Clearinghouse Rule 09-069

PROPOSED ORDER OF THE
DEPARTMENT OF ADMINISTRATION

The Wisconsin Department of Administration proposes an order to create Chapter Adm 13 relating to the use of electronic signatures by governmental units.

SUMMARY OF PROPOSED RULE

Statutes interpreted: s. 137.25(2) and 137.26, Stats.

Statutory authority: s. 16.004(1), 137.25(2), Stats.

Explanation of agency authority:
Section 137.25(2), Stats., requires the Department to adopt by rule, standards regarding the receipt of electronic signatures that promote consistency and interoperability with standards adopted by other governmental units of the state, other states, the federal government and nongovernmental persons interacting with governmental units of the State.

Related statute or rule: Section 137.25(2), Stats.

Plain language analysis:
Under the proposed rule, governmental entities that choose to use or accept electronic signatures are required to determine the level of assurance necessary for persons signing electronically. The rule identifies four levels of assurance and the standards that must be met for each signature level. The proposed rule also requires the Department to issue guidelines regarding the technical solutions available to accomplish the desired level of certainty for any given signature application.

Summary of, and comparison with, existing or proposed federal regulations: The Electronic Signatures in Global and National Commerce Act, commonly known as "E-sign", (Public Law 106-229) took effect in October, 2000, to facilitate the use of electronic records and signatures in interstate or foreign commerce. With certain exceptions, E-sign preempts state laws that are inconsistent with its provisions. One of the exceptions permits a state to supersede the effect of the primarily electronic commerce provision of Title I of the Act (15 USC 7001) by enacting a law that constitutes an enactment of the Uniform Electronic Transactions Act (UETA). Another section of E-sign preserves the rulemaking authority of a state regulatory agency responsible for rulemaking under any other statutes. UETA establishes a legal framework to facilitate and validate certain electronic transactions. UETA also provides that upon mutual agreement of the parties, electronic records and electronic signatures will have the same legal effect and enforceability as written reports. Wisconsin Act 294 enacts UETA in Wisconsin and applies to State transactions but is not intended to limit, modify or supersede certain provisions contained in 15 USC s. 7001. There are numerous Chapters in the Code of Federal

Regulations that pertain to the use of electronic signatures, some of which may impact state agencies' filings, grant applications or reporting with the federal government.

Comparison with rules in adjacent states:

Michigan passed a statute based on UETA in 2000. Intent based signatures and those using tiff images of signatures (with paper copies retained behind them) are in use currently. As part of business applications modernization plans, Michigan plans to deploy signature pads for driver and vehicle registrations.

Under the Michigan statutes, no rules have been written but the department of management and budget may "encourage and promote consistency and interoperability…." and "may specify differing requirements from which governmental agencies and officials of the state may chose in implementing the most appropriate standard for a particular application."[1]

Michigan has currently suspended work on secure electronic signatures.

Illinois passed an electronic signature statute in 1999[2] prior to UETA adoption. An Administrative Rule under the statute was developed by the Illinois Department of Commerce.[3] Illinois has a mature electronic signature program, including a public key infrastructure and requisite policies for digital signature and encryption applications, for certification practice and agreements for parties to the transactions.

Digital signing of electronic forms has been a major focus for Central Management Services in Illinois. As of 2008 Illinois has issued over 100,000 individual certificates for secure signing to date. As of the end of the year, they were adding nearly 900 new certificates per month.

Following a third party audit of their infrastructure in 2008, Illinois synchronized their policy and practices and modified them to meet current standards set under RFC 3647. They also purchased new hardware and software to upgrade their signature capacity.

Illinois is cross-certified with federal government signature efforts.

Kansas passed a statute based on UETA in 2000[4]. Kansas has a mature electronic signature program, including a public key infrastructure and requisite policies for digital signature and encryption applications, for certification practice and agreements for parties to the transactions.

---

[1] Sec. 450.849 Michigan Statutes

[2] Electronic Commerce Security Act 5 ILCS ss. 175/5-101 to 175/99-1

[3] Title 14 Chapter 1, Part 100

[4] Kansas KSA 2000 s. 16-1601 – 16-1620

Kansas has a mature and operational secure signature program, including a public key infrastructure. Administrative regulations are in place governing certification authorities[5] and their public key certificate policy originally developed in 2001[6] was updated in April 2008[7].

Like Illinois, Kansas has recently upgraded their infrastructure and expanded their signature capacity. They have brought in-house almost all functionality that was originally outsourced.

Kansas signatures are certified with the federal government.

Minnesota passed a statute based on UETA in 2000[8]. Before this they passed an Electronic Authentication Act[9] and digital signature guidelines[10] and in 2003 they published an Administrative Rule[11] based on this earlier act. The authentication rule addresses many of the challenges confronted in implementing a secure signature infrastructure.

