

# **BERMUDA- ELECTRONIC COMMERCE SECURITY ACT.**

## **ARTICLE 1. SHORT TITLE; PURPOSE**

Section 1-101. Short title. This Act may be cited as the Electronic Commerce Security Act.

Section 1-105. Purposes and construction. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to effectuate 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 promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce.
- (3) To facilitate electronic filing of documents with State and local government agencies, and 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 to 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.

Section 1-110. Variation by agreement. As between parties involved in generating, sending, receiving, storing, or otherwise processing electronic records, the applicability of provisions of this Act may be waived by agreement of the parties, except for the provisions of Sections 10-140, 15-210, 15-215, 15-220, and subsection (b) of Section 10-130 of this Act.

## **ARTICLE 5. ELECTRONIC RECORDS AND SIGNATURES GENERALLY**

Section 5-105. Definitions. "Asymmetric cryptosystem" means a computer-based system capable of generating and using a key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

"Certificate" means a record that at a minimum:

- (a) identifies the certification authority issuing it;
- (b) names or otherwise identifies its subscriber or a device or electronic agent under the control of the subscriber;

- (c) contains a public key that corresponds to a private key under the control of the subscriber;
- (d) specifies its operational period; and
- (e) is digitally signed by the certification authority issuing it.

"Certification authority" means a person who authorizes and causes the issuance of a certificate.

"Certification practice statement" is 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.

"Correspond", with reference to keys, means to belong to the same key pair.

"Digital signature" means 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 whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the transformation was made. A digital signature is a security procedure.

"Electronic" includes electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies.

"Electronic record" means a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another.

"Electronic signature" means a signature in electronic form attached to or logically associated with an electronic record.

"Information" includes data, text, images, sound, codes, computer programs, software, databases, and the like.

"Key pair" means, in an asymmetric cryptosystem, 2 mathematically related keys, referred to as a private key and a public key, having the properties that (i) one key (the private key) can encrypt a message that only the other key (the public key) can decrypt, and (ii) even knowing one key (the public key), it is computationally unfeasible to discover the other key (the private key).

"Message digest function" means an algorithm that maps or translates the sequence of bits comprising an electronic record into another, generally smaller, set of bits (the message digest) without requiring the use of any secret information such as a key, such that an electronic record yields the same message digest every time the algorithm is executed using such record as input and it is computationally unfeasible

that any 2 electronic records can be found or deliberately generated that would produce the same message digest using the algorithm unless the 2 records are precisely identical.

"Operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on a later date and time certain if stated in the certificate) and ends on the date and time it expires as noted in the certificate or is earlier revoked, but does not include any period during which a certificate is suspended.

"Person" means 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.

"Private Key" means the key of a key pair used to create a digital signature.

"Public key" means the key of a key pair used to verify a digital signature.

"Record" means 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.

"Repository" means a system for storing and retrieving certificates or other information relevant to certificates, including information relating to the status of a certificate.

"Revoke a certificate" means to permanently end the operational period of a certificate from a specified time forward.

"Rule of law" means any statute, ordinance, common law rule, court decision, or other rule of law enacted, established or promulgated by the State of Illinois, or any Agency, commission, department, court, other authority or political subdivision of the State of Illinois.

"Security procedure" means a methodology or procedure used for the purpose of

- (1) Verifying that an electronic record is that of a specific person or
- (2) Detecting error or alteration in the communication, content, or storage of an electronic record since a specific point in time. 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.

"Signature device" means unique information, such as codes, algorithms, letters, numbers, private keys, or personal identification numbers (PINs), 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.

"Signed" or "signature" 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.

"State agency" means and includes all officers, boards, commissions, courts, and agencies created by the Illinois Constitution, whether in the executive, legislative

or judicial branch, all officers, departments, boards, commissions, agencies, institutions, authorities, universities, bodies politic and corporate of the State; and administrative units or corporate outgrowths of the State government which are created by or pursuant to statute, other than units of local government and their officers, school districts and boards of election commissioners; all administrative units and corporate outgrowths of the above and as may be created by executive order of the Governor.

"Subscriber" means a person who is the subject named or otherwise identified in a certificate, who controls a private key that corresponds to the public key listed in that certificate, and who is the person to whom digitally signed messages verified by reference to such certificate are to be attributed.

"Suspend a certificate" means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

"Trustworthy manner" means through the use of computer hardware, software, and procedures that, in the context in which they are used:

- (a) can be shown to be reasonably resistant to penetration, compromise, and misuse;
- (b) Provide a reasonable level of reliability and correct operation;
- (c) are reasonably suited to performing their intended functions or serving their intended purposes;
- (d) comply with applicable agreements between the parties, if any; and
- (e) adhere to generally accepted security procedures.

