perform transactions on the MERS® eRegistry is required to have in place a current *eRegistry QA Plan* using MERSCORP Holdings' *QA Plan* template. The *eRegistry QA Plan* does not reference all of the requirements in the *Procedures* and *Addendum*. If a specific requirement is not included in the *eRegistry QA Plan*, a Participant must nonetheless comply with it.

By submitting an *eRegistry QA Plan*, a Participant confirms that it is in compliance with the requirements set forth in the *Procedures* and *Addendum* as of a given date. A submitted *eRegistry QA Plan* covers the Participant's activity since its last submitted *eRegistry QA Plan* and may include activity from the prior calendar year.

Each Participant must monitor and audit its performance against the requirements set forth in the *Procedures* and *Addendum* using a random sample of its loans with the results meeting or exceeding these requirements.

### *Requirements: MERS® eRegistry QA Plan*

Each Participant with the ability to perform transactions on the MERS® eRegistry is required to:

- Have a current *eRegistry QA Plan* in place for each active Org ID, which also covers any associated *Affiliate Org ID*, using MERSCORP Holdings' *QA Plan* template,
- Submit its completed *eRegistry QA Plan* by December 31st of the current year,
- Save a copy of its completed *eRegistry QA Plan* for its records,
- Review its implementation of the *eRegistry QA Plan* as needed to ensure it is accurate and effective and continues to support the requirements set forth in the *Procedures* and *Addendum*.
- Monitor its performance against its current *eRegistry QA Plan*, and
- Use a random sample of its loans when self-auditing its performance against its *eRegistry QA Plan* with the results meeting or exceeding the requirements in the *Procedures* and *Addendum*.

## *Procedure: MERS® eRegistry QA Plan Submission*

Only individuals listed as MERS® System mandatory contacts for an Org ID are authorized to complete and submit the Participant's *eRegistry QA Plan* to MERSCORP Holdings using the **eQARequirements** tool on the *Member website*.

To help protect the confidentiality of Member information, the **eQAPlan** tool does not email a copy of an accepted *eRegistry QA Plan* to a Participant.

# Data Reconciliation

Each Participant named as the Controller or Servicing Agent on the MERS® eRegistry is required to perform quarterly data reconciliations as detailed in this section to ensure that the data on the MERS® eRegistry is accurate and aligns with any corresponding data in the Participant's internal records (e.g., the Participant's loan origination or servicing system).

A Participant can access the data from the MERS® eRegistry required for this reconciliation by requesting a *Reconciliation eReport* in *MERS® eRegistry Online*. Refer to the *MERS® eRegistry OnLine User Guide* for details on requesting this report.

## *Requirements: Data Reconciliation*

- Each Participant named as the Controller or Servicing Agent on one (1) or more active eNote Records is required to perform quarterly data reconciliations.
- The data on the MERS® eRegistry for all of the Participant's active eNote Records must match the corresponding data in the Participant's internal records (e.g., the Participant's loan origination or servicing system).

### Controller Data Reconciliation Requirements

Each Participant named as the Controller on one (1) or more active eNote Records must reconcile:

**1. Controller:**

- The list, from the Participant's internal records, of all active eNotes for which the Participant has *Control* of the Authoritative Copy of the eNote *against*

- The list, from the MERS® eRegistry, of all active eNote Records that name the Participant as Controller.

**2. Location:**

- The list, from the Participant's internal records, of *Locations* for all active eNotes for which the Participant has *Control* of the Authoritative Copy of the eNote

  *against*

- The list, from the MERS® eRegistry, of Participants named as Location for all active eNote Records on which the Participant is named Controller.

**3. Servicing Agent:**

- The list, from the Participant's internal records, of servicing agents for all active eNotes for which the Participant has *Control* of the Authoritative Copy of the eNote

  *against*

- The list, from the MERS® eRegistry, of Participants named as Servicing Agents for all active eNote Records on which the Participant is named Controller.

