UTAH DIGITAL SIGNATURE ACT (SELECTED SECTIONS)

§46-3-101Title.

This chapter is known as the "Utah Digital Signature Act."

4§6-3-102 Purposes and construction.

This chapter shall be construed consistent with what is commercially reasonable under the circumstances and to effectuate the following purposes:

(1) to facilitate commerce by means of reliable electronic messages;

(2) to minimize the incidence of forged digital signatures and fraud in electronic commerce;

(3) to implement legally the general import of relevant standards, such as X.509 of the International Telecommunication Union (formerly International Telegraph and Telephone Consultative Committee or CCITT); and

(4) to establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.

§46-3-103. Definitions.

For purposes of this chapter, and unless the context expressly indicates otherwise:

(1) "Accept a certificate" means:

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

(b) to apply to a licensed certification authority for a certificate, without canceling or revoking the application, if the certification authority subsequently issues a certificate based on the application.

(2) "Asymmetric cryptosystem" means an algorithm or series of algorithms which provide a secure key pair.

(3) "Certificate" means a computer_based record which:

(a) identifies the certification authority issuing it;

(b) names or identifies its subscriber;

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

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

(4) "Certification authority" means a person who issues a certificate.

(5) "Certification authority disclosure record" means an on_line, publicly accessible record which concerns a licensed certification authority and is kept by the division. A certification authority disclosure record has the contents specified by rule of the division pursuant to Section 46-3-104.

(6) "Certification practice statement" means a declaration of the practices which a certification authority employs in issuing certificates generally, or employs in issuing a material certificate.

(7) "Certify" means the declaration of material facts by the certification authority regarding a certificate.

(8) "Confirm" means to ascertain through appropriate inquiry and investigation.

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

(10) "Digital signature" 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 whether:

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

(b) the message has been altered since the transformation was made.

(11) "Division" means the Division of Corporations and Commercial Code within the Utah Department of Commerce.

(12) "Forge a digital signature" means either:

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

(b) 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.

(13) "Hold a private key" means to be able to utilize a private key.

(14) "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.

(15) "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.

(16) "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.

(17) "Licensed certification authority" means a certification authority to whom a license has been issued by the division and whose license is in effect.

(18) "Message" means a digital representation of information.

(19) "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.

(20) "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:

(a) managerial or policy_making responsibilities for the certification authority; or

(b) duties directly involving the issuance of certificates, creation of private keys, or administration of a certification authority's computing facilities.

(21) "Person" means a human being or any organization capable of signing a document, either legally or as a matter of fact.

(22) "Private key" means the key of a key pair used to create a digital signature.

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

(24) "Publish" means to record or file in a repository.

(25) "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.

(26) "Recipient" means a person who receives or has a digital signature and is in a position to rely on it.

(27) "Recognized repository" means a repository recognized by the division pursuant to Section 46-3-501.

(28) "Recommended reliance limit" means the limitation on the monetary amount recommended for reliance on a certificate pursuant to Subsection 46-3-309(1).

(29) "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.

(30) "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.

(31) "Rightfully hold a private key" means to be able to utilize a private key:

(a) which the holder or the holder's agents have not disclosed to any person in violation of Subsection 46-3-305(1); and

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

(32) "Signer" means a person who creates a digital signature for a message.

(33) "Subscriber" means a person who:

(a) is the subject listed in a certificate;

(b) accepts the certificate; and

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

(34)(a) "Suitable guaranty" means either a surety bond executed by a surety authorized by the Utah Insurance Department to do business in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state by the Utah Department of Financial Institutions, which, in either event, satisfies all of the following requirements, that it:

(i) is issued payable to the division for the benefit of persons holding qualified rights of payment against the licensed certification authority named as the principal of the bond or customer of the letter of credit;

(ii) is in an amount specified by rule of the division pursuant to Section 46-3-104;

(iii) states that it is issued for filing pursuant to this chapter;

(iv) specifies a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority; and

(v) is in a form prescribed by rule of the division.

(b) A suitable guaranty may also provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty.

(c) A financial institution acting as a certification authority may satisfy the requirements of this subsection from its assets or capital, to the extent of its lending limit as provided in Title 7, Financial Institutions Act.

(35) "Suspend a certificate" means to make a certificate ineffective temporarily from a specified time forward.

(36) "Time-stamp" means either:

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

(b) the notation thus appended or attached.

(37) "Transactional certificate" means a valid certificate incorporating by reference one or more digital signatures.

(38) "Trustworthy system" means computer hardware and software which:

(a) are reasonably secure from intrusion and misuse;

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

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

(39)(a) "Valid certificate" means a certificate which:

(i) a licensed certification authority has issued;

(ii) the subscriber listed in it has accepted;

(iii) has not been revoked or suspended; and

(iv) has not expired.

