CMS

Illinois Department of
Central Management Services

State of Illinois
Public Key Infrastructure
Certification Practices Statement
For Digital Signature
And Encryption Applications Version 3.9
(IETF RFC 3647 format)

July 7, 2016

Redacted

This document contains practices used to meet Certificate Policy. As such some information in this Certification Practices Statement may be considered sensitive. In an effort to provide a publicly available version of this document some content has been redacted or removed.

Table of Contents

1. INTRODUCTION

This introduction is intended to be a layman's description of the State of Illinois Public Key Infrastructure (PKI). This introduction is not intended to describe the policies and procedures that govern PKI. Policies and procedures are described throughout the rest of this document and those sections govern all PKI operations.

The State of Illinois has created a Public Key Infrastructure to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies. This document and the associated Certification Practice Statement describe the policies and procedures that govern operation of the State of Illinois PKI. PKI provides tools that can identify users to an electronic application, that can help enforce or apply confidentiality and privacy requirements, and that provides electronic signatures that comply with the Federal E-Sign Act and the State of Illinois' Electronic Commerce Security Act (5 ILCS 175).

A Public Key Infrastructure includes many participating entities. The Certification Authority (CA) for the State of Illinois PKI is operated by the Department of Innovation & Technology. Policies and procedures for PKI are developed and approved by the Policy Authority (PA), which includes representatives from several State agencies. Subscribers are individuals who register and are issued digital certificates. A Relying Party is an entity that uses the digital certificates as part of an electronic process.

Public Key Infrastructure uses the technology of public key encryption to provide functionality to users and applications. Users (whether individuals, electronic applications, or devices) are registered and two encryption keys are created – one held privately by the user and one made publicly available. The keys are mathematically related in that each operates as the inverse of the other; however the value of one key cannot be determined by analyzing the other. The public key is also contained in the digital certificate, which is issued to the user by CA. This digital certificate contains information which identifies the user to the Certificate Authority (CA) and links the user's keys to that identity. The State of Illinois PKI operates using a model commonly referred to as a "dual key pair" in which registered users are issued one digital certificate consisting of a corresponding public/private key pair for encryption and a second corresponding public/private key pair for signature purposes. Data that is encrypted using a given public key can only be decrypted using the corresponding private key. Likewise, a digital signature created using a given private key can only be verified by using the corresponding public key.

Digital certificates that are issued by Certificate Authorities (CA's) are identified according to how rigorously the user is authenticated during the registration process. This identification is called the assurance level and can be used to determine whether a certificate can be relied on as part of a given process. High risk or highly sensitive transactions typically require a higher assurance level while a lower level of assurance may suffice for more mundane processes.

Subsequent sections of this document describe requirements, obligations, and procedures for each participant in PKI. More detailed and specific descriptions of the procedures are included in the associated Certification Practice Statement.

1.1 OVERVIEW

This Certification Practice Statement (CPS) describes the practices of the Certificate Authority (CA) operated by the State of Illinois Central Management Services ("State"). This CPS is applicable to all entities with relationships with the State CA, including end users, Registration Authorities (RAs) and Local Registration Authorities (LRAs). This CPS provides those entities with a clear statement of the practices and responsibilities of the State CA, as well as the responsibilities of each entity in dealing with the State CA.

Section 25-105 of the Illinois Electronic Commerce Security Act (5 ILCS 175/25-105 provides that the Illinois Department of Central Management Services (CMS) will have the exclusive authority to specify the policies and procedures for the issuance and use of digital signatures by State Agencies. The Certificate Policy (CP) and the Certification Practices Statement (CPS) are CMS's written description of the policies and procedures for the issuance and use of digital signatures. The Director of CMS has delegated responsibility for implementation and maintenance of the CP and the CPS to the State of Illinois Certificate Policy Authority (PA).

1.1.1 Certificate Policy (CP)

Each of the Certificate Policies supported by the State CA, and covered by this CPS, identifies the suitable applications for that Certificate Policy.

1.1.2 Relationship between the Illinois CP & the Illinois CPS

This CPS is called the State of Illinois Certificate Authority Certification Practices Statement for Digital Signatures and Encryption Applications. It is the supporting 'how to' document to the governing Illinois PKI certificate policy. This CPS is administered by the State PKI Operational Authority (OA) and is based on the policies agreed to by the State PKI Policy Authority (PA).

1.1.3 Relationship between the Illinois CP and Entity CP

The Illinois Policy Authority maps Entity CP(s) to one or more of the levels of assurance in the Illinois CP. The relationship between those CPs and the Illinois Root CA will be asserted in CA certificates in the *policyMappings* extension.

1.1.4 Scope

This CPS is managed by the State of Illinois Operational Authority (OA) and adheres to the policies established by the State of Illinois Policy Authority (PA). Contact information for these authorities is provided in section 1.5.2 below.

This CPS is applicable to all Certificates issued by the State CA, including those issued under the ‘Certificate Policy for Digital Signature and Encryption Applications’ policy.

The practices described in the CPS apply to the issuance and use of Certificates and Certificate Revocation Lists (CRLs) for users within the State CA domain.

1.1.5 Interaction with PKIs External to the State of Illinois

No Stipulation.

1.2 DOCUMENT NAME & IDENTIFICATION

This CPS is called the State of Illinois Certificate Authority Certification Practice Statement for Digital Signature and Encryption Applications.

This CPS is managed by the State of Illinois Operational Authority (OA) and adheres to the policies established by the State of Illinois Policy Authority (PA). Contact information for these authorities is provided in section 1.5 below.

The State CA issues Certificates for use in verification of digital signatures and Certificates for use in encryption. The State CA supports several Certificate Policies that cover both of these applications. Practices that differ from this policy are clearly indicated in this CPS. The Certificate Policies supported by the State CA and for which its practices are described in this CPS are identified below. Please refer to section 7.1.2.8 to see how the assurance level is linked to how the assurance level is defined for the subscriber certificates:

Certificate Policies for Digital Signature and Encryption Applications

Assurance Level	Object Identifier
Level-1 (software-based)	2.16.840.114273.1.1.1.1
Level-1 (hardware based)	2.16.840.114273.1.1.1.2
Level-2 (software-based)	2.16.840.114273.1.1.1.3
Level-2 (hardware based)	2.16.840.114273.1.1.1.4
Level-3 (software-based)	2.16.840.114273.1.1.1.5
Level-3 (hardware based)	2.16.840.114273.1.1.1.6
Level-4 (hardware token only)	2.16.840.114273.1.1.1.7
MEDI Single-Use	2.16.840.114273.1.1.2.1
SHA256-Level-1 (software-based)	2.16.840.1.114273.3.1.1.1
SHA256-Level-1 (hardware based)	2.16.840.1.114273.3.1.1.2
SHA256-Level-2 (software-based)	2.16.840.1.114273.3.1.1.3
SHA256-Level-2 (hardware based)	2.16.840.1.114273.3.1.1.4
SHA256-Level-3 (software-based)	2.16.840.1.114273.3.1.1.5

SHA256-Level-3 (hardware based)	2.16.840.1.114273.3.1.1.6
SHA256-Leve-4 (hardware token only)	2.16.840.1.114273.3.1.1.7
SHA256-MEDI Single-Use	2.16.840.1.114273.3.1.2.1

Unless stated otherwise in this document, the requirements for SHA256 assurance levels are the same as for their SHA1 corresponding levels.

1.3 PKI PARTICIPANTS

The sub-sections that follow describe in general terms, the functions of the major components of the PKI.

There is, created by the CP and this CPS, a State of Illinois Operational Authority (OA.) The Director of CMS will have supervisory responsibility for the OA. The OA will be responsible for interpretation of the certificate policies as stated by the PA, the creation and management of the CPS, and the correct operation of the State PKI, in accordance with the provisions of the CP and the CPS. The CMS Security Administrator will oversee the operations of the State PKI. The CMS PKI registration authority (RA) will manage the operations of the State PKI. CA functions described in the CP and the CPS will be performed by PKI Administrators. Registration Authority functions described in the CP and CPS may be delegated to Local Registration Authorities (LRAs.) Figure 1 illustrates the CMS organizational structure relating to the operation and management of the State CA.

In the State PKI, there are three Master Users who also serve as System Administrators. The OA manager will have Security Officer privileges. The PKI Operational Authority staff has Administrator privileges. The Agency/entity Local Registration Authorities are limited to performing Registration Authority functions while the CMS Internal Auditors and External Auditors would be granted read-only access.