**4. Paid Off and Charged Off Deactivations:**

Controllers must verify that any *Paid Off* and *Charged Off Deactivation* transactions submitted since the date of their last reconciliation, were submitted to the MERS® eRegistry no later than five (5) business days after the servicing event that triggered the pay-off or charge-off by reconciling:

- The Controller's internal records showing when the pay-off or charge-off occurred

  *against*

- The date when the corresponding *Paid Off* or *Charged Off* transactions was reported to the MERS® eRegistry.

Note: If the deactivated eNote Records identify a Servicing Agent, the Controller may requests that the Servicing Agent perform this reconciliation.

## Servicing Agent Data Reconciliation Requirements

Each Participant named as the Servicing Agent on one (1) or more active eNote Records must reconcile:

- The list, from the Participant's internal records, of all active eNotes for which the Participant is acting as the Servicing Agent

  *against*

- The list, from the MERS® eRegistry, of all active eNote Records that name the Participant as Servicing Agent.

# *Data Review*

In addition to the Data Reconciliation requirement, a Controller may be required to complete a Data Review in which the Controller provides a file containing data from its internal records that MERSCORP Holdings uses to verify that:

- The Controller is named as such on the appropriate active eNote Records,
- The correct Participant is named as Location, and
- The correct Participant is named as Servicing Agent.

The outcome of a Data Review may include an action plan for the Participant to address.

# MERS® eRegistry Processing Standards

Uniform processing standards for registering and maintaining eNotes Records are critical for the MERS® eRegistry because it is the *System of Record* for establishing the *Participant* with Control of eNotes and the Location of the Authoritative Copy of each eNote registered on the MERS® eRegistry.

The MERS® eRegistry processing standards for eNote Records, and data integrity follows.

## *eNote Registration Processing Standards*

- Participant has procedures in place to ensure that any eNote it registers, or for which it is subsequently named an *Authorized Rights Holder*, conforms to the requirements set forth in the *Procedures* and *Addendum*.
- Participant has procedures in place to ensure that any eNote it originates, or for which it is subsequently named as an Authorized Rights Holder, is registered on the MERS® eRegistry no later than one (1) business day after the final tamper sealing of the eNote.

## *Data Update Processing Standards*

- Participant has procedures in place to ensure that any update to an eNote Record's data on which it is named Controller is reported to the MERS® eRegistry no later than one (1) business day after it has discovered an error in the eNote Record information.

## *Modification Processing Standards*

- For electronic modifications, Participant has procedures in place to ensure that any eNote Record on which it is named Controller is updated to reflect electronic modifications no later than one (1) business day after the final tamper sealing of an electronic modification agreement.
- For paper modifications, the Participant has procedures in place to ensure that any eNote Record on which it is named Controller is updated to reflect the modification no later than three (3) business days after the date that the modification agreement was fully executed.
- For CEMA modifications where the CEMA note is an eNote, the Participant has procedures in place to ensure the following for any CEMA eNote it originates:
  - The CEMA eNote is registered on the MERS® eRegistry using a new MIN no later than one (1) business day after the final tamper sealing of the eNote, and
  - The CEMA modification is reported on the original eNote Record modified by the CEMA eNote on the same business day that the CEMA eNote was registered.

- For CEMA modifications where the CEMA note is paper, the Controller of the eNote being modified by the CEMA note has procedures in place to ensure that the eNote Record is deactivated on the MERS® eRegistry as *Converted to Paper* no later than five (5) business days after the eNote was converted to a paper note.

## Assumption Processing Standards

- Participant has procedures in place to ensure that any eNote Record on which it is named Controller is updated on the MERS® eRegistry to reflect a change in Borrower information due to an Assumption agreement no later than (3) business days after the date that the Assumption agreement was fully executed.

## Paid Off Processing Standards

- Participant has procedures in place to ensure that any eNote Record on which it is named Controller is deactivated on the MERS® eRegistry as *Paid Off* no later than five (5) business days after the underlying debt was cancelled due to a pay-off.