(b) A transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.

(40) "Verify a digital signature" means, in relation to a given digital signature, message, and public key, to determine accurately that:

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

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

§ 46-3-201. Licensure and qualifications of certification authorities.

(1) To obtain or retain a license a certification authority shall:

(a) be the subscriber of a certificate published in a recognized repository;

(b) employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception;

(c) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;

(d) file with the division a suitable guaranty, unless the certification authority is the governor, a department or division of state government, the attorney general, state auditor, state treasurer, the judicial council, a city, a county, or the Legislature or its staff offices provided that:

(i) each of the above_named governmental entities may act through designated officials authorized by ordinance, rule, or statute to perform certification authority functions; and

(ii) one of the above_named governmental entities is the subscriber of all certificates issued by the certification authority;

(e) have the right to use a trustworthy system, including a secure means for controlling usage of its private key;

(f) present proof to the division of having working capital reasonably sufficient, according to rules of the division, to enable the applicant to conduct business as a certification authority;

(g) maintain an office in Utah or have established a registered agent for service of process in Utah; and

(h) comply with all other licensing requirements established by division rule.

(2) The division shall issue a license to a certification authority which:

(a) is qualified under Subsection (1);

(b) applies in writing to the division for a license; and

(c) pays the required filing fee.

(3)(a) The division may classify and issue licenses according to specified limitations, such as a maximum number of outstanding certificates, cumulative maximum of recommended reliance limits in certificates issued by the certification authority, or issuance only within a single firm or organization.

(b) A certification authority acts as an unlicensed certification authority when issuing a certificate exceeding the limits of the license.

(4)(a) The division may revoke or suspend a certification authority's license for failure to comply with this chapter, or for failure to remain qualified pursuant to Subsection (1).

(b) The division's actions under this subsection are subject to the procedures for adjudicative proceedings in Title 63, Chapter 46b, Administrative Procedures Act.

(5) The division may recognize by rule the licensing or authorization of certification authorities by other governmental entities, provided that those licensing or authorization requirements are substantially similar to those of this state. If licensing by another governmental entity is so recognized:

(a) Part 4 of this chapter, which relates to presumptions and legal effects, applies to certificates issued by the certification authorities licensed or authorized by that governmental entity in the same manner as it applies to licensed certification authorities of this state; and

(b) the liability limits of Section 46_3_309 apply to the certification authorities licensed or authorized by that governmental entity in the same manner as they apply to licensed certification authorities of this state.

(6) Unless the parties provide otherwise by contract between themselves, the licensing requirements in this section do not affect the effectiveness, enforceability, or validity of any digital signature except that Part 4 of this chapter does not apply to a digital signature which cannot be verified by a certificate issued by a licensed certification authority. Further, the liability limits of Section 46_3_309 do not apply to unlicensed certification authorities.

§ 46-3-202. Performance audits and investigations.

(1) A certified public accountant having expertise in computer security, or an accredited computer security professional, shall audit the operations of each licensed certification authority at least once each year to evaluate compliance with this chapter. The division may specify qualifications for auditors in greater detail by rule.

***

§ 46-3-203. Enforcement of requirements for licensed certificate authorities.

(1) The division may investigate the activities of a licensed certification authority material to its compliance with this chapter and issue orders to a certification authority to further its investigation and insure compliance with this chapter.

***

§ 46-3-204. Dangerous activities by any certification authority prohibited.

(1) A certification authority, whether licensed or not, may not conduct its business in a manner that creates an unreasonable risk of loss to subscribers of the certification authority, to persons relying on certificates issued by the certification authority, or to a repository.

***

§ 46-3-301. General requirements for certification authorities.

(1) A licensed certification authority or subscriber shall use only a trustworthy system:

(a) to issue, suspend, or revoke a certificate;

(b) to publish or give notice of the issuance, suspension, or revocation of a certificate; and

(c) to create a private key.

(2) A licensed certification authority shall disclose any material certification practice statement, and any fact material to either the reliability of a certificate which it has issued or its ability to perform its services. A certification authority may require a signed, written, and reasonably specific inquiry from an identified person, and payment of reasonable compensation, as conditions precedent to effecting a disclosure required in this subsection.

§ 46-3-302. Issuance of a certificate.

(1) A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(a) the certification authority has received a request for issuance signed by the prospective subscriber; and

(b) the certification authority has confirmed that:

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate after due diligence;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(c) The requirements of this subsection may not be waived or disclaimed by the licensed certification authority or the subscriber.

