



H.B. 488

123rd General Assembly
(As Introduced)

Reps. Terwilleger, Amstutz, Householder, Harris, Gardner, Tiberi, Carey, Mottley, Corbin, Metzger, Hollister, Van Vyven, Willamowski, Olman, DePiero, Luebbers, Thomas, Trakas, Goodman, Hoops, Austria, Damschroder, Hartnett, Sykes, Maier, Brading, Peterson, Mead, Schuler, Metelsky, Taylor, Jolivette, Buehrer, Flannery

BILL SUMMARY

- Proposes the enactment of the Electronic Records and Signatures Act.
- Provides for the regulation of electronic signatures and electronic records both in the private sector and within state government.
- Establishes the Electronic Commerce Commission within the Department of Administrative Services to adopt rules for certification of security procedures relative to electronic records and digital signatures, to adopt rules relative to defining when a certificate issued in connection with a digital signature is trustworthy, and to investigate violations of the bill.
- Regulates the suspension and revocation of certificates issued in connection with digital signatures.
- Authorizes state agencies to use electronic records and signatures and provides limited rule-making authority in this area to the Department of Administrative Services.
- Provides civil remedies and criminal penalties for violations of the Electronic Records and Signatures Act.
- Exempts certain information from the application of Ohio's Public Records Law.
- Repeals the establishment of the Electronic Commerce Commission four years after the effective date of the bill.

TABLE OF CONTENTS

OVERVIEW AND GENERAL PROVISIONS

Overview.....	3
General provisions.....	3
Construction and purposes of the "Electronic Records and Signatures Act"	3
Scope of the bill	4

AUTHORIZATION FOR THE USE OF ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES

Validity of electronic format; exceptions.....	5
Validity of electronic format.....	5
Exceptions to the use of electronic records and electronic signatures.....	6
Maintenance of information in electronic form.....	7

SECURITY OF ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES; REGULATION OF CERTIFICATION AUTHORITIES

Use of a qualified security procedure	8
Secure electronic signatures and signature devices	10
Certification of a security procedure as a qualified security procedure	12
Certain digital signatures are to be considered to be a qualified security procedure	13
Rule-making authority granted to the Electronic Commerce Commission for determining trustworthy certificates	14
Certification authorities	15
Certification authorities	15
Issuance of certificates.....	16
Representations made by authority	17
When revocation of a certificate by a certification authority is required.....	18
Subscriber's acceptance of a certificate; subscriber's representations and duties	19

ENFORCEMENT OF THE ACT

Prohibitions and criminal penalties.....	20
Investigation and prosecution of violations authorized.....	21
Amendment of criminal law prohibiting forgery	21
Civil actions	22

CREATION AND DUTIES OF THE ELECTRONIC COMMERCE COMMISSION

Members of the Electronic Commerce Commission; repeal.....	23
Initial appointments, terms of office, and filling vacancies	24



Oath and compensation	24
Duties of the Department of Administrative Service relative to the ECC	24
ECC rule-making authority	25
Public record of meetings of the ECC	25

**STATE AGENCIES USE OF ELECTRONIC RECORDS AND THE ROLE OF
THE DEPARTMENT OF ADMINISTRATIVE SERVICES**

State agency's use of electronic records and signatures.....	25
Department of Administrative Services	27
Certain information confidential.....	28

CONTENT AND OPERATION

OVERVIEW AND GENERAL PROVISIONS

Overview

The bill proposes the enactment of sections within the Ohio Uniform Commercial Code that are to be known as the Electronic Records and Signatures Act. The bill provides a statutory framework for the creation and use of information and records in electronic form, both in the private sector and within state government. The bill gives legal effect to information, records, and signatures in electronic form; provides for the regulation of information, records, and signatures maintained in electronic form; and regulates the use of security procedures designed to authenticate information, records, and signatures in electronic form. Civil remedies and criminal penalties are established for the enforcement of the bill's provisions.

General provisions

Construction and purposes of the "Electronic Records and Signatures Act"

(sec. 1306.02)

The bill states that proposed sections 1306.01 to 1306.38 of the Revised Code may be cited as the Electronic Records and Signatures Act.

The Electronic Records and Signatures Act is to be construed consistently with what is commercially reasonable under the circumstances and to effect the following purposes:

- (1) To facilitate electronic communications by means of reliable electronic records;



(2) To facilitate and promote electronic commerce by eliminating barriers resulting from uncertainties over writing and signature requirements, and by promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(3) To facilitate electronic filing of documents with state agencies and local governments, and to promote efficient delivery of government services by means of reliable electronic records;

(4) To minimize the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce;

(5) To help establish uniformity of rules and standards regarding the authentication and integrity of electronic records;

(6) To promote public confidence in the integrity and reliability of electronic records and electronic commerce.

Scope of the bill

(secs. 1306.01(N) and (W), 1306.06, and 1306.07)

The bill states that nothing in the Electronic Records and Signatures Act is to be construed (1) to require any person to create, store, transmit, accept, or otherwise use or communicate information, records, or signatures by electronic means or in electronic form, or (2) to prohibit any person engaging in an electronic transaction from establishing reasonable requirements regarding the medium on which it will accept records or the method and type of symbol or security procedure it will accept as a signature.

A "person," for purposes of the bill, is "an individual, corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal or commercial entity."

Parties involved in generating, sending, receiving, storing, or otherwise processing electronic records are permitted, by agreement of the parties, to waive the application of most provisions of the Electronic Records and Signatures Act. However, the bill prohibits parties from waiving its prohibitions relating to the alteration, use, possession, and recreation of another person's signature device (sec. 1306.24; see "**Prohibitions**," below), and it prohibits parties from waiving the application of the bill in an agreement involving the attribution of an electronic signature in a consumer transaction.