## Charged Off Processing Standards

- Participant has procedures in place to ensure that any eNote Record on which it is named Controller is deactivated on the MERS® eRegistry as *Charged Off* no later than five (5) business days after the underlying debt was cancelled due to a charge-off.

## Member Information Update Standards

- Participant has procedures in place to ensure that the MERS® eRegistry information in its *Member Profile* is reviewed monthly to ensure that all information remains accurate and up to date. This includes, but is not limited to, the Participant's *MERS® eRegistry Contact*, MERS® eRegistry Relationships, and MERS® eRegistry settings and Member Profile options.
- The external eRegistry System Addresses in the Member Profile of the Participant's Org ID must be available to accept MERS® eRegistry *Notifications*.
- For MERS® eDelivery Participants, the external eDelivery Address in the Member Profile of the Participant's Org ID must be available to accept MERS® eDelivery Notifications.

## Data Integrity Standards

- The current borrower name(s) on the eNote Record must match the borrower name(s) on the eNote.
- For assumed loans, the current borrower name(s) on the eNote Record must match the borrower name(s) on the Assumption documents, and the original borrower name(s) on the eNote Record must match the borrower name(s) on the eNote.
- The borrower SSN or TIN on the eNote Record must match the SSN or TIN reported to the IRS on Form 1098.

- The property address on the eNote Record must match the property address on the eNote unless the subject address has been changed by governmental decree.
- The Tamperseal Date on the eNote Record must match the Note Date specified in the eNote.

# Appendix A: Secured Party Terms and Conditions

*MERSCORP Holdings* will not be a party to and does not have any obligation to have knowledge of, or to comply with, the terms and conditions of separate agreements between or among *Participants* pertaining to (i) the use of the *Secured Party* field, (ii) the rights or obligations of a Secured Party, (iii) the rights or obligations of a *Controller*, or (iv) the rights or obligations of a *Secured Party Delegatee*. Furthermore, MERSCORP Holdings shall not have any obligation to determine whether any Participant has complied with any such agreements.

The following, as applicable to their business arrangements, shall be determined solely by separate agreement between Participants that elect to utilize the Secured Party or Secured Party Delegatee fields on the *MERS® eRegistry*:

- The timing and conditions under which a Participant shall be named in the Secured Party field or the Secured Party Delegatee field;
- The timing and conditions under which the Participant named in the Secured Party field may reverse, or through its Secured Party Delegatee cause the reversal of, its entry in that field;
- The conditions under which the Participant named in the Secured Party field may permit or prohibit the deactivation of *eNote Records*;
- The timing and conditions under which the Participant named in the Secured Party field, or the Secured Party Delegatee field, shall initiate a *Change Data* transaction to release the Secured Party from the Secured Party field;
- The timing and conditions under which the Participant named in the Secured Party field, or the Secured Party Delegatee field, may initiate any transfers on the MERS® eRegistry to itself or another Participant;
- The timing and conditions under which the Participant named in the Secured Party field, or the Secured Party Delegatee field, shall provide its *Confirmation* of any transfers on the MERS® eRegistry that it did not initiate;
- The conditions under which a Participant may request that MERSCORP Holdings perform certain transactions on the MERS® eRegistry as described in the section of the *Procedures* titled *MERS® eRegistry Certificate Form Process*; or
- Any other conditions associated with a Participant’s business arrangements, agreements, or procedures with another Participant.

# Glossary

The following defined terms are intended to provide a general vocabulary for communication among MERSCORP Holdings and MERS® System Members in connection with their use of the MERS® eRegistry. The terms below are not intended to modify, alter, amend, supplement, nullify, or supersede the legal meaning of these same terms under the Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Uniform Electronic Transactions Act (UETA), as may be amended from time to time, or other applicable law.

