CMS

Illinois Department of

Central Management Services

State of Illinois

Public Key Infrastructure

Certificate Policy

For Digital Signature

And Encryption Applications Version 4.0

(IETF RFC 3647 format)

September 3, 2015

Signature Page

_____ _____

Chair, State of Illinois PKI Policy Authority Date

DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
2.0	Aug-31-2006	Anderson	Initial draft	Conversion to RFC2527 format.
2.0	5-Oct-2006	Anderson, Falzone, Corn, Baird, Anderson	Review of initial draft	Conversion to RFC2527 format.
2.0	11-Apr-2007	Anderson, Baird	Additional comments	Conversion to RFC2527 format.
2.0	21-Apr-2007	Baird	Additional comments	Conversion to RFC2527 format
2.0	30-Apr-2007	Anderson, Miller	Correction of references	Conversion to RFC2527 format
2.0	6-12-2007	Anderson	Removed highlighting, accepted changes.	Notified of email approval by Policy Authority 6/12/2007.
2.0	8-15-2007	Anderson	Correct “subscription agreement” to “subscriber’s agreement” throughout the document; Section 3.2 was modified to removed language concerning revoked or expired certificates. This language did not belong in this section; Section 5.1.1 was updated to reflect the new IP based monitoring systems which replaced the CCTV system;	Audit recommendations.
2.0	8-28-2007	Anderson	Approved version	Approved via email vote 8/28/2007 by PA.
3.0	8-27-2008	Anderson, Christensen	Conversion to RFC 3647	Approved by Policy Authority 8/27/08.
3.1	1-20-2009	Anderson	Section 1.1.3 was updated to correct a grammar error; Section 1.2.1.1 was updated to clarify the	

			role of the Policy Authority; Section 1.5.3 was updated to clarify the relationship of the CP to the CPS; Section 3.2.3 was updated for clarification purposes and to differentiate between the requirements for an individual subscriber versus bulk applications; Section 3.3.1.1 was updated to remove conflicting information; Section 4.9.11 was updated for clarification purposes; Section 4.9.12 was updated for clarification purposes; Section 4.12 was updated to include a reference to a related section; Section 4.12.2 was updated for clarification purposes; Section 4.5.2 was updated to indicate that expired certificates roll off of CRLs; Section 5.1.2.3 was updated for clarification purposes; Section 5.1.7 was updated to replace “confidential” with “sensitive”, and to specifically include media; Section 5.2.1.3 was updated to refer to the CPS; Section 5.2.4 was updated to clarify roles; Section 5.6 was updated to define link certificates; Section 5.7.1 was changed to indicate “successful”	

			attacks; Section 5.8 was updated to state that a CA key compromise would cause the CA key to be revoked; Section 6.2.4 was updated to correct a typographical error. Section 6.2.6 was updated to clarify CA private key export; Section 6.4.2 was updated to change the word “inactive” to “active”; Section 7.1.2 was updated to remove a reference to RFC 2459; Section 12 was updated to add the “LEADS” acronym;	
3.1	2-27-09	Anderson	Updates	Approved by Policy Authority 2/27/2009.
3.1	5-15-2009	Anderson	Section 7.1.2 was updated to correct a typo on the keyusage extension criticality.	Determined to be a minor change with no increment of version number.
3.3	7-15-2009	Anderson	Signature page added; Section 1.2 was updated to clarify biometric requirement for level 4 assurance level; Section 1.4.1 was updated to clarify accepted certificate usage; Section 3.1.4 was updated to clarify the requirement; Section 3.2.3 was modified to allow for user applications to be signed digitally in accordance with FBCA change proposal 2010-06**;** Section 3.2.3.3 was updated to clarify the relationship between	

			a device's public keys and the identity created by the certificate; Section 4.1 was updated to clarify Local Registration Authorities; Section 4.1.1 was updated to clarify the CMS Director's office; Section 4.9.6 was updated to remove the restriction on Relying Parties to validate the signature of CRLs; Section 5.1.8 was updated to clarify backup section; Section 5.5.3 was updated to clarify who can determine the format of the archive; Section 5.3.7 was updated to clarify contractor requirements; Section 6.1.1.2 was updated to clarify the key generation medium for level-4 certificates; Section 6.1.7 was updated to clarify the use of a single key pair; Section 6.2.1 was updated to clarify the cryptographic module requirements for level-3 software certificates; Section 6.3.2 was updated to indicate that the signing key lifetime was 25 months instead of 2 years; Section 7.1.3 was updated to remove duplicate language; Section 9.4.4 was updated to clean up the language about the release of	