"Valid certificate" means a certificate that a certification authority has issued and that the subscriber listed in the certificate has accepted.

"Verify a digital signature" means to use the public key listed in a valid certificate, along with the appropriate message digest function and asymmetric cryptosystem, to evaluate a digitally signed electronic record, such that the result of the process concludes that the digital signature was created using the private key corresponding to the public key listed in the certificate and the electronic record has not been altered since its digital signature was created.

Section 5-110. Legal recognition. Information, records, and signatures shall not be denied legal effect, validity, or enforceability solely on the grounds that they are in Electronic form.

Section 5-115. Electronic records.

- (a) Where 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.
- (b) The provisions of this Section shall not apply:
  - (1) when its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking

body or repugnant to the context of the same rule of law, provided that the mere requirement that information be "in writing", "written", or "printed" shall not by itself be sufficient to establish such intent;

- (2) to any rule of law governing the creation or execution of a will or trust, living will, or healthcare power of attorney; and
- (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, unless an electronic version of such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy.

#### Section 5-120. Electronic signatures.

- (a) Where 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.
- (b) 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.
- (c) The provisions of this Section shall not apply:
  - (1) when its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law, provided that the mere requirement of a "signature" or that a record be "signed" shall not by itself be sufficient to establish such intent;
  - (2) to any rule of law governing the creation or execution of a will or trust, living will, or healthcare power of attorney; and
  - (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, unless an electronic version of such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy.

Section 5-125. Original.

- (a) 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 of the information from the time when it was first generated in its final form, as an electronic record or otherwise.
- (b) The criteria for assessing integrity shall be 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 ensure that information has remained complete and unaltered shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.
- (c) The provisions of this Section do 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 such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy.

Section 5-130. Admissibility into evidence.

- (a) In any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic record or electronic signature into evidence:
  - (1) on the sole ground that it is an electronic record or electronic signature; or
  - (2) on the grounds that it is not in its original form or is not an original.
- (b) Information in the form of an electronic record shall be given due evidentiary weight by the trier of fact. In assessing the evidential weight of an electronic record or electronic signature where its authenticity is in issue, the trier of fact may consider the manner in which it was generated, stored or communicated, the reliability of the manner in which its integrity was maintained, the manner in which its originator was identified or the electronic record was signed, and any other relevant information or circumstances.

Section 5-135. Retention of electronic records.

- (a) Where a rule of law requires that certain documents, records or information be retained, that requirement is met by retaining electronic records of such information in a trustworthy manner, provided that the following conditions are satisfied:
  - (1) the electronic record and the information contained therein are accessible so as to be usable for subsequent reference at all times when such information must be retained;
  - (2) the information is 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; and
  - (3) such data as enables 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, if any, is retained.
- (b) An obligation to retain documents, records or information in accordance with subsection (a) does not extend to any data the sole purpose of which is to enable the record to be sent or received.
- (c) Nothing in this Section shall preclude any State agency from specifying additional requirements for the retention of records that are subject to the jurisdiction of such agency.

Section 5-140. Electronic use not required. Nothing in this Act shall be construed to:

- (1) 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) 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.

Section 5-145. Applicability of other statutes or rules.

Notwithstanding any provisions of this Act, if any other statute or rule requires approval by a State agency prior to the use or retention of electronic records or

the use of electronic signatures, the provisions of that other statute or rule shall also apply.

## **ARTICLE 10. SECURE ELECTRONIC RECORDS AND SIGNATURES**

### Section 10-105. Secure electronic record.

- (a) 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, then such electronic record shall be considered to be a secure electronic record from such specified point in time to the time of verification, if the relying party establishes that the qualified security procedure was:
  - (1) Commercially reasonable under the circumstances;
  - (2) Applied by the relying party in a trustworthy manner; and
  - (3) reasonably and in good faith relied upon by the relying party.
- (b) A qualified security procedure for purposes of this Section is a security procedure to detect changes in the content of an electronic record that is:
  - (1) previously agreed to by the parties; or
  - (2) certified by the Secretary of State in accordance with Section 10-135 as being capable of providing reliable evidence that an electronic record has not been altered.