Minnesota has currently suspended work on secure electronic signatures.

Iowa passed an act based on UETA in 2000.[12] Their act makes specific reference to digital signatures and makes specific reference to PKI. In 2007, Iowa developed the first version of Electronic Signature Guidelines. They developed draft digital signature guidelines roughly three years ago that have not been finalized to date.

Iowa has currently suspended work on secure electronic signatures.

---

[5] Kansas Administrative Regulations 7-41-4-1 7-41-13

[6] IT Policy 5200, Certificate Policy for Kansas Public Key Infrastructure, State of Kansas Information Technology Council, effective July 19, 2001

[7] ITEC Policy #9200 Attachment A, Certificate Policy for the State of Kansas Public Key Infrastructure Version 2, April 24, 208.

[8] Minnesota Uniform Electronic Transactions Act, 2000 c 371

[9] Minnesota Electronic Authentication Act, Section 1997 c. 178

[10] Minnesota Digital Signature Implementation and Use, November 1999 (4pp)

[11] Minnesota Chapter 8275 (October 27, 2003)

[12] Iowa 554D.101 – 554D.123

Summary of factual data and analytical methodologies:
The proposed rule was developed by the Department in collaboration with an inter-departmental workgroup comprised of state agency attorneys, program and information technology staff. The group researched laws and rules created by other states relating to the use of electronic signatures, federal government signature authentication efforts, and electronic authentication guidelines developed by the National Institute of Standards and Technology; the workgroup also met with representatives from the states of Illinois and Kansas to obtain information about their digital signature infrastructures, their federal interoperability, risk assessments and the levels of authentication on digital certificates they issue.

Analysis and supporting documents used to determine effect on small business or in preparation of economic impact report:

Section 227.114(1)(a), Stats., defines "small business" as a business entity, including its affiliates, which is independently owned and operated and not dominant in its field, and which employs 25 or fewer full-time employees or which has gross annual sales of less than $5,000,000.

Effect on small businesses:
There is no expected effect on small businesses under s. 227.114, Stats. The proposed rule pertains to state and local governmental units. Governmental entities that choose to use or accept electronic signature will need to determine which of the four levels of assurance defined in the rule will be required to accept an electronic signature on a particular type of document. Use of electronic signatures could generate costs for software and management of the process. The proposed rule does not require any entity to use or accept electronic signatures.

Agency Contact Person:

Donna Sorenson
Department of Administration
101 E. Wilson Street
P.O. Box 7864
Madison, WI 53707-7864
(608) 266-2887
Donna.Sorenson@Wisconsin.gov

Place where comments are to be submitted and deadline for submission:
Comments may be submitted to the agency contact person that is listed above until the date given in the future notice of public hearing. The deadline for submitting comments and the notice of public hearing will be posted on the Wisconsin Administrative Rules Website at:
http://adminrules.wisconsin.gov when the public hearing is scheduled.

Fiscal Estimate

State Effect

This rule will establish uniform standards and procedures for the use, authentication and interoperability of electronic signatures by governmental units that choose to use or accept electronic signatures. The rule covers state and local governmental units. The rule will also cover associations or societies that are provided with appropriations under statute. The rule does not require any entity to allow the use of or accept electronic signatures.

The rule requires entities that choose to use or accept electronic signatures to determine which of four levels of assurance defined in the rule will be required to accept an electronic signature on a particular type of document. Use of electronic signatures could generate costs for software and management of the process; and could result in process savings for both the accepting and submitting entity.

The Department of Administration is required to coordinate the interoperability of Levels 3 and 4 signatures between governmental units and covered associations. The Department is also required to issue guidelines on processes, procedures and technical solutions that will enable all covered entities to meet the requirements of the rule.

The Department will be able to absorb any additional required costs generated by the rule within the agency's existing budget. The fiscal impact of voluntary implementation by state agencies is indeterminate.

Local Effect
As noted above, the rule requires entities that choose to use or accept electronic signature to determine which of four levels of assurance defined in the rule will be required to accept an electronic signature on a particular type of document. Use of electronic signatures could generate costs for software and management of the process; and could result in process savings for both the accepting and submitting entity.

The fiscal impact on local units of government that choose to allow electronic signatures is indeterminate. The proposed rule would not require local government entities to incur any costs, since participation is voluntary.

TEXT OF PROPOSED RULE:

SECTION 1. Adm 13 is created to read:

Chapter Adm 13
Electronic Signatures

Adm 13.01 Authority. This chapter is promulgated under the authority of s. 137.25(2), Stats., relating to the use of electronic signatures by governmental units.

Adm 13.02 Purpose. The purpose of this chapter is to establish uniform standards and procedures for the use, authentication and interoperability of electronic signatures pursuant to ss. 137.25(2) and 137.26, Stats.