			sensitive information;	
3.3	8-7-2009	Anderson		Approved by PA
3.4	6-15-2010	Anderson	Section 1 was updated for clarification purposes; Section 1.5.2 was updated to correct contact email address; Sections 5.1.1 and 5.1.2.1 were updated to include remote terminals; Sections 5.1.4 and 5.1.5 were updated to simplify the language and avoid duplication with the CPS; Section 5.7.1 was updated to fix a grammar error; Section 6.2.8 was updated to remove references to obsolete software; Section 6.3.2 was updated to include the encryption key lifetime; Sections 6.5.1 and 6.7 were updated to include remote workstations.	
3.4	6-28-2010	Anderson		Approved by PA
3.5	9-07-2010	Anderson	Section 1.5.3 was modified to clarify that the CPS must conform to the CP; Section 5.1.8 was modified to remove specifics regarding backups (moved to CPS), and to change a reference to “level 1 or higher”; Section 6.1.1.2 was modified to indicate that single-key certificates may be issued; Section 6.1.7 was modified to remove an ambiguous reference to a “dual-use” certificate;	Recommendations by auditor

3.5	10-12-2010	Anderson		Approved by PA
3.6	10-31-2011	Wells	Section 1.5.2 was updated to reflect the new contact person for changes to the Certificate Policy; Section 3.2.4 removed the statement "Information that is not verified shall not be included in certificates"; Section 5.1.2.2 added "moderate" level to threat in the RA equipment environment; Section 5.4.4 added dot point "logs are monitored to assure there are no changes by the System Administrator"	Recommendations by Auditor
3.7	08-01-2012	Wells	Section 1.5.2 Changed contact person for CP to Steven Matthews; Section 5.3.3 deleted wording "Where competence was demonstrated in lieu of training, supporting documentation shall be maintained"; Section 5.3.4 deleted wording "any significant change to the operations shall have a training(awareness) plan, and the execution of such plan shall be documented"; Section 9.3.1 changed each dot point to start with "is" and deleted "Must be"	Recommendations by Auditor Approved by PA DATE

3.8	04-04-2013	Wells/Bouchard	New SHA-256 policy OID values added across the document; Replace FIPS 140-1 by FIPS 140-2 across the CP; Remove CA and HSM vendor names across the CP; FBCA policy mapping rules removed from section 1.2. Section 6.3.2: RSA-2048 CA certificate not to exceed January 31st 2031 rather than having a lifetime of 20 years.	Approved by Policy Authority DATE
3.9	08-29-13	Wells	Section 1.5.4 added language for the State of Illinois to show results of compliance audit to appropriate authority Section 5.1.2.1 add "FIPS 199 moderate" to level of threat Section 5.1.2.3 changed to "Not Applicable" Section 5.4.1 added the physical locations for the types of events recorded table Section 6.1.5 add the dates for SHA-1 certificate issuance and dates for SHA-256 acceptance Section 6.3.2 Added language to describe the validity period of certificates Section 8.6 State that we will annually report on our compliance audit and identify CP	Approved by Policy Authority DATE: 9/11/13

			and CPs versions	
4.0	9-3-15	Caceres	Updated hyperlinks throughout the document to reflect the exact address as per audit recommendation. Changed point of contact information to reference MFR appointing PA Chairperson. MFR will be retained by OA.	