| Term | Definition |
|---|---|
| ***Affiliate Org ID*** | An additional *Org ID* issued to a *Primary Member* pursuant to a *Primary/ Secondary Relationship Agreement*. An Affiliate Org ID may be used by a Primary Member to identify a department, line of business, or internal division of such Primary Member. An Affiliate Org ID shall not be used to identify a distinct legal entity. |
| ***Allow Servicing Agents*** | A Member Profile option in MERS® OnLine that determines if a Controller allows Servicing Agents to submit MERS® eRegistry transactions on its behalf. |
| ***Assumption*** | A MERS® eRegistry transaction used to report a change to one (1) or more borrowers on an eNote. |
| ***Assumption Reversal*** | The transaction used to reverse an *Assumption* transaction that was done in error. |
| ***Authoritative Copy*** | The unique, identifiable, and unalterable copy of the Transferable Record (eNote) maintained within the *Control* environment established by the Controller. |
| ***Authorized Rights Holders*** | Participants that are currently associated with the eNote Record on the MERS® eRegistry (Control, Location, Secured Party, Secured Party Delegatee, Delegatee for Transfers, and Servicing Agent). |
| ***Business Integration Resource (BIR)*** | The MERSCORP Holdings employee who helps a MERS® System Member incorporate the MERS® eRegistry into its business processes. |
| ***Broker*** | An *LOB* that allows a MERS® System Member to originate *eNotes* for sale to a *Participant* that will act as *Delegatee for Transfers* for the Broker, registering the eNote on the *MERS® eRegistry* on behalf of the Broker and then immediately processing a *Transfer of Control* from the Broker to the Delegatee for Transfers. |
| ***CEMA*** | A New York loan closed using a *Consolidation, Extension, and Modification Agreement* ("CEMA") to combine an existing promissory note(s) with a new promissory note and an existing mortgage(s) with a new mortgage to create a consolidated note and consolidated mortgage evidencing a single loan obligation. |

| Term | Definition |
|---|---|
| ***Certificate Authority*** | A trusted third-party entity authorized to issue, manage, revoke, and renew *Digital Certificates*. Also known as an Issuing Authority. A Certificate Authority, approved by *MERSCORP Holdings*, issues, manages, and revokes the Digital Certificates used to sign the MERS® eRegistry XML Requests. |
| ***Certificate Revocation List (CRL)*** | A list of *Digital Certificates* that were revoked prior to their expiration date by the *Certificate Authority* that issued them. The *MERS® eRegistry* uses a CRL as part of its Digital Certificate validation process. |
| ***Change Data*** | A MERS® eRegistry transaction used to request a change of data on the eNote Record. |
| ***Change Status*** | A MERS® eRegistry transaction used to request a change to the current status of the eNote Record and reverse certain transactions defined by the *Change Data* DTD. |
| ***Charged Off*** | In the context of these Procedures, a *Change Status* transaction and eNote status on the MERS® eRegistry used to report a charge-off when the borrower is no longer obligated to make payments or satisfy any other terms or conditions required by the eNote. |
| ***Check Digit*** | The final digit of the MIN calculated using the MOD 10 Weight 2 algorithm. The MERS® eRegistry uses the check digit during registration to verify that the MIN is valid. |
| ***Confirmation*** | An XML Request used by an *Authorized Rights Holder* to accept, reject, or reset a pending *Transfer* on the MERS® eRegistry or accept or reject an eDelivery. |
| ***Control*** | A *Participant* has control of a Transferable Record if a system employed for evidencing the transfer of interests in the Transferable Record reliably establishes that Participant as the Participant to which the Transferable Record was issued or transferred pursuant to Section 16 of UETA and Section 201 of E-SIGN. |
| ***Controller*** | The Participant named on the MERS® eRegistry that has *Control* of the *eNote* and its *Authoritative Copy*. |
| ***Controller Delegatee for Transfers*** | An eRegistry relationship that allows a Participant to register an eNote on behalf of a Broker that has no access to the MERS® eRegistry and then transfer Control of the eNote to itself or another Participant. |
| ***Converted to Paper*** | A *Change Status* transaction and eNote status that indicates the eNote has been converted to a paper note. |
| ***Data Point Registration*** | One of two (2) eNote *Registration* transactions. The eNote is not included in the *Registration* transaction for Digital Signature validation. See also, *eMortgage Package Registration*. |
| ***Counterparty Org ID*** | Optional field that allows the current Controller to identify another Participant associated with an eNote (e.g., original Lender or aggregator) when transferring Control of the eNote, allowing a *Warehouse Lender* to identity the |