### Section 10-110. Secure electronic signature.

- (a) If, through the use of a qualified security procedure, it can be verified that an electronic signature is the signature of a specific person, then such electronic signature shall be considered to be a secure electronic signature at the time of verification, if the relying party establishes that the qualified security procedure was:
  - (1) commercially reasonable under the circumstances;
  - (2) applied by the relying party in a trustworthy manner; and
  - (3) reasonably and in good faith relied upon by the relying party.
- (b) A qualified security procedure for purposes of this Section is a security procedure for identifying a person that is:
  - (1) previously agreed to by the parties; or
  - (2) certified by the Secretary of State in accordance with Section 10-135 as being capable of creating, in a trustworthy manner, an electronic signature that:
    - (A) is unique to the signer within the context in which it is used;
    - (B) can be used to objectively identify the person signing the electronic record;

- (C) was reliably created by such identified person, (e.g., because some aspect of the procedure involves the use of a signature device or other means or method that is under the sole control of such person), and that cannot be readily duplicated or compromised; and
- (D) is created, and is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.

Section 10-115. Commercially reasonable; reliance.

- (a) 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 the procedure was used, including the nature of the transaction, sophistication of the parties, volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered to but rejected by either of the parties, cost of alternative procedures, and procedures in general use for similar types of transactions.
- (b) Whether reliance on a security procedure was reasonable and in good faith is to be determined in light of all the circumstances known to the relying party at the time of the reliance, having due regard to the:
  - (1) information that the relying party knew or should have known of at the time of reliance that would suggest that 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 of trade, particularly trade conducted by trustworthy systems or other computer-based means; and
  - (5) whether the verification was performed with the assistance of an independent third party.

Section 10-120. Presumptions.

- (a) In resolving a civil dispute involving a secure electronic record, it shall be rebuttably presumed that the electronic record has not been altered since the specific point in time to which the secure status relates.
- (b) In resolving a civil dispute involving a secure electronic signature, it shall be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates.

- (c) The effect of presumptions provided in this Section is to place on the party challenging the integrity of a secure electronic record or challenging the genuineness of a secure electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the trier of fact that the nonexistence of the presumed fact is more probable than its existence.
- (d) In the absence of a secure electronic record or a secure electronic signature, nothing in this Act shall change existing rules regarding legal or evidentiary rules regarding the burden of proving the authenticity and integrity of an electronic record or an electronic signature.

Section 10-125. Creation and control of signature devices. Except as otherwise provided by another applicable rule of law, whenever the creation, validity, or reliability of an electronic signature created by a qualified security procedure under Section 10-105 or 10-110 is dependent upon the secrecy or control of a signature device of the signer:

- (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 such signature device must exercise reasonable care to retain control and maintain the secrecy of the signature device, and to protect it from any unauthorized access, disclosure, or use, during the period when reliance on a signature created by such device is reasonable;
- (3) in the event that the signer, or any other person that rightfully has access to such signature device, knows or has reason to know that the secrecy or control of any such signature device has been compromised, such person must make a reasonable effort to promptly notify all persons that such person knows might foreseeably be damaged as a result of such compromise, or where an appropriate publication mechanism is available (which, for State agencies, may include the official newspaper designated pursuant to Section 4 of the Illinois Purchasing Act where appropriate), to publish notice of the compromise and a disavowal of any signatures created thereafter.

Section 10-130. Attribution of signature.

- (a) Except as provided by another applicable rule of law, a secure electronic signature is attributable to the person to whom it correlates, whether or not authorized, if:
  - (1) the electronic signature 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 the appearance that it came from that party;
- (2) the access or use occurred under circumstances constituting a failure to exercise reasonable care by the alleged signer; and
  - (3) the relying party relied reasonably and in good faith to its detriment on the apparent source of the electronic record.
- (b) The provisions of this Section shall not apply to transactions intended primarily for personal, family, or household use, or otherwise defined as consumer transactions by applicable law including, but not limited to, credit card and automated teller machine transactions except to the extent allowed by applicable consumer law.

Section 10-135. Secretary of State Authority to certify security procedures.

- (a) A security procedure may be certified by the Secretary of State, as a qualified security procedure for purposes of Sections 10-105 or 10-110, following an appropriate investigation or review, if:
- (1) the security procedure (including any technology and algorithms it employs) is completely open and fully disclosed to the public, and has been so for a sufficient length of time, so as to facilitate a comprehensive review and evaluation of its suitability for the intended purpose by the applicable information security or scientific community; and
  - (2) the security procedure (including any technology and algorithms it employs) has been generally accepted in the applicable information security or scientific community as being capable of satisfying the requirements of Section 10-105 or 10-110, as applicable, in a trustworthy manner.
- (b) In marketing a determination regarding whether the security procedure including any tech technology and algorithms it employs) has been generally accepted in the applicable information security or scientific community, the Secretary of State shall consider the opinion of independent experts in the applicable field and the published findings of such community, including applicable standards organizations such as the American National Standards Institute (ANSI), International Standards Organization (ISO), International telecommunications Union (ITU), and the National Institute of Standards and Technology (NIST).
- (c) Such certification shall be done through the adoption of rules in accordance with the provisions of the Illinois Administrative Procedure Act and shall specify a full and complete identification of the security procedure, including requirements as to how it is to be implemented, if appropriate.

