**Section 100.40 Recognition of Qualified Security Procedures**

a) The security structure of technology known as public key cryptographyis certified by a CA as a qualified security procedure for use by 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 private industries in Illinois, provided that the digital signature is created consistent with this Section.

b) The 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.

(Source: Amended at 31 Ill. Reg. 7284, effective May 7, 2007)