(2)(a) If the subscriber accepts the issued certificate, the certification authority shall publish a signed copy of the certificate in a recognized repository agreed upon by the certification authority and the subscriber named in the certificate, unless the contract between the certification authority and the subscriber provides otherwise.

(b) If the subscriber does not accept the certificate, a licensed certification authority shall not publish the certificate or shall cancel its publication if the certificate has already been published.

(3) Nothing in this section precludes a licensed certification authority from conforming to standards, certification practice statements, security plans, or contractual requirements more rigorous than, but consistent with, this chapter.

(4)(a) A licensed certification authority which has issued a certificate:

(i) shall revoke a certificate immediately upon confirming that it was not issued as required by this section; or

(ii) may suspend, for a reasonable period of time not to exceed 48 hours, a certificate which it has issued in order to conduct an investigation to confirm grounds for revocation under Subsection (i).

(b) The certification authority shall give notice of the revocation or suspension to the subscriber as soon as practicable.

(5)(a) The division may order the licensed certification authority to suspend or revoke a certificate which the certification authority issued if, after giving the certification authority and subscriber any required notice and opportunity for a hearing in accordance with Title 63, Chapter 46b, Administrative Procedures Act, the division determines that:

(i) the certificate was issued without substantial compliance with this section; and

(ii) the noncompliance poses a significant risk to persons reasonably relying on the certificate.

(b) The division may suspend a certificate for a reasonable period of time not to exceed 48 hours upon determining that an emergency requires an immediate remedy and in accordance with Title 63, Chapter 46b, Administrative Procedures Act.

§ 46-3-303. Warranties and obligations of certification authority upon issuance of a certificate.

(1)(a) By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:

(i) the certificate contains no information known to the certification authority to be false;

(ii) the certificate satisfies all material requirements of this chapter; and

(iii) the certification authority has not exceeded any limits of its license in issuing the certificate.

(b) The certification authority may not disclaim or limit the warranties of this subsection.

(2) Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, shall:

(a) act promptly to suspend or revoke a certificate in accordance with Sections 46-3-306 and 46-3-307; and

(b) notify the subscriber within a reasonable time of any facts known to the certification authority which significantly affect the validity or reliability of the certificate once it is issued.

(3) By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate that:

(a) the information in the certificate and listed as confirmed by the certification authority is accurate;

(b) all foreseeable information material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(c) the subscriber has accepted the certificate; and

(d) the licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate

(4) By publishing a certificate, a licensed certification authority certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

§ 46-3-304. Representations and duties upon acceptance of a certificate.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that:

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) all representations made by the subscriber to the certification authority and material to information listed in the certificate are true;

(c) all material representations made by the subscriber to a certification authority or made in the certificate and not confirmed by the certification authority in issuing the certificate are true.

(2) An agent, requesting on behalf of a principal that a certificate be issued naming the principal as subscriber, certifies that the agent:

(a) holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and

(b) has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, that adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

(3) A person may not disclaim or contractually limit the application of this section, nor obtain indemnity for its effects, if the disclaimer, limitation, or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

(4)(a) By accepting a certificate, a subscriber undertakes to indemnify the issuing certification authority for any loss or damage caused by issuance or publication of a certificate in reliance on a false and material representation of fact by the subscriber, or the failure by the subscriber to disclose a material fact if the representation or failure to disclose was made either with intent to deceive the certification authority or a person relying on the certificate or was made with negligence.

(b) If the certification authority issued the certificate at the request of an agent of the subscriber, the agent personally undertakes to indemnify the certification authority pursuant to Subsection (a) as if the agent was an accepting subscriber in his own right. The indemnity provided in Subsection (a) may not be disclaimed or contractually limited in scope, however, a contract may provide consistent, additional terms regarding the indemnification.

(5) In obtaining information of the subscriber material to issuance of a certificate, the certification authority may require the subscriber to certify the accuracy of relevant information under oath or affirmation of truthfulness and under penalty of criminal prohibitions against false, sworn statements.

§ 46-3-305. Control of the private key.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature.

(2) A private key is the personal property of the subscriber who rightfully holds it.

(3) If a certification authority holds the private key corresponding to a public key listed in a certificate which it has issued, the certification authority holds the private key as a fiduciary of the subscriber named in the certificate, and may use that private key only with the subscriber's prior, written approval, unless the subscriber expressly grants the private key to the certification authority and expressly permits the certification authority to hold the private key according to other terms.

§ 46-3-306. Suspension of a certificate -- Criminal penalty.

(1)(a) Unless the certification authority and the subscriber agree otherwise, the licensed certification authority which issued a certificate which is not a transactional certificate shall suspend the certificate for a period not exceeding 48 hours:

(i) upon request by a person identifying himself as the subscriber named in the certificate, or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, business associate, employee, or member of the immediate family of the subscriber; or

(ii) by order of the division pursuant to Subsection 46-3-302(5).