- (d) The Secretary of State may also decertify a security procedure as a qualified security procedure for purposes of Sections 10-105 or 10-110 following an appropriate investigation or review and the adoption of rules in accordance with the provisions of the Illinois Administrative Procedure Act if subsequent developments establish that the security procedure is no longer sufficiently trustworthy or reliable for its intended purpose, or for any other reason no longer meets the requirements for certification.
- (e) The Secretary of State shall have exclusive authority to certify security procedures under this Section.

Section 10-140. Unauthorized use of signature device.

- (a) No person shall knowingly or intentionally access, copy, or otherwise obtain possession of or recreate 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 person convicted of a violation of this subsection shall be guilty of a Class A misdemeanor.
- (b) No person shall knowingly alter, disclose, or use 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 person convicted of a violation of this subsection shall be guilty of a Class 4 felony. A person convicted of a violation of this subsection who has previously been convicted of a violation of this subsection or Section 15-210 shall be guilty of a Class 3 felony. A person who violates this Section in furtherance of any scheme or artifice to defraud in excess of \$50,000 shall be guilty of a Class 2 felony.

## **ARTICLE 15. EFFECT OF A DIGITAL SIGNATURE**

Section 15-101. Secure electronic record. A digital signature that is created using an asymmetric algorithm certified by the Secretary of State under item (2) of subsection (b) of Section 10-105 shall be considered to be a qualified security procedure for purposes of detecting changes in the content of an electronic record under Section 10-105 if the digital signature was created during the operational period of a valid certificate, and is verified by reference to the public key listed in such certificate.

Section 15-105. Secure electronic signature. A digital signature that is created using an asymmetric algorithm certified by the Secretary of State under item (2) of Subsection (b) of Section 10-110 shall be considered to be a qualified security procedure for purposes of identifying a person under Section 10-110 if:

- (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, if any, and can be verified by reference to the public key listed in the certificate; and
- (2) the certificate is considered trustworthy (i.e., an accurate binding of a public key to a person's identity) because the certificate was issued by a certification authority in accordance with standards, procedures, and other requirements specified by the Secretary of State, or the trier of fact independently finds 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 otherwise finds that the material information set forth in the certificate is true.

Section 15-115. Secretary of State Authority to adopt rules.

- (a) The Secretary of State may adopt rules applicable to both the public and private sectors for the purpose of defining when a certificate is considered sufficiently trustworthy under Section 15-105 such that a digital signature verified by reference to such a certificate will be considered a qualified security procedure under Section 10-110. The rules may include (1) establishing or adopting standards applicable to certification authorities or certificates, compliance with which may be measured by becoming certified by the Secretary of State, becoming accredited by one or more independent accrediting entities recognized by the Secretary of State, or by other appropriate means and (2) where appropriate, establishing fees to be charged by the Secretary of State to recover all or a portion of its costs in connection therewith.
- (b) In developing the rules, the Secretary of State shall endeavor to do so in a manner that will provide maximum flexibility to the implementation of digital signature technology and the business models necessary to support it, that will provide a clear basis for the recognition of certificates issued by foreign certification authorities, and, to the extent reasonably possible, that will maximize the opportunities for uniformity with the laws of other jurisdictions (both within the United States and internationally).
- (c) The Secretary of State shall have exclusive authority to adopt rules authorized by this Section.

Section 15-201. Reliance on certificates foreseeable. It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified, during the operational period of such certificate and within any limits specified in such certificate.

Section 15-205. Restrictions on publication of certificate. No person may publish a certificate, otherwise knowingly make 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 such person knows that:

- (1) the certification authority listed in the certificate has not issued it;
- (2) the subscriber listed in the certificate has not accepted it; or
- (3) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such revocation or suspension, or giving notice of revocation or suspension.

Section 15-210. Fraudulent use. No person shall knowingly create, publish, alter, or otherwise use a certificate for any fraudulent or other unlawful purpose. A person convicted of a violation of this Section shall be guilty of a Class 4 felony. A person convicted of a violation of this Section who previously has been convicted of a violation of this Section or Section 10-140 shall be guilty of a Class 3 felony. A person who violates this Section in furtherance of any scheme or artifice to defraud in excess of \$50,000 shall be guilty of a Class 2 felony.

