

## ILLINOIS COMPILED STATUTES

### CHAPTER 5. GENERAL PROVISIONS ACT 175. ELECTRONIC COMMERCE SECURITY ACT

#### **Sec. 1-101. Short title.**

This Act may be cited as the Electronic Commerce Security Act.  
(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

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

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

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

**Sec. 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.  
(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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 making a determination regarding whether the security procedure (including any 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

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

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 15-205. Restrictions on publication of certificate.**

No person may publish a certificate, or 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

#### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

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

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

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

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

## **ARTICLE 27. ELECTRONIC COMMERCE SECURITY CERTIFICATION FUND**

### **Sec. 27-5. Electronic Commerce Security Certification Fund.**

Fees collected by the Secretary of State under Section 15-115 of this Act must be deposited into the Electronic Commerce Security Certification Fund, a special fund created in the State treasury. Subject to appropriation, moneys in the Fund shall be used by the Secretary of State for the administration of this Act.

(Source: P.A. 91-58, eff. 7-1-99.)

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

### **Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 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.

(Source: P.A. 90-759, eff. 7-1-99.)

**Sec. 30-110. Severability.**

The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

(Source: P.A. 90-759, eff. 7-1-99.)

**ARTICLE 95. AMENDATORY PROVISIONS**

**Sec. 95-1. (Amendatory provisions; text omitted).**

(Source: P.A. 90-759, eff. 7-1-99; text omitted.)

**Sec. 95-5. (Amendatory provisions; text omitted.)**

(Source: P.A. 90-759, eff. 7-1-99; text omitted.)

**Sec. 95-10. (Amendatory provisions; text omitted).**

(Source: P.A. 90-759, eff. 7-1-99; text omitted.)

**Sec. 95-15. (Amendatory provisions; text omitted).**

(Source: P.A. 90-759, eff. 7-1-99; text omitted.)

**ARTICLE 99. EFFECTIVE DATE**

**Sec. 99-1. Effective date.**

This Act takes effect July 1, 1999.

(Source: P.A. 90-759, eff. 7-1-99.)

**CHAPTER 765 PROPERTY**

**ACT 33. UNIFORM REAL PROPERTY ELECTRONIC RECORDING ACT.**

**765 ILCS 33/1. Short title.** This Act may be cited as the Uniform Real Property Electronic Recording Act.

(Source: P.A. 95-472, eff. 8-27-07.)

**765 ILCS 33/2. Definitions.** In this Act:

(1) "Document" means information that is:

(A) inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form; and

(B) eligible to be recorded in the land records maintained by the county recorder.

(2) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(3) “Electronic document” means a document that is received by the recorder in an electronic form.

(4) “Electronic signature” means an electronic sound, symbol, or process attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document.

(5) “Person” means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, public corporation, government, or governmental subdivision, agency, or instrumentality, or any other legal or commercial entity.

(6) “State” means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States.

(7) “Secretary” means the Secretary of State.

(8) “Commission” means the Illinois Electronic Recording Commission.

Any notifications required by this Act must be made in writing and may be communicated by certified mail, return receipt requested or electronic mail so long as receipt is verified.

(Source: P.A. 95-472, eff. 8-27-07.)

#### **765 ILCS 33/3. Validity of electronic documents.**

(a) If a law requires, as a condition for recording, that a document be an original, be on paper or another tangible medium, or be in writing, the requirement is satisfied by an electronic document satisfying this Act.

(b) If a law requires, as a condition for recording, that a document be signed, the requirement is satisfied by an electronic signature.

(c) A requirement that a document or a signature associated with a document be notarized, acknowledged, verified, witnessed, or made under oath is satisfied if the electronic signature of the person authorized to perform that act, and all other information required to be included, is attached to or logically associated with the document or signature. A physical or electronic image of a stamp, impression, or seal need not accompany an electronic signature.

(Source: P.A. 95-472, eff. 8-27-07.)

#### **765 ILCS 33/4. Recording of documents.**

(a) In this Section, “paper document” means a document that is received by the county recorder in a form that is not electronic.

(b) A county recorder:

(1) who implements any of the functions listed in this Section shall do so in compliance with standards established by the Illinois Electronic Recording Commission and must follow the procedures of the Local Records Act before destroying any original paper records as part of a conversion process into an electronic or other format.

