eVault Questionnaire, Attestations, and Requested Documentation

eVault System Provider:

Primary Contact Name:

Primary Contact Email:

Primary Contact Phone Number:

---

eVault System Provider Questionnaire

Please respond to the following questions regarding your eVault System. Terms not otherwise defined herein have the meaning ascribed to them in the *MISMO® Business Glossary*.

1. Does the eVault System support storage of both eNotes and other Electronic Records?

2. For how long are eNotes and other Electronic Records stored by the eVault System in their original version/format?

3. Please describe how the eVault System associates other Electronic Records with the corresponding copy of a stored eNote.

4. How does the eVault System indicate to a user whether a copy of a stored eNote is the Authoritative Copy?

5. What methods of user authentication are supported by the eVault System?

6. How does the eVault System restrict access to sensitive data and records?

7. Please describe the use of a firewall and other network perimeter security controls to safeguard the integrity of the eVault System and stored copies of eNotes and other Electronic Records.

8. What user(s) of the eVault System can access its Audit Trails?

9. Please describe any reviews of the eVault System performed to identify the presence of viruses or malicious code in software, hardware, or the network, including how frequently such reviews are performed.

10. Does the eVault System support replacement of an eNote with another eNote (e.g., in the context of an error in the eNote that requires a new note to be executed)? If yes, how does the eVault System make clear to users which copy is the replacement that is actively registered on the MERS® eRegistry and which copy is the one that was replaced and is therefore not actively registered on the MERS® eRegistry?

11. Please describe the steps a user of the eVault System must take to convert an eNote to a paper promissory note.

12. How does the eVault System ensure that the status of each stored copy of an eNote stays aligned with the status of the corresponding eNote Record on the MERS® eRegistry?

13. How often are copies of eNotes and other Electronic Records stored in the eVault System validated to ensure their integrity?

14. To which MISMO SMART Doc® version(s) does the eVault System support validation?

□ SMART Doc® v1.02

□ SMART Doc® v3 Verifiable

eVault System Provider Required Documentation

Please provide the following:

- Business continuity plan
- Disaster recovery plan
- Results of most recent review(s) of the eVault System performed to detect viruses or malicious code in software, hardware, or the network

eVault System Provider Attestations

I hereby attest that I am authorized by my organization, the eVault System provider (“Provider”), to make the following attestations on its behalf regarding its eVault System, that I am familiar with the features and functionality of the eVault System, and I understand each of the attestations that I am about to make on the Provider’s behalf. To the extent there are any exclusions or limitations to/on a particular attestation, I have indicated such and provided details in the space that follows or in a separate attachment, if necessary. Further, I attest to the accuracy and completeness of the information provided by the Provider in response to the Questionnaire and throughout the course of the MISMO eVault System Certification.

1. The eVault System complies with applicable requirements of ESIGN, UETA and any other state or federal laws, including, but not limited to, ensuring that all requirements associated with any safe harbor provisions under these laws are met.

2. The eVault System maintains the integrity of copies of eNotes and other Electronic Records stored in the eVault System in such a manner that supports their enforceability and admissibility in federal or state court.

3. For any eNote or other Electronic Record transmitted to the eVault System, the eVault System validates the Tamper-Evident Seal applied to such eNote/Electronic Record by recalculating the Tamper-Evident Seal and comparing the resulting value to the Tamper-Evident Seal applied to the eNote/Electronic Record, and, if such eNote/Electronic Record was registered on the MERS® eRegistry, by recalculating the Tamper-Evident Seal and comparing the resulting value to the value stored for such eNote/Electronic Record on the MERS® eRegistry.

4. The eVault System will not accept delivery of an eNote for which there is a failure of the Tamper-Evident Seal re-computation or validation against the value stored for the corresponding eNote Record on the MERS® eRegistry.

5. Any reproduction of an eNote or Electronic Record by the eVault System includes the contents, fonts, stylings, margins, and all other physical features required to comply under applicable state and federal laws, including an indication that it is a reproduction of an eNote or Electronic Record that was electronically signed.

6. The eVault System safeguards the integrity of the eVault System and eNotes and Electronic Records stored within the eVault System through a firewall and other network perimeter security controls.

7. The eVault System's encryption algorithms are compliant with NIST and FIPS 140-2 guidance.

8. The eVault System utilizes X.509 digital certificates for device/server-based TLS/SSL session authentication which support a minimum of SHA 256 signing hash.

9. The eVault System utilizes a minimum of 2048-bit RSA key and 128-bit AES key for the TLS session.

10. The eVault System ensures that data is encrypted both while in transit and at rest.

11. Any primary or backup data storage facilities (defined as any physical site offering equipment, servers, or any other computer storage device) used are permanently housed within the United States of America.

Exclusions/limitations to the above attestations:

Signature:

Name:

Title:

Date: