325K.01 DEFINITIONS.

Subdivision 1. **Scope.** Unless the context clearly requires otherwise, the terms used in this chapter have the meanings given them in this section.

Subd. 2. **Accept a certificate.** "Accept a certificate" means either:

(1) to manifest approval of a certificate, while knowing or having notice of its contents; or

(2) to apply to a licensed certification authority for a certificate, without canceling or revoking the application by delivering notice of the cancellation or revocation to the certification authority and obtaining a signed, written receipt from the certification authority, if the certification authority subsequently issues a certificate based on the application.

Subd. 3. **Asymmetric cryptosystem.** "Asymmetric cryptosystem" means an algorithm or series of algorithms that provide a secure key pair.

Subd. 4. **Certificate.** "Certificate" means a computer-based record that:

(1) identifies the certification authority issuing it;

(2) names or identifies its subscriber;

(3) contains the subscriber's public key; and

(4) is digitally signed by the certification authority issuing it.

Subd. 5. **Certification authority.** "Certification authority" means a person who issues a certificate.

Subd. 6. **Certification authority disclosure record.** "Certification authority disclosure record" means an online, publicly accessible electronic record that concerns a licensed certification authority and is kept by the secretary. A certification authority disclosure record has the contents specified by rule by the secretary under section 325K.03.

Subd. 7. **Certification practice statement.** "Certification practice statement" means a declaration of the practices that a certification authority employs in issuing certificates generally, or employed in issuing a material certificate.

Subd. 8. **Certify.** "Certify" means to declare with reference to a certificate, with ample opportunity to reflect, and with a duty to apprise oneself of all material facts.

Subd. 9. **Confirm.** "Confirm" means to ascertain through appropriate inquiry and investigation.

Subd. 10. **Correspond.** "Correspond," with reference to keys, means to belong to the same key pair.

Subd. 11. **Digital signature or digitally signed.** "Digital signature" or "digitally signed" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:

(1) whether the transformation was created using the private key that corresponds to the signer's public key; and

(2) whether the initial message has been altered since the transformation was made.

Subd. 12. **Financial institution.** "Financial institution" means a national or state-chartered commercial bank or trust company, savings bank, savings association, or credit union authorized to do business in the state of Minnesota and the deposits of which are federally insured.

Subd. 13. **Forge a digital signature.** "Forge a digital signature" means either:

(1) to create a digital signature without the authorization of the rightful holder of the private key; or

(2) to create a digital signature verifiable by a certificate listing as subscriber a person who either:

(i) does not exist; or

(ii) does not hold the private key corresponding to the public key listed in the certificate.

Subd. 14. **Hold a private key.** "Hold a private key" means to be authorized to utilize a private key.

Subd. 15. **Incorporate by reference.** "Incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated.

Subd. 16. **Issue a certificate.** "Issue a certificate" means the acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.

Subd. 17. **Key pair.** "Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, keys which have the property that the public key can verify a digital signature that the private key creates.

Subd. 18. **Licensed certification authority.** "Licensed certification authority" means a certification authority to whom a license has been issued by the secretary and whose license is in effect, or a certification authority who operates under a license issued by a governmental entity which has been certified pursuant to section 325K.05, subdivision 5.

Subd. 19. **Message.** "Message" means a digital representation of information.

Subd. 20. **Notify.** "Notify" means to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person.

Subd. 21. **Operative personnel.** "Operative personnel" means one or more natural persons acting as a certification authority or its agent, or in the employment of, or under contract with, a certification authority, and who have duties directly involving the issuance of certificates, creation of private keys, or administration of a certification authority's computing facilities.

Subd. 22. **Person.** "Person" means a human being or an organization capable of signing a document, either legally or as a matter of fact.

Subd. 23. **Private key.** "Private key" means the key of a key pair used to create a digital signature.

Subd. 24. **Public key.** "Public key" means the key of a key pair used to verify a digital signature.

Subd. 25. **Publish.** "Publish" means to record or file in a repository.

Subd. 26. **Qualified right to payment.** "Qualified right to payment" means an award of damages against a licensed certification authority by a court having jurisdiction over the certification authority in a civil action for violation of this chapter.

Subd. 27. **Recipient.** "Recipient" means a person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on it.

Subd. 28. **Recognized repository.** "Recognized repository" means a repository recognized by the secretary under section 325K.25.

Subd. 29. **Recommended reliance limit.** "Recommended reliance limit" means the monetary amount recommended for reliance on a certificate under section 325K.17.

Subd. 30. **Repository.** "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.

Subd. 31. **Revoke a certificate.** "Revoke a certificate" means to make a certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible.

Subd. 32. **Rightfully hold a private key.** "Rightfully hold a private key" means the authority to utilize a private key:

(1) that the holder or the holder's agents have not disclosed to a person in violation of section 325K.13, subdivision 1; and

(2) that the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

Subd. 33. **Secretary.** "Secretary" means the Minnesota secretary of state.

Subd. 34. **Subscriber.** "Subscriber" means a person who:

(1) is the subject listed in a certificate;

(2) accepts the certificate; and

(3) holds a private key that corresponds to a public key listed in that certificate.

Subd. 35. **Suitable guaranty.** (a) "Suitable guaranty" means:

(1) a surety bond or an irrevocable letter of credit issued for the benefit of persons holding qualified rights of payment against the licensed certification authority named as the principal of the bond or the customer of the letter of credit; or

(2) a policy of insurance that provides that claims may be made and resolved without obtaining a qualified right to payment.

(b) The suitable guaranty must:

(1) be in an amount specified by rule by the secretary under section 325K.03;

(2) state that it is issued under this chapter;

(3) specify a term of effectiveness of at least five years; and

(4) be in a form the content of which is described in rule by the secretary.

If the suitable guaranty is a surety bond, it must be issued by a surety authorized by the commissioner of commerce to do business in this state. If the suitable guaranty is an irrevocable letter of credit, it must be issued by a financial institution authorized to do business in this state. If the suitable guaranty is a policy of

insurance, it must be issued by an insurance company authorized by the commissioner of commerce to do business in this state.

Once a qualified right to payment or claim has been satisfied from the suitable guaranty, the licensed certification authority must provide evidence to the secretary that the amount required by rule is again available.

Subd. 35a. **Summary suspension.** "Summary suspension" means a temporary rescission of a certification authority's license by order of the secretary. The secretary may order the summary suspension of a license before holding a hearing. The summary suspension is effective for up to five business days. If an action for suspension or revocation is instituted within five business days, the summary suspension is extended until the action for suspension or revocation is ultimately determined.

Subd. 36. **Suspend a certificate.** "Suspend a certificate" means to make a certificate ineffective temporarily for a specified time forward.

Subd. 37. **Time stamp.** "Time stamp" means either:

(1) to append or attach to a message, digital signature, or certificate a digitally signed notation indicating at least the date, time, and identity of the person appending or attaching the notation; or

(2) the notation thus appended or attached.

Subd. 38. **Transactional certificate.** "Transactional certificate" means a valid certificate incorporating by reference one or more of the digital signatures.

Subd. 39. **Trustworthy system.** "Trustworthy system" means computer hardware and software that:

(1) are reasonably secure from intrusion and misuse;

(2) provide a reasonable level of availability, reliability, and correct operation; and

(3) are reasonably suited to performing their intended functions.

Subd. 40. **Valid certificate.** "Valid certificate" means a certificate that:

(1) a licensed certification authority has issued;

(2) the subscriber listed in it has accepted;

(3) has not been revoked or suspended; and

(4) has not expired.

However, a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.

Subd. 41. **Verify a digital signature.** "Verify a digital signature" means, in relation to a given digital signature, message, and public key, to determine accurately that:

(1) the digital signature was created by the private key corresponding to the public key; and

(2) the message has not been altered since its digital signature was created.

History: *1997 c 178 s 2; 1998 c 321 s 1-8*