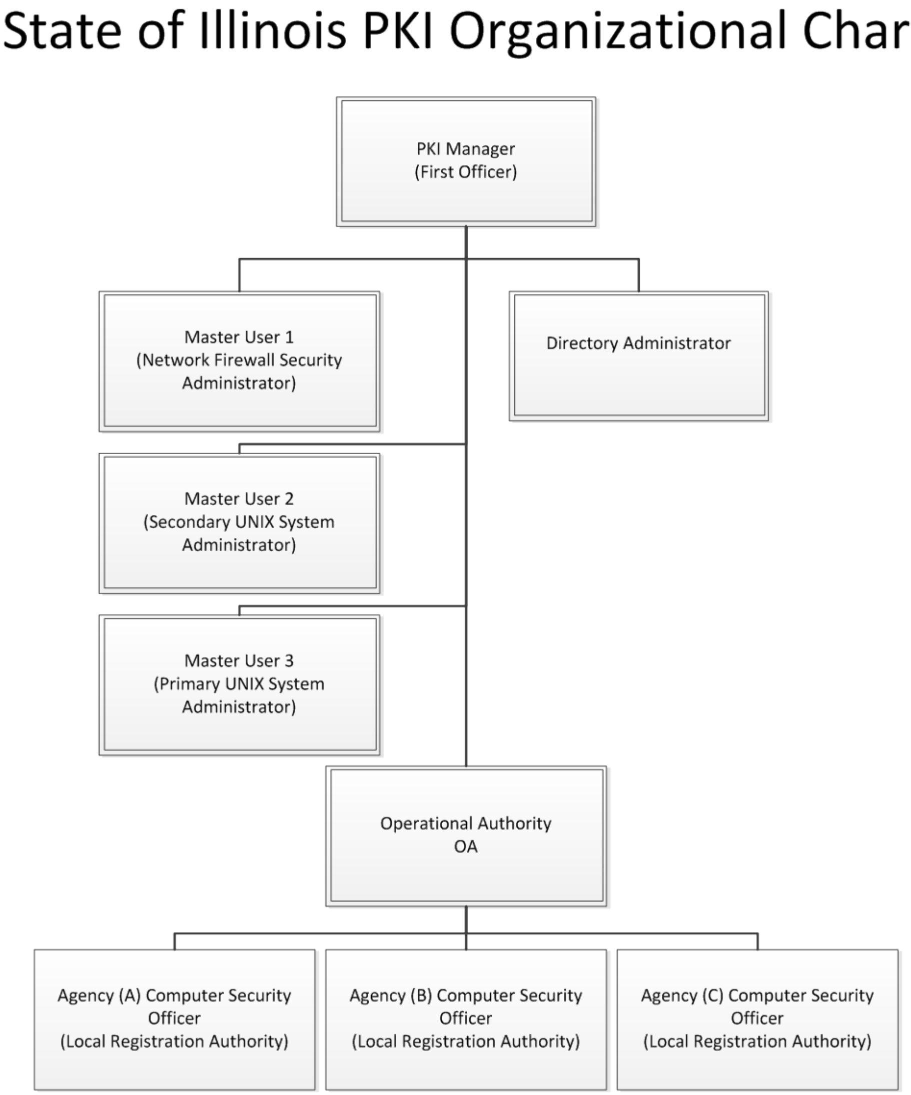
State of Illinois PKI Organizational Chart
PKI Manager (First Officer)
Master User 1 (Network Firewall Security Administrator)
Directory Administrator
Master User 2 (Secondary UNIX System Administrator)
Master User 3 (Primary UNIX System Administrator)
Operational Authority OA
Agency (A) Computer Security Officer (Local Registration Authority)
Agency (B) Computer Security Officer (Local Registration Authority)
Agency (C) Computer Security Officer (Local Registration Authority)

Figure 1

1.3.1 Certification Authorities

The State operates a single CA, which issues user Certificates to State Employees and other entities which conduct business with the State.

The State CA is operated using Entrust release 8.1 SP1 software and the CA is represented in the architecture by Entrust/Security Manager™. The authorized State personnel access Entrust/Security Manager™ via the Entrust/SMA interface to initiate and perform CA functions.

1.3.1.1 *Policy Authority ("PA")*

The State of Illinois Policy Authority is responsible for the certificate policy that governs this CPS. This CPS is updated by the OA to align practices with new or revised policy requirements released by the PA. The OA will continue to operate from the latest approved CPS until the PA has approved and issued the updated CPS to the OA.

The Policy Authority is responsible for:

- Dispute resolution.
- Selecting and/or defining Certificate Policies, in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527), for use in the Certificate Authority PKI or organizational enterprise.
- Approving of any interoperability agreements with external Certificate Authorities.
- Approving practices, which the Certificate Authority must follow by reviewing the Certification Practice Statement to ensure consistency with the Certificate Policies.
- Providing Policy direction to the Certificate Authority (CA) and the Operational Authority.
- Conducting policy mappings based on framework standards RFC 3647

The PA will be comprised of representatives of participating units of Illinois State government. The Director of CMS will have the exclusive authority to appoint and remove members of the PA. Members of the PA (or their designees) will have the authority to implement, maintain, and modify the CP and the CPS, and will perform all other duties required of them by the terms of the CP and the CPS.

1.3.1.2 *Operational Authority ("OA")*

The following chart illustrates the relationships of CMS individuals to PKI roles.

State Individual	Entrust Role
PKI Manager/Certificate Authority Administrator/Program Manager, Department of Innovation& Technology	Security Officer
Directory Administrator, Department of Innovation & Technology	CMS Administrator
Firewall Administrator	Master User 1
SUN System Administrator	Master User 2
Primary UNIX System Administrator	Master User 3
PKI System Administrator	CMS Administrator

Registration Authority	
Agency Assigned Individual	LRA

Where necessary, this CPS distinguishes the different users and roles accessing Entrust/Security Manager™ for CA functions. Where this distinction is not required, the term CA is used to refer to the total CA entity, including the software and its operations.

A public website is also maintained which contains links, policies, etc. vital to the PKI community. This website is located at www.illinois.gov/pki (redirects to: https://www2.illinois.gov/sites/doit/services/catalog/security/Pages/pki.aspx).

1.3.1.3 *Illinois Operational Authority Program Manager*

The Program Manager is the individual within the Illinois PKI Operational Authority who has principal responsibility for overseeing the proper daily operation of the Illinois PKI in accordance with this CPS.

1.3.1.4 *Entity Principal Certification Authority (CA)*

This entity is responsible for the day to day operation of the Illinois PKI, and for ensuring its availability to its subscribers, customers, and relying parties. As such, this entity has high privileges that allow them to perform these functions.

1.3.1.5 *Certificate Status Servers*

No CSS systems are in place and are not applicable to this PKI domain. When a CSS is implemented the requirements for compliance will have to be met as defined in the Illinois CP.

1.3.2 Registration Authority (RA)

The Registration Authority has privileges that are a proper subset of the Security Officer privileges as outlined in section 5.2.1 of this CPS. The State RA makes use of authorized individuals to function as Local Registration Authorities to verify the identity and roles of End Entities throughout the various State agencies and business partners, in accordance with the State of Illinois Certificate Policy.

1.3.2.1 *Local Registration Authority*

Each Agency will designate one or more individuals to perform the role of the Local Registration Authority within that agency, and has privileges that are a proper subset of Security Officer privileges as outlined in section 5.2.1 of this CPS. In this CPS, the term Local Registration Authority (LRA) is used to refer to an individual performing RA functions, while RA is used to refer to the total RA entity, including the software and its operations.

1.3.3 Subscribers

This CPS will be binding on each Subscriber that applies for and/or obtains Certificates, by virtue of the Subscriber Agreement, and governs each applicant's performance with respect to their application for, use of, and reliance on, Certificates issued by the CA. The Subscriber agreement may be viewed at http://www2.illinois.gov/PKI/Pages/pki_subscriber.aspx.

1.3.3.1 *End Entities*

End-Entities in this PKI may include State employees, individuals conducting electronic business with the State, hardware devices and/or specific applications. At the discretion of the PA, any person entity, hardware device or specific application may be a Subscriber (relying party taken out) (collectively referred to as an "End Entity") in the State PKI. End-Entities may also use Certificates issued by the CA to encrypt information for, and verify the digital signatures of, other End-Entities within the State PKI.

1.3.4 Relying Parties

An entity that needs to rely on a certificate issued by the State of Illinois PKI, but chooses not to use the Illinois recommended products for certificate verification and validation, is defined by the State of Illinois as a relying party. These entities are in a position to rely on the certificates presented to them, and have agreed to be bound by the terms of the CP. The term "Relying Parties" is also used for entities that wish to use State of Illinois certificates, but do not wish to use any of the software available from the State PKI. In these instances, the entity is responsible for all certificate verification, including certificate revocation list checking, certificate validation date checking and any checks necessary to validate the trustworthiness of the end user certificate. These entities must sign a Relying Party agreement as provided by the State PKI.

By accepting a certificate issued pursuant to the provisions of this CP, a relying party agrees to be bound by the provisions of the CP. The following factors, among others are significant in evaluating the reasonableness of a recipient's reliance upon a certificate, and upon digital signatures verifiable with reference to the public key listed in the certificate:

- Facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference;
- The value or importance of the digitally signed message, if known;
- The course of dealing between the relying person and the subscriber, and the available indicia of reliability or unreliability apart from the digital signature;
- The usage of trade, particularly trade conducted by trustworthy systems or other computer based means.