Table of Contents

1. INTRODUCTION 21

1.1 OVERVIEW..... 22

1.1.1 Certificate Policy (CP) 22

1.1.2 Relationship between the CP & the CPS 22

1.1.3 Relationship between the CP and the Entity CP 22

1.1.4 Scope 23

1.1.5 Interaction with External PKI's 23

1.2 DOCUMENT NAME & IDENTIFICATION..... 23

1.3 PKI PARTICIPANTS..... 24

1.3.1 Certification Authorities 24

1.3.2 Registration Authority (RA) 26

1.3.3 Subscribers 26

1.3.4 Relying Parties 27

1.3.5 Other Participants 27

1.4 CERTIFICATE USAGE..... 27

1.4.1 Appropriate Certificate Uses 27

1.4.2 Prohibited Certificate Uses 28

1.4.3 Appropriated Certificate Usage per Assurance Level 28

1.5 POLICY ADMINISTRATION..... 29

1.5.1 Organization administering the document 29

1.5.2 Contact Person 29

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy 30

1.5.4 CPS Approval Procedures 30

1.6 DEFINITIONS AND ACRONYMS..... 30

2. Publication & Repository responsibilitles 31

2.1 REPOSITORIES 31

2.1.1 Illinois PKI Repository Obligations 31

2.2 PUBLICATION OF CERTIFICATION INFORMATION..... 31

2.2.1 Publication of Certificates and Certificate Status 31
2.2.2 Publication of CA Information..... 32
2.2.3 Interoperability 32
2.3 FREQUENCY OF PUBLICATION 32
2.4 ACCESS CONTROLS ON REPOSITORIES..... 33
3. Identification & Authentication 34
3.1 NAMING 34
3.1.1 Types of Names..... 34
3.1.2 Need for Names to Be Meaningful 34
3.1.3 Anonymity or Pseudonymity of Subscribers..... 34
3.1.4 Rules for Interpreting Various Name Forms..... 34
3.1.5 Uniqueness of Names..... 35
3.1.6 Recognition, Authentication, & Role of Trademarks..... 35
3.2 INITIAL IDENTITY VALIDATION 35
3.2.1 Method to Prove Possession of Private Key 35
3.2.2 Authentication of Organization Identity..... 36
3.2.3 Authentication of Individual Identity..... 36
3.2.4 Non-verified Subscriber Information..... 38
3.2.5 Validation of Authority 38
3.2.6 Criteria for Interoperation 38
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 38
3.3.1 Identification and Authentication for Routine Re-key 38
3.3.2 Identification and Authentication for Re-key after Revocation..... 39
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 39
4. Certificate Life-Cycle 40
4.1 APPLICATION..... 40
4.1.1 Application of Behalf of a Device, Software Application, or process 41
4.1.2 Application for a Cross Certificate..... 41
4.2 CERTIFICATE APPLICATION PROCESSING 42

4.2.1 Performing Identification and Authentication Functions 42
4.2.2 Approval or Rejection of Certificate Applications 42
4.2.3 Time to Process Certificate Applications 42
4.3 ISSUANCE 43
4.3.1 CA Actions during Certificate Issuance 43
4.3.2 Notification to Subscriber of Certificate Issuance 43
4.4 CERTIFICATE ACCEPTANCE 43
4.4.1 Conduct constituting certificate acceptance 43
4.4.2 Publication of the Certificate by the CA 43
4.4.3 Notification of Certificate Issuance by the CA to other entities 43
4.5 KEY PAIR AND CERTIFICATE USAGE 44
4.5.1 Subscriber Private Key and Certificate Usage 44
4.5.2 Relying Party Public key and Certificate Usage 44
4.6 CERTIFICATE RENEWAL 44
4.6.1 Circumstance for Certificate Renewal 45
4.6.2 Who may request Renewal 45
4.6.3 Processing Certificate Renewal Requests 45
4.6.4 Notification of new certificate issuance to Subscriber 45
4.6.5 Conduct constituting acceptance of a Renewal certificate 45
4.6.6 Publication of the Renewal certificate by the CA 45
4.6.7 Notification of Certificate Issuance by the CA to other entities 45
4.7 CERTIFICATE RE-KEY 45
4.7.1 Circumstance for Certificate Re-key 45
4.7.2 Who may request certification of a new public key 45
4.7.3 Processing certificate Re-keying requests 46
4.7.4 Notification of new certificate issuance to Subscriber 46
4.7.5 Conduct constituting acceptance of a Re-keyed certificate 46
4.7.6 Publication of the Re-keyed certificate by the CA 46
4.7.7 Notification of certificate issuance by the CA to other Entities 46
4.8 MODIFICATION 46
4.8.1 Circumstance for Certificate Modification 47