Section 15-215. False or unauthorized request. No person shall knowingly misrepresent his or her identity or authorization in requesting or accepting a certificate or in requesting suspension or revocation of a certificate. A person convicted of a violation of this Section shall be guilty of a Class A misdemeanor. A person who violates this Section 10 times within a 12-month period, or in furtherance of any scheme or artifice to defraud, shall be guilty of a Class 4 felony. A person who violates this Section in furtherance of any scheme or artifice to defraud in excess of \$50,000 shall be guilty of a Class 2 felony.

Section 15-220. Unauthorized use of signature device. No person shall knowingly access, alter, disclose, or use 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 person convicted of a violation of this Section shall be guilty of a Class 3 felony. A person who violates this Section in furtherance of any scheme or artifice to defraud shall be guilty of a Class 2 felony.

Section 15-301. Trustworthy services. Except as conspicuously set forth in its certification practice statement, a certification authority and a person maintaining a repository must maintain its operations and perform its services in a trustworthy manner.

Section 15-305. Disclosure.

- (a) 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 to the subscriber and all such relying parties:
  - (1) its certification practice statement, if any, applicable thereto; and
  - (2) its 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 (its "certification authority certificate").
- (b) In the event of an occurrence that materially and adversely affects a certification authority's operations or system, its certification authority certificate, or any other aspect of its ability to operate in a trustworthy manner, the certification authority must act in accordance with procedures governing such an occurrence specified in its certification practice statement, or in the absence of such procedures, must use reasonable efforts to notify any persons that the certification authority knows might foreseeably be damaged as a result of such occurrence.

Section 15-310. Issuance of a certificate. A certification authority may issue a certificate to a prospective subscriber for the purpose of allowing third parties to verify digital signatures created by the subscriber only after:

- (1) the certification authority has received a request for issuance from the prospective subscriber; and
- (2) the certification authority has:
  - (A) complied with all of the relevant practices and procedures set forth in its applicable certification practice statement, if any; or
  - (B) in the absence of a certification practice statement addressing these issues, confirmed in a trustworthy manner that:
    - (i) the prospective subscriber is the person to be listed in the certificate to be issued;
    - (ii) the information in the certificate to be issued is accurate; and
    - (iii) 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 such private key.

Section 15-315. Representations upon issuance of certificate.

- (a) By issuing a certificate with the intention that it will be relied upon by third parties to verify digital signatures created by the subscriber, a certification authority represents to the subscriber, and to any person who reasonably relies on information contained in the certificate, in good faith and during its operational period, that:
- (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 or of which such person has notice, or in lieu thereof, in accordance with this 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, that 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; and
  - (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.
- (b) If a certification authority issued the certificate subject to the laws of another jurisdiction, the certification authority also makes all warranties and representations, if any, otherwise applicable under the law governing its issuance.

#### Section 15-320. Revocation of a certificate.

- (a) During the operational period of a certificate, the certification authority that issued the certificate must revoke the certificate in accordance with the policies and procedures governing revocation specified in its applicable certification practice statement, or in the absence of such policies and procedures, as soon as possible after:
- (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 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 confirmation 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; or
- (5) confirmation by the certification authority that:
  - (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;
  - or
  - (D) the subscriber's private key was compromised.
- (b) Upon effecting such a revocation, the certification authority must 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, promptly publish notice of the revocation in all repositories where the certification authority previously caused publication of the certificate, and otherwise disclose the fact of revocation on inquiry by a relying party.

## **ARTICLE 20. DUTIES OF SUBSCRIBERS**

Section 20-101. Obtaining a certificate. All material representations knowingly made by a person to a certification authority for purposes of obtaining a certificate naming such person as a subscriber must be accurate and complete to the best of such person's knowledge and belief.

Section 20-105. Acceptance of a certificate.

- (a) A person accepts a certificate that names such person as a subscriber by publishing or approving publication of it to one or more persons, or in a repository, or otherwise demonstrating approval of it, while knowing or having notice of its contents.
- (b) By accepting a certificate, the subscriber listed in the certificate represents to any person who reasonably relies on information contained in the certificate, in good faith and during its operational period, that:
  - (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.

Section 20-110. Revocation of certificate. Except as otherwise provided by another applicable rule of law, if the private key corresponding to the public key listed in a valid certificate is lost, stolen, accessible to an unauthorized person, or otherwise compromised during the operational period of the certificate, a subscriber who has learned of the compromise must promptly request the issuing certification authority to revoke the certificate and publish notice of revocation in all repositories in which the subscriber previously authorized the certificate to be published, or otherwise provide reasonable notice of the revocation.

## **ARTICLE 25. STATE AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES**

Section 25-101. State agency use of electronic records.