(2) may receive, index, store, archive, and transmit electronic documents.

(3) may provide for access to, and for search and retrieval of, documents and information by electronic means, including the Internet, and on approval by the county

recorder of the form and amount, the county board may adopt a fee for document detail or image retrieval on the Internet.

(4) who accepts electronic documents for recording shall continue to accept paper documents as authorized by State law and shall place entries for both types of documents in the same index.

(5) may convert paper documents accepted for recording into electronic form.

(6) may convert into electronic form information recorded before the county recorder began to record electronic documents.

(7) may accept electronically any fee or tax that the county recorder is authorized to collect.

(8) may agree with other officials of a state or a political subdivision thereof, or of the United States, on procedures or processes to facilitate the electronic satisfaction of prior approvals and conditions precedent to recording and the electronic payment of fees and taxes.

(Source: P.A. 95-472, eff. 8-27-07.)

### **765 ILCS 33/5. Administration and standards.**

(a) To adopt standards to implement this Act, there is established, within the Office of the Secretary of State, the Illinois Electronic Recording Commission consisting of 15 commissioners as follows:

(1) The Secretary of State or the Secretary's designee shall be a permanent commissioner.

(2) The Secretary of State shall appoint the following additional 14 commissioners:

(A) Three who are from the land title profession.

(B) Three who are from lending institutions.

(C) One who is an attorney.

(D) Seven who are county recorders, no more than 4 of whom are from one political party, representative of counties of varying size, geography, population, and resources.

(3) On the effective date of this Act, the Secretary of State or the Secretary's designee shall become the Acting Chairperson of the Commission. The Secretary shall appoint the initial commissioners within 60 days and hold the first meeting of the Commission within 120 days, notifying commissioners of the time and place of the first meeting with at least 14 days' notice. At its first meeting the Commission shall adopt, by a majority vote, such rules and structure that it deems necessary to govern its operations, including the title, responsibilities, and election of officers. Once adopted, the rules and structure may be altered or amended by the Commission by majority vote. Upon the election of officers and adoption of rules or bylaws, the duties of the Acting Chairperson shall cease.

(4) The Commission shall meet at least once every year within the State of Illinois. The time and place of meetings to be determined by the Chairperson and approved by a majority of the Commission.

(5) Eight commissioners shall constitute a quorum.

(6) Commissioners shall receive no compensation for their services but may be reimbursed for reasonable expenses at current rates in effect at the Office of the Secretary of State, directly related to their duties as commissioners and participation at Commission meetings or while on business or at meetings which have been authorized by the Commission.

(7) Appointed commissioners shall serve terms of 3 years, which shall expire on December 1st. Five of the initially appointed commissioners, including at least 2 county recorders, shall serve terms of one year, 5 of the initially appointed commissioners, including at least 2 county recorders, shall serve terms of 2 years, and 4 of the initially appointed commissioners shall serve terms of 3 years, to be determined by lot. The calculation of the terms in office of the initially appointed commissioners shall begin on the first December 1st after the commissioners have served at least 6 months in office.

(8) The Chairperson shall declare a commissioner's office vacant immediately after receipt of a written resignation, death, a recorder commissioner no longer holding the public office, or under other circumstances specified within the rules adopted by the Commission, which shall also by rule specify how and by what deadlines a replacement is to be appointed.

(c) The Commission shall adopt and transmit to the Secretary of State standards to implement this Act and shall be the exclusive entity to set standards for counties to engage in electronic recording in the State of Illinois.

(d) To keep the standards and practices of county recorders in this State in harmony with the standards and practices of recording offices in other jurisdictions that enact substantially this Act and to keep the technology used by county recorders in this State compatible with technology used by recording offices in other jurisdictions that enact substantially this Act, the Commission, so far as is consistent with the purposes, policies, and provisions of this Act, in adopting, amending, and repealing standards shall consider:

- (1) standards and practices of other jurisdictions;
- (2) the most recent standards promulgated by national standard-setting bodies, such as the Property Records Industry Association;
- (3) the views of interested persons and governmental officials and entities;
- (4) the needs of counties of varying size, population, and resources; and
- (5) standards requiring adequate information security protection to ensure that electronic documents are accurate, authentic, adequately preserved, and resistant to tampering.