4.8.2 Who may request Certificate Modification 47
4.8.3 Processing Certificate Modification Requests 47
4.8.4 Notification of new certificate issuance to Subscriber 47
4.8.5 Conduct constituting acceptance of modified certificate 47
4.8.6 Publication of the modified certificate by the CA 47
4.8.7 Notification of certificate issuance by the CA to other Entities 47
4.9 CERTIFICATE REVOCATION & SUSPENSION 48
4.9.1 Circumstances for Revocation 48
4.9.2 Who Can Request Revocation 49
4.9.3 Procedure for Revocation Request 49
4.9.4 Revocation Request Grace Period 51
4.9.5 Time within which CA must Process the Revocation Request 51
4.9.6 Revocation Checking Requirements for Relying Parties 51
4.9.7 CRL Issuance Frequency 51
4.9.8 Maximum Latency of CRLs 51
4.9.9 On-line Revocation/Status Checking Availability 51
4.9.10 On-line Revocation Checking Requirements 52
4.9.11 Other Forms of Revocation Advertisements Available 52
4.9.12 Special Requirements Related To Key Compromise 52
4.9.13 Circumstances for Suspension 52
4.9.14 Who can Request Suspension 52
4.9.15 Procedure for Suspension Request 52
4.9.16 Limits on Suspension Period 52
4.10 CERTIFICATE STATUS SERVICES 52
4.10.1 Operational Characteristics 52
4.10.2 Service Availability 52
4.10.3 Optional Features 52
4.11 END OF SUBSCRIPTION 52
4.12 KEY ESCROW & RECOVERY 52
4.12.1 Key Escrow and Recovery Policy and Practices 53
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 53

5. Facility Management & Operations Controls 54

5.1 PHYSICAL CONTROLS 54

5.1.1 Site Location & Construction 54
5.1.2 Physical Access 54
5.1.3 Power and Air Conditioning 56
5.1.4 Water Exposures 57
5.1.5 Fire Prevention & Protection 57
5.1.6 Media Storage 57
5.1.7 Waste Disposal 57
5.1.8 Off-Site backup 58

5.2 PROCEDURAL CONTROLS 58

5.2.1 Trusted Roles 58
5.2.2 Number of Persons Required per Task 61
5.2.3 Identification and Authentication for Each Role 61
5.2.4 Separation of Roles 62

5.3 PERSONNEL CONTROLS 63

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements 63
5.3.2 Background Check Procedures 63
5.3.3 Training Requirements 64
5.3.4 Retraining Frequency & Requirements 64
5.3.5 Job Rotation Frequency & Sequence 64
5.3.6 Sanctions for Unauthorized Actions 64
5.3.7 Independent Contractor Requirements 65
5.3.8 Documentation Supplied To Personnel 65

5.4 AUDIT LOGGING PROCEDURES 65

5.4.1 Types of Events Recorded 65
5.4.2 Frequency of Processing Log 71
5.4.3 Retention Period for Audit Logs 71
5.4.4 Protection of Audit Logs 72
5.4.5 Audit Log Backup Procedures 72

5.4.6 Audit Collection System (internal vs. external) 72
5.4.7 Notification to Event-Causing Subject 73
5.4.8 Vulnerability Assessments 73
5.5 RECORDS ARCHIVE 73
5.5.1 Types of Events Archived 73
5.5.2 Retention Period for Archive 75
5.5.3 Protection of Archive 76
5.5.4 Archive Backup Procedures 76
5.5.5 Requirements for Time-Stamping of Records 76
5.5.6 Archive Collection System (internal or external) 76
5.5.7 Procedures to Obtain & Verify Archive Information 77
5.6 KEY CHANGEOVER 77
5.6.1 Recovery at Subscriber Request 77
5.6.2 Involuntary Recovery at State Agency Request 77
5.6.3 Involuntary Recovery by Court Order 78
5.7 COMPROMISE & DISASTER RECOVERY 78
5.7.1 Incident and Compromise Handling Procedures 78
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 79
5.7.3 Entity (CA) Private Key Compromise Procedures 79
5.7.4 Business Continuity Capabilities after a Disaster 80
5.8 CA & RA TERMINATION 80
6. Technical Security Controls 82
6.1 KEY PAIR GENERATION & INSTALLATION 82
6.1.1 Key Pair Generation 82
6.1.2 Private Key Delivery to Subscriber 84
6.1.3 Public Key Delivery to Certificate Issuer 85
6.1.4 CA Public Key Delivery to Relying Parties 85
6.1.5 Key Sizes 86
6.1.6 Public Key Parameters Generation and Quality Checking 88
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) 88