| Term | Definition |
|---|---|
| | counterparty on whose behalf the Transfer of Control of an eNote is being made to the new Controller. |
| ***Delegatee for Transfers (DT)*** | A Participant that is authorized by a Controller to perform certain MERS® eRegistry transactions on the Controller's behalf. The DT can initiate registrations and transfers of control, but may not initiate *Change Status* transactions, or *Data Update* transactions except to remove itself as DT. |
| ***Digital Certificate*** | A computer-based file that is issued to a Participant by a Certificate Authority as a form of digital identification. The Digital Certificate used by the MERS® eRegistry binds together a cryptographic key pair (public and private), an application, and a Participant. A Participant uses its Digital Certificate to digitally sign the XML messages it submits to the MERS® eRegistry. |
| ***Digital Signature*** | An encrypted, algorithmically-generated string, calculated using an electronic message or document as input, that is used to establish the authenticity of that message or document and its sender. The MERS® eRegistry uses the Digital Signature applied by a Participant to its XML messages to authenticate the identity of the Participant, ensure the integrity of the data in the message, and verify that no changes were made to the message since the signature was applied. The MERS® eRegistry also applies a Digital Signature to the asynchronous XML messages it sends to Participants. Also known as a "Tamper-Evident Digital Signature" or "Tamperseal". |
| ***DTD*** | Acronym for **Document Type Definition**. A file that defines the structure of an XML message and describes the data in the message. The MERS® eRegistry *XML Interface* is defined by a set of DTD files. |
| ***eMortgage Package Registration*** | One of two (2) available eNote *Registration* transactions, The eNote is included in the *Registration* transaction for Digital Signature validation. See also, *Data Point Registration*. |
| ***eNote*** | A *Transferable Record* that is registered on the MERS® eRegistry. |
| ***eNote Modification*** | A *Change Data* transaction on the MERS® eRegistry reflecting a change to one (1) or more provisions of a specified eNote. |
| ***eNote Record*** | The data record that is created when a Participant registers an eNote on the MERS® eRegistry. |
| ***eNote Status*** | The field reflecting the current status of an eNote registered on the MERS® eRegistry. |
| ***eRegistry Contact*** | A *MERS® System* contact who is responsible for responding to *MERS® eRegistry* questions on behalf of a *Participant*. |
| ***E-SIGN*** | Acronym for **Electronic Signatures in Global and National Commerce Act**. A federal statute that establishes the legal validity and enforceability of electronic signatures, contracts, and other records in interstate and foreign commerce transactions, if not superseded by certain state laws otherwise authorizing such activities. |