1.3.5 Other Participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

This CPS is applicable to all Certificates issued by the State CA, including those issued under the ‘Certificate Policy for Digital Signature and Encryption Applications’ policy. The practices described in the CPS apply to the issuance and use of Certificates and Certificate Revocation Lists (CRLs) for users within the State CA domain. The Illinois PKI has issued one level 4 certificate to the IRCA, thus allowing the CA to operate at a high assurance level. All controls applicable to “high assurance” or “Level 4” are being applied to the hosting and protection of the Illinois root CA.

1.4.2 Prohibited Certificate Uses

Each of the Certificate Policies supported by the State CA, and covered by this CPS, identifies the suitable applications for that Certificate Policy. Any use of the State of Illinois certificate used in any illegal activities or illegal gains is prohibited and if detected the certificate will be revoked according to the procedures set forth in this CPS. State of Illinois certificates are to be used only for use of and/or interaction with Illinois Governmental entities, and not for private use.

1.4.3 Appropriate Certificate Usage per Assurance Level

The Illinois PKI allows the user entities to make the final determination as to the assurance level needed by their applications. Suggestions are provided in the CP in section 1.4.3.

1.5 POLICY ADMINISTRATION

The State of Illinois Policy Authority is responsible for the certificate policy that governs this CPS. This CPS is updated by the OA to align practices with new or revised policy requirements released by the PA. The OA will continue to operate from the latest approved CPS until the PA has approved and issued the updated CPS to the OA.

1.5.1 Organization administering the document

This CPS is administered by the State PKI Operational Authority (OA) and is based on the policies agreed to by the State PKI Policy Authority (PA).

1.5.2 Contact Person

The contact details for the CPS and PKI will be noted in a Memorandum for Record (MFR) and retained by the OA. This MFR will be in accordance with the template provided in Appendix 5.

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

This Certification Practice Statement is administered by the PA. The Operational Authority is responsible for operating the components of the Illinois PKI in compliance of this CPS as defined by the requirements stated in the Certificate Policy (CP). This will be done via a vote and approval process on all proposed changes.

The PA is responsible for approving and authorizes any CPS before the OA is bound by its guidance. The CPS conforms to the CP and is validated annually by the mandated compliance audit that is conducted. Upon receiving the annual audit, Illinois will electronically provide this document to cross0certified entities or as per any memorandum of agreements.

1.5.4 CPS Approval Procedures

In order to allow entities to modify their procedures as needed, all changes to this document will become effective 30 days after final publication on the State Repository (https://www2.illinois.gov/sites/doit/services/catalog/security/Pages/pki.aspx). It will be the responsibility of each Subscriber or Relying Party to periodically check this Repository for notices associated with this document and Illinois PKI activities. The use of or reliance upon a certificate after the 30-day comment period, regardless of when the certificate was issued, will be deemed acceptance of the modified terms and therefore binding arbitration has occurred by the parties.

The State PA approves this CPS. The State PA must approve any subsequent changes prior to promulgation or activities performed by the OA. The express waiver by the State or the Policy Authority of any provision, condition, or requirement of this CPS will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

1.6 DEFINITIONS AND ACRONYMS

See Sections 11 and 12.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

CMS will maintain a Certificate Repository containing information pertaining to State Certificates.

2.1 REPOSITORIES

The repository for the Illinois Root CA is provided by an X.500 directory system. The protocol used to access the Directory is the Lightweight Directory Access Protocol (LDAP) version 2 or higher.

The syntax of an LDAP call from a web browser to the repository to retrieve information is as follows:

Ldap://server.cmcf.state.il.us:389/full DN of object being retrieved.

The public LDAP repository will contain public keys and certificate revocation lists, as well as profiles (doubly encrypted) for roaming users.

2.1.1 Repository Obligations

The Entrust software contains an internal database that immediately publishes information to a public LDAP repository that supports the State PKI and maintains availability, reliability, and sufficient protections for its contents. The public LDAP repository will contain public keys and certificate revocation lists, as well as profiles (doubly encrypted) for roaming users.

A public website is also maintained which contains links, policies, etc. vital to the PKI community. This website is located at https://www2.illinois.gov/sites/doit/services/catalog/security/Pages/pki.aspx

2.2 PUBLICATION OF CERTIFICATION INFORMATION

This detailed CPS is not published publicly.

The following PKI information is published in the State Directory:

- all encryption public key Certificates issued by the State CA to PKI users;
- all revocations of PKI user public key Certificates performed by the State CA;
- all revocations of cross-certification certificates issued by the CA;
- Roaming profiles.

2.2.1 Publication of Certificates and Certificate Status

This CPS is re-issued and published as necessary. Certificates are published in the Directory as they are issued. CRLs are automatically published in the Directory as they are issued by the Entrust/Security Manager™ software. The frequency of CRL is discussed in Section 4.9.7 of this CPS. This information is accessible in the State of Illinois directory using the LDAP protocol.

2.2.2 Publication of CA Information

In order to allow entities to modify their procedures as needed, all changes to this document will become effective 30 days after final publication on the State Repository (https://www2.illinois.gov/sites/doit/services/catalog/Documents/SoI-CP-V4.1.pdf). It will be the responsibility of each Subscriber or Relying Party to periodically check this Repository for notices associated with this document and Illinois PKI activities. The use of or reliance upon a certificate after the 30-day comment period, regardless of when the certificate was issued, will be deemed acceptance of the modified terms and therefore binding arbitration has occurred by the parties. Refer to section 9.12.1 for information regarding the amending of the CPS.

The State PA approves this CPS. The State PA must approve any subsequent changes prior to promulgation or activities performed by the OA. The express waiver by the State or the Policy Authority of any provision, condition, or requirement of this CPS will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

2.2.3 Interoperability

Any certificates, CRLs, or other public information stored in the directory will be stored using standards based schemas for objects and attributes.

2.3 FREQUENCY OF PUBLICATION

This CPS is re-issued and published as necessary. Certificates are published in the Directory as they are issued. CRLs are published in the Directory as they are issued. The frequency of CRL is discussed in Section 4.9.7 of this CPS.

2.4 ACCESS CONTROLS ON REPOSITORIES

The State of Illinois Operational Authority will protect any information not intended for public dissemination or modification by utilizing data encryption and physically secured storage mechanisms. Public keys and certificate status information in the State of Illinois repository will be publicly available through the Internet. The use of certificates to access information in Agency repositories will be determined by the Agency pursuant to its authorizing and controlling statutes. These statutes include the following:

- 815 ILCS 530/Personal Information Protection Act
- 5ILCS 160/State Records Act
- 720 ILCS 5/Article 17, Subdivision 30 Computer Fraud
- 5 ILCS 175/State of Illinois Electronic Commerce and Security Act

The State of Illinois PKI utilizes shadow directories to make repository information available to subscribers, relying parties, and others who need access to public certificates or revocation lists. These shadow directories are read-only copies of the master repository, and are updated immediately as the master repository is updated.

3. IDENTIFICATION AND AUTHENTICATION

Subject to the requirements noted below, applications for State Certificates may be communicated from the applicant to the State RA or a State LRA and authorizations to issue State Certificates may be communicated from an authorized State LRA to the State CA, (1) electronically, provided that all communication is secure, or (2) in person.

The State CA expects to process three types of registrations:

- Web registration (both in-state and out-of-state recipients).
- Face-to-face registration authorized by the State RA or a State LRA.
- Bulk registration. Using a secure means determined on a case by case basis, authorized LRAs will authorize the issuance of Certificates to large groups of Subscribers that they have registered and communicate these to the State RA.

3.1 NAMING

Subject to the requirements noted below, applications for State Certificates may be communicated from the applicant to the State RA or a State LRA and authorizations to issue State Certificates may be communicated from an authorized State LRA to the State CA, (1) electronically, provided that all communication is secure, or (2) in person.

The State CA expects to process three types of registrations:

- Web registration (both in-state and out-of-state recipients).
- Face-to-face registration authorized by the State RA or a State LRA.
- Bulk registration. Using a secure means determined on a case by case basis, authorized LRAs will authorize the issuance of Certificates to large groups of Subscribers that they have registered and communicate these to the State RA

3.1.1 Types of Names

Names for Certificate issuers and Certificate subjects are of the X.500 Distinguished Name (DN) form.

The format used by this Certificate Authority is as follows:

DN:serialNumber=99999999+cn=common name,ou=??,ou=People,ou=CMS,o=State of Illinois,c=US

Where: serialNumber=99999999 is an 8 digit number assigned by the OA to ensure uniqueness.

Cn=common name of the requestor

Ou=?? Is an organizational unit based on the first letter of the person's last name

All other attributes are constant. All attributes are as defined in ITU-T Recommendation X.521.

The Illinois PKI will only generate and sign certificates that contain a non-null subject Distinguished Name (DN), as that is a mandatory certificate attribute for the Illinois PKI. This is controlled programmatically through the on-line registration system requiring all entries for the DN to be created.

3.1.2 Need for Names to Be Meaningful

The value of the commonName attribute used is the name by which the Certificate subject is officially known within the client organization.