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 89

6.2.1 Cryptographic Module Standards & Controls 89
6.2.2 Private Key Multi-Person Control 90
6.2.3 Private Key Escrow 90
6.2.4 Private Key Backup 91
6.2.5 Private Key Archival 92
6.2.6 Private Key Transfer into or from a Cryptographic Module 92
6.2.7 Private Key Storage on Cryptographic Module 92
6.2.8 Method of Activating Private Keys 92
6.2.9 Methods of Deactivating Private Keys 93
6.2.10 Method of Destroying Private Keys 93
6.2.11 Cryptographic Module Rating 93

6.3 OTHER ASPECTS OF KEY MANAGEMENT 93

6.3.1 Public Key Archival 93
6.3.2 Certificate Operational Periods/Key Usage Periods 94

6.4 ACTIVATION DATA 94

6.4.1 Activation Data Generation & Installation 94
6.4.2 Activation Data Protection 95
6.4.3 Other Aspects of Activation Data 95

6.5 COMPUTER SECURITY CONTROLS 95

6.5.1 Specific Computer Security Technical Requirements 96
6.5.2 Computer Security Rating 97

6.6 LIFE-CYCLE SECURITY CONTROLS 97

6.6.1 System Development Controls 97
6.6.2 Security Management Controls 98
6.6.3 Life Cycle Security Ratings 98

6.7 NETWORK SECURITY CONTROLS 98

6.8 TIME STAMPING 99

7. Certificate, CARL/CRL, And ocsp profiles Format 100

7.1 CERTIFICATE PROFILE 100

7.1.1 Version Numbers 100
7.1.2 Certificate Extensions 100
7.1.3 Algorithm Object Identifiers 102
7.1.4 Name Forms 104
7.1.5 Name Constraints 104
7.1.6 Certificate Policy Object Identifier 105
7.1.7 Usage of Policy Constraints Extension 105
7.1.8 Policy Qualifiers Syntax & Semantics 105
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 105

7.2 CRL PROFILE 105

7.2.1 Version Numbers 105
7.2.2 CRL Entry Extensions 105

7.3 OCSP PROFILE 106

8. Compliance Audit & Other Assessments 107

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS 107

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR 107

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 108

8.4 TOPICS COVERED BY ASSESSMENT 108

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 109

8.6 COMMUNICATION OF RESULTS 110

9. Other Business & Legal Matters 111

9.1 FEES 111

9.1.1 Certificate Issuance/Renewal Fees 111
9.1.2 Certificate Access Fees 111
9.1.3 Revocation or Status Information Access Fee 111
9.1.4 Fees for other Services 111
9.1.5 Refund Policy 111

9.2 FINANCIAL RESPONSIBILITY 111

9.2.1 Insurance Coverage 111
9.2.2 Other Assets 112
9.2.3 Insurance/warranty Coverage for End-Entities 112
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 112
9.3.1 Scope of Confidential Information 112
9.3.2 Information not within the scope of Confidential Information 113
9.3.3 Responsibility to Protect Confidential Information 113
9.4 PRIVACY OF PERSONAL INFORMATION 113
9.4.1 Privacy Plan 113
9.4.2 Information treated as Private 113
9.4.3 Information not deemed Private 113
9.4.4 Responsibility to Protect Private Information 113
9.4.5 Notice and Consent to use Private Information 113
9.4.6 Disclosure Pursuant to Judicial/Administrative Process 114
9.4.7 Other Information Disclosure Circumstances 114
9.5 INTELLECTUAL PROPERTY RIGHTS 114
9.6 REPRESENTATIONS & WARRANTIES 116
9.6.1 CA Representations and Warranties 116
9.6.2 RA Representations and Warranties 116
9.6.3 Subscriber Representations and Warranties 119
9.6.4 Relying Parties Representations and Warranties 120
9.6.5 Representations and Warranties of other Participants 120
9.7 DISCLAIMERS OF WARRANTIES 120
9.8 LIMITATIONS OF LIABILITY 121
9.9 INDEMNITIES 121
9.9.1 Hold Harmless: Relying Parties 121
9.9.2 Hold Harmless: Subscribers 121
9.10 TERM & TERMINATION 122
9.10.1 Term 122
9.10.2 Termination 122