The bill states that the Electronic Records and Signatures Act should not be construed to prevent the application of any other law, or any rule adopted by a state agency pursuant to the authority granted to state agencies under the bill requiring the approval of a state agency prior to the use or retention of electronic records or the use of electronic signatures. A "state agency," as defined in the bill, includes "every organized body, office, or agency established by the laws of the state for the exercise of any function of state government."

AUTHORIZATION FOR THE USE OF ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES

These provisions of the bill authorize the use of information, records, and signatures in electronic form, establishing the bases for their legal validity, and regulate the maintenance of electronic records.

Validity of electronic format; exceptions

Validity of electronic format

(secs. 1306.01(G), (H), (I), (J), (Q), (T), and (V) and 1306.03(A) to (C))

The bill states that information, records, and signatures are not to be denied legal effect, validity, or enforceability solely on the grounds that they are in "electronic" form. "Electronic" includes "electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies."

The bill defines "information" to include "data, text, images, sound, code, computer programs, software, databases, and the like." A "record" is defined as "information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." In addition, a "signature" or "signed" includes "any symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record."

The bill states that if a rule of law requires information to be "written" or "in writing," or provides for certain consequences if it is not, an "electronic record" satisfies that rule of law, with certain exceptions. An "electronic record" is defined as "a record generated, communicated, received, or stored by an electronic means for use in an information system or for transmission from one information system to another."

The bill states that if a rule of law requires a signature, or provides for certain consequences if a document is not signed, an "electronic signature"

satisfies that rule of law, with certain exceptions. An "electronic signature" is defined as "a signature in electronic form attached to or logically associated with an electronic record." An electronic signature may be proved in any manner, including by showing that a procedure existed by which a party must of necessity have executed a symbol or "security procedure" for the purpose of verifying that an electronic record is that of such party in order to proceed further with a transaction. (A "security procedure" is defined as "a methodology or procedure used for the purpose of verifying that an electronic record is that of a specific person or detecting error or alteration in the communication, content, or storage of an electronic record since a specific point in time." This definition states that a security procedure may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgment procedures, or similar security devices.)

Exceptions to the use of electronic records and electronic signatures

(sec. 1306.03(D))

The above provisions, authorizing the use of electronic records and electronic signatures when a rule of law requires information to be written or requires a signature, do not apply:

(1) If their application would involve a construction of a rule of law that is clearly inconsistent with the law or repugnant to the context of the same rule of law, provided that a requirement that information be "in writing," "written," or "printed," or that there be a "signature" or that the record be "signed," is not deemed sufficient in itself to establish this intent;

(2) To any rule of law governing the creation or execution of a will or trust, living will, or health care power of attorney;

(3) To any record that serves as a unique and transferable instrument of rights and obligations, including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title. This provision does not apply if there is an electronic version of the record created, stored, and transferred in a manner (a) that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, (b) that can be possessed by only one person, and (c) that cannot be copied except in a form that is readily identifiable as a copy.

Maintenance of information in electronic form

(secs. 1306.01(Z), 1306.04, and 1306.05)

The bill states that where a rule of law requires information to be presented or retained in its original form, or provides consequences for the information not being presented or retained in its original form, that rule of law is satisfied by an electronic record if there exists reliable assurance as to the integrity and reliability of the information from the time when it was first generated in its final form, as an electronic record or otherwise. This provision does not apply to any record that serves as a unique and transferable instrument of rights and obligations, including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title, unless an electronic version of the record is created, stored, and transferred in a manner (1) that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, (2) that can be possessed by only one person, and (3) that cannot be copied except in a form that is readily identifiable as a copy.

The bill's criterion for assessing integrity for this purpose is whether the information has remained complete and unaltered, apart from the addition of any endorsement or other information that arises in the normal course of communication, storage, and display. The standard of reliability required to be used for this purpose, to ensure that information has remained complete and unaltered, may vary and is to be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

The bill also provides that where a rule of law requires that certain documents, records, or information be retained (without specifying that these items be retained in their original form, as do those rules of law to which the provision above applies), that requirement is met by retaining electronic records of such information in a "trustworthy manner." (This provision does not apply to data, the sole purpose of which is to enable a record to be sent or received.) Certain conditions are placed upon this provision:

(1) The electronic record and the information contained therein must be accessible so as to be usable for subsequent reference at all times when such information must be retained;

(2) The information must be retained in the format in which it was originally generated, sent, or received, or in a format that can be demonstrated to represent accurately the information originally generated, sent, or received;

(3) Any data must be retained so as to enable the identification of the origin and destination of the information, the authenticity and integrity of the information, and the date and time when it was sent or received.

A "trustworthy manner" is defined in the bill as the use of computer hardware, software, and procedures that, in the context in which they are used, meet all of the following requirements: (1) they can be shown to be reasonably resistant to penetration, compromise, and misuse, (2) they provide a reasonable level of reliability and correct operation, (3) they are reasonably suited to performing their intended functions or serving their intended purposes, and (4) they comply with applicable agreements between the parties, if any.

Notwithstanding the requirements set forth in the bill for the *retention* of documents, records, and information, the bill states that nothing precludes any state agency from adopting rules, pursuant to the authority granted by the Electronic Records and Signatures Act, specifying additional requirements for the retention of records that are subject to the jurisdiction of that agency.

