

Kansas Information Technology Executive Council (ITEC)
ITEC Policy # 9200 Public Key Infrastructure Certificate Policy

ATTACHMENT A

Certificate Policy

for the
State of Kansas
Public Key Infrastructure

Version 2
Approved April 24, 2008

Table of contents

Introduction

1.1	Overview	4
1.2	Document name and identification	4
1.3	PKI participants.....	5
1.4	Certificate use.....	5

2 PKI participants responsibilities

2.1	CA responsibilities	6
2.2	RA and LRA responsibilities	7
2.3	Relying party responsibilities	8
2.4	Subscriber responsibilities	8
2.5	CA publication and repository responsibilities	9

3 Identification and Authentication (I&A)

3.1	Naming.....	9
3.2	Initial identity validation.....	10
3.3	I&A for renewal or updating.....	12

4 Certificate life cycle operations requirements

4.1	Certificate application	12
4.2	Certificate issuance.....	13
4.3	Certificate acceptance.....	13
4.4	Certificate use	14
4.5	Certificate renewal or update	14
4.6	Processing a request for a new key	14
4.7	Certificate modification	14
4.8	Certificate revocation.....	14
4.9	Certificate status service	16
4.10	End of subscription	16
4.11	Key escrow and recovery	16

5 Facility, management and operation controls

5.1	Physical controls.....	17
5.2	Procedural controls.....	19
5.3	Personnel controls	20
5.4	Audit logging procedures	21
5.5	Records archival.....	24
5.6	Key changeover	25
5.7	Compromise and disaster recovery	25
5.8	CA termination	26

6 Technical security controls

6.1	Key pair generation	26
6.2	CA private key protection.....	28
6.3	Other aspects of key pair management.....	29
6.4	Activation data	29
6.5	Computer security controls	30
6.6	Life cycle technical controls.....	31

6.7	Network security controls.....	31
6.8	Time stamping	31

7 Certificate and CRL profiles

7.1	Certificate profile	31
7.2	CRL profile	32

8 Compliance reviews and other assessments

8.1	Frequency.....	33
8.2	Identity and qualifications of auditor.....	33
8.3	Auditor’s neutrality	33
8.4	Scope of reviews	33
8.5	Actions taken as a result of review	33
8.6	Communication of results.....	33

9 Policy administration

9.1	Fee.....	34
9.2	Privacy and data protection policy	34
9.3	Intellectual property rights.....	34
9.4	Limitation on liability.....	35
9.5	Policy change procedures.....	35
9.6	Publication and notification policies.....	35
9.7	CPS approval procedures	36
9.8	Governing law	36
9.9	Severability	36
9.10	Waivers	36
9.11	Contact details	36

Appendices

10 Definitions

11 Acronyms and abbreviations

12 Agreements

12.1	Agreement between RA and LRA	44
12.2	Agreement between RA and LRA (Trusted partner involved).....	47
12.3	Agreement between LRA and Trusted Partner Subscriber	50
12.4	Individual Subscriber Agreement	53

13 Authentication of Identity For KS PKI Certificate

14 Article: “Authentication Assurance Levels and Risk Assessments”

15 Bibliography

15.1	KS laws on electronic transaction and signatures	62
15.2	Information on KS and federal PKI.....	62
15.3	Fundamental issues related to KS PKI infrastructure and identity management.....	62

1 Introduction

1.1 Overview

- 1.1.1 Policy adoption This certificate policy (CP) is adopted by the information technology executive council (ITEC).
- 1.1.2 Scope This CP governs the issuance and use of certificates for the purposes of authentication, signature and confidentiality among those persons and devices authorized to participate in the public key infrastructure (PKI) described by this CP. Under the Kansas uniform electronic transactions act (KUETA), "person" means an individual, corporation, business trust, estate trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity.
- 1.1.3 OBB infrastructure This policy describes an open-but-bounded (OBB) public key infrastructure. A CP adopted for an OBB PKI reflects the agreements and understandings of the parties using the PKI, *e.g.* the agreements appended to this CP.
- 1.1.4 Primary roles The State of Kansas owns the CP for the PKI described in this policy. Other primary roles authorized by this policy include: certification authority (CA), registration authority (RA), local registration authority (LRA), RA or LRA administrators (RAA or LRAA), subscribers and relying parties.
- 1.1.5 CP This CP applies to CAs who issue certificates for state agencies offering or providing the option of using a digital signature to persons doing business with that state agency. Such CAs must be registered by the secretary of state in accordance with KUETA. (KSA 16-1601 *et seq.*) Subscribers and relying parties within or without the State of Kansas may rely upon certificates issued under this policy and use such certificates for transactions, applications and communications, provided that the laws of the State of Kansas are applied as a matter of law, unless prohibited by federal law.
- 1.1.6 Relationship between the CP and the CPS This CP states what assurance may be placed in a certificate issued by a CA. A CA's certification practice statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates under this CP must have a corresponding CPS.
- 1.1.7 Identity assurance and certificate types This policy provides for four (4) types of certificates. One factor that differentiates each type is the degree of assurance relating to the subscriber's identity that is provided by (1) the procedures used to identify and authenticate (I&A) the subscriber prior to issuance of the certificate and (2) the degree of security a subscriber is required to use to protect his/her private key under this policy. The four certificate types are designated levels one, two, three and four.
- Security and convenience considerations must be balanced in selecting procedures for access to and use of electronic systems, because any increase in security may cause a decrease in convenience. The degrees of assurance provided by the four types of certificates permit subscribers and relying parties to select the preferred balance between security and convenience for their intended uses. The certificate type to be used for any given application, transaction or communication must be determined by the parties using or engaging in that application, transaction or communication.

- 1.2 Document name and identification Reserved.

1.3. PKI participants

1.3.1 PKI authorities

1.3.1.1 State of Kansas The State of Kansas enacted the KUETA and owns this policy.

1.3.1.2 ITEC As set forth in KSA 75-7201 *et seq.* the information technology executive council (ITEC) is comprised of seventeen members from both state and local government and the private sector. Private sector membership is by gubernatorial appointment. The secretary of administration in the executive branch chairs ITEC. ITEC is charged with:

- IT policies, procedures and data management standards for the enterprise;
- project management methodologies and project manager certification;
- enterprise information technology architecture; and
- strategic information technology management plans for state agencies.

As a result, the ITEC adopts, approves and administers this CP for the State of Kansas.

1.3.1.3 ITIMG The information technology identity management group (ITIMG) has delegated authority from the ITEC and is authorized by the ITEC to make day-to-day administrative and fiscal decisions for the PKI program. Upon recommendation of the secretary of state, the ITEC appoints members from various state agencies to serve on the group. The secretary of state is the chair of the ITIMG.

1.3.2 CA Equipped with operating personnel and a collection of hardware and software, a CA is a provider who has a contract with the State of Kansas or with a governmental agency to create, sign and issue public key certificates to subscribers. A CA is a legal entity independent of its subscribers and relying parties.

1.3.3 RAs or LRAs RAs (or LRAs who have executed an agreement with an RA to perform such functions on its behalf) collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. They are responsible for:

- control over the registration process; and
- the I&A process.

1.3.4 RAA or LRAA An RAA or LRAA is a person who satisfies all the trustworthiness requirements for an RA or LRA and who may be authorized to represent the RA or LRA in the issuance and revocation of certificates for subscribers.

1.3.5 Subscribers A subscriber is the person whose name appears as the subject in a certificate and uses the certificate and corresponding keys in accordance with this policy.

1.3.6 Relying parties A relying party is any person who relies upon a certificate issued under the terms of this policy. A relying party decides whether it will rely upon a certificate and, if so, to what financial or liability limits it will rely upon the certificate.

1.4 Certificate use

1.4.1 Appropriate certificate uses, evaluation of risk The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Before selecting the level of certificate to be used, an entity must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk it is willing to accept based on the sensitivity or significance of the information. This evaluation, or risk assessment, is conducted by each entity for each application and is not controlled by this CP. (See appendix 14.)

1.4.2 Prohibited certificate uses If certificates that reference this policy are proposed to be used by any entity having jurisdiction over an application requiring fail safe performance (such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or material environmental damage), the entity having jurisdiction over such

application and who proposes such use first must obtain written approval for use of the certificates from the ITEC.

- 1.4.3 Cross-certification The ITIMG may approve the issuance of a cross-certificate between CAs. Any such cross-certification only may occur after approval by the ITIMG and notice to the secretary of state and all RAs.

2 PKI participant responsibilities

- 2.1 CA responsibilities** A CA is responsible for the issuing and managing of certificates including:
- the certificate manufacturing process;
 - administration of the repository;
 - publication of certificates;
 - revocation of certificates;
 - generation and destruction of CA signing keys; and
 - ensuring that all aspects of the CA services, operation and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations and warranties of this CP.
- 2.1.1 Notification of certificate issuance and revocation A CA must make certificate revocation lists (CRLs) available to subscribers and relying parties in accordance with section 4.9. A CA must notify an RA or, when appropriate, a subscriber when a certificate bearing the subscriber's distinguished name (DN) is issued or revoked.
- 2.1.2 Accuracy of representations By issuing a certificate that references this policy, a CA certifies and warrants to the subscriber and to all parties who reasonably rely on the information contained in the certificate during its operational period and in accordance with this policy that:
- the CA has issued and will manage the certificate in accordance with this policy;
 - the CA has complied with the requirements of this policy and any applicable CPS when authenticating the subscriber and issuing the certificate;
 - there are no misrepresentations of fact in the certificate reasonably known to the CA, and the CA has taken reasonable steps to verify any additional information in the certificate;
 - information provided to the CA by the RA and/or subscriber in the certificate application for inclusion in the certificate has been transcribed accurately to the certificate; and
 - the certificate meets all material requirements of this policy and the CA's CPS.
- 2.1.3 Time between certificate request and issuance After completion of I&A, CAs must issue certificates within three (3) business days.
- 2.1.4 Certificate revocation and renewal A CA must ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this policy and will be expressly stated in the subscriber agreement and any other applicable document outlining the terms and conditions of the certificate use. A CA must ensure that key changeover procedures are in accordance with section 5.6. A CA also must ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in section 4.9. The address of the CRL must be defined in the certificate.
- 2.1.5 Protection of CA private keys A CA must ensure that its private keys and activation data are protected in accordance with parts 4 and 6 of this policy.

2.1.6	Restrictions on CA's private key use	A CA must ensure that its CA private signing key is used only to sign certificates and CRLs. A CA may issue certificates to subscribers, CA and RA personnel, devices and applications. A CA must ensure that private keys issued to its personnel, employees, officers, agents and subcontractors to access and operate CA applications are used only for such purposes.
2.1.7	Compliance with the law	Among other responsibilities, a CA must ensure that only it has access to, accepts and uses registration information transmitted as follows: (1) directly to the CA from subscribers or (2) directly from an RA. A CA must ensure that its certification and repository services, issuance and revocation of certificates and issuance of CRLs are in accordance with the law and this policy.
2.1.8	Customer service center	A CA must implement and maintain a customer service center to provide assistance and services to subscribers and relying parties consistent with this CP. The service must include a system for receiving, recording, responding to and reporting problems within its own organization and for reporting such problems to the ITIMG and the secretary of state.
2.1.9	Consequences of breach	Reserved.
2.1.10	Notification of breach	A CA must advise the secretary of state and the ITIMG at the earliest possible time of any breach or suspected breach.
2.1.11	Conflict	Nothing in this policy may be construed to conflict with, alter or eliminate any other obligation, responsibility or liability that may be imposed on any person by virtue of any contract or obligation that is otherwise determined to be controlling by applicable law.
2.1.12	Evidence of financial security	A CA must obtain and maintain a good and sufficient surety bond, certificate of insurance or other evidence of financial security in the amount of \$100,000. Pursuant to Kansas law, if the CA fails to comply with this provision, the CA's registration with the secretary of state may be deemed lapsed.
2.2	RA and LRA responsibilities	An RA and LRA with whom it has executed an agreement for RA services must comply with the law and this CP and the appended agreements when providing registration, authentication and other RA and LRA services, including:
2.2.1	RAA and LRAA	An RA or LRA may designate one or more persons as the RAA or LRAA to conduct registration activities and may authorize these persons to represent the RA or LRA in the issuance and revocation of certificates for subscribers. An RA, LRA, RAA or LRAA must authenticate certificate applicants in accordance with this policy.
2.2.2	Accept certificate applications	An RA or LRA may accept applications for certificates electronically, including by e-mail or web site, if the applicant has been positively identified and if all communication is secured by using a protocol providing encryption for transmitted information as defined by the registered CA's CPS. Applications for certificates also may be delivered to an RA or LRA in person or by first-class U.S. mail.
2.2.3	Ensure identity, documentation	An RA and LRA must ensure that the applicant's identity information is verified in accordance with this policy. Information that is not verified must not be included in certificates. An RA and LRA must ensure that the applicant's identity information and public key are related as specified by this policy and must document the processes to be followed and the information related to the issuance of each certificate. The documentation of certificates with security levels of two, three and four must include the following:

- the name of the person performing the identification;
- documentation that the RA or LRA verified the identity of the subscriber as required by the applicable procedure;
- the date of the verification; and
- if in-person identity verification is conducted, a declaration of identity executed in the presence of the person performing the identity authentication. The declaration must be signed by the certificate applicant, using a handwritten or other legal signature. (See appendix 13.)