9.10.3 Effect of Termination and Survival 122
9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS 122
9.12 AMENDMENTS 123
9.12.1 Procedure for Amendment 123
9.12.2 Notification Mechanism and Period 123
9.12.3 Circumstances under which OID must be changed 123
9.13 DISPUTE RESOLUTION PROVISIONS 123
9.14 GOVERNING LAW 123
9.15 COMPLIANCE WITH APPLICABLE LAW 124
9.16 MISCELLANEOUS PROVISIONS 124
9.16.1 Entire agreement 124
9.16.2 Assignment 124
9.16.3 Severability 125
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 125
9.16.5 Force Majeure 125
9.17 OTHER PROVISIONS 126
10. BIBLIOGRAPHY 127
11. ACRONYMS & ABBREVIATIONS 129
12. GLOSSARY 132

1. INTRODUCTION

This introduction is intended to be a layman's description of the State of Illinois Public Key Infrastructure (PKI). This section is not intended to describe the policies and procedures that govern PKI. Policies and procedures are described in Sections 1 through 9 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 Central Management Services. 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 document defines all certificate policies of the Certificate Authority ("CA") operated by The State of Illinois ("State") for the use of digital certificates for encryption and digital signatures for use in providing electronic identification of End-Entities as required for conducting State business. Unless specifically noted in this document by the inclusion of unique requirements for each individual policy, the requirements of this document apply to all certificates issued by this CA.

This policy defines a single private Public Key Infrastructure consisting of the Certificate Authority, at least one Registration Authority, Local Registration Authorities, and End-Entities.

This Policy is for use by all entities with relationships with the CA, including End-Entities, Registration Authorities ("RA") and Local Registration Authorities ("LRA") and other cross-certified Certificate Authorities (CA's) undertaking to adhere to this Policy.

This Policy is binding on the Certificate Authority (CA), and governs its performance with respect to all Certificates it issues. Specific practices and procedures by which the Certificate Authority (CA) implements the requirements of this Policy are maintained in a Certification Practice Statement ("CPS") that is approved by the State Policy Authority ("PA").

1.1.1 Certificate Policy (CP)

The Illinois PKI certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this Certificate Policy (CP) which shall be available to Relying Parties. Each certificate issued by the Illinois PKI will assert the appropriate level of assurance in the *certificate Policies* extension.

1.1.2 Relationship between the CP & the CPS

The Illinois CP states what assurance can be placed in a certificate issued by the State. The Illinois Certification Practices Statement (CPS) states how the State establishes that assurance.

1.1.3 Relationship between the CP and the Entity CP

The Illinois Policy Authority maps Entity CP(s) to one or more of the levels of

assurance in the CP. The relationship between this CPs and the Illinois Root CA shall be asserted in CA certificates in the *policyMappings* extension.

1.1.4 Scope

The Illinois PKI exists to facilitate trusted electronic business transactions for State governmental organizations and official registered entities.

1.1.5 Interaction with External PKI's

No Stipulation

1.2 DOCUMENT NAME & IDENTIFICATION

This document is called the State of Illinois Certificate Policy for Digital Signature and Encryption Applications (CP).

The Certificate Authority (CA) issues certificates for use in verification of digital signatures and certificates for use in encryption. The CA supports several certificate policies that cover both of these applications.

Each policy is uniquely represented by an "object identifier" which is a numeric string that is contained in a field of each certificate issued by the Certificate Authority (CA) under this CP. To ensure interoperability and uniqueness of this Object Identifier ("OID"), The State has registered the OIDs following the procedures specified in ISO/IEC and ITU standards.

There are fifteen policies specified at ten levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the Illinois PKI. The Illinois PKI policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

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

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

The procedures for implementing this policy are described in the State of Illinois Certification Practice Statement.

Several of the Illinois assurance levels are mapped to Federal PKI assurance levels. The specific mapping policy rules are defined in the Memorandum of Agreement (MOA) established between the State of Illinois PKI Policy Authority and the Federal PKI Policy Authority.

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the Illinois PKI :

1.3.1 Certification Authorities

Creates, signs, distributes and revokes Certificates binding the X.500 Distinguished Name of Subscribers and Registration Authorities with their respective signature verification key and their public encryption key;

- Publishes certificate status through certificate revocation lists (CRLs);
- Has designed, implemented, and operated its Certification Practice to reasonably achieve the requirements of this Policy.