SECURITY OF ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES; REGULATION OF CERTIFICATION AUTHORITIES

These provisions of the bill address the use of security procedures that are needed in order to establish when an electronic record may be considered to be a secure record. They also provide for the certification of qualified security procedures by the Electronic Commerce Commission and cover the use of digital signatures, including the regulation of certification authorities and their issuance of certificates.

Use of a qualified security procedure

(secs. 1306.08, 1306.09, and 1306.10)

The bill states that if, through the use of a qualified security procedure, it can be verified that an electronic *record* has not been altered since a specified point in time, the electronic record is to be considered to be a secure electronic record from that specified point in time to the time of the verification. A relying party must establish that the qualified security procedure was "commercially reasonable" under the circumstances in accordance with the bill, was applied by the relying party in a trustworthy manner, and was reasonably and in good faith relied upon by the relying party. For this purpose, a "qualified security procedure" is a security procedure used to detect changes in the content of an electronic record that either (1) has previously been agreed to by the parties, or (2) has been certified by the Electronic Commerce Commission (ECC) in accordance with the

provisions set forth in the Electronic Records and Signatures Act as being capable of providing reliable evidence that an electronic record has not been altered.

The bill also states that if, through the use of a qualified security procedure, it can be verified that an electronic *signature* is the signature of a specific person, the electronic signature is to be considered a secure electronic signature at the time of verification. A relying party must establish that the qualified security procedure (1) was "commercially reasonable," as defined by the bill, (2) was applied by the relying party in a trustworthy manner, and (3) was reasonably and in good faith relied upon by the relying party. For this purpose, a "qualified security procedure" is a security procedure used for identifying a person, that either has previously been agreed to by the parties or has been certified by the ECC in accordance with the provisions set forth in the Electronic Records and Signatures Act as being capable of creating, in a trustworthy manner, an electronic signature that is all of the following:

- (1) Unique to the signer within the context in which it is used;
- (2) Capable of being used to objectively identify the person signing the electronic record;
- (3) Has been reliably created by the identified person, and cannot readily be duplicated or compromised;
- (4) Is created and linked to the electronic record to which it relates, in such a manner that if the record or the signature is intentionally or unintentionally changed after signing, the electronic signature is invalidated.

The bill states that the commercial reasonableness of a security procedure is a question of law to be determined in light of the purposes of the procedure and the commercial circumstances at the time that the procedure was used, including consideration of all of the following:

- (1) The nature of the transaction;
- (2) The sophistication of the parties;
- (3) The volume of similar transactions engaged in by either or both of the parties;
- (4) The availability of alternatives offered to but rejected by either of the parties;
- (5) The cost of alternative procedures;

- (6) The procedures used for similar types of transactions.

The bill requires that, in determining whether reliance on a security procedure was reasonable and in good faith, consideration be given to all the circumstances known to the relying party at the time of the reliance, having regard to all of the following:

- (1) The information that the relying party knew or should have known of at the time of reliance that would suggest the reliance was or was not reasonable;

- (2) The value or importance of the electronic record, if known;

- (3) Any course of dealing between the relying party and the purported sender and the available indicia of reliability or unreliability apart from the security procedure;

- (4) Any usage or trade, particularly trade conducted by trustworthy systems or other computer-based means;

- (5) Whether the verification was performed with the assistance of an independent third party.

Secure electronic signatures and signature devices

(secs. 1306.01(U), 1306.11, and 1306.12)

The bill provides that whenever the creation, validity, or reliability of an electronic signature created by a qualified security procedure under the Electronic Records and Signatures Act is dependent upon the secrecy or control of a signature device of the signer, all of the following apply:

- (1) The person generating or creating the signature device must do so in a trustworthy manner;

- (2) The signer and all other persons that rightfully have access to the signature device must exercise reasonable care to retain control and maintain the secrecy of the signature device, and must protect it from any unauthorized access, disclosure, or use, during the period when reliance on a signature created by the device is reasonable;

- (3) In the event that the signer, or any other person that rightfully has access to the signature device, knows or has reason to know that the secrecy or control of the signature device has been compromised, (a) that person must make a reasonable effort to promptly notify all persons that the person knows might foreseeably be damaged as a result of such compromise, or (b) where an

appropriate publication mechanism is available, that person must publish notice of the compromise and a disavowal of any signatures created thereafter. If the person is a state agency, the notice must be published in a newspaper of general circulation in the city of Columbus, Ohio, and also published on the person's Internet home page for a minimum of 30 consecutive days.

The bill defines a "signature device" as "unique information, such as codes, algorithms, letters, numbers, private keys, or personal identification numbers, or a uniquely configured physical device, that is required, alone or in conjunction with other information or devices, in order to create an electronic signature attributable to a specific person."

Under the bill, a secure electronic signature is attributable to the person to whom it correlates, whether or not authorized, except as provided by another applicable rule of law. This attribution is conditional upon the applicability of all of the following:

(1) The electronic signature must have resulted from acts of a person that obtained the signature device or other information necessary to create the signature from a source under the control of the alleged signer, creating an appearance that it came from that party;

(2) The access or use must have occurred under circumstances constituting a failure to exercise reasonable care by the alleged signer;

(3) The relying party must have relied reasonably and in good faith on the apparent source of the electronic record, to that party's detriment.

The attribution of a secure electronic signature under this provision is not applicable to transactions that are intended primarily for personal, family, or household use, or to transactions that otherwise are consumer transactions.