2.2.4	Documentation and retention	The documentation related to the issuance of each certificate must be maintained by the RA and LRA throughout the period it remains active and for a period of not fewer than five years from and after it ceases to be active or it expires or terminates.
2.3	Relying party responsibilities	A relying party must decide pursuant to its own policies whether to rely upon a certificate and, if so, to what financial or liability limits it will rely upon the certificate.
2.3.1	Check certificate status	A relying party must check the status of the certificate through OCSP or against the appropriate and current CRL in accordance with the requirements stated in section 4.9. As part of this verification process, the digital signature of the CRL also must be validated.
2.4	Subscriber responsibilities	A certificate subscriber's responsibilities are:
2.4.1	Accurate responses	Upon application for a certificate and in all subsequent communications, a subscriber must provide complete and accurate responses to all appropriate requests for information made by the CA or RA during the applicant registration, certificate application and authentication of identity processes.
2.4.2	Individual subscriber agreement	When a subscriber receives notice of the issuance of a certificate naming the applicant as the subscriber, the subscriber must review the certificate to ensure that all subscriber information included in it is accurate, accept or reject the certificate in accordance with section 4.3 and execute the individual digital certificate subscriber agreement appended to this policy.
2.4.3	Security responsibilities	A subscriber must generate a key pair using a secure system and take appropriate precautions to prevent any compromise, modification, loss, disclosure or unauthorized use of the private key. "Appropriate precautions" and "secure system," for purposes of the different types of certificate provided for in this policy, mean the following:
2.4.3.1	Level one and level two certificates	A subscriber must use reasonable efforts to protect the private key for level one and level two certificates, which may be stored in the browser of any computer at the subscriber's election and risk. A subscriber must use a password or PIN to protect the private key.
2.4.3.2	Level three and level four certificates	A subscriber must use reasonable efforts to protect the private key for level three and level four certificates, which must be stored in a hardware token or software cryptographic module protected by a strong PIN or password.
2.4.4	Authorized key use	A subscriber must use the certificate and the corresponding private key only for purposes authorized by and consistent with the law, this CP and the appended agreements.
2.4.5	Notification upon private key compromise	A subscriber must instruct the CA, RA or LRA to revoke the certificate promptly upon any actual or suspected loss, disclosure or other compromise of the private key, or, in the case of a certificate issued to a subscriber who is affiliated with an entity, when

the subscriber no longer is affiliated with the entity.

- 2.4.6 Consequences of breach A subscriber who is found to have acted in a manner inconsistent with these obligations will have his or her certificate revoked and will forfeit all claims he or she may have against any other party to the PKI in the event of a dispute arising from the failure to fulfill the obligations above.
- 2.5 CA publication and repository responsibilities**
- 2.5.1 Publication of CA information A CA must operate a secure on-line repository that is available to relying parties and that contains:
- issued certificates that reference this policy;
 - a CRL or on-line certificate status database;
 - the CA's certificate for its CA private signing key;
 - past and current versions of the CA's CPS;
 - a copy of this policy; and
 - other relevant information relating to certificates that reference this policy.
- 2.5.2 Frequency of publication Certificates must be published following the subscriber acceptance procedure specified in section 4.3. The CRL must be published as specified in section 4.9.
- 2.5.3 Access controls A CA must not impose any access controls on this policy, the CA's certificate for its CA private signing key and past and current versions of the CA's CPS. A CA may impose access controls on certificates and certificate status information in accordance with provisions of this policy.
- 2.5.4 Location The location of publication must be one that is convenient to the certificate-using community and appropriate to the total security requirements. It must identify an X.500 directory and an LDAP interface.
- 2.5.5 Revocation information The sole sources of information regarding the validity or revocation of a certificate must be provided by an RA, LRA ,the CA or a repository.

3 I&A

3.1 Naming

- 3.1.1 Types of names A CA must assign X.501 distinguished names to all subscribers as follows:
- the subject name used for each certificate must be the subscriber's name;
 - each subscriber must have a unique X.501 name in the certificate's subject name field, in accordance with X.509;
 - any subscriber may use an alternative name by use of the subject alternate name field in accordance with X.509;
 - the subscriber's name must be in the form of an X.501 printable string and must not be blank;
 - each certificate subject name field and issuer name field must include components of the authenticated name of the subscriber;
 - the authenticated name for each individual must be a combination of the first name and the surname. The authenticated name may include initials;
 - the unique name for each device must include the authenticated name of the person responsible for the device;
 - the unique name may include the name of an organizational position or role; and
 - each certificate that contains a role or position must contain the identity of the person who holds that role or position.

3.1.2	Names must be meaningful	<p>The subscriber certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to whom they are assigned.</p> <p>The common name in the DN must represent the subscriber in a way that is easily understandable for humans. For individual persons, this typically will be a legal name, so the preferred common name form is <i>first name, initial, last name</i>.</p>
3.1.3	Anonymity or pseudonymity of subscribers	A CA must not issue anonymous certificates. CA certificates issued by a CA must not contain anonymous or pseudonymous identities.
3.1.4	Rules for interpreting various name forms	Rules for interpreting distinguished name forms are specified in X.501. An RA and LRA must follow the CA's policies on name interpretation and subordination.
3.1.5	Recognition, authentication and role of trademarks	<p>CAs operating under this policy must not issue a certificate knowing that it infringes upon the trademark of another.</p> <p>No RA or LRA who provides subscriber information to a CA may guarantee that a subscriber's name will contain a trademark, trade name, corporate name or other specific referential material, but the RA or LRA may attempt to accommodate these requests.</p> <p>If a civil court of competent jurisdiction has determined that a subscriber has no right to use a specific name, an RA or LRA will not knowingly allow the subscriber to use that name. No RA or LRA will be required to inquire about or investigate the existence or validity of any court order or the trademark status.</p>
3.2 Initial identity validation		
3.2.1	Certificates issued to individual subscribers	A CA may issue certificates only to individual subscribers. A CA may not issue certificates to groups of persons.
3.2.2	Authentication of individual subscribers	Procedures used to authenticate individual subscribers may be more stringent than the following:
3.2.2.1	Level four certificates	<p>For level four certificates, all of the following requirements must be met:</p> <ul style="list-style-type: none"> • an applicant must appear in person before an RA, LRA, RAA or LRAA; • except as specified in this paragraph, an applicant must present at least one Kansas government-issued official picture identification credential approved by the ITIMG or two non-Kansas but government-issued identification credentials, at least one of which must be a picture identification. Other methods of equivalent or greater verification may be used, including a comparison of biometric data to preverified identities as approved by the ITIMG; • an applicant must personally appear before the RA, LRA, RAA or LAA to receive the subscriber's hardware token or token activation data; and • the private key corresponding to the public key offered for the certificate must exist in a hardware token. The possession of the hardware token by the subscriber must be verified in accordance with the requirements of the X.509 certificate management protocol or an equivalent protocol specified in the registered CA's CPS and approved by the ITIMG. The certificate must

contain an X.500 unique name and may contain an optional alternative subject name if the certificate indicates that the alternative subject name is not required.

3.2.2.2 Level three certificates

For level three certificates, all of the following requirements must be met:

- an applicant must appear in person before an RA, LRA, RAA or LRAA;
- except as specified in this paragraph, an applicant must present at least one Kansas government-issued official picture identification credential approved by the ITIMG or two non-Kansas but government-issued official identification credentials, at least one of which must be a picture identification. Other methods of equivalent or greater verification may be used, including a comparison of biometric data to preverified identities as approved by the ITIMG;
- an applicant's identity must be verified personally by the RA, LRA, RAA or LRAA or the applicant must provide credential information that required a prior in-person appearance before an entity that is approved by the RA, LRA, RAA or LRAA;
- if private keys are delivered to subscribers using hardware tokens, the subscriber must personally appear before the RA, LRA, RAA or LRAA to receive the subscriber's hardware token or token activation data; and
- the private key corresponding to the public key offered for the certificate may exist in software or in a hardware token. The possession of the hardware token by the subscriber must be verified in accordance with the requirements of the X.509 certificate management protocol or an equivalent protocol specified in the registered CA's CPS and approved by the ITIMG. The certificate must contain an X.500 unique name and an optional alternative subject name if the certificate indicates that the alternative subject name is not required.

3.2.2.3 Level two certificates

For level two certificates, all of the following requirements must be met:

- an applicant may apply in person or through a computer network, including the internet. If a computer network is used, the connection between the applicant and the RA, LRA, RAA or LRAA must be secured using a protocol that provides encryption for transmitted information as defined by the registered CA's CPS and approved by the ITIMG;
- an applicant must provide the same proof of identity as specified for a level three certificate above, and the RA, LRA, RAA or LRAA must verify the information to confirm the applicant's identity. This verification may be accomplished by use of a database or by attestation of a person in the same organization who performs a trusted role and who has supervisory responsibility for the applicant; and
- the private key corresponding to the public key offered for the certificate may exist in software or a hardware token. The possession of the hardware token by the subscriber must be verified in accordance with the requirements of the X.509 certificate management protocol or an equivalent protocol specified in the registered CA's CPS. The certificate must contain a subject name and may contain an optional alternative subject name if the certificate indicates that the alternative subject name is not required.

3.2.2.4 Level one certificates

For level one certificates, all of the following requirements must be met:

- an applicant may apply in person, through a computer network, including the internet, or by correspondence;
- no verification of the applicant's identity is required; and
- the private key corresponding to the public key offered for the certificate may exist in any software or hardware form. The certificate must contain a subject name and may contain an optional alternative subject name if the certificate indicates that the alternative subject name is not required.

3.2.2.5	Electronic device certificates	<p>For electronic device certificates, all of the following requirements must be met:</p> <ul style="list-style-type: none"> • a person for whom an electronic device's signature is attributable for the purposes of accountability and responsibility may request a certificate identifying an electronic device as the subject of the certificate. I&A of the person responsible for the device must be conducted as if the person were personally applying for the certificate. The certificate issued for a device must include the authenticated name of the person responsible for the device; and • the private key corresponding to the public key offered for the certificate may exist in software or in a hardware token depending upon the level of certificate for which application is made. The possession of the hardware token by the subscriber must be verified in accordance with the requirements of the X.509 certificate management protocol or an equivalent protocol specified in the registered CA's CPS. The certificate must contain an X.500 unique name and an optional alternative subject name if the certificate indicates that the alternative subject name is not required.
3.3	I&A for renewal or updating	<p>A subscriber may request the renewal or updating of a certificate within three months before the scheduled expiration of a certificate that was issued following I&A in accordance with this policy:</p>
3.3.1	Certificate renewal	<p>A certificate may be renewed only if the public key is valid, the private key is not compromised and the user name and attributes are correct. For renewal, a subscriber's identity may be established through use of a current signature key, except that identity must be re-established through an in-person registration process at least once every nine years from the time of initial registration.</p>
3.3.2	Certificate update	<p>For updating, the subscriber's identity must be established with I&A as for initial registration in accordance with this policy.</p>
3.3.3	Revoked or expired certificates	<p>Revoked or expired certificates must not be renewed. Each applicant with a revoked or expired certificate must be reauthenticated with I&A as for initial registration in accordance with this policy. If the application is made after revocation or expiration, the newly-issued certificate must contain the same globally unique identifier (GUID) as that on the original certificate.</p>
4	Certificate life cycle operations requirements	
4.1	Certificate application	<p>The certificate application process must provide sufficient information to:</p> <ul style="list-style-type: none"> • establish the identity of the subject as provided in this CP; • obtain a public/private key pair for each certificate required; • prove to the CA that the public key forms a functioning key pair with the private key held by the user; and • provide a point of contact for verification of any roles or authorizations requested. <p>These steps may be performed in any order that is convenient for the RA, LRA, RAA and LRAA that complies with applicable security policies, but all steps must be completed before certificate issuance.</p>
4.1.1	Application form and individual subscriber agreement	<p>An applicant for a certificate must complete a certificate application in a form prescribed by the RA and enter into an individual subscriber agreement as set out in this CP. All applications are subject to review and acceptance or denial at the discretion of the RA.</p>

4.2 Certificate issuance

4.2.1 CA actions, certificate issuance

Upon successful completion of the subscriber I&A process and complete and final approval of the certificate application, the CA will:

- build and sign a certificate if all certificate requirements have been met;
- issue the requested certificate;
- notify the RA and applicant thereof; and
- make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the subscriber only.

The CA must not issue a certificate unless the subscriber has executed an individual subscriber agreement.

4.2.2 Notification of certificate issuance to subscribers

After successful validation of the certificate application and issuance of the certificate, the CA must notify the RA and subscriber in a trustworthy and confidential manner that the certificate has been issued. For device certificates, the CA must notify the RA and subscriber for whom the electronic device's signature is attributable for the purposes of accountability and responsibility.

4.3 Certificate acceptance

4.3.1 Certificate acceptance

Acceptance is the action by a subscriber that triggers the subscriber's duties and potential liability and that constitutes acceptance of the law, this CP and the related agreements and the CA's CPS. The CA must define in its CPS a technical or procedural mechanism to explain to the subscriber the subscriber responsibilities defined in this policy, to inform the subscriber of the creation of a certificate and the contents of the certificate and to require the subscriber to indicate acceptance of the responsibilities and the certificate. This process will depend on factors such as where the key is generated and how certificates are posted, *e.g.* a subscriber may agree to his or her responsibilities at the same time that he/she accepts the certificate, or agreeing to his/her responsibilities may be a precondition for requesting a certificate.

4.3.2 Subscriber acceptance of certificate

As a condition to issuance of the certificate, a subscriber must submit acceptance or rejection of the certificate to the registered RA or LRA and execute the individual subscriber agreement contained in this policy. The RA, LRA, RAA or LRAA must explain to the subscriber the responsibilities contained in the individual subscriber agreement and their importance to the entire PKI infrastructure. By accepting the certificate, the subscriber warrants that all information and representations made by the subscriber, which are included in the certificate, are true.

4.3.3 Publication of the certificate

After a subscriber accepts a certificate, the CA must publish the certificate in the repository.

4.3.4 Notification of certificate issuance to others

Notification of certificate issuance to others may be accomplished by publication of the certificate in a recognized repository.

4.3.5 Certificate acceptance, CA documentation

The acceptance of a certificate is an event which must be logged by the CA and which may consist of a record made when the subscriber downloads the certificate. The act of acceptance must be recorded and maintained in an auditable trail kept by the CA in a trustworthy manner that complies with the law, this CP and the appended agreements and the CA's CPS.

4.4 Certificate use

- 4.4.1 Operational period A certificate may be used for purposes of authentication, signing and non-repudiation during its operational period. After a certificate expires, it must not be used for such purposes unless the use has been waived by a relying party.
- 4.4.2 Verification, actions during operational period A relying party's digital signature verification application must be capable of verifying that the digital signature was created during the certificate's operational period
- 4.4.3 RA and CA responsibility The RA and CA assume no responsibility for the use of or reliance upon certificates except as provided in this policy.

4.5 Certificate renewal or update

- 4.5.1 Certificate renewal A certificate renewal requires the creation of a new certificate with the same name and authorizations as those in the previous certificate, but the new certificate must reference a new key pair, an extended validity period and a different serial number. The subscriber's account GUID must remain unchanged and appear in the new certificate. The old certificate may or may not be revoked, but it must not be further re-keyed, renewed or modified.
- 4.5.2 Certificate update A certificate update requires the creation of a new certificate. Each updated certificate must reference a new key pair, a different serial number and one or more other fields that are different from those on the previous certificate. The subscriber's account GUID must remain unchanged and must appear in the new certificate.

4.6 Processing a request for a new key

Reserved.

4.7 Certificate modification

Reserved.

