29-250 DEPARTMENT OF THE SECRETARY OF STATE

Chapter 950: RULES GOVERNING THE USE OF DIGITAL SIGNATURES

SUMMARY: These Rules establish the criteria for implementing Digital Signatures in transactions involving a State Agency, in accordance with the *Maine Digital Signature Act*, 10 M.R.S.A., Chapter 1053, Part 13.

SECTION 1. DEFINITIONS

A. **Digital Signature**: A computer-created Electronic Signature that:

1. Is intended by the person using it to have the same force and effect as the use of a manual signature;

2. Is unique to the person using it;

3. Is capable of verification;

4. Is under the sole control of the person using it; and

5. Is linked to data in such a manner that it is invalidated if the data are changed.

B. **Electronic Signature**: An electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

C. **Hash**: A mathematical function that converts a complex input into a unique numerical value.

D. **Signer**: The person affixing the Digital Signature, in their official capacity, in a transaction involving a State Agency.

E. **State Agency**: A department, agency, office, board, commission, quasi-independent agency, authority, or institution within Maine State Government.

SECTION 2. DIGITAL SIGNATURE ELEMENTS

The process of creating a Digital Signature has four mandatory elements: *Authentication*, *Signature Ceremony*, *Verification*, and *Tamper-Resistance*.

SECTION 3. AUTHENTICATION

A. Authentication establishes the unique identity of a Signer as the official of the organization using Digital Signatures in transactions involving a State Agency.

B. Authentication is determined by three standard factors:

1. **Knowledge**, meaning something the Signer knows. Examples include, without limitation, user name, password, pass phrase, PIN, and answers to security questionnaire.

2. **Possession**, meaning something the Signer has. Examples include, without limitation, a key fob, and a smart card.

3. **Intrinsic**, meaning something the Signer is. Examples include, without limitation, biometrics, such as fingerprint or retina scan.

C. The minimum requirement for on-premise Authentication is Knowledge (e.g., a password). The minimum requirements for remote Authentication are a combination of Knowledge and Possession (e.g., a password plus a key fob).

SECTION 4. SIGNATURE CEREMONY

A. The Signature Ceremony is the actual act of affixing a Digital Signature, and serves as the unambiguous substitute for affixing a manual ink signature.

B. The Signer must re-furnish Authentication credentials during the Signature Ceremony.

SECTION 5. VERIFICATION

Verification is the evidence confirming that the Signer is indeed the person whom the Signer claims to be, and that this same person actually affixed the Digital Signature. The evidence may include, without limitation, Hashes of credentials, and/or timestamps, and/or screen-captures.

SECTION 6. TAMPER-RESISTANCE

Tamper-Resistance is the raising of an explicit alert should the Digital Signature be compromised. The compromise could be with respect to the document contents, and/or the identity of the Signer, and/or the timestamp of the Digital Signature. At a minimum, this requires the visual display or audio communication of a prominent and explicit message stating that the Digital Signature is no longer valid.

SECTION 7. USER EDUCATION

A. User Education is a critical component for ensuring the viability of Digital Signatures.

B. The integrity of Digital Signatures rests upon the confidentiality of Authentication credentials. Signers must never share their Authentication credentials with anybody else.

C. Any State Agency using Digital Signatures must make it an explicit performance expectation for all its Signers to safeguard the confidentiality of their Authentication credentials.

SECTION 8. DIGITAL SIGNATURE PRODUCT APPROVAL

A. A Digital Signature product must be approved by the Chief Information Officer of the State of Maine in order to be accepted for transactions involving a State Agency.

B. The list of approved Digital Signature products for transactions involving a State Agency will be maintained at the Office of Information Technology (OIT) Internet site, and will be updated periodically by the Chief Information Officer.

C. Digital Signature product vendors may apply to the Chief Information Officer through the OIT Internet site at any time to request acceptance of their products for transactions involving a State Agency.

D. In order to be accepted for transactions involving a State Agency, a Digital Signature product must satisfy the requirements of this Rule, including *all* of the following criteria:

I. It must be based upon the X.509 Public Key Infrastructure;

2. It must provide seamless integration with the PDF document format;

3. It must provide seamless integration with Microsoft Active Directory;

4. The interface to the Signer must be either web-based or a free download;

5. The data center must be certified as either "SSAE 16 SOC 2 Type II (American Institute of Certified Public Accounts)" or "FedRAMP compliant Cloud Service Provider (Federal General Services Administration)",

6. All transmission between the Signer's device and the data center must be encrypted to either AES-256 or 3DES (National Institute of Standards and Technology) strength; and

7. The *Verification* and *Tamper-Resistance* elements must be embedded within the document, as well as stored in the data center.

E. Prior to implementing Digital Signatures, a State Agency must consult with the Chief Information Officer.

STATUTORY AUTHORITY: 10 MRSA §9503

EFFECTIVE DATE:
July 31, 2014 – filing 2014-152

AMENDED:
March 15, 2015 – filing 2015-027