MISMO eClosing System Certification Requirements

Version 1

February 5, 2021

Certification Requirements for eClosing Systems

Summary

This document outlines a baseline set of technical and procedural requirements ("Requirements") that should be considered applicable to real estate mortgage eClosing Systems. Parties may elect or otherwise be required to implement additional and/or more stringent requirements, practices, or processes for the items addressed by these Requirements. While not specifically addressed in these Requirements, the implementation of eClosing Systems should accommodate the Americans with Disabilities Act's (ADA) computer user interface standards and/or best practices, as may be required by state and/or federal law.

Capitalized terms not specifically defined throughout the Requirements or in Section 17, entitled "Definitions", shall have the meanings ascribed to them in the MISMO eMortgage Glossary.

1. **LEGAL & REGULATORY COMPLIANCE**
    a. eClosing System must be designed in compliance with applicable federal, state, and local laws, rules, and regulations concerning privacy, data security, record retention, and the content, display, presentation, and format of Electronic Records.
    b. eClosing System must present Electronic Records in compliance with applicable federal, state, and local laws, rules, and regulations. This includes, but is not limited to, the content, format, or physical location of information displayed in the Electronic Record, and any requirements associated with how information is organized in the Electronic Record.
2. **PRESENTATION OF ELECTRONIC RECORDS FOR ELECTRONIC SIGNATURES**
    a. eClosing System must permit signer to view the entire Electronic Record that he/she will review and electronically sign and the Electronic Record must remain accessible to the signer as he/she completes the Electronic Signature[1] process.
    b. There should be no watermarks or other overlays displayed in the view of the Electronic Record when it is presented by the eClosing System to the signer as he/she completes the Electronic Signature process.
    c. All Electronic Records presented by the eClosing System to the signer for Electronic Signature must clearly and legibly display the signer's printed name directly above, below, or in close proximity to the location that the Electronic Signature will be applied.
3. **SIGNER'S CONSENT TO ELECTRONIC SIGNATURE PROCESS**
    a. eClosing System must obtain and record signer's consent to conduct the closing transaction electronically, to adopt the symbol or process to be used as his/her

[1] "Electronic Signature" is defined in the MISMO eMortgage Guide as "An action by a person to electronically apply an electronic sound, a symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record". However, for purposes of these Requirements, and as noted in these Requirements, an Electronic Signature is not permitted to be an audio or video recording or comprised solely of biometric data.

Electronic Signature, and to electronically sign the Electronic Records. This consent must be obtained on the same date as the date the signer electronically signs the Electronic Records, even if a similar consent was obtained from the signer on an earlier date.

b. eClosing System must securely store the content of any consent obtained from a signer and be able to reproduce such consent in its original form, as it was displayed and agreed to by the signer.
c. eClosing System must also support the disclosures and/or processes relating to:
    - **i.** Obtaining signer's express consent to opt-in or opt-out of electronically signing the Electronic Records;
    - **ii.** Identifying what the consent applies to;
    - **iii.** The right to withdraw consent and the consequences of doing so;
    - **iv.** How to withdraw consent;
    - **v.** Signer's right to receive a paper copy of the Electronic Records;
    - **vi.** The hardware, software, and system requirements necessary to conduct the closing transaction;
    - **vii.** A reasonable demonstration that the signer can access Electronic Records regarding consent and the information that is the subject matter of the consent; and,
    - **viii.** Changes to hardware, software, and other system changes that require notice to the signer and the right to withdraw consent without fees or consequences not previously disclosed.

4. VERIFICATION OF SIGNER'S IDENTITY

a. eClosing System must support the verification of the signer's identity utilizing a Multi-Factor Authentication process.

5. ELECTRONIC SIGNATURE SYMBOL/PROCESS

a. eClosing System must clearly identify the symbol or process to be used as the signer's Electronic Signature and the purpose of the Electronic Signature.
b. The signer's Electronic Signature is not permitted to be an audio or video recording or comprised solely of biometric data.