3.1.3 Anonymity or Pseudonymity of Subscribers

The State of Illinois PKI does not allow Anonymity of subscribers. Certificate names of device certificates will be constructed so that the agency owning or responsible for the device is easily ascertained.

3.1.4 Rules for Interpreting Various Name Forms

In a Certificate, the issuer DN and subject DN fields contain the full X.500 Distinguished Name of the Certificate issuer or Certificate subject. If the subjectAltName extension is present in a Certificate, it contains the Certificate subject's rfc822Name (email address).

3.1.5 Uniqueness of Names

Names are unambiguously defined for each object in the naming hierarchy. The common name (cn) will be a combination of first name(s) and surname. Middle initials and other identifiers may also be used. The serialNumber attribute within the DN is used to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity {serialNumber must be a sequential counter number – 8 digits; devices may use MAC number from the network interface device}. This combination of serial number/MAC address plus the common name will guarantee uniqueness among the distinguished names.

3.1.6 Recognition, Authentication, & Role of Trademarks

The Illinois PKI will not seek any evidence that a subject's name is a registered trademark.

3.2 INITIAL IDENTITY VALIDATION

The RA and appropriate LRAs will accept certificate applications from state employees or individuals who need to conduct electronic business with the State of Illinois through three primary registration means: web, in-person and bulk applications.

Web registration is available for users of Agency-based web applications. The registration process is handled entirely through the internet, with the applicant providing necessary identification information on a web form. The RA validates the identity information provided by the applicant against one or more trusted data sources.

A web registration process is available for out-of-state residents who desire a State of Illinois digital certificate. This process instructs the recipient to download a form, take it to a notary public, present proper identification, and have the form notarized. This form is then mailed to the OA, where activation codes are created and distributed to the recipient in a secure manner. These codes are then entered into a secure web page to generate the certificate. All out-of-state certificates are created as a level 1 certificate as described in section 3.2.3.

In-person applications will be accepted by the RA or any authorized LRA. The applicant must submit a completed State of Illinois Digital Certificate Application in person at the time of application.

Bulk applications for state agency staff or other definable groups of individuals will be accepted by the RA from appropriate LRAs in accordance with procedures developed on a case by case basis. Certificates will be issued at the assurance level determined from evaluating the authentication provided by the bulk registration process using the authentication requirements described in Section 3.2.3.

For each Certificate application, prospective Subscribers will satisfy the following requirements:

- Provide proof of identity as required in Section 3.2.3
- Submit a completed State of Illinois Digital Certificate Application to the RA or appropriate LRA;
- Indicate agreement with the terms and conditions for use of the State's public key infrastructure as described in the Subscriber's Agreement;
- Initialize the client software on their workstation (if appropriate); and,
- Demonstrate to the RA that the private keys have been successfully installed.

3.2.1 Method to Prove Possession of Private Key

Digital Certificates bind a public key to the identity of the individual to assure Relying Parties that encryption or signing performed by the private key was done by the individual whose public key appears on the Certificate. This requires that an individual safeguard their profile and Entrust password and that the CA require proof of possession of the private key before creating and signing a Certificate containing the associated public key. Proof of possession of private key is handled automatically by the operations of the PKIX.

For the signature private key, a PKIX operation initiated by the Subscriber is digitally signed using the signature private key itself.

For the decryption private key, this key is transferred to the Subscriber, together with the corresponding Certificate, in a PKIX operation, which is digitally signed by the State CA.

3.2.2 Authentication of Organization Identity

The State of Illinois PKI does not issue certificate to organizations.

3.2.3 Authentication of Individual Identity

Removed

3.2.3.1 *Authentication of Human Subscribers*

Refer to section 3.2.3.

3.2.3.2 *Authentication of Human Subscribers For Group Certificates*

Illinois does not issue group certificates.

3.2.3.3 *Authentication of Devices*

Application for a device or an application to be an End-Entity must be made by an individual to whom the device or application’s signature is attributable for the purposes of accountability and responsibility. If the certificate is generated manually, the identity of the certificate is bound to the public keys generated by the OA member during the certificate generation process of Entrust Security Manager Administration™. If the certificate is generated via Entrust Enrollment Server for Web™, the identity is bound to the certificates via the CMP protocol used during the certificate creation process.

Identification and authentication of the applicant follows section 4.1.1 of this CPS as if the organization or individual were applying for a Certificate on their own behalf. In addition, an LRA, the RA or PA must verify the authority of the individual to receive Certificates for that device or application and authorize the issuance of the certificate. Identification and authentication procedures are dealt with in section 3.2.3 of this CPS. The application should be from a properly vetted, registered PKI sponsor, commiserate with the assurance level of the certificate being issued for the device.

Device certificates will be valid for 3 years. At this time, the viability of this certificate must be validated by the responsible LRA. Device certificates will be assigned a level-1 assurance level.

3.2.4 Non-verified Subscriber Information

Non-verifiable information will not be included in Illinois PKI certificates.

3.2.5 Validation of Authority

For cross-certification, the State of Illinois Policy Authority will validate the representative’s authorization to act in the name of the organization. For device certificates, the Local Registration Authority will be validated before the certificate is issued by comparing the LRA signature to the list of valid LRA’s maintained by the OA. This validation can take the form of emails, telephone conversations, and letters provided on entity letterhead.

3.2.6 Criteria for Interoperation

The State of Illinois Operational Authority will determine the operational criteria required for cross-certification, keeping in mind the best interests of the State of Illinois. These criteria will be then be presented to the PA for review.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

For cross-certification relationships, no automatic key update process is applied. If the State PA determines that a cross-certification agreement is to extend beyond the original period, a new cross-certificate is issued, prior to expiration of the current one. The same identification and authentication process used for initial cross-certification agreements applies to the issuance of new keys.

A provision of cross-certification with the Federal Bridge requires subscribers to be re-authenticated after nine years.

3.3.1 Identification and Authentication for Routine Re-key

Removed

3.3.1.1 *Routine Re-key – Device or Application*

Removed

3.3.2 Identification and Authentication for Re-key after Revocation

For users whose Certificates have been revoked, recovery after revocation will not be permitted until the identification and authentication requirements for initial registration described in section 3.2.3 of this CPS are repeated. Registration Authorities may allow exceptions only in the following situation:

- A certificate holder is temporarily unable to present themselves in person (e.g. on extended travel) and the revocation was not due to a key compromise.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Removed

3.4.1.1 *Involuntary recovery at governmental entity request*

- A Governmental entity may request involuntary recovery of a Subscriber’s private encryption keys if that person is or has recently been employed by the entity, the entity has reason to believe that data necessary to agency operations has been encrypted using the Subscriber’s keys, and the entity is unable to contact the Subscriber or the Subscriber is unable or unwilling to decrypt the data.
- The entity’s request will be made in writing to the PA, describing why the Subscriber’s private encryption key is necessary to entity operations and specifying what use will be made of the key. The request will be signed by the Director of the Agency. The Subscriber’s keys will not be recovered until said request is reviewed by the PA or those designated by the PA to review such requests.
- Prior to recovering the Subscriber’s profile, the CA will alter the Distinguished Name by appending the word “Recovered”, then the Subscriber’s Certificate will be recovered and the profile will be

delivered to the entity LRA on physical media. The LRA will sign for receipt of the profile, will supervise all entity use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked.

No recovery will be performed until the request has been approved by the Policy Authority.

3.4.1.2 *Involuntary recovery by court order*

- The PA and OA will comply with all official, authorized, and verified court orders to recover a Subscriber's keys.
- Prior to recovering the Subscriber's profile, the CA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA will sign for receipt of the profile, will supervise all Agency use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked.

4. CERTIFICATE LIFE-CYCLE

4.1 APPLICATION

Removed

4.1.1 Application of Behalf of a Device, Software Application, or process

Rmoved

4.1.2 Application for a Cross Certificate

Removed

4.2 CERTIFICATE APPLICATION PROCESSING

Refer to section 3.2.3.

4.2.1 Performing Identification and Authentication Functions

Removed

4.2.2 Approval or Rejection of Certificate Applications

The Illinois OA may approve or reject certificate applications. Applications may be rejected if they are incomplete, illegible, or give the OA reason to believe that the application is invalid or fraudulent.

4.2.3 Time to Process Certificate Applications

Removed

4.3 ISSUANCE

Removed

4.3.1 CA Actions during Certificate Issuance

Removed

4.3.2 Notification to Subscriber of Certificate Issuance

Once a certificate is issued to an individual, a “congratulations” message is displayed, indicating that the certificate has been created.

4.4 CERTIFICATE ACCEPTANCE

As the PKIX operations are themselves secured and the two entities (Subscriber and CA) authenticated, successful completion of the PKIX request and response operations constitutes acceptance by the user of the resulting public key Certificates. By accepting the State Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the State Certificate are true. Subscribers must either agree to the subscriber agreement online before creating a certificate, or must sign a copy of the certificate application form which contains the subscriber agreement. Either of these actions will indicate acceptance of the terms of the agreement.