(e) The Commission shall review the statutes related to real property and the statutes related to recording real property documents and shall recommend to the General Assembly any changes in the statutes that the Commission deems necessary or advisable.

(f) Funding. The Secretary of State may accept for the Commission, for any of its purposes and functions, donations, gifts, grants, and appropriations of money, equipment, supplies, materials, and services from the federal government, the State or any of its departments or agencies, a county or municipality, or from any institution, person, firm, or corporation. The Commission may authorize a fee payable by counties engaged in electronic recording to fund its expenses. Any fee shall be proportional based on county population or number of documents recorded annually. On approval by a county recorder of the form and amount, a county board may authorize payment of any fee out of the special fund it has created to fund document storage and electronic retrieval, as authorized in Section 3-5018 of the Counties Code. Any funds received by the Office of the Secretary of State for the Commission shall be used entirely for expenses approved by and for the use of the Commission.

(g) The Secretary of State shall provide administrative support to the Commission, including the preparation of the agenda and minutes for Commission meetings,

distribution of notices and proposed rules to commissioners, payment of bills and reimbursement for expenses of commissioners.

(h) Standards and rules adopted by the Commission shall be delivered to the Secretary of State. Within 60 days, the Secretary shall either promulgate by rule the standards adopted, amended, or repealed or return them to the Commission, with findings, for changes. The Commission may override the Secretary by a three-fifths vote, in which case the Secretary shall publish the Commission's standards.

(Source: P.A. 95-472, eff. 8-27-07.)

**765 ILCS 33/6.** (Blank).

(Source: P.A. 95-472, eff. 8-27-07.)

**765 ILCS 33/7. Relation to Electronic Signatures in Global and National Commerce Act.** This Act modifies, limits, and supersedes the federal Electronic Signatures in Global and National Commerce Act (15 U.S.C. Section 7001, et seq.) but does not modify, limit, or supersede Section 101(c) of that Act (15 U.S.C. Section 7001(c)) or authorize electronic delivery of any of the notices described in Section 103(b) of that Act (15 U.S.C. Section 7003(b)).

(Source: P.A. 95-472, eff. 8-27-07.)

**765 ILCS 33/99. Effective date.** This Act takes effect upon becoming law.

(Source: P.A. 95-472, eff. 8-27-07.)

## **ILLINOIS ADMINISTRATIVE CODE**

### **TITLE 14: COMMERCE**

#### **SUBTITLE A: REGULATION OF BUSINESS**

#### **CHAPTER I: SECRETARY OF STATE**

#### **PART 100: ILLINOIS ELECTRONIC COMMERCE SECURITY ACT**

##### **Section 100.10 Scope and Definitions**

a) The purpose of this Part is to provide maximum flexibility to the implementation of digital signature technology under the Illinois Electronic Commerce Security Act [5 ILCS 175].

b) For the purposes of this Part, and unless the context expressly indicates otherwise, definitions are as follows:

“Act” means the Illinois Electronic Commerce Security Act [5 ILCS 175].

“Applicant” means the person, organization or entity seeking certification by the Secretary as a certification authority in the State of Illinois.

“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:

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

contains a public key that corresponds to a private key under the control of the

subscriber;

specifies its operational period; and  
is digitally signed by the certification authority issuing it.

“Certification authority” or “CA” means a person or entity who authorizes and causes the issuance of a certificate.

“Certification practice statement” or “CPS” 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.

“Certificate policy” or “CP” is a statement published by a certification authority that specifies the policies of the certification authority.

“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.

“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:

one key (the private key) can encrypt a message that only the other key (the public key) can decrypt; and

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, so 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.

“Secretary” means the Secretary of State of Illinois.

“Security procedure” means 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.

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 that 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:

- can be shown to be reasonably resistant to penetration, compromise, and misuse;
- provide a reasonable level of reliability and correct operation;
- are reasonably suited to performing their intended functions or serving their intended purposes;
- comply with applicable agreements between the parties, if any; and

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 100.20 Certification of a Qualified Security Procedure for Electronic Records and Signature**

a) In order to obtain the Secretary’s certification of a qualified security procedure, an applicant must file an application form, designated by the Secretary, at the following location:

Certification Authority Application Section  
Room 461  
Howlett Building  
Springfield, Illinois 62756

b) The applicant must document security procedures, policies and practices that delineate full and complete identification of security procedures. The documentation shall be submitted for review, in the form of a Certification Practice Statement (CPS) and Certificate Policy (CP), to the Secretary’s Electronic Signature Steering Committee.