4.8 Certificate revocation

- 4.8.1 Circumstances for revocation, permissive revocation An RA, LRA or subscriber may request revocation of a certificate at any time for any reason. A sponsoring organization may request revocation of an affiliated individual certificate at any time for any reason. A CA also may revoke a certificate upon failure of the subscriber or any sponsoring organization to meet its obligations under this policy and the appended agreements and the CA's CPS. This includes revoking a certificate when a suspected or known compromise of the private key has occurred. If the failure is that of an RA or sponsoring organization, the CA first must notify the ITIMG of its proposed action.
- 4.8.2 Required revocation An RA, LRA, subscriber or a sponsoring organization must promptly request revocation of a certificate:
- when identifying information or affiliation components of any names in the certificate becomes invalid;
 - when privilege attributes asserted in the subscriber's certificate are reduced;
 - when the subscriber can be shown to have violated the provisions of its subscriber agreement;

- when the private key, or the medium holding the private key associated with the certificate is known to be or suspected to be lost, disclosed, compromised or subjected to unauthorized use in any way; or
- when an affiliated individual no longer is affiliated with an RA, LRA or sponsoring organization.

A CA must revoke a certificate:

- upon request of the RA, LRA subscriber or sponsoring organization;
- upon failure of the subscriber, LRA or the sponsoring organization to meet its material obligations under the law, this policy and the appended agreements or the CA's CPS;
- if knowledge or reasonable suspicion of compromise is obtained; or
- if the CA determines that the certificate was not properly issued in accordance with this policy and/or the CA's CPS.

The CA first must notify the ITIMG of its proposed action to revoke a certificate if the failure or violation is that of an RA, LRA or sponsoring organization.

4.8.3	Summary revocation, CA	A CA summarily may revoke certificates within its domain, provided that notice and cause are given.
4.8.4	Who can request revocation	An RA or LRA may request the revocation of a subscriber's certificate on behalf of the subscriber, the subscriber's sponsoring organization or another authorized party. The subscriber or the subscriber's sponsoring organization is authorized to request the revocation of the subscriber's certificate.
4.8.5	Procedure for revocation request	A certificate revocation request must be communicated promptly to the CA, either directly or through the RA or LRA authorized by the ITIMG to accept such notices. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber or the sponsoring organization. Alternatively, the subscriber or sponsoring organization may request revocation in accordance with the CA's CPS.
		Where subscribers use hardware tokens, revocation is optional if all of the following conditions are met: <ul style="list-style-type: none"> • the revocation request was not based upon key compromise; • the hardware token does not permit the user to export the signature private key; • the subscriber surrendered the token to the RA or LRA; • the token was zeroized or destroyed promptly upon surrender; • the token has been protected from unauthorized use between surrender and zeroization or destruction. <p>In all other cases, revocation of the certificates is mandatory. Even where all of the above conditions have been met, revocation of the associated certificates is recommended.</p>
4.8.5.1	Revocation request grace period	A CA must revoke a certificate as quickly as practical upon receipt of a proper revocation request and always must revoke certificates within the time periods described in section 4.9. Notwithstanding the foregoing, there will be a grace period of three (3) hours between the time a subscriber makes a revocation request and the time a certificate is revoked.
4.8.5.2	Suspension	A certificate may be suspended following an unsigned request for certificate revocation, pending authentication of the revocation request.

4.8.6	Time to process a revocation request	Promptly following revocation of a certificate, a CA must update the CRL or certificate status database in the repository, as applicable. All revocation requests and the resulting actions taken by the CA must be archived. Revoked certificates must be included on all new publications of the CRL until the certificates expire.
4.9	Certificate status services	
4.9.1	CRLs	CRLs must be issued periodically as follows:
4.9.2	CRL issuance frequency	To ensure timeliness of information, CRLs must be issued daily, even if there are no changes or updates to be made. CRLs may be issued more frequently than required. If there are circumstances for which the CA will post early updates, the circumstances must be described with specificity in the CPS. The CA must ensure that superseded CRLs are removed from the directory system upon posting of the latest CRL. If a CRL is issued as a result of a key compromise or revocation, the CRL must be posted as quickly as feasible, but in any event must be posted no later than six hours after notification of the compromise or decision to revoke by the CA. CAs must make public the details of certificate revocation information posting, including an explanation of the consequences of using dated revocation information. This information must be given to subscribers during certificate request or issuance and must be readily available to relying parties.
4.9.3	CRL latency	Interim CRLs must be made available to relying parties.
4.9.4	On-line revocation/status checking	When an on-line certificate status database is used as an alternative to a CRL, such database must be updated and checked in accordance with the same requirements as defined for a CRL.
4.9.5	Online revocation/status checking availability	CAs must validate online, near real time the status of the certificate identified in a certificate validation request message.
4.9.6	Online revocation checking requirements	A relying party must validate every certificate it receives in connection with a transaction in accordance with and by the means identified in the certificate. If it becomes infeasible to obtain revocation information, then the relying party either must reject use of the certificate or make an informed decision to accept the risk, responsibility and consequences for using a certificate for which authenticity cannot be established pursuant to the standards of this policy.
4.9.7	Other forms of revocation notices available	A CA also may use other methods to publicize revoked certificates. Any alternative method must meet all of the following requirements: <ul style="list-style-type: none"> • the alternative method must be described in the CA's approved CPS; • the alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified; and • the alternative method must meet the issuance and latency requirements for CRLs stated in this section.
4.10	End of subscription	If a person's subscription to the PKI ends prior to the expiration of any certificate issued under that subscription, the CA must revoke any certificates issued or held under the subscription.
4.11	Key escrow and recovery	

- 4.11.1 Key escrow and recovery, policy and practices CA private keys must never be escrowed.
- Subscriber key management keys may be escrowed to provide key recovery. CAs who support private key escrow for subscriber key management keys must detail the escrow practices in the CA's CPS. At a minimum, escrowed keys must be protected at the same level of security in which they are generated, delivered and protected by the subscriber.
- A subscriber's private signature key must never be escrowed or otherwise held in trust by a third party.

5 Facility, management and operational controls

5.1 Physical controls

- 5.1.1 Site location and construction CA equipment must be protected from unauthorized access while the cryptographic module is installed and activated. The CA must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens must be protected against theft, loss and unauthorized use.

The location and construction of the facility housing the CA equipment must be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, must provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical access

- 5.1.2.1 Physical access for CA equipment At a minimum, CA physical access controls must:
- ensure that no unauthorized access to the hardware is permitted;
 - ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers;
 - be manually or electronically monitored for unauthorized intrusion at all times;
 - ensure that an access log is maintained and inspected periodically, and
 - require two-person physical access control to both the cryptographic module and computer system.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules and CA equipment must be placed in secure containers. Activation data must be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data must not be stored with the cryptographic module.

A security check of the facility housing the CA equipment must occur if the facility is to be left unattended. At a minimum, the check must verify the following:

- the equipment is in a state appropriate to the current mode of operation, *e.g.* that cryptographic modules are in place when "open" and secured when "closed" and, for the CA, that all equipment other than the repository is shut down;
- any security containers are properly secured;
- physical security systems, *e.g.* door locks, vent covers are functioning properly; and
- the area is secured against unauthorized access.

A person or group of persons must be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance must be maintained. If the facility is not continuously attended, the last person to depart must initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

- 5.1.2.2 Physical access for RA and LRA equipment
- The office of each RA and LRA must be located in an area that can be entered only through a reception zone, and the activity in each reception zone must be monitored by personnel or security staff. Each RA and LRA must implement security procedures necessary to restrict access to the hardware and software used to provide RA and LRA services, including servers, workstations and any external cryptographic hardware modules or tokens. Access to the hardware and software must be restricted to personnel performing in a trusted role.

Each registration workstation used for on-line certificate management with registered CAs must be located in either a security zone or an attended operations zone with all media securely protected when unattended.

If an RA or LRA has possession of a cryptographic module, system software or private keys, the RA or LRA must provide the following security:

- a secure container or safe for the storage of the cryptographic module and the RA or LRA administrator's private key;
- security containers for recording personal identification numbers and passwords accessible only by designated personnel;
- workstations containing private keys that are physically secure using an appropriate access control product;
- hardware cryptographic modules that are physically protected, which may be accomplished using site protection; and
- procedures to ensure that the employees of RAs and LRAs do not leave their workstations unattended when the cryptographic module is in an unlocked state.

All security procedures used must be commensurate with the risk level associated with the environment in which the RA's and LRA's equipment is located.

- 5.1.3 Power and air conditioning
- CA equipment must have backup capability sufficient to automatically lock out input, finish any pending actions and record the state of the equipment before lack of power or air conditioning causes a shutdown. Users who require extended operation hours or short response times may contract with the CA for additional requirements for backup power generation. The revocation operations must be supported by uninterruptible power supplies and sufficient backup power generation.

- 5.1.4 Water exposure
- This policy makes no provision for prevention of or exposure of CA equipment to water beyond that called for by practices that are commercially reasonable within the industry. CA equipment must be installed so that it is not in danger of exposure to water, *e.g.* placement on tables or elevated floors. Moisture detectors must be installed in areas susceptible to flooding. CA operators who have sprinklers for fire control must have a contingency plan for recovery should the sprinklers malfunction or cause water damage outside of the fire area. Potential water damage from fire prevention and protection measures, *e.g.* sprinkler systems, are excluded from this requirement.

- 5.1.5 Fire prevention and protection
- This policy makes no provision for prevention of exposure of CA equipment to fire beyond that called for by practices that are commercially reasonable within the industry. An automatic fire extinguishing system must be installed in accordance with local code. A CA must have a contingency plan, which contemplates and addresses damage by fire.

- 5.1.6 Media storage Media must be stored in a manner that protects it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive or backup information must be stored in a location separate from the CA equipment.
- 5.1.7 Waste disposal Normal office waste must be removed or destroyed in accordance with practices that are commercially reasonable within the industry. Before disposal, media used to collect or transmit information discussed in section 9.2 must be erased.
- 5.1.8 Off-site backup System backups, sufficient to provide recovery from system failure, must be made on a periodic schedule, which must be described in the CA's CPS. At least one backup copy must be stored at an offsite location separate from the CA equipment. Only the latest backup is required to be retained. The backup must be stored at a site with physical and procedural controls commensurate with that of the operational CA system.

5.2 Procedural controls

- 5.2.1 Trusted roles A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or intentionally. The persons selected to fill these roles must be extraordinarily responsible, or the integrity of the CA, RA or LRA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI infrastructure. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any unauthorized or illegal activity would require collusion.

The primary trusted roles defined by this policy are administrator, officer, auditor and operator. These roles act on behalf of the CA, RA, LRA and SOS in the conduct of the PKI. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA's, RA's, LRA's or SOS' operation, *e.g.* the agreements appended to this CP.

- 5.2.1.1 Administrator The administrator role is responsible for:
 - installation, configuration and maintenance of the CA and CRL;
 - establishing and maintaining CA and CRL system accounts;
 - configuring certificate profiles or templates;
 - configuring CA, RA, LRA and CRL audit parameters;
 - configuring CRL response profiles; and
 - generating and backing up CA and CRL keys.
 Administrators do not issue certificates to subscribers. The administrator role is performed by CA personnel.
- 5.2.1.2 Officer, RA The RA officer role is responsible for administering certificates, that is:
 - registering new subscribers and requesting the issuance of certificates;
 - approving and executing the issuance of certificates; and
 - requesting, approving and executing the revocation of certificates.
 The officer role is performed by RA personnel. In the absence of an LRA, an RA officer, specifically the RAA, also is responsible for verifying the identity of subscribers and accuracy of information included in certificates.
- 5.2.1.3 Officer, LRA The LRA officer role is performed by LRA personnel, specifically the LRAA, when verifying the identity of subscribers and accuracy of information included in certificates.

5.2.1.4	Auditor, CA	<p>The CA auditor role is responsible for:</p> <ul style="list-style-type: none"> • reviewing, maintaining and archiving audit logs; and • performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with the law, this policy and the appended agreements and the CA's CPS. <p>The CA auditor role is performed by CA personnel.</p>
5.2.1.5	Auditor, RA/LRA	<p>The RA/LRA auditor role is responsible for performing or overseeing compliance audits to ensure that RAs and LRAs are operating in accordance with the law, this policy and the appended agreements and the CA's CPS. The RA/LRA auditor role is performed by persons appointed by the ITIMG.</p>
5.2.1.6	Operator, CA, RA and LRA	<p>The operator role is responsible for the routine operation of the CA, RA and LRA equipment and operations such as system backups and recovery or changing recording media. The operator role is performed by CA, RA and LRA personnel.</p>
5.2.2	Number of persons required per task	<p>A CA, RA and LRA must use commercially reasonable practices to ensure that one person acting alone cannot compromise security. To ensure that one person acting alone cannot compromise security, responsibilities for the CA, RA and LRA hardware and software must be shared by multiple roles and persons. Each user of the hardware and software must have capabilities limited to and commensurate with the role of the user identity.</p> <p>A person serving in a trusted role related to the PKI as auditor for a CA, RA, LRA or SOS must not serve in another trusted role related to the PKI for the CA, RA, LRA or SOS.</p>
5.2.3	Identification and authentication for each role	<p>A person must identify and authenticate him/herself before being permitted to perform any actions for a trusted role.</p>
5.3 Personnel controls		
5.3.1	Qualifications of personnel	<p>CAs, RAs and LRAs must implement and follow personnel and management policies sufficient to ensure the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this policy.</p>
5.3.2	Background check procedures	<p>At a minimum CA, RA and LRA personnel must pass a background investigation covering the following areas:</p> <ul style="list-style-type: none"> • employment; • education; • place of residence; • law enforcement; and • references. <p>The period of investigation must cover at least the last five years for each area, except the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified. Any personnel who fail an initial or periodic background check must not serve in a trusted role. The ITIMG or the secretary of state may request conduct of periodic background checks at their discretion.</p>
5.3.3	Training requirements	<p>All personnel performing duties related to the operation of the CA, RA or LRA must receive comprehensive training appropriate to their roles, and the training must be documented. Training must be conducted in the following areas:</p> <ul style="list-style-type: none"> • CA, RA or LRA security principles and mechanisms; • all PKI software versions in use on the CA, RA or LRA systems; • all PKI duties they are expected to perform;

- disaster recovery and business continuity procedures; and
- provisions of the law, this CP and the appended agreements and the CA's CPS.