| Term | Definition |
|---|---|
| ***eVault*** | An application that serves as an electronic repository for delivery and storage of eNotes and other mortgage-related files. |
| ***Executive Sponsor*** | Mandatory MERS® System contact responsible for an organization's MERS® eRegistry and MERS® System operations. |
| ***Help Desk*** | The point of contact regarding the use of the MERS® products and services. Phone: (888) 680-MERS, Email *helpdesk@mersinc.org*. |
| ***Integration*** | The process by which a Participant completes the required procedural changes, training, system testing, and unit testing of transactions prior to being live in the MERS® eRegistry production environment. |
| ***Investor*** | As it pertains to the MERS® eRegistry, the entity that is the owner of the Mortgage Loan represented by the eNote. |
| ***Lender*** | The payee on the eNote. |
| ***LOB*** | Acronym for **Line of Business**. The types of business in which a Member is active on the MERS® System. These are listed on the Member Profile. |
| ***Location*** | The Participant named on the MERS® eRegistry that maintains the Authoritative Copy of the eNote. |
| ***Member Profile*** | Contains a Participant's transaction processing options and configuration settings for the MERS® eRegistry. This information is provided by a Participant during *Integration* and is maintained in MERS® OnLine. |
| ***Membership Agreement*** | The *MERS® System Membership Application*, *Rules of Membership*, and *Procedures Manual* collectively constitute the Membership Agreement. If a Member elects to become a Participant, it is also bound by the *MERS® eRegistry Addendum to MERS® System Membership Agreement*. |
| ***MERS*** | Acronym for **Mortgage Electronic Registration Systems, Inc.**, a Delaware corporation and wholly-owned subsidiary of *MERSCORP Holdings*. |
| ***MERS®*** | The trademark used by *MERSCORP Holdings* in connection with certain products and/or services. |
| ***MERS® eDelivery*** | A secure method for distributing eMortgage packages from one (1) Participant to another, using the existing MERS® eRegistry infrastructure and transaction security requirements. |
| ***MERS® eRegistry*** | The *System of Record* that identifies the *Controller* of a registered eNote and the *Location* of the *Authoritative Copy* of the *eNote*. |
| ***MERS® eRegistry OnLine*** | Browser-based inquiry access to the MERS® eRegistry. URL: *https://www.merseregistryonline.org*. |
| ***MERS® eRegistry Participant ("Participant")*** | A MERS® System Member that has signed and submitted the *MERS® eRegistry Addendum to MERS® System Membership Agreement* to MERSCORP Holdings and completed its Integration to the MERS® eRegistry. |

| Term | Definition |
|---|---|
| ***MERS® eRegistry Procedures Manual ("Procedures")*** | Sets out requirements pertaining to the use of the *MERS® eRegistry* and the MERS® eRegistry Quality Assurance Program. |
| ***MERS® Integration Contact*** | Person responsible for managing the implementation and Integration of the MERS® eRegistry process into the Participant's operations. |
| ***MERS® OnLine*** | The browser-based interface to the *MERS® System* used to view and update registered Mortgage loans and update a Participant's *Member Profile*. URL: *https://www.mersonline.org*. |
| ***MERS® System*** | The national electronic registry owned and operated by MERSCORP Holdings that tracks changes in Mortgage servicing rights and beneficial ownership interests in loans secured by residential real estate. |
| ***MERSCORP Holdings*** | MERSCORP Holdings, Inc. (formerly known as MERSCORP, Inc.), a Delaware corporation that owns and operates the various MERS® products and services including the MERS® eRegistry and MERS® eDelivery. MERSCORP Holdings is the parent company and service provider to MERS. |
| ***MIN*** | Acronym for **Mortgage Identification Number**, a unique 18-digit number permanently assigned to an eNote registered on the MERS® eRegistry or a Mortgage loan registered on the MERS® System. |
| ***MISMO*** | Acronym for Mortgage Industry Standards Maintenance Organization, the voluntary standards development body for the mortgage industry. MISMO® is a wholly owned subsidiary of the Mortgage Bankers Association. |
| ***Modification*** | The transaction used to report that the terms of an eNote registered on the MERS® eRegistry have been modified. |
| ***Modification Reversal*** | The transaction used to reverse a *Modification* transaction that was done in error. |
| ***MOM*** | A loan secured by a MERS as Original Mortgagee security instrument. The language written into a MOM Security Instrument establishes MERS as the Mortgagee and Nominee for the Lender, its successors and assigns. |
| ***Mortgage*** | An interest in or a lien against property created by a written instrument providing security for the repayment of a debt and/or the performance of a duty. References herein include deed(s) of trust, Mortgages and security deeds, and any other form of security instrument under applicable law. |
| ***Mortgagee*** | The party that takes, holds, or receives a pledge of an interest in or lien against property as security for the payment of debt; the pledge is evidenced by a Mortgage and recorded in the applicable public land records. References herein to "Mortgagee" include the named beneficiary or nominee of the lender under a deed of trust in those jurisdictions where deeds of trust are used to secure loans, and any similar status as used in connection with any other form of security instrument under applicable state law. |