c) Applicants certified by the Secretary shall:

- 1) have adopted secure policies and procedures as designated by a recognized industry organization;
- 2) meet the criteria for acceptance of electronic signatures and records and the criteria for recognition of qualified security procedures as delineated in Sections 100.30 and 100.40 of this Part;
- 3) maintain an office in this State or maintain a registered agent for service of process in this State;
- 4) submit a suitable guaranty described in Section 100.50 of this Part;
- 5) submit an annual audit that complies with Section 100.60 of this Part;
- 6) pay an annual application fee of \$2,000. The fee shall be paid by certified check upon the annual submittal of the application and be made payable to the Illinois Secretary of State. Such fee shall not be applicable to agencies of State government applying for the Secretary’s certification pursuant to this Part; and
- 7) maintain records in accordance with Section 100.100 of this Part.

### **Section 100.30 Criteria for Acceptance of Electronic Signatures**

A qualified security procedure is a security procedure for identifying a person that is 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 and that cannot be readily duplicated or compromised;

d) is created and is linked to the electronic record to which it relates in a manner that, if the record or the signature is intentionally or unintentionally changed after signing, the electronic signature is invalidated; and

e) complies with this Part.

#### **Section 100.40 Recognition of Qualified Security Procedures**

a) The security structure of technology known as Public Key Cryptography is certified by a CA as a qualified security procedure for use by public and private entities in Illinois, provided that the digital signature is created consistent with this Section. Cryptography is a commercially reasonable standard and procedure for use by public and private industries in Illinois, provided that the digital signature is created consistent with this Section.

b) The Illinois Electronic Commerce Security Act requires that a digital signature be unique to the signer within the context in which it is used. A public key-based digital signature may be considered unique to the signer using it if:

1) the digital signature is created using an asymmetric algorithm;

2) the private key used to create the signature on the document is known only to the signer;

3) the digital signature can be verified by reference to the public key listed in a CA certificate;

4) the digital signature is created during the operational period of a valid CA certificate;

5) it is computationally infeasible to derive the private key from knowledge of the public key; and

6) the digital signature is created within the scope of any other restrictions specified or incorporated by reference in the CA certificate.

c) The Act requires that a digital signature can be used to objectively identify the person signing the electronic record. A public-key based digital signature is capable of objectively identifying the person signing the electronic record if:

1) the acceptor of the digitally signed document can verify the document was digitally signed by using the signer's public key and message digest function to decrypt the message; and

2) the issuing certification authority, through a process defined in the CP or CPS, authenticates the subscriber and the subscriber's public key and identifies the forms of identification required of the signer prior to issuing the CA certificate.

d) The Act requires that the digital signature be reliably created by an identified person and cannot be readily duplicated or compromised. The signer and all other persons that rightfully have access to signature devices assume a duty to exercise reasonable care to retain control and maintain 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.

e) The Act requires that the digital signature be created, and be linked to the electronic record to which it relates, in a manner that, if the record or the signature is intentionally or unintentionally changed after signing, the electronic signature is invalidated.

#### **Section 100.50 Suitable Guaranty**

In order to receive the Secretary's certification of a qualified security procedure, an

applicant is required to:

- a) Provide suitable guaranty in the form of a surety bond executed by an insurer lawfully operating in this State or an irrevocable letter of credit issued by a financial institution lawfully operating in this State in the amount of \$100,000.
- b) The form of the suitable guaranty or letter of credit must:
  - 1) identify the insurer;
  - 2) identify the applicant;
  - 3) be made payable to the Secretary for the purpose of persons holding qualified rights of payment against the applicant named as principal of the bond or customer of the letter of credit;
  - 4) state that the bond or letter of credit is issued under the Act; and
  - 5) specify a term of effectiveness of at least five years.