Certification of a security procedure as a qualified security procedure

(sec. 1306.13)

The bill provides that a security procedure may be certified by the Electronic Commerce Commission (ECC) as a qualified security procedure, following an appropriate investigation or review, for use in the verification of the accuracy of electronic signatures or electronic records under sections 1306.08 and 1306.09 of the Electronic Records and Signatures Act (see above). The bill grants the ECC exclusive authority to certify security procedures for these purposes. Both of the following must apply to a security procedure in order for that procedure to be certified:

(1) The security procedure, including any technology and algorithms it employs, must be completely open and fully disclosed to the public, and must have been so for a length of time sufficient to facilitate a comprehensive review and evaluation of its suitability for the intended purpose by the applicable information security or scientific community;

(2) The security procedure, including any technology and algorithms it employs, must be generally accepted in the applicable information security or scientific community as being capable of satisfying the requirements pertaining to the verification of electronic signatures or electronic records in a trustworthy manner. In making this determination, the ECC is required to consider the opinion of independent experts in the applicable field and the published findings of the applicable information security or scientific community, including applicable standards organizations such as the American National Standards Institute, International Standards Organization, International Telecommunications Union, and National Institute of Standards and Technology.

The bill requires that the certification of a security procedure be done through the adoption of rules in accordance with the Administrative Procedure Act, and requires a full and complete identification of the security procedure be specified, including requirements, if appropriate, as to how the security procedure is to be implemented.

The bill authorizes the ECC to decertify a qualified security procedure that is used in the verification of the accuracy of electronic signatures or electronic records under sections 1306.08 and 1306.09 of the Electronic Records and Signatures Act, following an appropriate investigation or review, if (1) subsequent developments establish that the security procedure is no longer sufficiently trustworthy or reliable for its intended purpose, or (2) for any other reason, the security procedure no longer meets the requirements for certification. In order to decertify a security procedure, the ECC is required to adopt rules in accordance with the Administrative Procedure Act.

Certain digital signatures are to be considered to be a qualified security procedure

(secs. 1306.01(B), (F), (L), (O), (P), (X), and (A)(A) and 1306.15)

The bill provides that a "digital signature" that is created using an asymmetric algorithm, certified by the Electronic Commerce Commission (ECC) as a qualified security procedure pursuant to the provisions of the Electronic Records and Signatures Act pertaining to the verification of electronic records through the use of qualified security procedures (sec. 1306.08(B)(2)), is to be considered to be a qualified security procedure for purposes of detecting changes

in the content of an electronic record, if the digital signature (1) was created during the operational period of a "valid certificate," and (2) is verified by reference to the "public key," which is the key of a key pair used to verify a digital signature, listed in the certificate.

The bill defines a "digital signature" as a security procedure and a type of electronic signature created by transforming an electronic record using a "message digest function" and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key such that any person having the initial untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial electronic record has been altered since the transformation was made. A "message digest function" is defined by the bill as an algorithm that maps or translates the sequence of bits comprising an electronic record into a message digest, which is generally a smaller set of bits, without requiring the use of any secret information, such that (1) an electronic record yields the same message digest every time the algorithm is executed using such record as input, and (2) it is computationally unfeasible that any two electronic records can be found or deliberately generated that would produce the same message digest using the algorithm unless the two records are precisely identical.

A "valid certificate" is defined as a "certificate" that a certification authority has issued and the listed subscriber has accepted. A "certificate" is defined as a record that at a minimum does all of the following: (1) identifies the certification authority issuing it (see "*Certification authorities*," below), (2) names or otherwise identifies its "subscriber" or a device or electronic agent under the control of the subscriber, (3) contains a public key that corresponds to a "private key," which is the key of a key pair used to create a digital signature, under the control of the subscriber, (4) specifies its operational period, and (5) is digitally signed by the certification authority issuing it. A "subscriber" is defined as a person who is all of the following: (1) the subject named or otherwise identified in a certificate, (2) the person who controls a private key that corresponds to the public key listed in the certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed.

The bill provides that a digital signature that is created using an asymmetric algorithm, certified by the ECC as a qualified security procedure pursuant to the provisions of the Electronic Records and Signatures Act pertaining to the verification of electronic signatures through the use of qualified security procedures (sec. 1306.09(B)(2)), is to be considered to be a qualified security procedure for purposes of identifying a person, provided that both of the following apply:

(1) The digital signature was created during the operational period of a valid certificate, was used within the scope of any other restrictions specified or incorporated by reference in the certificate, and can be verified by reference to the public key listed in the certificate;

(2) The certificate is considered trustworthy and an accurate binding of a public key to a person's identity either (a) as a result of being issued by a certification authority in accordance with standards, procedures, and other requirements specified by the ECC, or (b) as a result of an independent finding of a trier of fact in a legal proceeding that the certificate was issued in a trustworthy manner by a certification authority that properly authenticated the subscriber and the subscriber's public key, or any other finding by the trier of fact in a legal proceeding that the material information set forth in the certificate is true.

The bill states that, for these purposes, it is foreseeable that persons relying on a digital signature also will rely on a valid certificate containing the public key by which the digital signature can be verified, during the operational period of that certificate and within any limits specified in the certificate.

Rule-making authority granted to the Electronic Commerce Commission for determining trustworthy certificates

(sec. 1306.17)

The bill grants rule-making authority to the Electronic Commerce Commission (ECC), permitting the ECC to adopt rules, in accordance with the Administrative Procedure Act, applicable to both the public and private sectors for the purpose of defining the circumstances under which a certificate is to be considered sufficiently trustworthy under the above provisions pertaining to digital signatures, such that a digital signature verified by reference to the certificate will be considered to be a qualified security procedure under the provisions of the Electronic Records and Signatures Act pertaining to the verification of electronic signatures through the use of qualified security procedures (sec. 1306.09). If the ECC adopts such rules, the rules are required (1) to provide maximum flexibility to the implementation of digital signature technology and the business models necessary to support it, (2) to provide a clear basis for the authorities, and (3) to the extent reasonably possible, to maximize the opportunities for uniformity with the laws of other jurisdictions within the United States and internationally.

Rules adopted by the ECC may include both of the following:

(1) Rules establishing or adopting standards applicable to certification authorities (see "**Certification authorities**," below) or certificates, compliance with which may be measured (a) by becoming certified by the ECC, (b) by becoming

accredited by one or more independent accrediting entities recognized by the ECC, or (c) by other appropriate means;

(2) Where appropriate, rules establishing fees to be charged by the ECC to recover all or a portion of costs in connection with becoming certified by the ECC.

Certification authorities

Certification authorities

(secs. 1306.01(C), (D), and (R) and 1306.18)

The bill requires a certification authority to maintain its operations, and to perform its services, in a trustworthy manner, "except as conspicuously set forth in its certification practice statement." The bill defines a "certification authority" as "a person that authorizes and causes the issuance of a certificate."

The bill also requires a person maintaining a repository to maintain its operations, and to perform its services, in a trustworthy manner, "except as conspicuously set forth in its certification practice statement." The bill defines a "repository" as "a system for storing and retrieving certificates or other information relevant to certificates, including information relating to the status of a certificate."

Under the bill, for each certificate issued by a certification authority with the intention that it will be relied upon by third parties to verify digital signatures created by subscribers, a certification authority must publish or otherwise make available both of the following to the subscribers and all such relying parties:

(1) Its certification practice statement, if any (the bill defines a "certification practice statement" as "a statement published by a certification authority that specifies the policies or practices that the certification authority employs in issuing, managing, suspending, and revoking certificates and providing access to them");

(2) Its certification authority certificate that identifies the certification authority as a subscriber and that contains the public key corresponding to the private key used by the certification authority to digitally sign the certificate.

In the event of an occurrence that materially and adversely affects the certification authority's operations or system, its certification authority certificate, or any other aspects of its ability to operate in a trustworthy manner, the bill requires the certification authority to act in accordance with procedures governing such an occurrence specified in its certification practice statement or, in the

absence of such procedures, to use reasonable efforts to notify any persons that the certification authority knows might foreseeably be damaged as a result of such occurrence.

Issuance of certificates

(sec. 1306.19)

The bill permits a certification authority to issue a certificate to a prospective subscriber for the purpose of allowing third parties to verify digital signatures created by the subscriber, but only after both of the following occur:

(1) The certification authority has received a request for issuance from the prospective subscriber;

(2) The certification authority has done either of the following:

(a) Complied with all of the relevant practices and procedures set forth in its applicable certification practice statement; or

(b) In the absence of a certification practice statement addressing issues related to the issuance of a certificate, confirmed in a trustworthy manner: (1) that the prospective subscriber is the person to be listed in the certificate to be issued, (2) that the information in the certificate to be issued is accurate, and (3) that the prospective subscriber rightfully holds a private key capable of creating a digital signature, and the public key to be listed in the certificate can be used to verify a digital signature affixed by that private key.

Representations made by authority

(sec. 1306.20)

The bill provides that a certification authority, by issuing a certificate with the intention that it will be relied upon by third parties to verify digital signatures created by subscribers, represents all of the following to the subscribers and to those persons who reasonably rely upon information contained in the certificate in good faith during the certificate's operational period:

(1) The certification authority has processed, approved, and issued, and will manage and revoke if necessary, the certificate in accordance with its applicable certification practice statement stated or incorporated by reference in the certificate of which such person has notice or, in lieu thereof, in accordance with the Electronic Records and Signatures Act or the law of the jurisdiction governing issuance of the certificate;

(2) The certification authority has verified the identity of the subscriber to the extent stated in the certificate or its applicable certification practice statement, or in lieu thereof, the certification authority has verified the identity of the subscriber in a trustworthy manner;

(3) The certification authority has verified that the person requesting the certificate holds the private key corresponding to the public key listed in the certificate;

(4) Except as conspicuously set forth in the certificate or its applicable certification practice statement, to the certification authority's knowledge as of the date the certificate was issued, all other information in the certificate is accurate and not materially misleading.

The bill provides that if a certification authority issues a certificate subject to the laws of another jurisdiction, the certification authority also makes all warranties and representations otherwise applicable under the law governing the certificate's issuance.

When revocation of a certificate by a certification authority is required

(secs. 1306.01(S) and 1306.21)

A certification authority is required under the bill to revoke a certificate that it has issued, during the operational period of the certificate, in accordance with the policies and procedures governing revocation specified in the certification authority's applicable certification practice statement, or in the absence of such policies and procedures, as soon as possible after any of the following:

(1) Receiving a request for revocation by the subscriber named in the certificate, and confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber, or is an agent of the subscriber with authority to request the revocation;

(2) Receiving a certified copy of an individual subscriber's death certificate, or upon confirming by other reliable evidence that the subscriber is dead;

(3) Being presented with documents effecting a dissolution of a corporate subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist;

(4) Being served with an order requiring revocation that was issued by a court of competent jurisdiction;

(5) Confirmation by the certification authority that any of the following apply:

- (a) A material fact represented in the certificate is false;
- (b) A material prerequisite to issuance of the certificate was not satisfied;
- (c) The certification authority's private key or system operations were compromised in a manner materially affecting the certificate's reliability;
- (d) The subscriber's private key was compromised.