| Term | Definition |
|---|---|
| ***Notification*** | An asynchronous XML message generated by the MERS® eRegistry to inform the appropriate parties named on an eNote Record that a pending transaction is awaiting their review and decision, or that an event or action has occurred. See the *Programming Interface* for the complete list of Notifications generated by the MERS® eRegistry. |
| ***Nominee*** | A person or entity designated to act for another as representative in a limited sense; the agency relationship specifically expressed in the terms of the Fannie Mae / Freddie Mac Uniform security instruments identifying MERS as Original Mortgagee (MOM). |
| ***Org ID*** | Acronym for **Organization Identification Number,** a seven (7) digit number uniquely identifying a Member of the MERS® System and optionally a Participant of the MERS® eRegistry. |
| ***Original Borrower*** | The person(s) listed as the borrower on the original note. In the case of an Assumption, this field on the MERS® eRegistry reflects the person(s) who were originally named as the borrowers on the associated eNote. |
| ***Paid Off*** | A *Change Status* transaction and eNote status on the MERS® eRegistry reflecting a payoff of a specified eNote. |
| ***Paper Modification*** | The Modification Agreement is done on a paper instrument, instead of electronically. The MERS® eRegistry must be updated to reflect that the paper modification exists. |
| ***PKI*** | Public Key Infrastructure. A cryptographic framework that provides the basis for establishing and maintaining a trustworthy networking environment through the generation and distribution of keys and Digital Certificates. |
| ***Primary Member*** | The *Participant* designated as the Primary Member on a *Primary/Secondary Relationship Agreement*. |
| ***Primary/Secondary Relationship Agreement (PSRA)*** | An agreement establishing a relationship between a *Primary Member* and a *Secondary Member*(s) and/or *Affiliate Org ID(s)* creating certain obligations and benefits based on such relationship. |
| ***Quality Assurance Officer*** | Mandatory MERS® System contact responsible for the Participant's MERS® eRegistry QA Program. |
| ***Registration*** | The transaction used to send the required information to the MERS® eRegistry to report that an eNote exists that was originated with the MERS® eRegistry language. |
| ***Registration and Transfer of Control*** | The transaction used by a Delegatee for Transfers to submit a *Registration* transaction on behalf of another Participant with which it has a Broker relationship and then transfer Control of the eNote from the Broker to itself or a Warehouse Lender. |
| ***Registration Reversal*** | The transaction used to reverse an eNote Registration that was registered on the MERS® eRegistry. |

| Term | Definition |
|---|---|
| ***Registry Transaction Identifier*** | Participant-defined value that can be used to identify the Request in the initiating system (e.g., GUID ("Global Unique Identifier")). |
| ***Requesting Party*** | The Participant identified in a MERS® eRegistry XML Request as being authorized to submit the transaction to the MERS® eRegistry. |
| ***Seasoned Transfer*** | A billing designation for a transfer transaction with a Transfer Date that is more than 270 calendar days after the eNote's Registration Date. The seasoned loan transfer fee is charged to the Participant initiating the transaction. |
| ***Secondary Member*** | The *Participant* designated as the Secondary Member on a *Primary/Secondary Relationship Agreement*. |
| ***Secured Party*** | The Participant named on the MERS® eRegistry that has been sold, pledged, assigned, or granted a security interest in the *eNote* by the *Controller*. |
| ***Secured Party Delegatee*** | The Participant authorized by the *Secured Party* to perform certain MERS® eRegistry transactions on the Secured Party's behalf. |
| ***Servicing Agent*** | A Participant that is authorized by the Controller to perform certain MERS® eRegistry transactions on the Controller's behalf. |
| ***SMART® Doc*** | An electronic document based on a *MISMO* specification that locks together a document's data, visual presentation, and signatures such that it prevents subsequent tampering and can be programmatically validated to guarantee the original document's integrity. |
| ***SMART® Doc Presented*** | A field that indicates if a SMART® Doc *eNote* was presented successfully to the MERS® eRegistry for *Digital Signature* validation. |
| ***SSN*** | Acronym for Social Security Number. |
| ***Submitting Party*** | A Participant that submits a transaction to the MERS® eRegistry on behalf of another Participant identified as the *Requesting Party* in an XML Request. |
| ***System of Record*** | Authoritative system recognized to establish the identity of the *Controller* of a registered *eNote* and the *Location* of the *Authoritative Copy* of the eNote. See *MERS® eRegistry*. |
| ***System-to-System*** | A method of transmitting data directly between a Participant's or Vendor's external system and the MERS® eRegistry. |
| ***Tamperseal Date*** | The date and time a Digital Signature was applied to an electronic document. Also known as a Tamper-Evident Digital Signature Date. |
| ***TIN*** | Acronym for Tax Identification Number. |
| ***Tracking Number*** | A unique number that the MERS® eDelivery assigns to each eDelivery request for identification purposes. |
| ***Transfer All*** | A MERS® eRegistry transfer transaction used to request a change to the current Controller, Location, and Servicing Agent. |