Subscribers are bound by the subscriber agreement found at http://www2.illinois.gov/PKI/Pages/pki_subscriber.aspx. Continued use of or reliance on a certificate after the 30 day waiting period as described in the State of Illinois Certificate Policy section 8.1.2 will be deemed acceptance of the modified terms.

4.4.1 Conduct constituting certificate acceptance

For the Illinois PKI, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.4.1.1 *Multiple certificates caused by different registration methods*

Due to differences between the original certificate creation method and the web registration model, some recipients have received multiple certificates (i.e., same common name with a different serial number). This generally occurs when someone has undergone a face-to-face registration and activation codes have been generated, but the recipient has never activated their certificate. In this case, the old entries in the database and directory are removed. If the older certificate has been created, further checking is done to see if the certificate has been used for signing or encryption. If not, the older certificate is archived (since no key compromise is suspected). If the older certificate has been used, then the new certificate is archived.

4.4.2 Publication of the Certificate by the CA

Once created, the public portions of the certificate are posted in the repository. If the certificate is a “roaming” certificate, then the actual certificate (doubly-encrypted) is stored in the repository.

4.4.3 Notification of Certificate Issuance by the CA to other entities

For end-entity certificates, no stipulation. For CA certificates, any other cross-certified CA will be given notice of new cross-certifications.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

All certificate subscribers should protect their private keys from access by other parties This can be achieved by not providing their PIN/password to others, and by maintaining physical control of hardware tokens and smartcards. Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate. For end-entities that utilize Entrust products (either the desktop suite or Truepass™), all certificate validation is performed automatically.

Certificates issued by the Illinois PKI can only be used for State/Governmental business. Private use of the certificate and associated software is prohibited.

4.5.2 Relying Party Public key and Certificate Usage

Relying parties will rely on a valid Certificate for purposes of verifying the digital signature only if prior to reliance, the Relying Party will:

(1) Agreed to be bound by the terms of this CP;

(2) Verified the digital signature by reference to the public key in the Certificate; and

(3) Referred to the most recent CRL.

Relying party understands that certificates are subject to revocation and such action will not be reflected in the Certificate itself, but must be verified by consulting the most recent certificate revocation list.

Certificates issued by the Illinois PKI can only be used for State/Governmental business. Private use of the certificate and associated software is prohibited.

4.6 CERTIFICATE RENEWAL

Removed

4.6.1 Circumstance for Certificate Renewal

Removed

4.6.2 Who may request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a Renewal certificate

Not applicable.

4.6.6 Publication of the Renewal certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to other entities

Not applicable.

4.7 CERTIFICATE RE-KEY

Removed

4.7.1 Circumstance for Certificate Re-key

Removed

4.7.2 Who may request certification of a new public key

Removed

4.7.3 Processing certificate Re-keying requests

For both CAs and end-entities, the Illinois PKI Operational Authority will identify and authenticate Principal CAs by either manual or automated means. This identification can take the form of emails, telephone conversations, certificate thumbprints, and letters provided on entity letterhead.

4.7.4 Notification of new certificate issuance to Subscriber

For CA certificates, the requesting CA will be notified of the re-keying of a new certificate. For end-entities, no stipulation.

4.7.5 Conduct constituting acceptance of a Re-keyed certificate

For the Illinois PKI, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed certificate by the CA

All CA and end-entity certificates will be published in the Illinois PKI repository.

4.7.7 Notification of certificate issuance by the CA to other Entities

The Illinois PKI Operational Authority will inform any cross-certified entity of any new cross-certificate issuance or rekey.

For Entity CAs, no stipulation.

4.8 MODIFICATION

Removed

4.8.1 Circumstance for Certificate Modification

Removed

4.8.2 Who may request Certificate Modification

Removed

4.8.3 Processing Certificate Modification Requests

Removed

4.8.4 Notification of new certificate issuance to Subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

For the Illinois PKI, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the modified certificate by the CA

All updated certificates are published in the Illinois PKI repository.

4.8.7 Notification of certificate issuance by the CA to other Entities

Notification will be given to any cross-certified entity if another cross-certificate is modified. For end-entities, no stipulation..

4.9 CERTIFICATE REVOCATION & SUSPENSION

4.9.1 Circumstance for Revocation

Removed

4.9.2 Who can request Revocation

Removed

4.9.3 Procedure for Revocation Request

Removed

4.9.4 Revocation Request Grace Period

Removed

4.9.5 Time within which CA must Process the Revocation Request

Removed

4.9.6 Revocation Checking Requirements for Relying Parties

CRL checking is done automatically by the CA software.

4.9.7 CRL Issuance Frequency

Removed

4.9.8 Maximum Latency of CRLs

Removed

4.9.9 On-line Revocation/Status Checking Availability

Not supported.

4.9.10 On-line Revocation Checking Requirements

Not supported.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.11.1 Checking requirements for other forms of revocation advertisements

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

Removed

4.9.13 Circumstances for Suspension

The Illinois PKI does not support the suspension of certificates.

4.9.14 Who can Request Suspension

No stipulation

4.9.15 Procedure for Suspension Request

No stipulation

4.9.16 Limits on Suspension Period

No stipulation

4.10 CERTIFICATE STATUS SERVICES

The Illinois PKI does not support Certificate Status Services.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW & RECOVERY

The Illinois PKI does not utilize key escrow.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

The focus of physical security controls is to minimize exposure from environmental hazards and malicious actions that could harm data or information, severely delay the timeliness of processing, or threaten the safety of personnel.

5.1 PHYSICAL CONTROLS

Subscribers and Relying Parties will be made aware of any security practices they need to follow in the protection of their computers and cryptographic devices. The LRA is responsible for communicating these practices to all Subscribers and Relying Parties within its domain.

5.1.1 Site Location & Construction

Removed

5.1.2 Physical Access

Removed

5.1.2.1 *Physical Access for CA Equipment*

- Removed

5.1.2.2 *Physical Access for RA Equipment*

The RA and LRAs will implement at a minimum the following controls:

- Removed

5.1.2.3 *Physical Access for CSS Equipment*

No Stipulation.

5.1.2.4 *Physical Security Controls for Subscribers*

Removed

5.1.3 Power and Air Conditioning

Removed

5.1.4 Water Exposures

Removed

5.1.5 Fire Prevention & Protection

Removed

5.1.6 Media Storage

Removed

5.1.7 Waste Disposal

Removed

5.1.8 Off-Site backup

Removed

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Removed

5.2.2 Number of Persons Required per Task

Removed

5.2.3 Identification and Authentication for Each Role

Refer to section 3.2.3 of this CPS for identification and authentication procedures for individuals filling the Trusted Roles in the State PKI.

5.2.4 Separation of Roles

Removed

5.3 PERSONNEL CONTROLS

Removed

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

Removed

5.3.2 Background Check Procedures

Removed

5.3.3 Training Requirements

CA and RA personnel will receive proper (informal, formal, or on-the-job training) and continuous training in relation to their assigned duties as well as disaster recovery, business continuity, and system administration. Documentation will be maintained identifying all personnel receiving training and the level of training completed and maintained by the Security Officer.

5.3.4 Retraining Frequency & Requirements

All Operational Authority members will receive proper and continuous training in relation to their assigned duties throughout the calendar year. Documentation will be maintained identifying all personnel receiving training and the level of training completed.

5.3.5 Job Rotation Frequency & Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any member of the Operational Authority performing unauthorized functions will have their role changed so that rights to administrative functions are removed. Additionally, disciplinary action may be pursued depending on the severity of the action.

5.3.7 Independent Contractor Requirements

Removed

5.3.8 Documentation Supplied To Personnel

Removed

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

Removed

5.4.2 Frequency of Processing Log

Removed

5.4.3 Retention Period for Audit Logs

Removed

5.4.4 Protection of Audit Logs

Removed

5.4.5 Audit Log Backup Procedures

Removed.

5.4.6 Audit Collection System (internal vs. external)

Removed

5.4.7 Notification to Event-Causing Subject

Removed

5.4.8 Vulnerability Assessments

The State of Illinois Operational Authority will review system and application logs in accordance with section 5.4.2. This assessment activity is the internal audit activity related to the Illinois PKI. This activity in conjunction with the external compliance audit satisfies the auditing requirements for a High assurance CA.

5.5 RECORDS ARCHIVE

Removed

5.6 KEY CHANGEOVER

The PKI Security Administrator and Certificate Authority Administrator Certificates are set up for automatic key update. As such, both the encryption and digital signature key pairs are automatically updated prior to expiry.