(b) The certification authority need not confirm the identity or agency of the person requesting suspension under Subsection (1)(a)(i).

****

§ 46-3-307. Revocation of a certificate.

(1) A licensed certification authority shall revoke a certificate which it issued, but which is not a transactional certificate, after:

(a) receiving a request for revocation by the subscriber named in the certificate; and

(b) confirming that the person requesting revocation is that subscriber, or is an agent of that subscriber with authority to request the revocation.

(2) A licensed certification authority shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the suspension.

(3) A licensed certification authority shall revoke a certificate which it issued:

(a) upon receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead; or

(b) upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

(4) A licensed certification authority may revoke one or more certificates which it issued if the certificates are or become unreliable, regardless of whether the subscriber consents to the revocation.

(5) Immediately upon revocation of a certificate by a licensed certification authority, the licensed certification authority shall publish signed notice of the revocation in any repository specified in the certificate for publication of notice of revocation. If any repository specified in the certificate no longer exists or refuses to accept publication, or is no longer recognized pursuant to Section 46-3-501, the licensed certification authority shall publish the notice in any recognized repository.

(6) A subscriber ceases to certify the information, as provided in Section 46-3-304, and has no further duty to keep the private key secure, as required by Section 46-3-305, in relation to a certificate whose revocation the subscriber has requested, beginning with the earlier of either:

(a) when notice of the revocation is published as required in Subsection (5); or

(b) two business days after the subscriber requests revocation in writing, supplies to the issuing certification authority information reasonably sufficient to confirm the request, and pays any contractually required fee.

(7) Upon notification as required by Subsection (5), a licensed certification authority is discharged of its warranties based on issuance of the revoked certificate and ceases to certify the information, as provided in Section 46-3-303, in relation to the revoked certificate.

§ 46-3-308. Expiration of a certificate.

A certificate shall indicate the date on which it expires. When a certificate expires, the subscriber and certification authority cease to certify the information in the certificate as provided in this chapter and the certification authority is discharged of its duties based on issuance of that certificate.

§ 46-3-309. Recommended reliance limits and liability.

(1) By specifying a recommended reliance limit in a certificate, the issuing certification authority and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

(2) Unless a licensed certification authority waives application of this subsection, a licensed certification authority is:

(a) not liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of this chapter;

(b) not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(ii) failure to comply with Section 46-3-302 in issuing the certificate;

(c) liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate, which damages do not include:

(i) punitive or exemplary damages;

(ii) damages for lost profits, savings, or opportunity; or

(iii) damages for pain or suffering.

§ 46-3-401. Satisfaction of signature requirements.

(1) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if:

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer either:

(i) breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(2) Nothing in this chapter precludes any symbol from being valid as a signature under other applicable law, including Uniform Commercial Code, Subsection 70A-1-201(39).

(3) This section does not limit the authority of the State Tax Commission to prescribe the form of tax returns or other documents filed with the State Tax Commission.

§ 46-3-402. Unreliable digital signatures.

Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. If the recipient determines not to rely on a digital signature pursuant to this section, the recipient shall promptly notify the signer of its determination not to rely on the digital signature.

§ 46-3-403. Digitally signed document is written.

(1) A message is as valid, enforceable, and effective as if it had been written on paper, if it:

(a) bears in its entirety a digital signature; and

(b) that digital signature is verified by the public key listed in a certificate which:

(i) was issued by a licensed certification authority; and

(ii) was valid at the time the digital signature was created.

(2) Nothing in this chapter precludes any message, document, or record from being considered written or in writing under other applicable state law.

§ 46-3-404. Digitally signed originals.

A copy of a digitally signed message is as effective, valid, and enforceable as the original of the message, unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, effective, and enforceable message.

§ 46-3-406. Presumptions in adjudicating disputes.

In adjudicating a dispute involving a digital signature, a court of this state shall presume that:

(1) a certificate digitally signed by a licensed certification authority and either published in a recognized repository or made available by the issuing certification authority or by the subscriber listed in the certificate is issued by the certification authority which digitally signed it and is accepted by the subscriber listed in it;

(2) the information listed in a valid certificate, as defined in Section 46-3-103, and confirmed by a licensed certification authority issuing the certificate is accurate;

(3) if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:

(a) that the digital signature is the digital signature of the subscriber listed in that certificate;

(b) that the digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient of that digital signature has no knowledge or notice that the signer:

(i) breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature; and

(4) a digital signature was created before it was time stamped by a disinterested person utilizing a trustworthy system.