| Term | Definition |
|---|---|
| ***Transfer Effective Date*** | The date a pending transfer transaction will be processed by the MERS® eRegistry. |
| ***Transfer Identifier*** | A unique tracking number assigned to a group of one or more *eNote Records* in a *Transfer* transaction when the MERS® eRegistry successfully processes a *Transfer Initiation Request*. |
| ***Transfer of Control*** | A MERS® eRegistry transfer transaction used to request a change to the current Controller. |
| ***Transfer of Control and Location*** | A MERS® eRegistry transfer transaction used to request a change to the current Controller and Location. |
| ***Transfer of Control and Servicing Agent*** | A MERS® eRegistry transfer transaction used to request a change to the current Controller and Servicing Agent. |
| ***Transfer of Location*** | A MERS® eRegistry transfer transaction used to request a change to the current Location. |
| ***Transfer of Servicing Agent*** | A MERS® eRegistry transfer transaction used to request a change to the current Servicing Agent. |
| ***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*. |
| ***Transferred to Proprietary Registry*** | A *Change Status* transaction and eNote status that indicates the eNote has been transferred out of the MERS® eRegistry to another registry. |
| ***UETA*** | Uniform Electronic Transaction Act. A uniform form of statute that various states have enacted to establish the legal validity and enforceability of electronic signatures, contracts, and other records within the enforcing state. |
| ***UTC*** | Coordinated Universal Time. UTC is also referred to as GMT (Greenwich Mean Time) and is the global standard for time. All date and time data submitted to, sent by, and recorded in the MERS® eRegistry must be represented using the UTC time standard.<br>Example: Wednesday, midnight UTC is equivalent to Tuesday, 8:00 PM EDT (UTC-4 hours) and Tuesday 5:00 PM PDT (UTC-7 hours). |
| ***Vault Identifier*** | Provides additional information for locating the *Authoritative Copy* of an eNote. |
| ***Vendor*** | A Participant that has been contracted by an Authorized Rights Holder to (1) enter data, initiate transactions, or register loans on the MERS® eRegistry on their behalf or (2) act as a technology provider enabling them to enter data, initiate transactions, or register loans on the MERS® eRegistry. |

| Term | Definition |
|---|---|
| ***Warehouse Lender*** | A Participant with an interim funding interest in an eNote prior to the transfer of the eNote to an Investor. |
| ***W3C*** | World Wide Web Consortium. The World Wide Web Consortium was created to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. |
| ***X509*** | The standard that defines the format of the public certificates (i.e., Digital Certificates) in the Public Key Infrastructure ("PKI") used by the MERS® eRegistry to encrypt data transmitted to/from the MERS® eRegistry and digitally sign the XML messages sent to/by the MERS® eRegistry. |
| ***XML*** | Acronym for **Extensible Markup Language** which, in the context of the Procedures, defines the set of rules for encoding synchronous System-to-System transactions to or from the MERS® eRegistry. |
| ***XML Interface*** | The synchronous *System-to-System* interface that uses XML messages (Requests and Responses) to transact with the *MERS® eRegistry*. The XML Requests and Responses are defined by the MERS® eRegistry *DTDs*. |