5.6.1 Recovery at Subscriber Request

When a subscriber requests that their own profile be recovered due to the subscriber no longer being able to access his/her private keys due to the password being lost or the electronic file being corrupted, the subscriber must provide proof of identity through secured shared secrets or other authentication prior to recovery of the Subscriber's profile. The recovery will then be performed using the following procedures:

- If the subscriber is in possession of an Illinois driver's license or identification card, they will perform a self-recovery by accessing the web site www.illinois.gov/pki (redirects to the following page: https://www2.illinois.gov/sites/doit/services/catalog/security/Pages/pki.aspx)and choosing the "forgot password" link.
- If the subscriber does not possess an Illinois driver's license or identification card, the user must contact the Operational Authority, who will verify their identity against the paper application forms. Once the subscriber's identification has been verified, the subscriber will be manually put into a key recovery state by an OA member. One of the authentication codes will be provided to the user at the time of the identification verification, and the other will be emailed to the subscriber, along with a URL to visit to complete the key recovery.

5.6.2 Involuntary Recovery at State Agency Request

Removed

5.6.3 Involuntary Recovery by Court Order

The PA and OA will comply with all official, authorized, and verified court orders to recover a Subscriber's keys.

5.7 COMPROMISE & DISASTER RECOVERY

In the event of a disaster or serious compromise, the following steps, as a minimum, are taken to recover a secure environment:

- Removed

5.8 CA & RA TERMINATION

Removed:

6. TECHNICAL SECURITY CONTROLS

The State will implement comprehensive technical controls for the State PKI, will ensure that the system is continuously operated within the approved security parameters and that all required technical controls remain in place and properly configured.

6.1 KEY PAIR GENERATION & INSTALLATION

Removed

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

Removed

6.2.2 Private Key Multi-Person Control

Removed

6.2.3 Private Key Escrow

Escrow of private keys by an external third party is not performed.

6.2.3.1 *Escrow of Illinois CA private signature key*

The Illinois PKI does not utilize key escrow.

6.2.3.2 *Escrow of Illinois CA encryption keys*

The Illinois PKI does not utilize key escrow.

6.2.3.3 *Escrow of Subscriber private signature keys*

The Illinois PKI does not utilize key escrow.

6.2.3.4 *Escrow of Subscriber private encryption and dual use keys*

The Illinois PKI does not utilize key escrow.

6.2.4 Private Key Backup

Removed

6.2.5 Private Key Archival

Removed

6.2.6 Private Key Transfer into or from a Cryptographic Module

Removed

6.2.7 Private Key Storage on Cryptographic Module

Removed

6.2.8 Method of Activating Private Keys

Removed

6.2.9 Methods of Deactivating Private Keys

Removed

6.2.10 Method of Destroying Private Keys

Removed

6.2.11 Cryptographic Module Rating

Removed

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

Removed

6.3.2 Certificate Operational Periods/Key Usage Periods

Removed.

6.4 ACTIVATION DATA

6.5 COMPUTER SECURITY CONTROLS

Removed

6.6 LIFE-CYCLE SECURITY CONTROLS

The effectiveness and appropriateness of the security settings described in this CPS are reviewed as part of the audit procedures specified in the CP.

6.6.1 System Development Controls

Removed

6.6.2 Security Management Controls

Removed

6.6.3 Life Cycle Security Ratings

Not applicable: Dependent on vendor standards.

6.7 NETWORK SECURITY CONTROLS

Removed

6.8 TIME STAMPING

Removed

7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

Removed

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

In order to ensure compliance with policies and practices, an annual compliance audit will be conducted of the State of Illinois PKI in accordance with Certificate Policy section 8.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

Removed

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

Removed

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Removed

8.4 TOPICS COVERED BY ASSESSMENT

The annual audit will investigate the operations of the CA and RA functions of the State PKI to ensure their compliance with the CP and the CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Removed

8.6 COMMUNICATION OF RESULTS

Results of the annual audit will be provided to the State PA, Removed

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

No direct fees will be assessed by the CA or OA.

In cross-certification or hosting agreements with business partner organizations, the costs will be expected to balance naturally between the State and the business partner organization. Any exceptions, which may result in additional fees for any of the services outlined in this section and its subsections, will be addressed in the specific cross-certification agreement itself.

9.1.1 Certificate Issuance/Renewal Fees

The Illinois PKI will issue, renew, and revoke Subscribers certificates at no cost.

9.1.2 Certificate Access Fees

The Illinois PKI will not impose any certificate access fees on Subscribers with respect to its own Certificate(s) or the status of such Certificate(s).

9.1.3 Revocation or Status Information Access Fee

The State will not impose fees for certificate revocation or status services.

9.1.4 Fees for other Services

The Illinois PKI will not impose fees for access to policy information.

9.1.5 Refund Policy

Because no fees will be charged for certificate services, as specified in this CPS or by the Illinois PKI, there is no need to provide procedures for refunds.

9.2 FINANCIAL RESPONSIBILITY

No stipulation.

Interested parties will refer to section 9.2 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

The State of Illinois PKI will maintain the confidentiality of certain information in accordance with Certificate Policy section 9.3 and its sub-sections. In accordance with Certificate Policy section 9.3, the CA, RA, or any LRA will not disclose certificate or certificate-related information to any third party except when:

- authorized to do so by the CP,
- required to be disclosed by law or court order, or
- authorized to do so by the certificate holder

Any requests for disclosure of information must be signed and submitted to the CA. The CA will communicate all such requests to the PA. The Policy Authority Chairperson should be the initial contact point, and the request will then be passed to CMS legal to approve FOIA disclosure of information.

All subscriber information is considered confidential and is kept under lock and key. Only members of the Operational Authority have access to the subscriber information.

9.3.1 Scope of Confidential Information

In accordance with Certificate Policy section 9.3, the following provisions will apply:

The Subscriber’s private signing key must be kept confidential by the Subscriber. The CA and RA are not provided any access to those keys. The Subscriber’s private encryption key must be kept confidential by the Subscriber; however, the CA may recover private encryption keys for State of Illinois employees as described in Section 4.7 (Key Recovery) of the CP. Personal information held by the CA, other than that which is explicitly published as part of a certificate, CRL, certificate policy, or this document is considered confidential and will not be released unless required by law.

In addition, personal information submitted to the CA by Subscribers:

- Is made available to the subscriber for individual review following an authenticated request by said subscriber;
- Is subject to correction and/or update by said subscriber; and
- Is protected by the CA in such a way as to ensure the integrity of said collected personal identifiable information.

9.3.2 Information not within the scope of Confidential Information

Information included in public certificates and CRLs issued by the CA are not considered confidential. Likewise, information contained in the public repository is not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

When a certificate is revoked by the CA, a revocation reason code will be included in the CRL entry for the revoked certificate. This revocation reason code is not considered confidential and can be shared with all users and Relying Parties. No other details concerning the revocation of a certificate will be disclosed by the Illinois PKI.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information treated as Private

All subscriber information should be treated as private information. As such, it should be stored in a locked cabinet in a room which can be locked when staff is not present.

9.4.3 Information not deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Sensitive information will be stored securely, and may be released only in accordance with other stipulations in Section 9.4.7 of the Certificate Policy.

9.4.5 Notice and Consent to use Private Information

For information related to this topic, the enquiring party should refer to the Illinois certificate policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

- The PA and OA will comply with all official, authorized, and verifiable court orders to recover a Subscriber's keys.
- Prior to recovering the Subscriber's profile, the CA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA will sign for receipt of the profile, will supervise all Agency use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked following the procedures in Section 4.9 "Certificate Revocation".

- A Subscriber whose profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 3.3 to be re-authenticated and issued a new Certificate.

9.4.7 Other Information Disclosure Circumstances

If a subpoena seeking information that is considered confidential under the Certificate Policy is provided to the Operational Authority, the Operational Authority will consult with legal counsel and will follow whatever directives are given by said counsel.

No Stipulation for owner request for disclosure.

9.5 INTELLECTUAL PROPERTY RIGHTS

No stipulation.

9.6 REPRESENTATIONS & WARRANTIES

9.6.1 CA Representations and Warranties

The OA’s responsibility is to “Provide CA services with a maximum available application target of 100% and allowing for normal maintenance” (CP section 9.6.1). To accomplish this task, the following steps will be taken:

9.6.2 RA Representations and Warranties

Removed

9.6.2.1 *Disclaimers*

No stipulation.

9.6.2.2 *Loss Limitations*

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.8 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP

9.6.2.3 *Other Exclusions*

No stipulation.

9.6.2.4 *Hazardous Activities*

No stipulation.

9.6.3 Subscriber Representations and Warranties

Subscribers are required to:

- Make true representation at all times to the CA, the RA and the appropriate LRAs regarding information in their certificates; and other identification and authentication information;
- Use certificates in a manner consistent with this Certificate Policy;
- Take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of their private keys;
- Protect their Certificate user password;
- Upon issuance of a Certificate naming the applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the Certificate;
- Inform the RA or appropriate LRA within 48 hours of a change to any information included in their certificate or certificate application request;
- Inform the RA or appropriate LRA within 8 hours of a suspected compromise of one/both of their private keys; and
- Rightfully hold private keys corresponding to the public keys listed in their certificate.

9.6.4 Relying Parties Representations and Warranties

Relying parties will rely on a valid Certificate for purposes of verifying the digital signature only if prior to reliance, the Relying Party will:

(1) Agree to be bound by the terms of this CP;

(2) Verify the digital signature by reference to the public key in the Certificate; and

(3) Refer to the most recent CRL.