Adm 13.03 Scope. This chapter establishes the requirements, standards and guidelines to be used by governmental units to consider electronic signatures to be trustworthy, reliable and generally equivalent to handwritten signatures executed on paper. This chapter does not require governmental units to use or accept electronic signatures or records.

Adm 13.04 Definitions. In this chapter:

(1) "Communication" means a document or message transmitted by any medium that may be utilized for the purpose of disseminating or broadcasting information.

(2) "Department" means the department of administration.

(3) "Electronic record" means a record that is created, generated, sent, communicated, received, or stored by electronic means.

(4) "Electronic signature" means 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.

(5) "Electronic signatory" means the person authorized to generate an electronic signature.

(6) "Governmental unit" means:

(a) An agency, department, board, commission, office, authority, institution instrumentality, political subdivision or special purpose district within the state of Wisconsin, regardless of the branch or branches of government in which it is located.

(b) A political subdivision or special purpose district within the state of Wisconsin.

(c) An association or society for which appropriations are made by law.

(d) Any body within one or more of the entities specified in pars. (a) to (c) that is created or authorized to be created by the constitution, by law, or by action of one or more of the entities specified in pars. (a) to (c).

(e) Any combination of any of the entities specified in pars. (a) to (d).

(7) “Handwritten signature” means the scripted name or legal mark of an individual that is written and executed or adopted with the intent to authenticate a writing in a permanent form.

(8) “Information” means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(9) “Person” means any individual, corporation, association, business enterprise or other legal entity either public or private and any legal successor, representative, agent or agency of that individual, corporation, association, business enterprise or other legal entity.

(10) “Record” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(11) “Secure signature” means an electronic signature providing high confidence of the identity of the signer that is unique to the signer within the context in which it is used and that is linked to a specific record at the time of signing.

(12) “Security procedure” means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, callback, or other acknowledgment procedures.

(13) “State” means the state of Wisconsin.

(14)“Transaction” means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Adm 13.05 Electronic signatures. In any written communication or transaction with a governmental unit in which a signature is required or used, any party to that communication may, with the governmental unit’s acceptance, affix an electronic signature which shall have the same force and effect as the use of a handwritten signature. Governmental units shall require an electronic signature that adequately addresses the level of risk associated with the communication or transaction being signed.

Adm 13.06 Use of electronic signatures. Governmental units shall comply with all statutes and rules relating to the use and acceptance of electronic signatures and related security procedures. Each governmental unit shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store and rely upon electronic records and electronic signatures. When a governmental unit decides to send or receive electronic signatures, the governmental unit shall specify the following:

(1) The electronic signature required, the manner and format in which such signature must be affixed to the electronic record, and the criteria that must be met by any third party used by the person filing the document to facilitate the process;

(2) Control processes, security and audit procedures to ensure adequate integrity, security, confidentiality, and auditability of such electronic signatures; and

(3) Any other required attributes for such electronically signed records that are currently specified for corresponding paper documents, or that are reasonably necessary under the circumstances.

Adm 13.07 Assurance of electronic signatory. (1) Governmental units shall determine which of the following four levels of assurance they require for persons signing electronically:

(a) Level 1. No significant confidence in the identity of the electronic signatory.
(b) Level 2. Confidence in the identity of the electronic signatory.
(c) Level 3. High confidence in the identity of the electronic signatory.
(d) Level 4. Very high confidence in the identity of the electronic signatory.

[2] Determinations requiring level 1 or level 2 confidence can be met by a simple electronic signature indicating intent and do not require a secure signature.

(3) Determinations requiring level 3 or level 4 confidence shall employ a secure signature in accordance with s. Adm 13.08.

(4) The department shall coordinate level 3 and level 4 interoperability between governmental units.

Adm 13.08 Standards for electronic signatures. (1) The department shall issue guidelines on processes, procedures, and technical solutions to enable governmental units to meet the requirements of s. Adm 13.06 and 13.07.

[2] Each governmental unit shall determine what standards and guidelines it will apply to level 1 and level 2 signatures.

(3) Governmental units shall ensure that all of the following standards are met for level 3 and level 4 signatures.

[a] Signatures can be used to identify the individual signing the record.

[b] Signatures are reliably created by identified individuals and cannot be readily duplicated or compromised.

[c] Signatures are created and linked to the electronic record to which they relate in a manner that, if the record or the signature is intentionally or unintentionally changed after signing, the electronic signature is invalidated.

[4] Subsequent signatures on an electronic record are not considered a change for the purpose of this section.

SECTION 2. EFFECTIVE DATE: This rule shall take effect first day of the month six months following publication in the Wisconsin Administrative Register as provided in s. 227.22 (2), Stats.

Dated: August 28, 2009

_____

Michael L. Morgan
Secretary of Administration