5.3.4 Retraining frequency and requirements All persons responsible for PKI roles must be made aware of changes in the CA, RA or LRA operations appropriate to their roles. Any significant change to the operations must have a training awareness plan, and the execution of the plan must be documented. Examples of changes are software or hardware upgrades, changes in automated security systems and relocation of equipment. In any event, CAs, RAs and LRAs must review PKI operation requirements with persons performing PKI roles at least once a year.

CAs, RAs and LRAs must document the identity of all personnel who receive training and the level of training completed.

5.3.5 Job rotation frequency and sequence Reserved.

5.3.6 Sanctions for unauthorized actions A CA, RA or LRA must take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA, RA or LRA that are not authorized by law, this CP and the appended agreements and the CA's CPS.

5.3.7 Contracting personnel requirements Contractors fulfilling trusted roles are subject to all personnel requirements contained in this CP.

Contractors who provide services must establish procedures to ensure that any subcontractors perform in accordance with the law, this CP and the appended agreements and the CA's CPS.

5.3.8 Documentation supplied to personnel Documentation sufficient to define duties and procedures for each role must be provided to the personnel assigned to the role.

5.4 Audit logging procedures Audit log files must be generated for all events relating to the security of the CA. Events may be attributable to human action in any role or automatically invoked by the equipment. Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, paper form or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section must be maintained as archived records in accordance with section 5.5.

5.4.1 Types of events recorded All security auditing capabilities of CA operating system and CA applications must be enabled during installation. At a minimum, each audit record must include the following, either recorded automatically or manually for each auditable event:

- the type of event;
- the date and time the event occurred;
- a success or failure indicator when executing the CA's signing process;
- a success or failure indicator when performing certificate revocation; and
- the identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA is an auditable event. The corresponding audit record must also include message date and time, source, destination and contents.

A CA must document auditable events, which include but are not limited to those identified in the list below. Where these events cannot be electronically logged, the CA must supplement electronic audit logs with physical logs as necessary.

- security audit:

- any changes to the audit parameters, *e.g.* audit frequency, type of event audited
- any attempt to delete or modify the audit logs
- obtaining a third-party time stamp
- identification and authentication:
 - successful and unsuccessful attempts to assume a role
 - the value of maximum authentication attempts is changed
 - maximum authentication attempts unsuccessful authentication attempts occur during user login
 - an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
 - an administrator changes the type of authenticator, *e.g.* from password to biometrics
- local data entry:
 - all security-relevant data that is entered in the system
- remote data entry:
 - all security-relevant messages that are received by the system
- data export and output:
 - all successful and unsuccessful requests for confidential and security-relevant information
- key generation:
 - when the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- private key load and storage:
 - the loading of component private keys
 - all access to certificate subject private keys retained within the CA for key recovery purposes
- trusted public key entry, deletion and storage:
 - all changes to the trusted public keys, including additions and deletions
- secret key storage:
 - the manual entry of secret keys used for authentication
- private and secret key export:
 - the export of private and secret keys (keys used for a single session or message are excluded)
- certificate registration:
 - all certificate requests
 - all acceptance of certificates by subscribers
- certificate revocation:
 - all certificate revocation requests
- certificate status change approval:
 - the approval or rejection of a certificate status change request
- CA configuration:
 - any security-relevant changes to the configuration of the CA
- account administration:
 - roles and users are added or deleted
 - the access control privileges of a user account or a role are modified
- certificate profile management:
 - all changes to the certificate profile
- revocation profile management:
 - all changes to the revocation profile
- certificate revocation list profile management:
 - all changes to the certificate revocation list profile
- miscellaneous:
 - appointment of an individual to a trusted role
 - designation of personnel for multiparty control
 - installation of the operating system
 - installation of the CA
 - installing hardware cryptographic modules

- removing hardware cryptographic modules
- destruction of cryptographic modules
- system startup
- logon attempts to CA applications
- receipt of hardware / software
- attempts to set passwords
- attempts to modify passwords
- backing up CA internal database
- restoring CA internal database
- file manipulation, *e.g.* creation, renaming, moving
- posting of any material to a repository
- access to CA internal database
- all certificate compromise notification requests
- loading tokens with certificates
- shipment of tokens
- zeroizing tokens
- re-key of the CA
- configuration changes to the CA server involving:
 - hardware
 - software
 - operating system
 - patches
 - security profiles
- physical access/site security:
 - personnel access to room housing CA
 - access to the CA server
 - known or suspected violations of physical security
- anomalies:
 - software error conditions
 - software check integrity failures
 - receipt of unauthorized or otherwise suspicious messages
 - misrouted messages
 - network attacks (suspected or confirmed)
 - equipment failure
 - electrical power outages
 - uninterruptible power supply (UPS) failure
 - obvious and significant network service or access failures
 - violations of certificate policy
 - violations of certification practice statement
 - resetting operating system clock

5.4.2	Audit log review	A CA must ensure that its audit logs are reviewed by CA personnel at least weekly and that all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities recorded in the logs. Supporting manual and electronic logs from the CA and RA must be compared when any action is deemed suspicious. Actions taken following these reviews must be documented.
5.4.3	Retention period for audit log	The information generated on CA equipment must be maintained on the CA equipment until the information is moved to an appropriate archive facility. Removal of the audit log from the CA equipment for archiving must be performed by a person different from the CA operator. This person must be identified in the CA's CPS.
5.4.4	Protection of audit log	The audit log, to the extent possible, must not be open for reading or modification by any person or by any automated process other than those that perform audit processing. Because a person who has modification access may delete information,

only a person who does not have modification access to the audit log may archive it. Audit data must be moved weekly to a safe, secure storage location separate from the CA equipment.

- 5.4.5 Audit log backup procedures Audit logs and audit summaries must be backed up at least monthly. A copy of the audit log must be sent off site on a monthly basis.
- 5.4.6 Audit collection system, internal vs. external There is no requirement for the audit log collection system to be external to the CA system and equipment. The audit process must run independently and must not in any way be controlled by the CA operator. Audit processes must be invoked at system startup and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, the CA operation must cease until the audit function can be restored. If it is unacceptable to cease CA operation, other procedures, which have been arranged previously with the CA's auditor, must be employed to provide the audit function until the problem causing the failure has been remedied.
- 5.4.7 Notification to event-causing subject When an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device or application that caused the event.
- 5.4.8 Vulnerability assessments The CA must ensure that a vulnerability assessment is performed, reviewed and revised following an examination of audit events.
- 5.5 Records archival**
- 5.5.1 Types of events archived CA archive records must be sufficiently detailed to establish the proper operation of the CA or the validity of any certificate (including those revoked or expired) issued by the CA. The archive records include, but are not limited to, the following information, which must be recorded for archive for all assurance levels:
- CA accreditation, if applicable;
 - certificate policy;
 - certification practice statement;
 - contractual obligations;
 - other agreements concerning operations of the CA;
 - system and equipment configuration;
 - modifications and updates to system or configuration;
 - certificate requests;
 - all certificates issued and/or published;
 - security audit data;
 - revocation requests;
 - subscriber identity authentication data as stated in section 3.2;
 - documentation of receipt and acceptance of certificates;
 - subscriber agreements;
 - documentation of receipt of tokens;
 - CA re-key;
 - all CRLs issued and/or published;
 - all audit logs;
 - other data or applications to verify archive contents;
 - documentation of personnel background investigations;
 - documentation of PKI training for personnel; and
 - documentation required by compliance auditors.
- 5.5.2 Retention periods for archive Except as follows, a CA must maintain archive records throughout the period they remain active and for a period of not fewer than 10 years from and after they cease to be active or they expire or terminate.

A CA must maintain the following archive records permanently:

- all CA and subscriber certificates issued and
- all CRLs issued and/or published.

5.5.3 Protection of archive

A CA must not permit any unauthorized user to write to, modify or delete the archive. The contents of the archive may not be released except as determined by the ITIMG or as required by law. Archived records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archived media must be stored in at least two safe, secure storage facilities separate from the CA.

The CA must secure its records pursuant to standards that are commercially reasonable within the industry. The records must be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible to an auditor. They must be in the English language.

If the original medium cannot retain the archived data for the required retention period, the CA must transfer the data to a new medium approved by the ITIMG. Applications required to process the archived data also must be maintained for the retention period. Before the end of the archive retention period, the CA must provide the archived data and the applications necessary to read the data to an ITIMG approved archival facility, which must retain the applications necessary to read the archived data.

5.5.4 Requirements for time stamping of records

All CA archived records must be automatically time stamped as they are created. The CA's CPS must describe how system clocks used for time stamping are maintained in synchrony with an authoritative time standard.

5.5.5 Procedures to obtain and verify archived information

During any reviews required by this policy, the auditor must verify the integrity of the archives. Procedures detailing how to create, verify, package, transmit and store the archive information must be detailed in the CA's CPS.

5.6 Key changeover

5.6.1 CA certificate validity period

A CA must not issue subscriber certificates that extend beyond the expiration dates of the respective CA certificates. In addition, the CA certificate validity period must extend one user certificate validity period past the last use of the CA private key.

To minimize risk from compromise of a CA's private signing key, that key may be changed more frequently, and only the new key may be used for certificate signing purposes from that time. The older, but still valid, certificate must be available to verify old signatures until all of the certificates signed under it also have expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

A CA's CPS must describe limitations on and maximum validity periods for CA certificates.

5.7 Compromise and disaster recovery

5.7.1 Disaster recovery and business continuity plan

A CA must establish an appropriate disaster recovery and business continuity plan. The plan must set up and render operational a facility that is located in a different geographic area and that is capable of providing CA services in accordance with this policy within forty-eight (48) hours of an unanticipated emergency. The plan must include a complete and periodic test of readiness for such facility. The plan must be

detailed in the CA's CPS or other appropriate documentation and must be readily available to relying parties for inspection.

- 5.7.2 Secure facility after a natural or other type of disaster A CA must establish a disaster recovery and business continuity plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster, including the compromise of keys or related data. Where a repository is not under the control of the CA, the CA must ensure that any agreement with the repository provides that a disaster recovery and business continuity plan must be established and documented by the repository.
- 5.7.3 CA's certificate is revoked In the event a CA's certificate is revoked, the CA immediately must notify: the ITIMG, the secretary of state, all CAs to whom it has issued cross-certificates, RAs, LRAs, subscribers and all individuals or organizations who are responsible for a certificate used by a device or application. The CA also must publish the certificate serial number on an appropriate CRL and revoke all cross-certificates signed with the revoked digital signature certificate. After addressing the factors that led to revocation, the CA may generate a new CA signing key pair and re-issue certificates to all entities and ensure that all CRLs are signed using the new key. In the event the revocation of any other entity's digital signature certificate is required, see section 4.9.
- 5.7.4 CA's private key is compromised In the event of the compromise, or suspected compromise, of a CA signing key, the CA immediately must notify the ITIMG, the secretary of state, all CAs to whom it has issued cross-certificates, RAs, LRAs, subscribers and all individuals or organizations who are responsible for a certificate used by a device or application. In the event of the compromise, or suspected compromise, of any other entity's signing key, an entity must notify the CA immediately. The CA must ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the procedures it will use to provide notice of compromise or suspected compromise. In the event of the compromise of a CA's digital signature key, the CA must revoke all certificates issued using that key and provide appropriate notice as stated above. After addressing the factors that led to key compromise, the CA may generate a new CA signing key pair; re-issue certificates to all entities; and ensure that all CRLs are signed using the new key.
- 5.7.5 CA's public key is downgraded If the level of assurance for a CA's certificate is downgraded, a CA immediately must notify all interested parties including the ITIMG, RAs, LRAs, subscribers and all other CAs with whom it cross-certified.

5.8 CA termination

- 5.8.1 Procedure upon termination A CA who terminates operations before all certificates have expired must give written notification of the termination to the ITIMG, the secretary of state, all CAs to whom it has issued cross-certificates, RAs, LRAs, subscribers and all individuals or organizations who are responsible for a certificate used by a device or application and must perform either of the following: (1) revoke all valid certificates and return all records concerning them to the appropriate subscriber; or (2) submit the records to another CA or authorities as ordered by the secretary of state. A CA's CPS must describe a termination plan to minimize disruption to customers, RAs, LRAs, subscribers and all other CAs with whom it has cross-certified.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation Key pairs for CAs, RAs, repositories and subscribers must be generated so that the private key is known only to the authorized user of the key pair. Acceptable ways of accomplishing this include having all users generate their own keys on a secure system, not revealing the private keys to anyone else and generating keys in hardware cryptographic modules from which the private key cannot be extracted. CA and RA keys must be generated in FIPS 140 validated hardware cryptographic modules. Key pairs for repositories and subscribers may be generated in FIPS 140 validated hardware or software cryptographic modules.

CA key pair generation must create a verifiable audit trail which confirms that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party must validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.2 Private key delivery to subscriber If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- anyone who generates a private key signing key for a subscriber must not retain any copy of the key after delivery of the private key to the subscriber;
- the private key(s) must be protected from activation, compromise or modification during the delivery process;
- the subscriber must acknowledge receipt of the private key(s); and
- delivery must be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
 - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
 - For electronic delivery of private keys, the key material must be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data must be delivered using a separate secure channel.

The CA must maintain a record of the subscriber's acknowledgment of receipt of the token.

6.1.3 Public key delivery to CA Public keys must be delivered to a CA in a secure and trustworthy manner. The delivery mechanism must bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA key used to sign the certificate.

In those cases where public/private key pairs are generated by the CA on behalf of

the subscriber, the CA must implement secure procedures to ensure that the token on which the public/private key pair is held is securely sent to the proper subscriber and that the token is not activated prior to receipt by the proper subscriber.