Under the bill, a revocation of a certificate permanently ends the operational period of a certificate from a specified time forward.

Upon effecting such a revocation, the certification authority is required to do all of the following:

- (1) Notify the subscriber and relying parties in accordance with the policies and procedures governing notice of revocation specified in its applicable certification practice statement or, in the absence of such policies and procedures, promptly notify the subscriber;
- (2) Promptly publish notice of the revocation in all repositories where the certification authority previously caused publication of the certificate;
- (3) Otherwise disclose the fact of revocation on inquiry by a relying party.

Subscriber's acceptance of a certificate; subscriber's representations and duties

(secs. 1306.22 and 1306.23)

Under the bill, a person accepts a certificate that names that person as a subscriber by publishing or approving publication of the certificate to one or more persons or in a repository, or by otherwise demonstrating approval of the certificate, while knowing or having notice of the certificate's contents.

By accepting a certificate, the subscriber represents all of the following to any person that reasonably relies on information contained in the certificate in good faith during the certificate's operational period: (1) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate, (2) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true, and (3) all information in the certificate that is within the knowledge of the subscriber is true.

The bill requires that all material representations to a certification authority, knowingly made by the person to be named in a certificate as a subscriber for purposes of obtaining a certificate, be accurate and complete to the best of that person's knowledge and belief.

The bill places duties upon a subscriber who learns that a private key has been compromised. Except as provided by another rule of law, if the private key corresponding to the public key listed in a valid certificate is lost, stolen, becomes accessible to an unauthorized person, or is otherwise compromised during the operational period of a certificate, a subscriber is required either (1) to promptly request the issuing certification authority to revoke the certificate and publish notice of its revocation in all repositories in which the subscriber previously authorized the certificate to be published, or (2) to provide reasonable notice of the revocation.

ENFORCEMENT OF THE ACT

These provisions of the bill prohibit specified actions relative to improperly creating, obtaining, or using electronic signatures and certificates; both criminal penalties and civil remedies for violations are set forth.

Prohibitions and criminal penalties

(secs. 1306.24 and 1306.99)

The bill prohibits persons from knowingly accessing, copying, or otherwise obtaining possession of or recreating the signature device of another person without authorization, for the purpose of creating, or allowing or causing another person to create, an unauthorized electronic signature using such signature device. A violation of this provision is a misdemeanor of the first degree.

The bill prohibits persons from knowingly altering, disclosing, or using the signature device of another person without authorization, or in excess of lawful authorization, for the purpose of creating, or allowing or causing another person to create, an unauthorized electronic signature using such signature device. A violation of this provision is a felony of the fourth degree. A violation of this provision is a felony of the third degree if the violator has previously violated this provision. A violation of this provision is a felony of the second degree if the violation is in furtherance of any scheme or artifice to defraud in excess of \$50,000.

The bill prohibits persons from knowingly creating, publishing, altering, or otherwise using a certificate issued in connection with a digital signature for any fraudulent or other unlawful purpose. A violation of this provision is a felony of

the fourth degree. A violation of this provision is a felony of the third degree if the violator has previously violated this provision. A violation of this provision is a felony of the second degree if the violation is in furtherance of any scheme or artifice to defraud in excess of \$50,000.

The bill prohibits persons from knowingly misrepresenting the person's identity or authorization in requesting or accepting a certificate or in requesting the suspension or revocation of a certificate issued in connection with a digital signature. A violation of this provision is a misdemeanor of the first degree. A violation of this provision is a felony of the fourth degree if the violation is in furtherance of any scheme or artifice to defraud, or if a violator violates this provision ten times in a 12-month period. A violation of this provision is a felony of the second degree if the violation is in furtherance of any scheme or artifice to defraud in excess of \$50,000.

The bill prohibits persons, in connection with a digital signature, from knowingly accessing, altering, disclosing, or using the signature device of a certification authority used to issue certificates without authorization, or in excess of lawful authorization, for the purpose of creating, or allowing or causing another person to create, an unauthorized electronic signature using such signature device. A violation of this provision is a felony of the third degree. A violation of this provision is a felony of the second degree if the violation is in furtherance of any scheme or artifice to defraud.

The bill also prohibits persons from publishing a certificate, or otherwise knowingly making it available to anyone likely to rely on the certificate or on a digital signature that is verifiable with reference to the public key listed in the certificate, if the person has knowledge (1) that the certification authority listed in the certificate has not issued it, (2) that the subscriber listed in the certificate has not accepted it, or (3) that the certificate has been revoked or suspended (unless the publication is for the purpose of verifying a digital signature created prior to the revocation or suspension, or giving notice of the revocation or suspension). This provision does not appear to be subject to a criminal penalty, but a violation of this provision (as in the case of a violation of any of the above provisions) is subject to the bill's civil actions (see "*Civil actions*," below).

Investigation and prosecution of violations authorized

(sec. 1306.29)

The bill authorizes the Electronic Commerce Commission (ECC) to investigate complaints filed with the ECC, and other information brought to the attention of the ECC, which complaints or information indicate a violation of the Electronic Records and Signatures Act or of the rules adopted under the Act.

Upon the request of the ECC, the Attorney General, or a county prosecutor located in the county in which the subject of a complaint resides, is authorized to commence and prosecute any appropriate action or proceeding against a person for a violation of the Act. However, if the Department of Administrative Services is the subject of a complaint filed pursuant to the bill, the bill specifies that the Auditor of State is to investigate the complaint.