### **Section 100.60 Audit Requirements**

a) Upon application for the Secretary's certification of a qualified security procedure, the applicant shall submit annually to the Secretary an independent third party audit with an unqualified opinion. If the applying certification authority has been in operation for one year or less, the applicant shall submit an American Institute of Certified Public Accountants Statement of Standards (S.A.S. 70) Type One Audit. If the applying certification authority has been in operation for longer than one year, the applicant shall submit a Type Two Audit. (The American Institute of Certified Public Accountants Statement of Standards (S.A.S. 70) (December 15, 1999; no subsequent dates or editions) is hereby incorporated and is available from the Institute at 1211 Avenue of the Americans, New York NY 10036.)

b) The auditor shall be a certified public accountant licensed in the State of Illinois, and shall have a current and valid certificate as either a certified information systems auditor by the Information Systems Audit and Control Foundation or as a certified information systems security professional by the International Information Systems Security Certification Consortium.

c) The auditors shall attest that they have demonstrated significant experience in the application of public key cryptographic technologies and computer security.

d) The audit shall include the auditor's opinion or attestation that the applicant has implemented and designed CA certification practices and policies to achieve the requirements of the applicant authority's policy and stated control objectives. The audit shall also establish that the applicant authority has the use of a trustworthy system.

### **Section 100.70 Certification Authorities**

Certification authorities shall:

- a) inform each subscriber of its agreement to be bound by the CPS and CP before obtaining a CA certificate;
- b) provide each subscriber with a copy of the CPS and CP, or the Universal Resource Locator where the CPS and CP can be obtained;
- c) include warranty disclaimers, liability limitations and indemnification provisions in their CPS or CP;
- d) inform each subscriber as to changes made to the CPS or CP on a timely basis;
- e) inform each subscriber as to its responsibility to maintain the confidentiality of its private key; and

d) inform each subscriber as to the applicant's responsibility to maintain a private key and utilize a trustworthy system.

#### **Section 100.80 Decertification of Certification Authorities**

a) The Secretary may decertify a security procedure employed by a certification authority, in accordance with 5 ILCS 175/10-135d, for failure to comply with any requirement of this Part, for failure to remain qualified for the Secretary's certification, for failure to revoke a CA certificate pursuant to 5 ILCS 175/15-320, or for failure to comply with a lawful order of the Secretary.

b) Certification authorities in the State of Illinois shall notify the Secretary in writing, within 10 days, if the certification authority has had its accreditation, licensing, Secretary's certification or approval revoked, lapsed or terminated by any other means by another state or authority.

c) The Secretary may order the summary suspension of the Secretary's certification of a certification authority following an appropriate investigation or review.

d) Any applicant or certification authority adversely affected by a decision of the Secretary of State pursuant to this Part may seek administrative review of that decision pursuant to the administrative hearings procedure set forth at 92 Ill. Adm. Code 1001.10-1001.130.

#### **Section 100.90 Performance of Services**

The certification authority is solely responsible for all duties and responsibilities of contracted services and functions.

#### **Section 100.100 Records Retention**

State records shall be retained in accordance with Section 5-13 of the Act and the State Records Act [5 ILCS 160], when applicable.

#### **Section 100.110 Provisions for Promoting Uniformity**

a) The Secretary, the Department of Central Management Services or designated State agencies may act as a certification authority under the Act.

b) The Secretary, the Department of Central Management Services or designated State agencies may contract with an outside vendor to acquire the certification authority services required by this Part.

c) The Secretary's Electronic Signature Steering Committee, after review, may recognize proposed technologies as a qualified security procedure for the purpose of the Secretary's certification.

#### **Section 100.120 Foreign and Other Jurisdictional Certificates**

a) The Secretary of State may recognize foreign certification authorities, provided that the foreign certification authority:

1) is certified:

A) as a certification authority by the Secretary; or

B) licensed by another state of the United States; or

C) licensed by the federal government or a federal government agency; and

2) the foreign certification authority agrees to be bound to the terms of the Illinois CP

and CPS.

b) A foreign certification authority shall provide to the Secretary a certified copy of a license or certification issued by a government entity. A license or certification recognized under this subsection (b) shall be valid in Illinois only during the time it is valid in the issuing jurisdiction.

c) A foreign certification authority recognized in the State of Illinois shall provide notification, within 10 days, to the Secretary in writing if the certification authority has had its accreditation, licensing, certification or approval revoked, lapsed or terminated by any other means by another state or authority.

d) Certification authorities certified by the Secretary shall not be required to accept certificates issued by international entities.

e) A foreign certification authority doing business in the State of Illinois shall be subject to the laws of Illinois.

D) The certification authority's CPS shall indicate whether the CA accepts foreign certificates.