- 6.1.4 CA public key delivery to relying parties
When a CA updates its signature key pair, the CA must distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate or in cross-certificates.
- 6.1.5 Key sizes
Minimum key length for level four certificates is 1024 bits. Minimum key length for levels three and two must be between 512 and 1024 bits. Minimum key length for level one certificates is 512. Certificates that expire on or after December 31, 2010 must be generated with 2048 bit keys.
- 6.1.6 Public key parameters generation
The digital signature standard must require key parameters in accordance with FIPS 186-2 as amended.
- 6.1.7 Parameter quality checking
Parameters for the digital signature standard must be as specified in FIPS 186 as amended.
- 6.1.8 Hardware/software key generation
The generation of digital signature keys for all entities must be generated randomly in a hardware cryptographic module. Any pseudo-random numbers used for key generation material must be generated by a FIPS approved method.
- 6.1.9 Key use purposes, X.509 v3 key use field
Keys may be used for authentication, non-repudiation and message integrity. They also may be used for session key establishment. CA signing keys are the only keys that may be used for signing certificates and CRLs. The certificate key use field must be used in accordance with PKIX-1 certificate and CRL profile. One of the following key use values must be present in all certificates: digital signature or non-repudiation. One of the following additional values must be present in CA certificate-signing certificates: Key cert sign or CRL sign. Keys must be certified for use in signing or encrypting, but not both, unless otherwise provided herein. The use of a specific key is determined by the key use extension in the X.509 certificate. This restriction does not prohibit use of protocols like the secure sockets layer that provide authenticated connections using key management certificates.
- 6.2 CA private key protection**
A CA and repository each must protect its private key(s) in accordance with the provisions of this policy.
- 6.2.1 Standards for cryptographic module
The applicable standard for cryptographic modules must be FIPS 140 level 2 as amended, unless ITEC, with the assistance of the ITIMG, determines that other comparable validation, certification or verification standards are sufficient. In that event the standards will be transmitted to CA's by the ITIMG and published by the CA's. Subscribers must use cryptographic modules, which at a minimum meet the criteria specified in this policy. RAs must have at least level 2 hardware cryptographic modules. A higher level may be used if available or desired. RAs and CAs must provide the option of using any acceptable cryptographic module, to facilitate the management of certificates. A CA may use hardware or software cryptographic modules for CA key generation and protection, validated at level three. Certificates must be signed using a hardware cryptographic module that meets level three.
- 6.2.2 Private key multi-person control
A CA must not permit a single individual to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery must be under at least two-person control. The names of the parties used for two-person control must be maintained on a list that must be made

available for inspection during compliance audits.

- 6.2.3 Private key escrow CA private signature keys must never be escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.11 of this CP.
- 6.2.4 Private key backup
 - 6.2.4.1 Backup, CA private signature key The CA private signature keys must be backed up under the same multiperson control as the original signature key. At least one copy of the private signature key must be stored off-site. All copies of the CA private signature key must be accounted for and protected in the same manner as the original. Backup procedures must be detailed in the CA's CPS.
 - 6.2.4.2 Backup, subscriber private signature key Subscriber private signature keys must not be backed up.
 - 6.2.4.3 Backup, subscriber private key management key Backed up subscriber private key management keys must not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.
 - 6.2.4.4 Backup, CRL private key CRL private keys may be backed up. If backed up, all copies must be accounted for and protected in the same manner as the original.
- 6.2.5 Private key archival CA private signature keys and subscriber private signature keys must not be archived. CAs who retain subscriber private encryption keys for business continuity purposes must archive such subscriber private keys in accordance with section 4.11 of this CP.
- 6.2.6 Private key transfer into or from cryptographic module Private keys must be generated and kept inside cryptographic modules validated to at least FIPS 140 level 3 as amended. For the purposes of routine recovery and disaster recovery only, a CA may transfer CA key pairs from one cryptographic module to another. The key pair must be encrypted during transport. Private keys may never exist in plain text form outside the cryptographic module boundary.
- 6.2.7 Activating private key Private keys must be activated by activation data stored securely and separately from cryptographic modules.
- 6.2.8 Deactivating private key Cryptographic modules that have been activated must not be left unattended or otherwise open to unauthorized access. After use they must be deactivated, *e.g.* by a manual logout procedure or by a passive timeout. Hardware cryptographic modules must be removed and stored or must be within the CA's sole control when not in use.
- 6.2.9 Destroying private key Private keys must be destroyed when they no longer are needed or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, destruction may mean overwriting the data. For hardware tokens, destruction may mean executing an erase command. Physical destruction of hardware is not required.
- 6.3 Other aspects of key pair management**
 - 6.3.1 Public key archival A CA must retain all public keys as part of the certificate archival.

6.3.2 Root CA key pairs, operational and use periods Root CA key pairs must not have validity periods longer than twenty years.

6.4 Activation data

6.4.1 Activation data generation and installation A pass-phrase or PIN (activation data) must be used to protect access to use of the private key. The activation data may be user selected. The strength of the activation data must meet or exceed the requirements for authentication mechanisms validated to Level 2 in FIPS 140-2 as amended.

If the activation data must be transmitted, it must be transmitted via a channel of appropriate protection and distinct in time and place from the associated cryptographic module. If transmission is not accomplished by hand, the user must be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, users will sign and return a delivery receipt. In addition, users also must receive and acknowledge a user advisory statement to help them understand responsibilities in the use and control of the cryptographic module.

6.4.2 Activation data protection Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources. Activation data must be:

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module and must not be stored with the cryptographic module.

6.4.3 Other aspects of activation data Activation data must be changed periodically to decrease the likelihood that it has been discovered. A CA must define activation data requirements in its CPS.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements All CA servers must include the following functionality, either provided by the operating system or through a combination of operating system, software and physical safeguards:

- require authenticated logins;
- enforce access control to CA services and PKI roles;
- enforce separation of duties for PKI roles;
- require identification and authentication of PKI roles and associated identities;
- prohibit object reuse or require separation for CA random access memory;
- require use of cryptography for session communication and database security;
- archive CA history and audit data;
- provide security audit capabilities;
- require self-test of security-related CA services
- require a trusted path for identification of PKI roles and associated identities;
- require recovery procedures for keys and the CA system; and
- enforce domain integrity boundaries for security-critical processes.

6.5.1.1 Same, RAs and LRAs, as their roles RAs and LRAs, as their roles provide, must provide the computer security functions listed below. These functions may be provided by the operating system or through

	provide	<p>a combination of operating system, software and physical safeguards:</p> <ul style="list-style-type: none"> • authenticate the identity of users before permitting access to the system or applications; • manage privileges of users to limit users to their assigned roles; • generate and archive audit records for all transactions; • enforce domain integrity boundaries for security critical processes; and • support recovery from key or system failure.
6.5.2	Computer security rating	A CA's equipment must meet and be operated to at least a C2 [TCSEC – trusted computer system evaluation criteria] or E2/F-C2 [ITSEC – international trusted system evaluation criteria] rating as amended, or equivalent.
6.6	Life cycle technical controls	
6.6.1	System development controls	The CA's system development controls must be detailed in the CA's CPS.
6.6.2	Security management controls	The configuration of the CA system, in addition to any modifications and upgrades, must be documented and controlled. There must be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, must be verified as being that supplied from the vendor with no modifications and the version intended for use. At the time of installation and at least once every 24 hours, the CA must verify the integrity of the software as specified in the CA's CPS.
6.7	Network security controls	<p>A network guard, firewall or filtering router must protect network access to CA equipment. The network guard, firewall or filtering router must limit services allowed to and from the CA equipment to those required to perform CA functions.</p> <p>Protection of CA equipment must be provided against known network attacks. All unused network ports and services must be turned off. Any network software present on the CA equipment must be necessary to the functioning of the CA application.</p> <p>Any boundary control devices used to protect the network on which PKI equipment is hosted must deny all but the necessary services to the PKI equipment.</p> <p>Directories and certificate status servers must employ appropriate network security controls. Networking equipment must turn off unused network ports and services. Any network software present must be necessary to the functioning of the equipment.</p>
6.8	Time stamping	Times asserted for certificates, CRLs and other revocation database entries must be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.
7	Certificate and CRL profiles	
7.1	Certificate profile	
7.1.1	Requirements	Certificates that reference this policy must contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages, <i>e.g.</i> public keys used for digital signature verification. All certificates that reference this policy must be issued in the X.509 version 3 as

amended format and may include a reference to the OID for this policy within the appropriate field. The CPS must identify the certificate extensions supported and the level of support for those extensions.

7.1.2	Version number and base fields	A CA must issue X.509 version 3 certificates, in accordance with the PKIX certificate and CRL Profile. The PKI end-entity software must support all the base (non-extension) X.509 fields as follows:
	version	version of X.509 certificate, version 3(2)
	serial number	unique serial number for certificate, as well as the certificate extensions defined in section 7.1.3
	signature	CA signature to authenticate certificate
	issuer	name of CA
	validity period	activation and expiration date for certificate
	subject	subscriber's distinguished name, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of certificates issued by the CA
7.1.3	Certificate extensions	No extension will modify or undermine the use of X.509 base fields.
7.1.3.1	Certificate policies	If the state of Kansas secures an object identifier (OID), the certificate policies field may be populated in all certificates with one of the policy OIDs and may be set as a non-critical extension.
7.1.3.2	Policy constraints	Reserved.
7.1.3.3	Critical extensions	All entity PKI software must correctly process critical extensions identified in this policy.
7.1.3.4	Supported extensions	A CA's CPS must define the use of any extensions supported by the CA and RAs.
7.1.4	Name forms	Every DN must be in the form of an X.501 printable string.
7.1.5	Name constraints	Subject and issuer DNs must comply with PKIX standards and be present in all certificates.
7.1.6	Certificate policy object identifier	If the state of Kansas secures an OID, a CA must ensure that the policy OID is contained within the certificates it issues.
7.1.7	Use of key use extension	A CA must populate and mark as critical the key use extension in a certificate and identify the subscriber's private key as being used either for signing and non-repudiation or for encryption.
7.1.8	Policy qualifiers syntax and semantics	A CA must populate the policy qualifiers extension with the URL of its CP.
7.2	CRL profile	
7.2.1	Version numbers	A CA must issue X.509 version 2 CRLs in accordance with the PKIX certificate and CRL profile. The CA's CPS must identify the CRL extensions supported and the level of support for these extensions.
7.2.2	CRL and CRL	All PKI software must correctly process all CRL extensions identified in the certificate

entry extensions and CRL profile.

8 Compliance reviews and other assessments

- 8.1 Frequency** A CA must submit to and pay for compliance reviews applicable to CAs under Kansas law. An applicant CA and a CA must file the review report with the secretary of state upon initial registration as a CA and thereafter once every two years unless ordered as follows.
- The secretary of state or the ITIMG may order a compliance review at any time at their discretion.
- 8.2 Identity and qualifications of auditor** A compliance auditor must be qualified to conduct a compliance review pursuant to Kansas law and must be sufficiently familiar with the best practices of a CA. The auditor must be thoroughly familiar with the subject CA's CPS and this CP.
- 8.3 Auditor's neutrality** The auditor and CA must have a contractual relationship for the performance of the review, and the auditor must be sufficiently separated legally and organizationally from the CA to provide an arms-length, unbiased and independent evaluation.
- 8.4 Scope of reviews** Reviews must be conducted in accordance with Kansas law and in accordance with the most current version of "CSPP – guidance for COTS security protection profiles," published by the U.S. department of commerce. The purpose of the compliance review is to verify that a CA complies with all of the requirements of Kansas law, this CP and the appended agreements and the CA's CPS.
- 8.5 Actions taken as a result of review** If a review reports any material noncompliance with Kansas law, this CP and the appended agreements and the CA's CPS, the following actions must be performed:
- the compliance auditor must note the discrepancy;
 - the compliance auditor must notify the parties in section 8.6 of the discrepancy; and
 - the party responsible for correcting the discrepancy will propose a remedy, including an expected time for completion, to the ITIMG.
- Depending upon the nature and severity of the noncompliance, the registration of the subject CA may be deemed lapsed in accordance with Kansas law. If the severity of the noncompliance is determined by the ITIMG not to warrant lapse of the CA's registration, it may recommend to the secretary of state an alternative remedy, including a temporary halt of the subject CA's operations pending the successful completion of the remedy. The final order concerning the remedy and the status of the CA's registration will be made by the secretary of state.
- 8.6 Communication of results** A compliance review report must be reported to the subject CA and filed with the ITIMG and with the secretary of state as required by Kansas law. A special compliance review may be ordered to confirm the successful implementation and effectiveness of any remedy ordered.

9 Policy administration

9.1 Fee Reserved

9.2 Privacy and data protection policy

9.2.1 Use of subscriber information A CA will use subscriber information only for the purpose of performing the authentication process and issuing a certificate.

9.2.2 Private key information Digital signature private keys will be confidential. Any private key management keys held by a CA will be confidential. No private key may appear unencrypted outside the cryptographic module.

9.2.3 CA information All information stored locally on CA equipment must be secured as confidential information, and access to it must be restricted to those with an official need-to-know in order to perform their official duties related to the PKI. Private keys used to sign certificates that will assert security privileges must be classified at the same level as the privileges that are to be asserted by the related certificates. If a CA does not independently verify security privilege information, this requirement must be executed by the RAs.

9.2.4 Compliance review information Compliance review information is confidential and must not be disclosed to anyone for any purpose except for conduct of the compliance review, reporting obligations pursuant to the law, this policy and the appended agreements and the CA contract with the secretary of state.

9.2.5 Permitted acquisition of private information; disclosure A CA only may collect such personal information about a subscriber that is required for the issuance of a certificate to the subscriber. For the purpose of proper administration of certificates, a CA or RA may request non-certificate information to be used in issuing and managing certificates, *e.g.* identifying numbers, business or home addresses and telephone numbers. Collection of personal information is subject to collection, maintenance, retention and protection requirements of applicable state and federal law.

9.2.6 Opportunity of owner to correct private information Upon the written request of a subscriber, a CA or RA must provide the subscriber's information to him/her. Thereafter the subscriber may offer corrected subscriber information to the CA or RA.

9.2.7 Release of information for criminal or civil matter Only the ITIMG or secretary of state may authorize disclosure of certificate or certificate-related information to a law enforcement agency or other duly-authorized agent in a criminal or civil matter and only under the following circumstances: when (1) required to be disclosed by law, governmental rule or regulation or court order; or (2) authorized by the subscriber when necessary to effect an appropriate use of the certificate. Any request for such disclosure of private and/or confidential information must be made in accordance with applicable law.

9.3 Intellectual property rights

9.3.1 Private key ownership The private key must be treated as the sole property of the legitimate holder of the corresponding public key identified in a certificate.