Relying party understands that certificates are subject to revocation and such action will not be reflected in the Certificate itself, but must be verified by consulting the most recent certificate revocation list.

9.6.5 Representations and Warranties of other Participants

None.

9.7 DISCLAIMERS OF WARRANTIES

No stipulation.

9.8 LIMITATIONS OF LIABILITY

9.8.1 CA liability

Interested parties will refer to section 9.6.1 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.4.2 of the CP.

9.8.2 RA liability

Interested parties will refer to section 9.6.1 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.9 INDEMNITIES

Interested parties will refer to section 9.9 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.9.1 Hold Harmless: Relying Parties

Relying parties shall hold the State harmless from and against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to (i) any use or reliance by a relying party on the Certificate or any service or transaction provided by the State or performed by a relying party in connection with the Certificates, (ii) lack of proper validation of a Certificate Authority (CA) certificate by a relying party, (iii) reliance by the relying party on an expired or revoked the Certificate, (iv) use of a Certificate other than as permitted by the State Certificate Policy, Certification Practice Statement , the subscriber agreement, any relying party agreement, and applicable law, (v) failure by a relying party to exercise reasonable judgment in the circumstances in relying on a Certificate, or (vi) any claim or allegation that the reliance by a relying party on a Certificate or the contents of a Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates the rights (including intellectual property rights) of any third party in any jurisdiction. Notwithstanding the foregoing, Relying Parties shall not be obligated to hold the State harmless in respect to any liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to any willful misconduct by the State.

9.9.2 Hold Harmless: Subscribers

Subscriber will hold the State harmless from and against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to (i) any use or reliance by the subscriber on any Certificate or any service or transaction provided by the State or performed by the subscriber in connection with the Certificates, (ii) any misrepresentation made by subscriber in using or applying for a Certificate, (iii) modification made by subscriber to the contents of a Certificate, (iv) use of a Certificate other than as permitted by the State Certificate Policy, Certification Practice Statement, the subscriber agreement, any relying party agreement, and applicable law, (v) loss, disclosure, compromise or unauthorized use of the private key corresponding to the public key in subscriber's the Certificate, or (vi) any allegation that the use of a subscriber's the Certificate or the contents of a subscriber's the Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates the rights (including intellectual property rights) of any third party in any jurisdiction. Notwithstanding the foregoing, a subscriber will not be obligated to hold the State harmless in respect to any liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to any willful misconduct by the State.

9.10 TERM & TERMINATION

9.10.1 Term

In the event of a conflict between the provisions of the CP and this CPS and a cross-certification agreement executed between the PA and the entity responsible for another CA, the terms of the cross-certification agreement will take precedence.

9.10.2 Termination

In the event that the State CA ceases operation or is otherwise terminated:

- All Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation;

- All CAs with which cross-certification agreements are current at the time of cessation will be informed so that cross-Certificates to the State CA may be revoked;
- All State Certificates issued by the State CA will be revoked no later than the time of cessation; and
- All current and archived State identity proofing, Certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data will be archived according to the State data archive policy.

Notification methods could include but are not be limited to web site notification, mass email, media advertisements, etc.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.4.5 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Changes to items within this CPS which, in the judgment of the OA and PA, will have no/minimal impact on the users managed by this CA, may be made with no change to the CPS version number and no notification to the users.

Changes to the Certificate Policies supported by this CPS as well as changes to items within this CPS which, in the judgment the OA and PA may have significant impact on the users managed by this CA, may be made with 60-day notice to the user community and the version number of this CPS must be increased accordingly.

9.12.2 Notification Mechanism and Period

The State CA will make available copies of the CP both online and in hard copy form. The dissemination of the complete and sensitive version of this CPS to requesting parties will be made at the sole discretion of the Policy Authority. A “sanitized” or truncated version of this CPS will be available for viewing at https://www2.illinois.gov/sites/doit/services/catalog/Documents/SoI-CPS-V3.9-redacted.pdf.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.13 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

By incorporating Subject names into State Certificates, the State does not determine whether the use of the Subject name infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property or other rights of any person, entity or organization. The State neither acts as an arbitrator nor provides dispute resolution between Subscribers and third party complainants in respect to disputes in relation to the registration or use of a Subject name in a State Certificate. This CPS does not bestow any procedural or substantive rights on any third party complainant in respect to the Subject name in a Certificate. The State will in no way be precluded from seeking legal or equitable relief (including injunctive relief) in respect to any dispute between a Subscriber and third party complainant or in respect to any dispute between a Subscriber and the State arising out of the Subject name in a State Certificate. The State will have the right to revoke a State Certificate upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of the State Certificate or State Certificates containing a Subject name in dispute. Since both the commonName and serialNumber attributes are used to create the RDNs for Certificate subjects, such disputes are expected to be rare.

9.14 GOVERNING LAW

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.14 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.15 COMPLIANCE WITH APPLICABLE LAW

The Illinois OA will comply with applicable law. Please refer to the Illinois Statues Act 175 Electronic Commerce Security Act (Appendix 4).

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16 for more details and action sanctioned by the

State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP

9.16.2 Assignment

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16.2 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.16.3 Severability

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16.3 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

Affected parties will refer to section 9.16.4 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.16.5 Force Majeure

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16.5 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

9.17 OTHER PROVISIONS

The express waiver by the State or the Policy Authority of any provision, condition, or requirement of this CPS will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

10. BIBLIOGRAPHY

Many of the following documents were used in part to develop this CPS:

ABADSG Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.

CIMC Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.

FIPS 140-2 Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 186-2 Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS#12 Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 3647 Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

11. ACRONYMS AND ABBREVIATIONS

AICPA	American Institute of Certified Public Accounts
AIX	Advanced Interactive Executive
ANSI	American National Standards Institute
CARL	Certificate Authority Revocation List
CBC	Cipher Block Chaining
CIMC	Certificate Issuing and Management Components
CMM	Capability Maturity Model
CMS	Central Management Services
COMSEC	Communications Security
COTS	Commercial off the Shelf
CPS	Certification Practice Statement
CRL	Certificate Revocation Lists
CSS	Certificate Status Server
DB2	Database 2
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI Profile
FPKIPA	Federal PKI Policy Authority
FPKISC	Federal PKI Steering Committee
FTP	File Transfer Protocol
GPEA	Government Paperwork Elimination Act
HACMP	High Availability Cluster Multi Processing
IBM	International Business Machines
IETF	Internet Engineering Task Force
IL	Illinois

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union Telecommunications
ITU-TSS	International Telecommunications Union Telecommunications Sector
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authorities
MAC	Message Authentication Code
MD5	Message Digest 5
MOA	Memorandum of Agreement
N/A	Not Applicable
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority
RDN	Relational Distinguished Name
RFC	Request for Comments
RSA	Rivest Shimar Adleman
S/MIME	Secure Multipurpose Internet Mail Extension

SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
U.S	United States
U.S.C	United States Code
UPS	Uninterrupted Power Supply
URL	Used by Relying
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Network
WWW	World Wide Web

12. GLOSSARY

Access
Ability to make use of any information system (IS) resource. [NS4009]

Access Control
Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]

Accreditation
Defined in ISO-IEC Guide 2 as a: “procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.” The accrediting body is a recognized entity which accredits the auditor as qualified to perform its evaluation of CAs or other PKI components, applying standards derived from the Certificate Policies adopted by the Policy-adopting body. Examples of bodies that have or might perform such a role include NIST’s National Voluntary Laboratory Accreditation Program (NVLAP), or the American Institute of Certified Public Accounts (AICPA) which accredits Third Party Auditing Firms to audit various entities.

Activation Data
Private data, other than keys, that are required to access cryptographic modules.

Applicant
The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Assurance Level
A representation of how rigorously the Registration Authority authenticates the identity claimed by an Applicant prior to issuing a Certificate.

Archive
Long-term, physically separate storage.

Authority Revocation List (ARL)
A list of revoked Certificate Authority Certificates. An ARL is a Certificate Revocation List for Certificate Authority certificates.

Authentication
The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.

Audit
An Independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Audit Data
Chronological record of system activities to enable the

reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

Authenticate

To confirm the identity of an entity when that identity 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. [NS4009]

Backup

Copy of files and programs made to facilitate recovery if necessary. [NS4009]

Binding

Process of associating two related elements of information. [NS4009]

Biometric

A physical or behavioral characteristic of a human being.

CA Facility

The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate

A Certificate issued under this Policy by a Certificate Authority and identified as such by the inclusion of the registered object identifier for this Certificate Policy in the Certificate Policies field, and at a minimum:

- Identifies the Certificate Authority issuing it.
- Names or otherwise identifies its Subscriber.
- Contains a public key that corresponds to a private key under the control of the Authorized Subscriber.
- Identifies its operational period.
- Contains a Certificate serial number and is digitally signed by the Certificate Authority issuing it.

The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.

Certificate Authority (CA)

A Certificate Authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. A Certificate Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities.