- (a) Each State agency 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.
- (b) In any case where a State agency decides to send or receive electronic records, or to accept document filings by electronic records, the State agency may, by appropriate agency rule (or court rule where appropriate), giving due consideration to security, specify:
  - (1) the manner and format in which such electronic records must be created, sent, received, and stored;
  - (2) if such electronic records must be signed, the type of electronic signature required, the manner and format in which such signature must be affixed to the electronic record, and 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; and
  - (4) any other required attributes for such electronic records that are currently specified for corresponding paper documents, or reasonably necessary under the circumstances.
- (c) All rules adopted by a State agency shall include the relevant minimum security requirements established by the Department of Central Management Services, if any.

- (d) Whenever any 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 an electronic record shall 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.
- (e) Nothing in this Act shall be construed to require any State agency to use or to permit the use of electronic records or electronic signatures.

Section 25-105. Department of Central Management Services to adopt State standards.

- (a) The Department of Central Management Services may adopt rules setting forth minimum security requirements for the use of electronic records and electronic signatures by State agencies.
- (b) The Department of Central Management Services shall 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.
- (c) Each State agency shall have the authority to issue, or contract for the issuance of, certificates to (i) its employees and agents and (ii) persons conducting business or other transactions with such State agency and to take other actions consistent therewith, including the establishment of repositories and the suspension or revocation of certificates so issued, provided that the foregoing is conducted in accordance with all the rules, procedures, and policies specified by the Department of Central Management Services. The Department of Central Management Services shall have the authority to specify the rules, procedures, and policies whereby State agencies may issue or contract for the issuance of certificates.
- (d) The Department of Central Management Services may specify appropriate minimum standards and requirements that must be satisfied by a certification authority before:
  - (1) its services are used by any State agency for the issuance, publication, revocation, and suspension of certificates to such agency, or its employees or agents (for official use); or
  - (2) the certificates it issues will be accepted for purposes of verifying digitally signed electronic records sent to any State agency by any person.
- (e) Where appropriate, the rules adopted by the Department of Central Management Services pursuant to this Section shall specify differing levels of

minimum standards from which implementing State agencies can select the standard most appropriate for a particular application.

- (f) The General Assembly, through the Joint Committee on Legislative Support Services, and the Supreme Court, separately for the respective branches, may adopt rules setting forth the minimum security requirements for the use of electronic records and electronic signatures by the respective branches. The rules shall generally be consistent with the rules adopted by the Department of Central Management Services. The Joint Committee on Legislative Support Services and the Supreme Court may also accept the rules adopted by the Department of Central Management Services for the use of electronic records and electronic signatures by the respective branches.
- (g) Except as provided in subsection (f) and in Section 25-101, the Department of Central Management Services shall have exclusive authority to adopt rules authorized by this Section.

Section 25-115. Interoperability. To the extent reasonable under the circumstances, rules adopted by the Department of Central Management Services or a State agency relating to the use of electronic records or electronic signatures shall be drafted in a manner designed to encourage and promote consistency and interoperability with similar requirements adopted by government agencies of other states and the federal government.

### **ARTICLE 30. ENFORCEMENT; CIVIL REMEDY; SEVERABILITY**

Section 30-1. Enforcement. The Secretary of State may investigate complaints or other information indicating violations of rules adopted by the Secretary of State under this Act. The Secretary of State shall certify to the Attorney General, for such action as the Attorney General may deem appropriate, all information he or she obtains that discloses a violation of any provision of this Act or the rules adopted by the Secretary of State under this Act.

Section 30-5. Civil remedy. Whoever suffers loss by reason of a violation of Section 10-140, 15-210, 15-215, or 15-220 of this Act or Section 17-3 of the Criminal Code of 1961 may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorneys fees and other litigation expenses.

Section 30-110. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

## ARTICLE 95. AMENDATORY PROVISIONS

Section 95-1. The Statute on Statutes is amended by changing Section 1.15 as follows:

(5 ILCS 70/1.15) (from Ch. 1, par. 1016) Sec. 1.15. "Written" and "in writing" may include printing, electronic, and any other mode of representing words and letters; but when the written signature of any person is required by law on ~~to~~ any official or public writing or bond, required by law, it shall be (1) ~~in~~ the proper handwriting of such person or, in case he is unable to write, his proper mark or (2) an electronic signature as defined in the Electronic Commerce Security Act, except as otherwise provided by law. (Source: P.A. 88-672, eff. 12-14-94.)

Section 95-5. The Freedom of Information Act is amended by changing Section 7 as follows:

(5 ILCS 140/7) (from Ch. 116, par. 207)

Sec. 7. Exemptions.