9.3.2	CP and OID	This CP and its OID are the property of the ITEC and may be used by an RA or a CA in accordance with the provisions of this policy. Any other use of the above without the express written permission of the ITEC through the ITIMG is prohibited.
9.4	Limitation on liability	Reserved.
9.5	Policy change procedures	
9.5.1	Policy review	This policy must be reviewed by the ITIMG every year.
9.5.2	Suggested changes	Suggested changes to this policy must be communicated to the ITIMG contact on or before October 1 each year. Such communication must include a description of the change, a change justification and contact information for the person requesting the change.
9.5.3	Notice of suggested changes	On or before October 31 each year, the ITIMG must provide notice of any proposed policy changes to CAs and RAs.
9.5.4	Review and comment period	CAs, RAs and other interested parties may file comments concerning the proposed changes with the ITIMG on or before November 31 each year. After receipt of the comments, the ITIMG must use its best efforts to review the comments and provide its recommendations for policy changes, if any, to the ITEC by December 31 each year.
9.5.5	Final decision	Final decisions on the proposed changes to this CP are at the sole discretion of the ITEC with the advice of ITIMG. If a proposed change is adopted as a result of the CP review, a notice of the change must be given to all CAs and RAs.
9.5.6	Changes outside annual review	Notwithstanding the foregoing, if, in the judgment of the ITEC or the ITIMG, it is determined changes to the policy should be made prior to the annual review, the ITEC reserves the right to modify the policy upon notification of the proposed changes to CAs and RAs. CAs and RAs must be given reasonable time to comment and to comply with the proposed changes.
9.5.7	Changes subject to notification requirement	All CAs and RAs must be provided notice of any proposed change to this policy.
9.6	Publication and notification policies	
9.6.1	Posting of policy	All CAs must post a copy of this policy in electronic form available to the public on their Internet Web sites.
9.6.2	Notification procedure	Provided in section 9.5 above.
9.6.3	Procedure for comments	Written and signed comments on proposed changes must be directed to the ITIMG.
9.6.4	Final change notice	The ITEC will determine the period of time for notice of any final change to this policy.

9.6.5	Provisions for which change requires a new policy	If the State of Kansas secures an OID and a policy change is determined by the ITEC or the ITIMG to warrant the issuance of a new policy, the ITEC may require a new object OID for the modified policy.
9.7	CPS approval procedures	
9.7.1	Person determining CPS suitability for CP	The ITIMG will determine the suitability of any CPS to this policy.
9.7.2	Disclosure	When a CA's CPS contains security information, that information is not required to be made available publicly. Upon written request of the CA and a finding by the ITIMG that the information constitutes security information, the ITIMG will prescribe a method for confidential communication of the security information it requires, and the CA will provide it in that method. The security information provided in this manner will not be disclosed by the ITIMG unless it is determined that it does not qualify as information related to the security of the CA and, therefore, is not exempted under the Kansas open records act.
9.8	Governing law	The laws of the United States of America and the State of Kansas will govern the enforceability, construction, interpretation and validity of this CP.
9.8.1	Merger and notice	A CA must ensure that any agreements by that CA will contain provisions governing severability, survival, merger or notice consistent with Kansas law.
9.8.2	Dispute resolution procedures	ITEC, with assistance from the ITIMG, will resolve any disputes associated with the use of the CA or certificates issued by the CA.
9.9	Severability	Should it be determined that one section of this CP is invalid, the other sections of this CP will remain in effect until the CP is updated. The process for updating this CP is described in section 9.5.
9.10	Waivers	Waivers from this policy will not be granted for any level of assurance. Variation in a CA's practice either will be deemed compliant with this policy, or a change must be requested to this policy in conformance with section 9.5.
9.11	Contact details	Communication to the ITIMG should be addressed to: ITIMG Secretary of State First Floor, Memorial Hall 120 SW 10 th Ave Topeka, KS 66612-1594

Appendices

10 Definitions

Activation data	Private data, but not keys, that are required to access or activate cryptographic modules.
Affiliated person	An individual person who is authorized by an entity to hold a certificate containing the entity's name as an employee, partner, member, officer, agent, licensee, permittee or other associate of the entity.
Applicant	A subscriber after applying to a CA for a certificate but before the certificate is issued.
Archive	Long-term, physically-separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls; to ensure compliance with established policies and operational procedures; and to recommend necessary changes in controls, policies, or procedures.
Authenticate	To confirm the identity of a person when the person's identity information is presented.
Authentication	Security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Backup	Copy of files and programs made to facilitate recovery, if necessary.
Biometric	A physical characteristic of a human being, including a photograph for visual identification. For the purposes of this CP, biometrics do not include handwritten signatures.
Certificate	A computer-based record or electronic message that at a minimum: (1) identifies the CA issuing it; (2) names or identifies a subscriber; (3) contains the subscriber's public key; (4) identifies the certificate's operations period; and (5) is digitally signed by a CA.
Certificate policy (CP)	A specialized form of administrative policy applicable to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. A CP also states a named set of rules that indicate the applicability of a certificate to particular communities and classes of applications with common security requirements.
Certificate profile	The protocol stated in section 7 of this policy, which establishes the allowed format and contents of data fields within a certificate.
Certificate revocation list (CRL)	A list maintained by a CA of the certificates it has issued that are revoked before their stated expiration dates.
Certification authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CARLs or CRLs.

CA certificate	The certificate at the beginning of a certification chain within the State of Kansas PKI hierarchy, which is self-issued in a secure and trustworthy manner.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a CA to perform certificate issuance and revocation.
CA private root key	The private key used to sign the CA certificate and certify the CA's public/private key pair.
CA private signing key	The private key that corresponds to a CA's public key, is listed in the CA certificate and is used to sign certificates.
Certification authority revocation list (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
Certification practice statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them in compliance with the law, this CP and the appended agreements.
Compliance review	Documentation in the form of an information systems audit report verifying the applicant has the use of a trustworthy system, as defined in Kansas law.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized, intentional or unintentional disclosure, modification, destruction or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-certificate	A certificate used to establish a trust relationship between two CAs.
Cryptographic module	The set of hardware, software, firmware or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and that is contained within the cryptographic boundary of the module.
Data integrity	Assurance that the data are unchanged from creation to reception.
Digital signature	A type of electronic signature consisting of a transformation of an electronic message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (1) the transformation was created using the private key that corresponds to the signer's public key; and (2) the initial message has not been altered since the transformation was made.
Distinguished name (DN)	The unique identifier for a subscriber so that the person or device can be located in a directory.
Electronic device	Computer software or hardware or other electronic or automated means configured and enabled by the subscriber to act as its agent and to initiate or respond to electronic records or actions, in whole or in part, without review or intervention by the subscriber.
Erase	To remove all the data stored on a magnetic storage medium.
Federal information processing standards (FIPS)	FIPS are a set of standards that describe document processing, provide standard algorithms for searching and provide other information processing standards for use within US government agencies.

Globally unique identifier (GUID)	Also called a universally unique identifier (UUID); the result of a process that yields a character string, containing combinations of numbers, letters and/or special characters and that is appended to the common name (CN) in individual or entity certificates. This CP makes no provision for the length of the character string beyond that called for by practices that are commercially reasonable within the industry. The GUID may contain only those characters found in the following character set: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789[] –
Governmental agency	An executive, legislative or judicial agency, department, board, commission, authority, institution or instrumentality of the federal government or of a state or of a county, municipality or other political subdivision of a state.
Hardware token	A physical object (<i>e.g.</i> smartcard or a USB token) that is authenticated to and grants access to a system. It may store a subscriber’s private keys and certificates.
High-security zone	An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors, accessible only from security zones and separated from security zones and operations zones by a perimeter.
Identification and authentication (I&A)	To ascertain and confirm through appropriate inquiry and investigation the identity of a subscriber or other person.
Information technology executive council (ITEC)	The Kansas information technology executive council, acting in accordance with KSA 75-7202 <i>et seq.</i>
Information technology identity management group (ITIMG)	The information technology identity management group, which has delegated authority from the ITEC and is authorized by the ITEC to make day-to-day administrative and fiscal decisions for the PKI program.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage and eventual receipt by the destination.
Issue certificates	The acts performed by a CA in creating a certificate, listing itself as “issuer” and notifying the RA or other certificate applicant of its contents and that the certificate is ready and available for acceptance.
Kansas uniform electronic transactions act (KUETA)	KSA 16-1601 <i>et seq.</i> , as amended.
Key escrow	A deposit of the private encryption key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber’s private encryption key for the benefit of the subscriber, an employer or other party in accordance with provisions set forth in the agreement.
Key generation	The trustworthy process of creating a public/private key pair.
Key pair	For encryption, two mathematically related keys having the properties that (1) one

key can be used to encrypt a message that only can be decrypted using the other key; and (2) even knowing one key, it is computationally infeasible to discover the other key. For a digital signature, two mathematically related keys having the properties that (1) one key can be used to digitally sign a message that can only be authenticated using the other key; and (2) even knowing one key, it is computationally infeasible to discover the other key.

Level one certificate	A certificate issued that is not based upon I&A procedures. An applicant may apply and receive a certificate by providing his or her name and e-mail address.
Level two certificate	A certificate issued based upon I&A procedures, which include the applicant's application through a network such as the Internet, by correspondence or in person. An applicant must provide appropriate proof of identity, which may be accomplished by use of a database or by attestation of a trusted individual in the same organization who has supervisory responsibility for the applicant.
Level three certificate	A certificate issued based upon I&A procedures, which includes personal appearance before the RA and the providing of at least one approved Kansas government-issued official picture identification credential or two non-Kansas government-issued official identification credentials, at least one of which must be a picture identification.
Level four certificate	A certificate issued based upon I&A procedures, which includes the requirements of a level three certificate and may include biometric data. The private key must exist in a hardware token.
Local registration authority (LRA)	An entity that, because of its relationship of trust with subscribers, has a contractual relationship with an RA to accept certificate applications and conduct I&A for those subscribers. In the conduct of these responsibilities, an LRA acts in compliance with the law, the provisions of this CP and the appended agreements.
Local registration authority administrator (LRAA)	A person or persons who may be designated by an LRA to conduct registration activities and represent the LRA in the issuance and revocation of certificates for subscribers.
Nonrepudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical nonrepudiation refers to the assurance a relying party has that, if a public key is used to validate a digital signature, the signature had to have been made by the corresponding private signature key. Legal nonrepudiation refers to how well possession or control of the private signature key can be established.
Object identifier (OID)	A specialized formatted number that is registered with an internationally-recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
Online certificate status checking protocol (OCSP)	A protocol identified by RFC internet engineering task force's (IETF) request for comment 2560 that enables an application to determine the status of an identified certificate by issuing a status request to an OCSP responder and suspending acceptance of the certificate in question until the responder has provided the application with a response.
Operations zones	Areas where access is limited to personnel who work there and to properly escorted visitors. Operations zones should be entered from a reception zone and must be monitored as frequently as a threat assessment determines will secure the area.
Out-of-band	Communication between parties using a means or method that differs from the

current method of communication.

Person	Under the KUETA, an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity.
Private key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair used to decrypt confidential information. In both cases, this key must be kept secret.
Public key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.
Public key infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain and revoke public key certificates.
Reception zone	The entry to a facility where the initial contact between the public and a CA or RA occurs, where services are provided, information is exchanged and access to restricted (operations, security and high-security) zones is controlled.
Registration	The process of receiving or obtaining a request for a certificate from a subscriber and collecting and entering the information needed from that subscriber to include in and support I&A and issuance of a certificate.
Registration authority (RA)	A person who has been authenticated by a CA, issued a registration authority certificate by the CA and approved by ITEC to process subscriber applications for certificates and to conduct I&A of subscribers in accordance with the law, this policy and the related agreements.
Registration authority administrator (RAA)	A person or persons who may be designated by an RA to conduct registration activities and represent the RA in the issuance and revocation of certificates for subscribers.
Relying party	A person or governmental agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and that is in a position to rely on them.
Renew a certificate	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	Also directory; an online system maintained by or on behalf of a CA for storing and retrieving certificates and other information relating to certificates and digital signatures.
Revoke a certificate	To prematurely end the operational period of a certificate, effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (<i>i.e.</i> , the beginning of trust paths) for a security domain.
Security zone	An area to which access is limited to authorized personnel and to authorized and properly escorted visitors.

Sponsoring organization	An organization that has authorized the issuance of a certificate identifying the subscriber as having an affiliation with the organization (<i>e.g.</i> , as an employee, partner, member, officer, agent, licensee, permittee or other associate).
Subscriber	A subscriber is a person who (1) is the subject named or identified in a certificate issued to that entity; (2) holds a private key that corresponds to the public key listed in the certificate; and (3) does not issue certificates to another party. A subscriber includes, but is not limited to, an individual or network device.
Trusted role	A role whose incumbent performs functions that may introduce security problems if not carried out properly, whether accidentally or intentionally.
Time stamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy system	Computer hardware, software and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally-accepted security procedures.
Two-person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

11 Acronyms and abbreviations

CA	certification authority
CP	certificate policy, used interchangeably with "ITEC policy"
CPS	certificate practice statement
CRL	certification revocation list
DN	distinguished name
FIPS	U.S. federal information processing standard
GUID	globally unique identifier
I&A	identify and authenticate or identification and authentication
IETF	internet engineering task force
ITEC	information technology executive council
ITIMG	information technology identity management group
KAR	Kansas administrative regulations
KSA	Kansas statutes annotated
KUETA	Kansas uniform electronic transactions act

LRA	local registration authority
LRAA	local registration authority administrator
OCSP	online certificate status protocol
OID	object identifier
OBB	open-but-bounded
PKI	public key infrastructure
PKIX	public key infrastructure X.509
RA	registration authority
RAA	registration authority administrator
SOS	secretary of state
X.500	The standard published by the international telecommunication union-T (ITU-T) in February 2001 that establishes a distributed, hierarchical directory protocol organized by country, region and organization. This X.500 standard, including annex A, as amended, is hereby adopted by reference.
X.501	The standard published by the international telecommunication union-T (ITU-T) in February 2001 that establishes models for the directory of other ITU-T recommendations in the X.500 series. This X.501 standard, including annexes A through H, as amended, is hereby adopted by reference.
X.509	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, as amended, is hereby adopted by reference.

12 Agreements

12.1 AGREEMENT between RA and LRA

This agreement is entered into this ___ day of _____, 20__ by and between the Information Network of Kansas, registration authority (RA) for the State of Kansas, and _____,
_____ (address), local registration authority (LRA).