Amendment of criminal law prohibiting forgery

(sec. 2913.31)

Continuing provisions of Ohio's Criminal Law prohibit a person, which person has the purpose to defraud or knowing that they are facilitating a fraud, from engaging in acts of forgery, including forging the writing of another without that person's authority. The bill adds that a person is prohibited from knowingly using a signature device of another person to create an electronic signature of that other person. A violation of this provision is a felony of the third degree. As used in this provision, "signature device" and "electronic signature" have the same meanings as in the Electronic Records and Signatures Act.

Civil actions

(secs. 1306.25, 1306.26, and 1306.28)

A person that suffers a loss due to a violation of one of the listed prohibitions in the Electronic Records and Signatures Act, or due to a violation of section 2913.31 of Ohio's Criminal Law (forgery), is authorized by the bill to bring a civil action in a court of competent jurisdiction. In addition to other appropriate relief, that person is entitled to recover reasonable attorney's fees and other court costs.

The bill provides that in any legal proceeding, nothing in the rules of evidence is to be applied to deny the admissibility of an electronic record or electronic signature into evidence on the sole ground that it is an electronic record or electronic signature, or on the grounds that it is not in its original form or is not an original. Information in the form of an electronic record is to be given due evidentiary weight by the trier of fact, and in assessing the evidential weight of an electronic record or electronic signature, where its authenticity is in issue, the trier of fact is permitted to consider any relevant information or circumstances, including, but not limited to: (1) the manner in which it was generated, stored, or communicated, (2) the reliability of the manner in which its integrity was maintained, and (3) the manner in which its originator was identified or the electronic signature was signed.

In resolving a civil dispute involving a secure electronic *record*, the bill provides that it must be rebuttably presumed that the electronic record has not been altered since the specific time to which the secure status relates. In resolving a civil dispute involving a secure electronic *signature*, it must be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates. The bill states that the effect of these presumptions is to place on the party challenging the integrity of a secure electronic record or challenging the genuineness of a secure electronic signature (1) the burden of going forward with evidence to rebut the presumption, and (2) the burden of persuading the trier of fact that the nonexistence of the presumed fact is more probable than its existence.

The bill provides that in the absence of a secure electronic record or a secure electronic signature, nothing in the Electronic Records and Signatures Act alters existing rules regarding legal or evidentiary rules regarding the burden of proving the authenticity and integrity of an electronic record or an electronic signature.

CREATION AND DUTIES OF THE ELECTRONIC COMMERCE COMMISSION

The bill establishes the Electronic Commerce Commission (ECC) within the Department of Administrative Services to (1) adopt rules relative to certification of security procedures relative to electronic records and digital signatures, (2) adopt rules relative to defining when a certificate issued in connection with a digital signature is trustworthy, and (3) investigate violations of the bill's provisions.

Members of the Electronic Commerce Commission; repeal

(sec. 1306.32(A), (B), and (D); Section 4)

The bill establishes the ECC in the Department of Administrative Services consisting of seven members: four ex officio members and three members appointed by the Governor. The four ex officio members of the ECC are: (1) the Director of Administrative Services or the Director's designee, (2) the Director of Commerce or the Director's designee, (3) the Secretary of State or the Secretary of State's designee, and (4) the Auditor of State or the Auditor of State's designee.

The three appointed members of the ECC are: (1) an individual who is an attorney at law licensed to practice in Ohio and who has significant knowledge of intellectual property law or Internet security law, or both areas of the law, (2) an individual employed by a for-profit business with offices in Ohio, the primary business of which is *other* than providing information systems products or

services, and who has significant knowledge of Internet security issues and experience with the development of Internet-based electronic commerce, and (3) an individual employed by a for-profit business with offices in Ohio, the primary business of which is providing information systems products or services, and who has significant knowledge of Internet security issues and experience with the development of Internet-based electronic commerce.

Under the bill, provisions establishing the ECC are repealed four years after the bill's effective date. This repeal is consistent with law unaffected by the bill (sec. 101.84).

Initial appointments, terms of office, and filling vacancies

(sec. 1306.32(C)(1) and (2))

The bill provides that within 30 days after the bill's effective date, the Governor must make the initial appointments to the ECC. The terms of these initial appointments are to be staggered. Specifically, (1) one is for a one-year term ending one year after the bill's effective date, (2) one is for a two-year term ending two years after the bill's effective date, and (3) one is for a term ending three years after the bill's effective date. Thereafter, terms of office are three years, with each term ending on the same day of the same month as did the term that it succeeds.

Each member appointed by the Governor holds office from the date of appointment until the end of the term for which the member was appointed. And any member appointed to fill a vacancy occurring prior to the expiration of the term for which the member's predecessor was appointed, holds office for the remainder of that term. The bill provides that any member continues in office subsequent to the expiration date of the member's term until the member's successor takes office, or until a period of 60 days has elapsed, whichever occurs first.

Oath and compensation

(sec. 1306.32(C)(3) and (4))

Before entering upon their official duties, the bill requires that each ECC member appointed by the Governor take an oath of office as specified in the Ohio Constitution. In addition, each member appointed by the Governor receives compensation for actual and necessary expenses incurred in the performance of official duties. The amount of the expenses must be certified by the chairperson of the ECC and paid in the same manner as the expenses of employees of the Department of Administrative Services are paid.

Duties of the Department of Administrative Services relative to the ECC

(sec. 1306.32(D) and (E))

The Director of Administrative Services or the Director's designee is to be the chairperson of the ECC. In addition, the bill requires the Department of Administrative Services to provide administrative services to the ECC and assign experts required by the ECC to enable the ECC to carry out its duties as required by the bill.

