Kansas Administrative Regulations

Secretary of State

Article 41.—Kansas Uniform Electronic Transactions Act

7-41-1. Definitions.

(a) "Certificate" means a computer-based record or electronic message that at a minimum meets the following conditions:

(1) Identifies the registered certification authority issuing the certificate;

(2) names or identifies a subscriber;

(3) contains the public key of the subscriber;

(4) identifies the period of time during which the certificate is effective; and

(5) is digitally signed by the registered certification authority.

(b) "Certificate policy" means the policy that identifies the applicability of a certificate to particular communities and classes of applications with common security requirements. This term is also known as "CP."

(c) "Certificate revocation list" means a list maintained by a registered certification authority of the certificates the registered certification authority has issued that are revoked before their stated expiration dates. This term is also known as "CRL."

(d) "Certification practice statement" means a statement published by a registered certification authority that specifies the policies or practices that the registered certification authority employs in issuing, publishing, suspending, revoking, and renewing certificates. This term is also known as "CPS."

(e) "Compliance review" means documentation in the form of an information systems audit report verifying that the applicant or registered certification authority has the use of a trustworthy system as defined in subsection (r).

(f) "Identification and authentication" means the process of ascertaining and confirming through appropriate inquiry and investigation the identity of a certificate applicant in compliance with the requirements for certificate security levels specified in the ITEC certificate policy or the CP. This term is also known as "I and A."

(g) "Information technology executive council" means the Kansas information technology executive council, pursuant to K.S.A. 75-7201 et seq. and amendments thereto, and is also known as "ITEC."

(h) "Information technology executive council policy 9200" means the "certificate policy for the state of Kansas public key infrastructure," version 2, including the appendices, approved by the ITEC, amended on April 24, 2008, and hereby adopted by reference. This document applies to state agencies offering or providing the option of using a digital signature to persons with whom the state agencies do business. This term is also known as "ITEC certificate policy."

(i) "Information technology identity management group" means the group that has been delegated authority by the ITEC and is authorized by the ITEC to make day-to-day administrative and fiscal decisions for the public key infrastructure program. This term is also known as "ITIMG."

(j) "Local registration authority" means a person operating under the ITEC certificate policy that has a relationship of trust with a community of potential subscribers and, for that reason, has a contractual relationship with a registration authority to perform duties including accepting applications and conducting identification and authentication for certificate applicants in accordance with the law, the ITEC certificate policy, and the appended agreements. This term is also known as "LRA."

(k) "Local registration authority's trusted partner" means a person operating under the ITEC certificate policy that has a relationship of trust with an LRA and that executes a trusted partner agreement with an LRA, as contained in the appendices to the ITEC certificate policy, in order to secure LRA services for the community of potential subscribers of the local registration authority's trusted partner. This term is also known as "LRA's trusted partner."

(l) "Private key" means the key in a subscriber's key pair that is kept secret and is used to create digital signatures and to decrypt messages or files that were encrypted with the subscriber's corresponding public key.

(m) "Public key" means the key in a subscriber's key pair that can be used by another person to verify digital signatures created by a subscriber's corresponding private key or to encrypt messages or files that the person sends to the subscriber.

(n) "Public key infrastructure" means the architecture, organization, techniques, practices, policy, and procedures that collectively support the implementation and operation of a certificate-based, public key cryptography system. This term is also known as "PKI."

(o) "Registered certification authority" has the meaning specified in K.S.A. 16-1602, and amendments thereto. This term is also known as "registered CA."

(p) "Registration authority" means a person operating under the ITEC certificate policy who has been authenticated by a registered CA, issued a registration authority certificate by the registered CA, approved by the ITEC to process subscriber applications for certificates and, if required by the ITEC certificate policy, to conduct I and A of certificate applicants in accordance with the law, the ITEC certificate policy, and the appended agreements. This term is also known as "RA."

(q) "Subscriber" means a person operating under the ITEC certificate policy who meets the following criteria:

(1) Is the subject of a certificate;

(2) accepts the certificate from a registered certification authority; and

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

(r) "Trustworthy system" means a secure computer system that materially satisfies the most recent common criteria protection profile for commercial security, known as "CSPP—guidance for COTS security protection profiles," published by the U.S. department of commerce in December 1999 and hereby adopted by reference.

(s) "X.509" means the standard published by the international telecommunication union-T (ITU-T) in March 2000 that establishes a model for certificates. This X.509 standard, including annexes A and B, is hereby adopted by reference.

(Authorized by K.S.A. 16-1605 and 16-1618; implementing K.S.A. 16-1605, 16-1617, and 16-1619; effective July 6, 2001; amended Aug. 19, 2005; amended March 6, 2009.)