The parties agree as follows:

1. Subject to the terms and conditions of this agreement, RA agrees to furnish registration authority services for the LRA for the period from _____, 20__ through _____, 20__ at the following price: \$__ per certificate per year.
2. The parties agree that this agreement is subject to state contract 04294 for digital signature services, the Information Technology Executive Council (ITEC) policy 9200 and its *Certificate Policy for the State of Kansas Public Key Infrastructure* (CP) as amended. <http://da.ks.gov/itec>
3. The parties understand and agree that the provisions set out in the DA146a, attached; the CP; and any modifications to this agreement are incorporated and made a part of this contract by reference as though fully set forth herein. The parties agree that these documents are listed in their order of precedence and that these documents are controlling over any other document.
4. The business conducted by LRA to which the services will be dedicated is a lawful business.
5. *Limitations on use.* The parties agree that certificates issued under the trusted network are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage. RA is not responsible for assessing the appropriateness of the use of a certificate. The parties agree that they will not use or rely upon certificates beyond the limitations set forth in this agreement.
6. RA agrees to process applications for subscriber certificates upon a request from the LRA. The LRA agrees to submit such request in the form approved by the RA. Because of the State of Kansas' interest in the security of the trusted network, the LRA agrees to exercise due diligence in vetting the subscribers in accordance with the CP.
7. LRA agrees that it immediately will report to RA any breach or suspected breach of security by its individual subscribers. The latter includes, but is not limited to, the following:
 - a. inaccurate information provided by a subscriber in response to a certificate application;
 - b. infringement upon the intellectual property rights of any third parties resulting from information provided by a subscriber (including an e-mail address);
 - c. use by a subscriber of certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;
 - d. failure by a subscriber to remain the only person in possession of the private key and the only person with access to the private key;
 - e. failure by a subscriber to remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;
 - f. use of a subscriber of the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;
 - g. use by a subscriber of a private key to create a digital signature when the related certificate is expired, suspended or revoked;
 - h. attempt by a subscriber to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network.
8. *Payment terms.* RA will invoice LRA for all fees set forth in paragraph 1, and LRA will pay the fees within thirty

(30) days of LRA's receipt of the invoice for such fees. If fees are not paid in accordance with this paragraph, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

9. LRA has reviewed the Kansas CP requirements and agrees that the following level of certificate is appropriate for the business application subject to this agreement:

- 1
- 2
- 3
- 4

10. *Confidentiality.* Any request by either party for treatment of information as confidential shall be resolved by application of the provisions of the Kansas open record act (KORA). KSA 45-215 *et seq.*

11. *Export compliance.* This agreement expressly is made subject to any laws, regulations, orders or other restrictions on the export from the United States of America of software, hardware, or technical information, which may be imposed from time-to time by the government of the United States of America. Regardless of any disclosure made by LRA to RA of an ultimate destination of the software, hardware, or technical information and, notwithstanding anything contained in this agreement to the contrary, LRA will not modify, export, or re-export, either directly or indirectly, any software, hardware, or technical information, or portion thereof, without first obtaining any and all necessary licenses from the United States government or agencies or any other country for which such government or any agency thereof requires an export license or other governmental approval at the time of modification, export, or re-export.

12. *Notices.* All notices, demands, requests, approvals, reports, instructions, consents or other communications which may be required or desired to be given by one party to the other shall be in writing and addressed to the RA or LRA administrators as follows:

RAA name: _____	LRAA name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____

The RAA(s) or LRAA(s) identified above is the individual authorized to request of the RA issuance or other appropriate action concerning certificates related to this agreement.

13. The parties agree that each of them shall maintain copies of all active agreements and records related to PKI services that are subject to this agreement (*e.g.* agreements required by ITEC policy 9200 and vetting documentation, among other), and they further agree that such agreements and records shall be maintained for a period not fewer than five (5) years from and after their expiration dates or periods of effectiveness. The records shall be secured pursuant to standards that are commercially reasonable within the industry. They shall be maintained in the form of paper-based documents, retrievable computer-based documents or any form of reproduction approved by the Secretary of State. They shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible for audit by the Secretary of State.

14. *Compliance with laws.* Each party agrees that it shall comply with the CP and all applicable federal, state and local laws, regulations, ordinances and codes in connection with its performance under this agreement.

15. *Assignment.* The parties agree that any rights under this agreement are not assignable or transferable.

16. *Severability.* If any provision of this agreement, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this agreement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

17. *Force majeure.* Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this paragraph (a) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (b) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event the force majeure event described in this paragraph extends for a period in excess of thirty (30) days in aggregate, the other party immediately may terminate this agreement.

18. *Termination.* Because of the State of Kansas' interest in the security of the trusted network, if LRA violates any condition of this agreement, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

RA
by _____
title _____
signature _____

LRA
by _____
title _____
signature _____

12.2

AGREEMENT between RA and LRA

(Trusted partner involved)

This agreement is entered into this ____ day of _____, 20__ by and between the Information Network of Kansas, registration authority (RA) for the State of Kansas, and _____, _____ (address), local registration authority (LRA).

The parties agree as follows:

1. Subject to the terms and conditions of this agreement, RA agrees to furnish registration authority services for the LRA for the period from _____, 20__ through _____, 20__ at the following price: \$__ per PKI certificate per year.
2. The parties agree that this agreement is subject to state contract 04294 for digital signature services, the Information Technology Executive Council (ITEC) policy 9200 and its *Certificate Policy for the State of Kansas Public Key Infrastructure* (CP) as amended. <http://da.ks.gov/itec>
3. The parties understand and agree that the provisions set out in the DA146a, attached; the CP; and any modifications to this agreement are incorporated and made a part of this contract by reference as though fully set forth herein. The parties agree that these documents are listed in their order of precedence and that these documents are controlling over any other document.
4. The business conducted by LRA and its trusted partner subscriber for which the PKI services will be used is a lawful business. The LRA and its trusted partner subscriber have executed the AGREEMENT between LRA and Trusted Partner Subscriber governing the business to be conducted, which is attached hereto. (If LRA has executed multiple and identical agreements with trusted partners, LRA may attach one copy of the agreement and a list of the trusted partners and their addresses.)
5. *Limitations on use.* The parties agree that certificates issued under the trusted network are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage. RA is not responsible for assessing the appropriateness of the use of a certificate. The parties agree that they will not use or rely upon certificates beyond the limitations set forth in this agreement.
6. RA agrees to process applications for trusted partner subscriber certificates upon a request from the LRA. The LRA agrees to submit such request in the form approved by the RA. Because of the State of Kansas' interest in the security of the trusted network, the LRA agrees to exercise due diligence in vetting the subscribers in accordance with the CP.
7. LRA agrees that it immediately will report to RA any breach or suspected breach of security by its individual trusted partner subscribers. The latter includes, but is not limited to, the following:
 - a. inaccurate information provided by a subscriber in response to a certificate application;
 - b. infringement upon the intellectual property rights of any third parties resulting from information provided by a subscriber (including an e-mail address);
 - c. use by a subscriber of certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;
 - d. failure by a subscriber to remain the only person in possession of the private key and the only person with access to the private key;
 - e. failure by a subscriber to remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;
 - f. use of a subscriber of the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;
 - g. use by a subscriber of a private key to create a digital signature when the related certificate is expired, suspended or revoked;
 - h. attempt by a business partner subscriber to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network.

8. *Payment terms.* RA will invoice LRA for all fees set forth in paragraph 1, and LRA will pay the fees within thirty (30) days of LRA's receipt of the invoice for such fees. If fees are not paid in accordance with this paragraph, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

9. LRA has reviewed the Kansas CP requirements and agrees that the following level of certificate is appropriate for the business application subject to this agreement:

- 1
- 2
- 3 currently not available
- 4 currently not available

10. *Confidentiality.* Any request by either party for treatment of information as confidential shall be resolved by application of the provisions of the Kansas open record act (KORA). KSA 45-215 *et seq.*

11. *Export compliance.* This agreement expressly is made subject to any laws, regulations, orders or other restrictions on the export from the United States of America of software, hardware, or technical information, which may be imposed from time-to time by the government of the United States of America. Regardless of any disclosure made by LRA to RA of an ultimate destination of the software, hardware, or technical information and, notwithstanding anything contained in this agreement to the contrary, LRA will not modify, export, or re-export, either directly or indirectly, any software, hardware, or technical information, or portion thereof, without first obtaining any and all necessary licenses from the United States government or agencies or any other country for which such government or any agency thereof requires an export license or other governmental approval at the time of modification, export, or re-export.

12. *Notices.* All notices, demands, requests, approvals, reports, instructions, consents or other communications which may be required or desired to be given by one party to the other shall be in writing and addressed to the RA or LRA administrators as follows:

RAA	LRAA
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____

The RAA(s) or LRAA(s) identified above is the individual authorized to request of the RA issuance or other appropriate action concerning certificates related to this agreement.

13. The parties agree that each of them shall maintain copies of all active agreements and records related to PKI services that are subject to this agreement (*e.g.* agreements required by ITEC policy 9200 and vetting documentation, among other), and they further agree that such agreements and records shall be maintained for a period not fewer than five (5) years from and after their expiration dates or periods of effectiveness. The records shall be secured pursuant to standards that are commercially reasonable within the industry. They shall be maintained in the form of paper-based documents, retrievable computer-based documents or any form of

reproduction approved by the Secretary of State. They shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible for audit by the Secretary of State.

14. *Compliance with laws.* Each party agrees that it shall comply with the CP and all applicable federal, state and local laws, regulations, ordinances and codes in connection with its performance under this agreement.

15. *Assignment.* The parties agree that any rights under this agreement are not assignable or transferable.

16. *Severability.* If any provision of this agreement, or the application thereof is for any reason and to any extent found to be invalid or unenforceable, the remainder of this agreement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

17. *Force majeure.* Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this paragraph (a) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (b) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event the force majeure event described in this paragraph extends for a period in excess of thirty (30) days in aggregate, the other party immediately may terminate this agreement.

18. *Termination.* Because of the State of Kansas' interest in the security of the trusted network, if LRA violates any condition of this agreement, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

RA
by _____
title _____
signature: _____

LRA
by _____
title _____
signature: _____

12.3

AGREEMENT between LRA and Trusted Partner Subscriber

This agreement is entered into this ___ day of _____, 20__ by and between _____, _____ (address), local registration authority (LRA), and _____, _____ (address), trusted partner subscriber (subscriber).

The parties agree as follows:

1. The business conducted by LRA and subscriber to which the services will be dedicated is a lawful business.
2. The parties agree that this agreement is subject to state contract 04294 for digital signature services, the Information Technology Executive Council (ITEC) policy 9200 and its *Certificate Policy for the State of Kansas Public Key Infrastructure* (CP) as amended. <http://da.ks.gov/itec>
3. The parties understand and agree that the provisions set out in the DA146a, attached; the CP; and any modifications to this agreement are incorporated and made a part of this contract by reference as though fully set forth herein. The parties agree that these documents are listed in their order of precedence and that these documents are controlling over any other document.
4. To facilitate the issuance of certificates to subscriber, LRA agrees to vet subscriber's credentials and submit them in the proper form to the Kansas registration authority (RA). Subscriber agrees to provide LRA accurate vetting information in accordance with the CP. In order to ensure protection of the Kansas trusted network, the parties agree they will diligently observe the security provisions of the Kansas CP and this agreement.
5. *Limitations on use.* The parties agree that certificates issued under the trusted network are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage. RA is not responsible for assessing the appropriateness of the use of a certificate. The parties agree that they will not use or rely upon certificates beyond the limitations set forth in this agreement.
6. Trusted partner subscriber agrees that subscriber and its individual trusted partner subscribers immediately will report to LRA and RA any breach or suspected breach of security by its subscribers. The latter includes, but is not limited to, the following:
 - a. inaccurate information provided by a subscriber in response to a certificate application;
 - b. infringement upon the intellectual property rights of any third parties resulting from information provided by a subscriber (including an e-mail address);
 - c. use by a subscriber of certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;
 - d. failure by a subscriber to remain the only person in possession of the private key and the only person with access to the private key;
 - e. failure by a subscriber to remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;
 - f. use of a subscriber of the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;
 - g. use by a subscriber of a private key to create a digital signature when the related certificate is expired, suspended or revoked;
 - h. attempt by a subscriber to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network.
7. *Indemnity.* Subscriber agrees to release, indemnify, defend and hold harmless LRA and RA from all liabilities, claims, damages, costs and expenses, including reasonable attorney's fees and expenses relating to or arising out of this agreement or the breach of subscriber warranties, representations and obligations under this agreement.

8. The parties have reviewed the Kansas CP requirements and agree that the following level of certificate is appropriate for the business application subject to this agreement

- 1
- 2
- 3 currently not available.
- 4 currently not available.

9. *Confidentiality.* Any request by either party for treatment of information as confidential shall be resolved by application of the provisions of the Kansas open record act (KORA). KSA 45-215 *et seq.*

10. *Export compliance.* This agreement expressly is made subject to any laws, regulations, orders or other restrictions on the export from the United States of America of software, hardware, or technical information, which may be imposed from time-to time by the government of the United States of America. Regardless of any disclosure made by subscriber to LRA of an ultimate destination of the software, hardware, or technical information and, notwithstanding anything contained in this agreement to the contrary, subscriber will not modify, export, or re-export, either directly or indirectly, any software, hardware, or technical information, or portion thereof, without first obtaining any and all necessary licenses from the United States government or agencies or any other country for which such government or any agency thereof requires an export license or other governmental approval at the time of modification, export, or re-export.

11. *Notices.* All notices, demands, requests, approvals, reports, instructions, consents or other communications which may be required or desired to be given by one party to the other shall be in writing and addressed to the LRA and subscriber administrators as follows:

LRAA	Subscriber Administrator
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____
name: _____	name: _____
e-mail: _____	e-mail: _____
signature: _____	signature: _____

The LRAA(s) or Subscriber Administrator(s) identified above is the individual authorized to request of the RA issuance or other appropriate action concerning certificates related to this agreement.

12. The parties agree that each of them shall maintain copies of all active agreements and records related to PKI services that are subject to this agreement (*e.g.* agreements required by ITEC policy 9200 and vetting documentation, among other), and they further agree that such agreements and records shall be maintained for a period not fewer than five (5) years from and after their expiration dates or periods of effectiveness. The records shall be secured pursuant to standards that are commercially reasonable within the industry. They shall be maintained in the form of paper-based documents, retrievable computer-based documents or any form of reproduction approved by the Secretary of State. They shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible for audit by the Secretary of State.

13. *Compliance with laws.* Each party agrees that it shall comply with the CP and all applicable federal, state and local laws, regulations, ordinances and codes in connection with its performance under this agreement.

14. *Assignment.* The parties agree that any rights under this agreement are not assignable or transferable.

15. *Severability.* If any provision of this agreement, or the application thereof is for any reason and to any extent found to be invalid or unenforceable, the remainder of this agreement and the application of the invalid or unenforceable provision to other persons or circumstances shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

16. *Force majeure.* Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this paragraph (a) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (b) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event the force majeure event described in this paragraph extends for a period in excess of thirty (30) days in aggregate, the other party immediately may terminate this agreement.