ECC rule-making authority generally

(sec. 1306.32(F); Section 3)

The ECC is authorized to adopt rules of procedure and may change them at its discretion. The bill specifies that the votes of four of the members of the ECC are required for the adoption of any rule or any amendment or rescission of a rule. Under the bill, the ECC, no later than 90 days after the bill's effective date, must file the original version of the proposed rules pursuant to provisions of the Administrative Procedure Act requiring that proposed rules be filed with the Secretary of State, the Legislative Service Commission, and the Joint Committee on Agency Rule Review (JCARR) prior to a public hearing on these proposed rules.

Public record of meetings of the ECC

(sec. 1306.32(G))

The bill requires that a full and complete record of all proceedings of the ECC be kept open to public inspection and authenticated in the manner provided in current law authorizing each state department to use a state seal to authenticate records for that department.

STATE AGENCIES USE OF ELECTRONIC RECORDS AND THE ROLE OF THE DEPARTMENT OF ADMINISTRATIVE SERVICES

These provisions of the bill require state agencies to review their potential use of electronic records and signatures. If a state agency decides to use electronic records and signatures, the agency may include minimum security requirements established by the Department of Administrative Services in accordance with the bill.

State agency's use of electronic records and signatures

(sec. 1306.35)

Under the bill, each state agency is required to determine if, and the extent to which, the agency 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. Nothing in the Electronic Records and Signatures Act is to be construed to require any state agency to use or permit the use of electronic records or electronic signatures.

In any case in which a state agency decides to send or receive electronic records, or to accept document filings by electronic records, the state agency, by rule and giving due consideration to security, is authorized to specify all of the following:

- (1) The manner and format in which the electronic records are to be created, sent, received, and stored;
- (2) If the electronic records must be signed, all of the following:
 - (a) The type of electronic signature required;
 - (b) The manner and format in which such signature must be affixed to the electronic record;
 - (c) The identity of, or criteria that must be met by, any third party used by the person filing the document to facilitate the process.
- (3) Control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of such electronic records;
- (4) Any other required attributes for electronic records that are currently specified for corresponding paper documents or are reasonably necessary under the circumstances.

Any rules that are adopted by a state agency may include the relevant minimum security requirements established by the Department of Administrative Services, as discussed below. In addition, under the bill, any state agency that, prior to the bill's effective date, used or permitted the use of electronic records or electronic signatures pursuant to laws enacted or rules adopted before the bill's effective date may use or permit the use of electronic records or electronic signatures pursuant to those previously enacted laws or adopted rules.

Under the bill, if a rule of law requires or authorizes the filing of any information, notice, lien, or other document or record with any state agency, a filing made by electronic record is to have the same force and effect as a filing made on paper in all cases where the state agency has authorized or agreed to such electronic filing and the filing is made in accordance with applicable rules or agreement.

For purposes of these provisions governing a state agency's use of electronic records and signatures, the bill specifies that "state agency" does not include the General Assembly or the Supreme Court.

Department of Administrative Services

(secs. 1306.36 and 1306.37)

The bill authorizes the Department of Administrative Services (DAS) to adopt rules, in accordance with the Administrative Procedure Act, setting forth minimum security requirements for the use of electronic records and electronic signatures by state agencies.

With respect to verifying a digital signature, DAS is authorized to adopt rules, procedures, and policies whereby state agencies may issue or contract for the issuance of certificates. The bill authorizes each state agency (1) to issue, or contract for the issuance of, certificates to its employees and agents and persons conducting business or other transactions with the state agency, and (2) to take other consistent actions, including the establishment of repositories and the suspension or revocation of certificates issued, provided that these actions are conducted in accordance with all rules, procedures, and policies adopted by DAS pursuant to the authority granted.

Where appropriate, the rules adopted by DAS must specify differing levels of minimum standards from which implementing state agencies are to select the standards most appropriate for a particular application. The bill states that, to the extent reasonable under the circumstances, rules adopted by DAS, the Electronic Commerce Commission, or any other state agency pursuant to the provisions of the Electronic Records and Signatures Act and relating to the use of electronic records or electronic signatures, are to encourage and promote consistency and interoperability with similar requirements adopted by agencies of other states and the federal government.

The bill authorizes DAS to specify appropriate minimum security requirements to be implemented and followed by state agencies for (1) the generation, use, and storage of key pairs, (2) the issuance, acceptance, use, suspension, and revocation of certificates, and (3) the use of digital signatures.

DAS also may specify appropriate minimum standards and requirements that must be satisfied by a certification authority before either of the following occurs:

(1) The services of the certification authority are used by any state agency for the issuance, publication, revocation, and suspension of certificates of authority to such agency or its employees or agents;

(2) The certificates issued by the certification authority will be accepted for purposes of verifying digitally signed electronic records sent to any state agency by any person.

The bill also provides that the General Assembly and the Ohio Supreme Court may adopt rules pertaining to the use of electronic records and electronic signatures; otherwise, for purposes of this portion of the bill, a "state agency" is not to include the General Assembly or the Supreme Court.

Certain information confidential

(sec. 1306.38)

Under the bill, information that would disclose, or may lead to the disclosure of, secret or confidential information, codes, algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Records and Signatures Act are not public records for purposes of Ohio's Public Records Law.

HISTORY

ACTION	DATE	JOURNAL ENTRY
Introduced	10-27-99	p. 1325

H0488-I.123/rss