6. ATTRIBUTION OF ELECTRONIC SIGNATURE TO SIGNER

a. eClosing System must attribute the Electronic Signature to the applicable signer. This attribution must be evident in the Audit Trail maintained by the eClosing System.

7. INDIVIDUAL ELECTRONIC SIGNATURES/ACKNOWLEDGMENTS

a. eClosing System shall not permit a signer to simultaneously apply multiple Electronic Signatures or acknowledgments to the same or separate Electronic Records. It must instead require a separate Electronic Signature, or acknowledgment, for each instance requiring the signer's signature or acknowledgment.

8. IDENTIFICATION OF ELECTRONIC RECORDS PRESENTED FOR ELECTRONIC SIGNATURES

a. eClosing System must clearly identify the Electronic Record being presented to the signer for Electronic Signature.

9. SIGNER'S INTENT TO APPLY ELECTRONIC SIGNATURES TO ELECTRONIC RECORDS

a. eClosing System must require the signer to take action to apply his/her Electronic Signature and retain record of this action as evidence of the signer's intent to electronically sign the Electronic Record.

b. eClosing System must support the following actions to facilitate the signer's awareness of the legal consequences of the application of his/her Electronic Signature:
    i. Provide the signer with notice of the effect the Electronic Signature will have;
    ii. Provide a mechanism or process for the signer to confirm that the signer intends to electronically sign the Electronic Records presented to him/her;
    iii. Provide the signer with notice that an Electronic Signature will be attached to, or logically associated with, an electronic promissory note ("eNote") and other Electronic Records, as applicable; and,
    iv. Capture the signer's acknowledgment that his/her Electronic Signature has been attached to, or logically associated with, the eNote or other Electronic Records, as applicable.

10. ASSOCIATION OF ELECTRONIC SIGNATURES TO ELECTRONIC RECORDS

a. eClosing System must associate the signer's Electronic Signature to an Electronic Record once it has been electronically signed by the signer.
b. This association must be evident in the Audit Trail maintained by the eClosing System.

11. DATE/TIME OF ELECTRONIC SIGNATURES APPLIED TO ELECTRONIC RECORDS

a. Once the signer has electronically signed the Electronic Record, the eClosing System must support the ability to determine the date and time the Electronic Signature was applied by the signer to the Electronic Record.

12. APPLICATION OF TAMPER-EVIDENT SEALS & VALIDATION OF ELECTRONICALLY SIGNED ELECTRONIC RECORDS

a. A Tamper-Evident Seal must be applied to the Electronic Record immediately after the last signer has applied his/her Electronic Signature.
    i. The minimum encryption method utilized for the Tamper-Evident Seal must be SHA-256.
    ii. For an eNote, the date and time that the Tamper-Evident Seal is applied to the eNote must follow the ISO 8601 date and time standard and be represented in Coordinated Universal Time (UTC) using the UTC designator "Z".
b. eClosing System must permit validation of any Electronic Records electronically signed in the eClosing System by including the Tamper-Evident Seal in the Electronic Record so that it is accessible to validate that the Electronic Record has not been altered after it was electronically signed by all signers.
c. eClosing System must prevent alterations to an Electronic Record between the application of Electronic Signatures to an Electronic Record by multiple signors, and before the Tamper-Evident Seal is applied to the Electronic Record.

13. UNAUTHORIZED ACCESS TO OR ALTERATION OF ELECTRONICALLY SIGNED ELECTRONIC RECORDS

a. eClosing System must provide reasonable evidence that Electronic Records electronically signed in and maintained by the eClosing System are not and have not been subject to unauthorized access or alterations. In the event of unauthorized access or alterations, the eClosing System provider must have procedures in place to promptly notify applicable parties.

14. CONTENT AND INTEGRITY OF AUDIT TRAILS

a. eClosing System must record the date, time, and recipient of any transfers of Electronic Records from the eClosing System to an eVault System or other electronic repository system.
b. eClosing System must record all of the following activities that have occurred on the eClosing System in a transaction-specific Audit Trail[2]:
    i. Date and time the signer(s) accessed the eClosing System;
    ii. Date and time the signer(s) consented to conduct the closing transaction electronically;
    iii. The version or other system identifier which can be used to determine the content of the consent to conduct the closing transaction electronically that was displayed to the signer;
    iv. Date and time of any alterations that were made to an Electronic Record and the user that made such alterations;
    v. Date and time that the signer successfully completed each and ultimately all factors of the applicable authentication process;
    vi. Date, time, and system identifier of each Electronic Record accessed by a user;
    vii. Date and time each Electronic Record is electronically signed, the type of Electronic Signature used, the attribution of the Electronic Signature to the signer, and the attribution of the signer's Electronic Signature to the Electronic Record;
    viii. Internet Protocol (IP) Address of the computer used by each user; and,
    ix. Tamper-Evident Seal for each electronically signed Electronic Record including the date and time the Tamper-Evident Seal was applied to the Electronic Record.
c. eClosing System must protect the integrity of transaction-specific Audit Trails by the application of a Tamper-Evident Seal.
d. eClosing System's Audit Trails and the information contained within them must be readily accessible and retrievable to parties with rights to such access.

15. REPRODUCTION OF ELECTRONICALLY SIGNED ELECTRONIC RECORDS

a. eClosing System must be capable of accurately reproducing any Electronic Record electronically signed in the eClosing System. This includes both the capability to electronically display the Electronic Record and print it to paper. Such reproduction must include the contents, fonts, styling, margins, and all other physical features of the Electronic Record as may be required to comply under applicable state and federal laws, including an indication that it is a reproduction of an Electronic Record that was electronically signed.
b. eClosing System must permit the party viewing or printing the Electronic Record to ascertain:
    i. The content of the Electronic Record;

[2] For all references to times recorded by the eClosing System in a transaction-specific Audit Trail, the time zone must be ascertainable from the Audit Trail.

ii. The name of the signer of the Electronic Record, and the name of the borrower or principal associated with the Electronic Record (to the extent the borrower or principal associated with the Electronic Record may differ from the signer of the Electronic Record); and,
iii. The legal capacity in which the signer electronically signed the Electronic Record.

16. INFORMATION SECURITY

a. eClosing System providers must have comprehensive information security programs in place to ensure consumer data, privacy and information security laws and regulations are satisfied. Such programs must include, but are not limited to, sufficient and documented plans for disaster recovery, business continuity, redundancy, data back-up, archival/retrieval capabilities, and annual tests of these components.
b. eClosing System providers should review and perform tests of information security programs no less than annually to ensure continued compliance.

17. DEFINITIONS

a. **"Audit Trail"** means a chronological and detailed list of critical events and actions, as outlined in Section 14 of these Requirements, that either occurred on the eClosing System or was reported to the eClosing System.
b. **"eClosing System"** means a secure environment(s) where one or more mortgage loan closing documents are accessed, presented, and signed electronically.
c. **"eVault System"** means a secure storage solution that meets the requirements of eSignature Laws. The concept is analogous to a paper note vault administered by a document custodian in the industry today.
d. **"Internet Protocol (IP) Address"** means a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication.
e. **"Multi-Factor Authentication"** means a method of access control in which a user is granted access after successfully presenting identity evidence through a minimum of two of the following mechanisms: something they have (e.g., an identity credential, such as a driver's license or passport), something they know (e.g., knowledge-based authentication), something they are (e.g., iris/retina/thumbprint scans, facial recognition, and other forms of biometric identification).
f. **"SHA-256"** means a cryptographic hash function which takes an input and produces a 256-bit hash value known as a message digest, which is typically rendered as a 64-digit hexadecimal number.