A Certificate Authority performs two essential functions. First, it is responsible for identifying and authenticating the intended Authorized Subscriber to be named in a Certificate, and verifying that such Authorized Subscriber possesses the private key that corresponds to the public key that shall be listed in the Certificate. Second, the Certificate Authority actually creates and digitally signs the Authorized Subscriber’s Certificate. The Certificate issued by the Certificate Authority then represents that CA’s statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private key pair.

Certificate Extension

A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.

Certificate Management Authority (CMA)

A Certification Authority or a Registration Authority.

Certificate Manufacturing

The process of accepting a public key and identifying information from an authorized Subscriber, producing a digital certificate containing that and other pertinent information, and digitally signing the Certificate.

Certification Authority Software

Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP)

A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of Certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certificate Authority Software

The application software required to manufacture certificates by the CA

Certification Practice Statement (CPS)

A statement of the practices, which a Certificate Authority (CA) employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the Certificate Authority (CA) uses to satisfy the requirements specified in the CP that are supported by it.

Certificate-Related Information

Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL)

A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate’s validity period. In some cases, the Certificate Authority (CA) may choose to split a CRL into a series of smaller CRLs. When an End Entity chooses to accept a certificate the Relying Party Agreement requires that this Relying Party check that the certificate is not listed on the most recently issued CRL.

Certificate Status Authority

A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Client (application)

A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

Common Criteria

A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

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. [NS4009]

Computer Security Objects Registry (CSOR)

Computer Security Objects Registry operated by the National Institute of Standards and Technology.

Confidentiality

Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate

A Certificate used to establish a trust relationship between two Certification Authorities.

A Cross-Certificate is a Certificate issued by one Certificate Authority (CA) to another CA which contains a CA key associated with the private CA signature key used for issuing Certificates. Typically a cross-certificate is used to allow End Entities in one CA to communicate security with End Entities in another CA. A cross-certificate issued by CA#1 to CA#2 allows Entity #a, who has a Certificate issued by CA#1, to accept a Certificate used by Entity #b, who has a Certificate issued by CA#2.

Cryptographic Module

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]

Cryptoperiod

Time span during which each key setting remains in effect. [NS4009]

Data Integrity

Assurance that the data are unchanged from creation to reception.

Digital Signature

The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine:

Whether the transformation was created using the private signing key that corresponds to the signer’s public verification key.

Whether the message has been altered since the transformation was made.

Directory

A directory system that conforms to the ITU-T X.500 series of Recommendations.

Distinguished Name

A string created during the certification process and included in the Certificate that uniquely identifies the End Entity within the Certificate Authority (CA) domain.

Dual Use Certificate

A certificate that is intended for use with both digital signature and data encryption services.

Duration

A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”.

E-commerce

The use of network technology (especially the internet) to buy or sell goods and services.

Encrypted Network

A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.

Encryption Certificate

A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

Encryption Key Pair

A public and private key pair issued for the purposes of encrypting and decrypting data.

End Entity

A person, device or application that uses the keys and Certificates created within the PKI for purposes other than the management of the aforementioned keys and Certificates. An End Entity may have the roles of a Subscriber or a Relying Party.

Entity

Any autonomous element within the PKI. This may be a CA, a RA or an End Entity.

Entity CA

A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.

Employee

An employee is any person employed in or by the State; as well as contractors and other persons who have been authorized to access electronic networks.

FBCA Operational Authority (FPKI OA)

The Federal Public Key Infrastructure Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.

Federal Information Processing Standards (FIPS)

Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.

Federal Public Key Infrastructure Policy Authority (FPKI PA)

The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-entity PKI interoperability that uses the FBCA.

Firewall

Gateway that limits access between networks in accordance with local security policy. [NS4009]

Governing Body

Authorities that dictate Policy and procedures that may impact the Policy Authority and Operational Authority.

Hardware Token

A hardware device that can hold private keys, digital certificates, or other electronic information that can be used for authentication or authorization. Smartcards and USB tokens are examples of hardware tokens.

High Assurance Guard (HAG)

An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Internet Engineering Task Force(IETF)

The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Information System Security Officer (ISSO)

Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]

Inside threat

An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity

Protection against unauthorized modification or destruction of information. [NS4009]. 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.

Intellectual Property

Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA

A CA that is subordinate to another CA, and has a CA subordinate to itself.

Issuing CA

In the context of a particular Certificate, the issuing Certificate Authority is the Certificate Authority that signed and issued the Certificate.

Key Escrow

A deposit of the private 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 key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange

The process of exchanging public keys in order to establish secure communications.

Key Generation

The process of creating a Private Key and Public Key pair.

Key Generation Material

Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair

Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the public key, it is computationally infeasible to discover the other key which is called the private key.

Local Registration Authority (LRA)

An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is delegated certain tasks on behalf of a RA or CA).

Memorandum of Agreement (MOA)

Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA.

Mutual Authentication

Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority

An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

Non-Repudiation

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. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID)

An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognized standards organization.

Operational Authority (OA)

An agent of the State PKI CA. The Operational Authority is responsible to the Policy Authority for:

- Interpreting the Certificate Policies that were selected or defined by the Policy Authority.
- Developing a Certification Practice Statement (CPS), in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527), to document the CA's compliance with the Certificate Policies and other requirements.
- Maintaining the CPS to ensure that it is updated as required.
- Operating the Certificate Authority in accordance with the CPS.

Operational Period of a Certificate

The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or is earlier revoked.

Organization

Department, agency, partnership, trust, joint venture or other association.

Out-of-Band

Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat

An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

PKIX

A set of IETF Working Group developed technical specifications for PKI components based on X.509 Version 3 Certificates.

Person

A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.

PIN

Personal Identification Number. See activation data for definition

PKIX

“Public Key Infrastructure X.509”. A set of standards for using X.509 certificates and certificate revocation lists on the Internet.

Policy

This Certificate Policy.

Policy Authority (PA)

An agent of the Certificate Authority. The Policy Authority is responsible for:

- Dispute resolution.
- Selecting and/or defining Certificate Policies, in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527), for use in the Certificate Authority PKI or organizational enterprise.
- Approving of any interoperability agreements with external Certificate Authorities.
- Approving practices, which the Certificate Authority must follow by reviewing the Certification Practice Statement to ensure consistency with the Certificate Policies.
- Providing Policy direction to the Certificate Authority (CA) and the Operational Authority.

Principal CA

The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.

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.

Private Key

(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

“Promptly”

“done, spoken, etc. at once or without delay” (www.yourdictionary.com reference)

Public Key

(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public/Private Key Pair

Two mathematically related keys, having the properties that:

- One key can be used to encrypt a message that can only be decrypted using the other key.
- Even knowing the public key, it is computationally infeasible to discover the private key.

Registration

The process whereby a user applies to the Certification Authority for a digital certificate and the Certificate Authority (CA) issues a Certificate for that user.

Registration Authority (RA)

An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (i.e., an RA is delegated certain tasks on behalf of a Certificate Authority (CA)).

Re-key (a certificate)

To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party

A Relying Party is a recipient of a Certificate signed by the State PKI Certificate Authority (CA) who acts in reliance on those Certificates and/or digital signatures verified using that Certificate and who has agreed to be bound by the terms of this CP and the CPS.

Relying Party Agreement

An agreement subscribed to by a recipient of a Certificate signed by the State PKI Certificate Authority (CA) prior to gaining access to any State PKI CA CRL.

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

The logical single Repository operated for all Subscribers and Relying Parties on the Network. All Certificates issued by all CAs, and all Certificate Revocation Lists relating thereto, shall be published in the Repository. Also known as a “Directory”.

Revocation

To prematurely end the operational period of a Certificate from a specified time forward.

Root CA

The Certificate Authority (CA) that issues Certificates to each CA operating under this Policy.

Security Accreditation Authority

An agent of the CA. Responsible for:

- Approving the operation of the Certificate Authority (CA) in a particular mode using particular safeguards.
- Accepting residual security risks on behalf of the CA domain or enterprise.

Signature Certificate

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Signature Key Pair

A public and private key pair used for the purposes of digitally signing electronic documents and verifying digital signatures.

Software-based Certificate

A digital certificate (and associated private keys) that are created and stored in software – either on a local workstation or on a secure server.

Sponsoring Organization

An organization with which an Authorized Subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer etc.).

Subscriber

An entity that is the subject of a Certificate and which is capable of using, and is authorized to use, the private key, that corresponds to the public key in the Certificate. Responsibilities and obligations of the Subscriber shall be as required by the Certificate Policy.

Subordinate CA

In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Superior CA

In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

Threat

Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Token

A hardware security device containing an End Entity’s Private Key(s) and Public Key Certificate. (see “Hardware Token”)

Trusted Certificate

A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trustworthy System

Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) 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. [NS4009]

Update (a certificate)
The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Valid Certificate
A Certificate that (1) a Certificate Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not “valid” until it is both issued by a Certificate Authority (CA) and has been accepted by the Subscriber.

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. [FIPS1401]