- (1) The following shall be exempt from inspection and copying:
  - (a) Information specifically prohibited from disclosure by federal or State law or rules and regulations adopted under federal or State law.
  - (b) Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy. Information exempted under this subsection (b) shall include but is not limited to:
    - (i) files and personal information maintained with respect to clients, patients, residents, students or other individuals receiving social, medical, educational, vocational, financial, supervisory or custodial care or services directly or indirectly from federal agencies or public bodies;
    - (ii) Personnel files and personal information maintained with respect to employees, appointees or elected officials of any public body or applicants for those positions;
    - (iii) files and personal information maintained with respect to any applicant, registrant or licensee by any public body cooperating with or engaged in professional or occupational registration, licensure or discipline;

- (iv) information required of any taxpayer in connection with the assessment or collection of any tax unless disclosure is otherwise required by State statute; and
  - (v) information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement or penal agencies; provided, however, that identification of witnesses to traffic accidents, traffic accident reports, and rescue reports may be provided by agencies of local government, except in a case for which a criminal investigation is ongoing, without constituting a clearly unwarranted per se invasion of personal privacy under this subsection.
- (c) Records compiled by any public body for administrative enforcement proceedings and any law enforcement or correctional agency for law enforcement purposes or for internal matters of a public body, but only to the extent that disclosure would:
- (i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency;
  - (ii) interfere with pending administrative enforcement proceedings conducted by any public body;
  - (iii) deprive a person of a fair trial or an impartial hearing;
  - (iv) unavoidably disclose the identity of a confidential source or confidential information furnished only by the confidential source;
  - (v) disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct;
  - (vi) constitute an invasion of personal privacy under subsection (b) of this Section;
  - (vii) endanger the life or physical safety of law enforcement personnel or any other person; or
  - (viii) obstruct an ongoing criminal investigation.
- (d) Criminal history record information maintained by State or local criminal justice agencies, except the following which shall be open for public inspection and copying:
- (i) chronologically maintained arrest information, such as traditional arrest logs or blotters;
  - (ii) the name of a person in the custody of a law enforcement agency and the charges for which that person is being held;
  - (iii) court records that are public;
  - (iv) records that are otherwise available under State or local law; or

- (v) records in which the requesting party is the individual identified, except as provided under part (vii) of paragraph (c) of subsection (1) of this Section.

"Criminal history record information" means data identifiable to an individual and consisting of descriptions or notations of arrests, detentions, indictments, informations, pre-trial proceedings, trials, or other formal events in the criminal justice system or descriptions or notations of criminal charges (including criminal violations of local municipal ordinances) and the nature of any disposition arising therefrom, including sentencing, court or correctional supervision, rehabilitation and release. The term does not apply to statistical records and reports in which individuals are not identified and from which their identities are not ascertainable, or to information that is for criminal investigative or intelligence purposes.

- (e) Records that relate to or affect the security of correctional institutions and detention facilities.
- (f) Preliminary drafts, notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body. The exemption provided in this paragraph (f) extends to all those records of officers and agencies of the General Assembly that pertain to the preparation of legislative documents.
- (g) Trade secrets and commercial or financial information obtained from a person or business where the trade secrets or information are proprietary, privileged or confidential, or where disclosure of the trade secrets or information may cause competitive harm, including all information determined to be confidential under Section 4002 of the Technology Advancement and Development Act. Nothing contained in this paragraph (g) shall be construed to prevent a person or business from consenting to disclosure.
- (h) Proposals and bids for any contract, grant, or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person proposing to enter into a contractor agreement with the body, until an award or final selection is made. Information prepared by or for the body in preparation of a bid solicitation shall be exempt until an award or final selection is made.
- (i) Valuable formulae, designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss.

- (j) Test questions, scoring keys and other examination data used to administer an academic examination or determined the qualifications of an applicant for a license or employment.
- (k) Architects' plans and engineers' technical submissions for projects not constructed or developed in whole or in part with public funds and for projects constructed or developed with public funds, to the extent that disclosure would compromise security.
- (l) Library circulation and order records identifying library users with specific materials.
- (m) Minutes of meetings of public bodies closed to the public as provided in the Open Meetings Act until the public body makes the minutes available to the public under Section 2.06 of the Open Meetings Act.
- (n) Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies.
- (o) Information received by a primary or secondary school, college or university under its procedures for the evaluation of faculty members by their academic peers.
- (p) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.
- (q) Documents or materials relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.
- (r) Drafts, notes, recommendations and memoranda pertaining to the financing and marketing transactions of the public body. The records of ownership, registration, transfer, and exchange of municipal debt obligations, and of persons to whom payment with respect to these obligations is made.
- (s) The records, documents and information relating to real estate purchase negotiations until those negotiations have been completed or otherwise terminated. With regard to a parcel involved in a pending or actually and reasonably contemplated eminent domain proceeding under Article VII of the Code of Civil Procedure, records, documents and information relating

to that parcel shall be exempt except as may be allowed under discovery rules adopted by the Illinois Supreme Court. The records, documents and information relating to a real estate sale shall be exempt until a sale is consummated.