17. *Termination.* Because of the State of Kansas' interest in the security of the trusted network, if subscriber violates any conditions of this agreement, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

LRA
by _____
title _____
signature: _____

Trusted Party Subscriber
by _____
title _____
signature: _____

INDIVIDUAL SUBSCRIBER AGREEMENT

Certificate subscribers must read and execute the following subscriber agreement before accepting or using a State of Kansas digital certificate.

This subscriber agreement will become effective on the date you accept your State of Kansas digital certificate from the state registration authority (RA).

The State of Kansas digital certificate services are governed by state contract 04294 for digital signature services, the Information Technology Executive Council (ITEC) policy 9200 and its *Certificate Policy for the State of Kansas Public Key Infrastructure* (CP), as amended. <http://da.ks.gov/itec>

The RA provides limited warranties, disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability and excludes all liability for incidental, consequential and punitive damages as stated in the CP.

As a subscriber, you agree to use the certificate and any related registration authority services only in accordance with the CP and amendments and applicable law.

As a subscriber, you demonstrate your knowledge and acceptance of the terms of this subscriber agreement by accepting a digital certificate from the State of Kansas RA and by using the certificate.

As a subscriber, you warrant that you:

- a. have provided accurate information in response to a certificate application;
- b. upon issuance of a certificate naming you as the subscriber, have reviewed the certificate information to ensure that all subscriber information included in it is accurate and have expressly indicated acceptance or rejection of the digital certificate;
- c. have not infringed upon the intellectual property rights of any third parties by providing information that would do so (including an e-mail address);
- d. have not and will not use certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;
- e. will remain the only person in possession of the private key and the only person with access to the private key;
- f. will remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;
- g. will not use the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;
- h. will not use a private key to create a digital signature when the related certificate is expired, suspended or revoked;
- i. will not attempt to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network;
- j. will inform the RA within 48 hours of a change to any information included in the certificate or certificate application request; and
- k. immediately will report to the RA any breach or suspected breach of security concerning digital certificate services of which the subscriber becomes aware, including but not limited to those listed in this section.

Signed _____

Date _____

Authentication Assurance Levels and Risk Assessments

Introduction

This document is designed to assist Kansas state agencies when assessing the level of electronic authentication assurance that may be needed for applications involving an electronic transaction with a private entity or federal, state agency, county or local organization. This document describes four identity authentication assurance levels for e-government “transactions” as established by the Office of Management and Budget M-04-04. KSA 2003 Supp. 16-1601 et. seq provides the rules governing electronic transactions for the State of Kansas. Further, KSA 2003 Supp. 16-1618 assigns the administrative oversight and administration regulation creation to the Secretary of State. For a review of the rules and regulations governing the Kansas Uniform Electronic Transactions Act, please refer to KAR 7-41-1 through KAR 7-41-33 and KAR 7-43-1 through 7-43-6.

Description of Assurance Levels

Each authentication assurance level describes the agency's degree of certainty that the user has presented an identifier that refers to his or her identity. In this context, assurance is defined as

- 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and
- 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

The four assurance levels are:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Reasonable confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

Risks, Responses, Potential Impacts, Probability and Assurance Levels

While, this guidance addresses only general principles for identifying those potential risks associated with electronic authentication, NIST Special Publication 800-30, “Risk Management Guide for Information Technology Systems,” recommends a general methodology for managing risk in Federal and State information systems. In addition, other means of risk management, (e.g., network access restrictions, intrusion detection, and event monitoring) may help reduce the need for higher levels of authentication assurance.

Risk Response: There are generally four things we can do about risk:

- **Avoid the Risk** – Is there anything we can do to remove the risk entirely?
- **Transfer the Risk** – Can we make someone else responsible for the risk?
- **Mitigate the Risk** – What can we do to lessen the impact of the risk if it occurs?
- **Accept the Risk** – Is the type of risk such that we will simply accept it or cost/benefit analysis does not justify the cost of the steps required to completely mitigate it and plan to deal with it if it occurs?

Potential Impact Categories: To determine the appropriate level of assurance in the user's asserted electronic identity; agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially more serious consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

- a) potential harm or impact, and
- b) the *probability* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information

- Personal safety
- Civil or criminal violations
- Binding Transactions

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are:

- Low impact
- Moderate impact
- High impact.

The next section defines the potential impacts for each category. Note: If authentication errors cause no measurable consequences for a category, there is "no" impact.

Determining Potential Impact of Authentication Errors:

Potential impact of *inconvenience, distress, or damage to standing or reputation*:

- **Low**—at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- **Moderate**—at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **High**—severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

Potential impact of *financial loss*:

- **Low**—at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- **Moderate**—at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High**—severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

Potential impact of *harm to agency programs or public interests*:

- **Low**—at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness or (ii) minor damage to organizational assets or public interests.
- **Moderate**—at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness or (ii) significant damage to organizational assets or public interests.
- **High**—a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions or (ii) major damage to organizational assets or public interests.

Potential impact of *unauthorized release of sensitive information*:

- **Low**—at worst, a limited release of personal, U.S. government-sensitive or commercially-sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.
- **Moderate**—at worst, a release of personal, U.S. government-sensitive, or commercially-sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.
- **High**—a release of personal, U.S. government-sensitive or commercially-sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

Potential impact to *personal safety*:

- **Low**—at worst, minor injury not requiring medical treatment.

- **Moderate**—at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- **High**—a risk of serious injury or death.

Potential impact of *civil or criminal violations* is:

- **Low**—at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- **Moderate**—at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- **High**—a risk of civil or criminal violations that are of special importance to enforcement programs.

Potential impact of *binding transactions*

- Low – the transaction with the user does not require signature to be binding to entities
- Moderate – the transaction with the user does require signature to be binding to entities

Risk Probability Quantification.

Once risks are identified and the potential impacts are categorized, each impact needs to be quantified with the probability of it occurring. This can be done ad hoc for each risk by a group of experienced managers, users, IT staff and perhaps vendor, using a simple scale of “High, Moderate, or Low” for each dimension of risk, (impact and probability) or using a simple matrix where probability is measured along one axis and impact along the other. Note that if impact is high, even if probability is low, it’s a high priority risk. Even a remote chance of a serious problem requires serious attention to the risk.

Probability	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	High
Low	Low	Moderate	High

Determining Authentication Assurance Level:

Compare the impact and probability profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (as noted in step 2 below).

Table 1 – Maximum Potential Impacts for Each Authentication Assurance Level

Potential Impact Categories for Authentication	Authentication Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	LOW	MOD	MOD	HIGH
Financial loss or agency liability	LOW	MOD	MOD	HIGH
Harm to agency programs or public interests	N/A	LOW	MOD	HIGH
Unauthorized release of sensitive information	N/A	LOW	MOD	HIGH

Personal Safety	N/A	N/A	LOW	MOD HIGH
Civil or criminal violations	N/A	LOW	MOD	HIGH
Binding Transactions	LOW	MOD	MOD	MOD

In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms to agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

In some cases (as shown in Table 1), impact may correspond to multiple assurance levels.

For example, Table 1 shows that a moderate risk of financial loss corresponds to assurance levels 2 and 3. In such cases, agencies should use the context to determine the appropriate assurance level.

Determining Assurance Levels and selecting authentication solutions using Risk

Assessment agencies shall use the following steps to determine the appropriate assurance level:

Step 1: Conduct a risk assessment of the e-government system. Guidance for agencies in conducting risk assessments is available in A-130, Section 5 of OMB's Government Paper Elimination Act (GPEA) guidance and NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems." These risk assessments will assist in the agency's measurement of the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error. Note: An E-government system may have multiple categories or types of transactions, which may require separate analysis within the overall risk assessment. An E-government system may also span multiple agencies whose activities may require separate consideration by each agency.

Risk analysis is to some extent a subjective process, in which agencies must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. Agencies should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process. It is better to be over-inclusive than under-inclusive in conducting this analysis. Once risks have been identified, there may also be ways to adjust the business process to mitigate particular risks by reducing the likelihood that they will occur (see Step 4).

Step 2: Map identified risks to the required assurance level. The risk assessment should be summarized in terms of the potential impact categories. To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact and probability category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact together with the probability are appropriate for Level 1, and one category of potential impact and probability is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

Step 3: Select technology based on the NIST e-authentication technical guidance. After determining the assurance level, the agency should refer to the NIST e-authentication technical guidance to identify and implement the appropriate technical requirements.

Step 4: After implementation, validate that the information system has operationally achieved the required assurance level. Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the system's authentication requirements as part of required security procedures (e.g., certification and accreditation).

Step 5: Periodically reassess the information system to determine technology refresh requirements. The agency must periodically reassess the information system to ensure that the identity authentication requirements

continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

Assurance Levels and Risk Profiles: Descriptions and Examples

Based upon the score of your risk profile, as identified in Table 1, the following levels and suggested authentication methods are provided as guidance to agencies for determining the appropriate level of authentication for access to the respective application.

Level 1—*Little or no confidence exists in the asserted identity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.*

Acceptable Authentication Methods:

- No authentication
- Pin and Password
- PKI Certificate (Level 1)

Examples:

- In some instances, the submission of forms by individuals in an electronic transaction will be a Level 1 transaction: (i) when all information is flowing to the State organization from the individual, (ii) there is no release of information in return, and (iii) the criteria for higher assurance levels are not triggered. For example, if an individual applies to a State agency for an annual park visitor's permit (and the financial aspects of the transaction are handled by a separate contractor and thus analyzed as a separate transaction, the transaction with the State agency would otherwise present minimal risks and could be treated as Level 1.
- A user presents a self-registered user ID or password to an agency web page, which allows the user to create a customized web page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal.
- A user participates in an online discussion on the agency website, which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.

Level 2—*On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any State action).*

Acceptable Authentication Methods:

- PIN and Strong Password and/or
- PKI Certificate (Level 2)
 - Physical Vetting
 - RA to LRA Agreement
 - LRA/Business or other Trusted Partner Subscriber Agreement
 - Individual Subscriber Agreement

Examples:

- A user subscribes to an Online Learning Center. The site's training service must authenticate the person to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student's privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.
- A beneficiary changes her address of record through an agency web site. The site needs authentication to ensure that the entitled person's address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the

beneficiary's address of record, it entails moderate risk of unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication.

- An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate.
- An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create *moderate* potential impact for unauthorized release, but the system's security measures reduce the overall risk to *low*.

Level 3—*Level 3 is appropriate for transactions needing high confidence in the asserted identity's accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.*

Acceptable Authentication Methods:

- PIN and Strong Password and
- PKI Certificate (Level 3)
 - Physical Vetting
 - RA to LRA Agreement
 - LRA/Business or other Trusted Partner Subscriber Agreement
 - Individual Subscriber Agreement

Examples:

- Security System Administrators
- A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office. Improper disclosure would give competitors a competitive advantage.
- A supplier maintains an account with a Department of Administration Procurement Office for a large government procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate.
- A First Responder accesses a disaster management reporting website to report an incident, share operational information, and coordinate response activities.
- An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. He works in a restricted-access State office building. This limits physical access to his computer, but system transactions occur over the Internet. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.

Level 4—*Level 4 is appropriate for transactions needing very high confidence in the asserted identity's accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls.*

Acceptable Authentication Methods:

- Smart Cards, Hardware Tokens, Biometrics, Busses, among other storage devices and/or
- PKI Certificate (Level 4)
 - Physical Vetting
 - RA to LRA Agreement
 - LRA/Business or other Trusted Partner Subscriber Agreement
 - Individual Subscriber Agreement

Examples:

- KDOR: FM Secure – Fed/State Offset Program
- KBI: CJIS Hard Token/Continual Hashing
- A law enforcement official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations.
- A pharmacist dispenses a controlled drug. She would need full assurance that a qualified doctor prescribed it. She is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount.
- An agency investigator uses a remote system giving her access to potentially sensitive personal client information. Using her laptop at client worksites, personal residences, and businesses, she accesses information over the Internet via various connections. The sensitive personal information she can access creates only a moderate potential impact for unauthorized release, but her laptop's vulnerability and her non-secure Internet access raise the overall risk.

References:

Executive Office of the President, Office of Management and Budget, Dec. 2003, Document ID: M-04-04, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems, February 2004, <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

National Institute of Standards and Technology, US Department of Commerce, Risk Management Guide for Information Technology Systems, Document ID: 800-30, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

Kansas Information Technology Executive Council, Certificate Policy for the State of Kansas Public Key Infrastructure, Document ID: Policy #5200A, http://www.da.ks.gov/itec/documents/itecitpolicy5200_A1.pdf

Enterprise Project Management Office, Feasibility Study Reports 2.4, <http://www.da.ks.gov/kito/ITProposedPlans.htm>

Enterprise Project Management Office, IT Project Planning Instructions (Revised July 2006), <http://www.da.ks.gov/kito/ITProposedPlans.htm>

Kansas Information Technology Executive Council, Project Management, Document ID: Policy #2530, <http://www.da.ks.gov/itec/Documents/itecitpolicy2530.htm>

OMB Circular A-130 Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf

OMB Circular A-130 Appendix II, Implementation of the Government Paperwork Elimination Act and III, <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf>

OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, http://www.whitehouse.gov/omb/circulars/a130/appendix_iii.pdf

OMB Memorandum No. 99-20, Security of Federal Automated Information Resources, http://www.cio.gov/archive/m_99_20_security_of_it_resources.html

Midwest Tax Council, Project Risk Management, DRAFT, 9/26/2006

15 Bibliography

15.1 See the following for KS laws on electronic transaction and signatures:

Kansas Uniform Electronic Transactions Act (KUETA), KSA 16-1601 et seq.

<http://www.kslegislature.org/legsrv-statutes/statutesList.do>

KUETA regulations, KAR 7-41-4 through 7-41-33

<http://www.kslegislature.org/legsrv-kars/search.do?kar=/7-41-1.html>

Kansas Electronic Notarization regulations, KAR 7-43-1 through 7-43-6

15.2 See the following for information on KS and federal PKI:

<http://www.kansas.gov/pki>

<http://www.cio.gov/fpkipa/>

15.3 See the following articles for fundamental issues related to KS PKI infrastructure and identity management:

Risk and Trust Management Techniques for an "Open But Bounded" Public Key Infrastructure, Daniel J. Greenwood, 38 Jurimetrics J. 277-294 (1998)

<http://www.usenix.org/events/ec98/pki/greenwood.pdf>