- (t) Any and all proprietary information and records related to the operation of an intergovernmental risk management association or self-insurance pool or jointly self-administered health and accident cooperative or pool.
- (u) Information concerning a university's adjudication of student or employee grievance or disciplinary cases, to the extent that disclosure would reveal the identity of the student or employee and information concerning any public body's adjudication of student or employee grievances or disciplinary cases, except for the final outcome of the cases.
- (v) Course materials or research materials used by faculty members.
- (w) Information related solely to the internal personnel rules and practices of a public body.
- (x) Information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of a public body responsible for the regulation or supervision of financial institutions or insurance companies, unless disclosure is otherwise required by State law.
- (y) Information the disclosure of which is restricted under Section 5-108 of the Public Utilities Act.
- (z) Manuals or instruction to staff that relate to establishment or collection of liability for any State tax or that relate to investigations by a public body to determine violation of any criminal law.
- (aa) Applications, related documents, and medical records received by the Experimental Organ Transplantation Procedures Board and any and all documents or other records prepared by the Experimental Organ Transplantation Procedures Board or its staff relating to applications it has received.
- (bb) Insurance or self insurance (including any intergovernmental risk management association or self insurance pool) claims, loss or risk management information, records, data, advice or communications.
- (cc) Information and records held by the Department of Public Health and its authorized representatives relating to known or suspected cases of sexually transmissible disease or any information the disclosure of which is restricted under the Illinois Sexually Transmissible Disease Control Act.
- (dd) Information the disclosure of which is exempted under Section 30 of the Radon Industry Licensing Act.
- (ee) Firm performance evaluations under Section 55 of the Architectural, Engineering, and Land Surveying Qualifications Based Selection Act.

- (ff) Security portions of system safety program plans, investigation reports, surveys, schedules, lists, data, or information compiled, collected, or prepared by or for the Regional Transportation Authority under Section 2.11 of the Regional Transportation Authority Act or the State of Missouri under the Bi-State Transit Safety Act.
- (gg) Information the disclosure of which is restricted and exempted under Section 50 of the Illinois Prepaid Tuition Act.
- (hh) Information that would disclose or might 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 Commerce Security Act.

(2) This Section does not authorize withholding of information or limit the availability of records to the public, except as stated in this Section or otherwise provided in this Act. (Source: P.A. 90-262, eff. 7-30-97; 90-273, eff. 7-30-97; 90-546, eff. 12-1-97; revised 12-24-97.)

Section 95-10. The State Comptroller Act is amended by changing Section 14.01 as follows: (15 ILCS 405/14.01)

Sec. 14.01. Digital signatures.

- (a) In any communication between a State agency and the Comptroller in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this Section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:
  - (1) It is unique to the person using it.
  - (2) It is capable of verification.
  - (3) It is under the sole control of the person using it.
  - (4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
  - (5) It conforms to regulations adopted by the Comptroller.
- (b) The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this Section shall require a State agency to use or permit the use of a digital signature.
- (c) "Digital signature" has the meaning ascribed to that term in the Electronic Commerce Security Act  
(Source: P.A. 90-37, eff. 6-27-97.)

Section 95-15. The Criminal Code of 1961 is amended by changing Section 17-3 as follows:

(720 ILCS 5/17-3) (from Ch. 38, par. 17-3)

Sec. 17-3. Forgery.

- (a) A person commits forgery when, with intent to defraud, he knowingly:
- (1) makes or alters any document apparently capable of defrauding another in such manner that it purports to have been made by another or at another time, or with different provisions, or by authority of one who did not give such authority; or
  - (2) issues or delivers such document knowing it to have been thus made or altered; or
  - (3) possesses, with intent to issue or deliver, any such document knowing it to have been thus made or altered; or-
  - (4) unlawfully uses the signature device of another to create an electronic signature of that other person, as those terms are defined in the Electronic Commerce Security Act.
- (b) An intent to defraud means an intention to cause another to assume, create, transfer, alter or terminate any right, obligation or power with reference to any person or property.
- (c) A document apparently capable of defrauding another includes, but is not limited to, one by which any right, obligation or power with reference to any person or property may be created, transferred, altered or terminated. A document includes any record or electronic record as those terms are defined in the Electronic Commerce Security Act.
- (d) Sentence.
- Forgery is a Class 3 felony. (Source: P.A. 77-2638.)

**ARTICLE 99. EFFECTIVE DATE**

Section 99-1. Effective date. This Act takes effect July 1, 1999.