The Certificate Authority (CA) may use one or more representatives or agents to perform its obligations under this Policy, provided that the CA remains responsible for complying with this Policy.

Where necessary, this Policy distinguishes the different users and roles accessing the Certificate Authority (CA) functions. Where this distinction is not required, the term CA shall refer to the total CA entity, including the software and its operations.

The Certificate Authority (CA) may issue cross-certificates to other CAs where expressly authorized by the Policy Authority (PA). Cross-certificates shall be issued to other CAs where a cross-certification agreement has been developed between the Policy Authority (PA) and the policy governing body of the other CA. Cross-certification shall be implemented according to the requirements defined in that agreement.

1.3.1.1 *Policy Authority ("PA")*

The Policy Authority ("PA") is responsible for ensuring that both the policy and the practices that the Certificate Authority (CA) employs in issuing certificates, as may be more comprehensively described in the CPS, are consistent with the policies described in this CP.

The Policy Authority (PA) shall consist of individuals representing constitutional offices, state agencies, and local governments, which are utilizing the State of Illinois public key infrastructure.

The Illinois PKI Policy Authority is a group of PKI users chartered by the Illinois Department of CMS. The Illinois Policy Authority owns this policy and represents the interest of the Illinois PKI. The Illinois Policy Authority is responsible for:

- The Illinois CP,
- The Illinois CPS,
- Accepting applications from Entities desiring to interoperate using the State of Illinois ("State"),
- Determining the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth in the Illinois CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the Illinois), and
- After an Entity is authorized to interoperate using The State of Illinois, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the State of Illinois.
- The State of Illinois will execute a Memorandum of Agreement (MOA) with each cross-certified Entity setting forth the respective responsibilities and obligations of both parties and the mappings between the certificate levels of assurance contained in this CP and those in the Entity CP.

1.3.1.2 *Operational Authority ("OA")*

The Illinois Department of Central Management Services shall serve as the Operational Authority (OA). The Operational Authority ("OA") is responsible for

the operation of the Certificate Authority (CA) in accordance with this CP and the practices described in the CPS.

The State Operational Authority ("OA") on behalf of the Illinois PA shall make a copy of this CP available to all End-Entities within its CA.

1.3.1.3 *The Illinois PKI 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 the applicable CPS.

1.3.1.4 *Entity Principal Certification Authority (CA)*

No Stipulation

1.3.1.5 *Certificate Status Servers*

No Stipulation

1.3.2 Registration Authority (RA)

The RA collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's public key certificate. The Illinois PKI Operational Authority acts as the RA for the Illinois PKI, and performs its function in accordance with a CPS approved by the Illinois PKI Policy Authority.

At least one Registration Authority (RA) shall be appointed by the State Policy Authority (PA) and shall be responsible for the identification and authentication of End-Entities in accordance with this CP.

1.3.2.1 *Local Registration Authorities ("LRA")*

Each State Agency participating in the State PKI, and other entities as determined by the PA, may appoint one or more Local Registration Authorities (LRAs) to be responsible for the identification and authentication of End-Entities within the Agency organization and its constituency in accordance with this CP.

1.3.3 Subscribers

A Subscriber is the user or device to whom or to which a certificate is issued.

This CP and applicable subscriber agreement shall 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 athttps://www.illinois.gov/bccs/services/catalog/security/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 or Relying Party (collectively referred to as an "**End Entity**") in the State PKI. End-Entities may also use Certificates issued by the Certificate Authority (CA) to encrypt information for, and verify the digital signatures of, other End-Entities within the State PKI.

1.3.4 Relying Parties

A Relying Party can be any entity that has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them, and which has agreed to be bound by the terms of this CP and the CPS.

By accepting a certificate issued pursuant to the provisions of this CP, a relying party agrees to be bound by the provisions of this 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

The sensitivity of the information processed or protected using certificates issued by Illinois PKI can vary significantly. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at ten increasing, qualitative levels of assurance: Level-1, Level-2, Level-3, Level-4, MEDI Single-Use, SHA256-Level-1, SHA256-Level-2, SHA256-Level-3 and SHA256-Level-4. It is assumed that the Illinois PKI will issue at least one SHA256-Level-4 assurance certificate, so the Illinois PKI will be operated at that level. The Illinois PKI is intended to support

applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations. State of Illinois certificates are to be used for governmental interaction and operational purposes, and not for private use.

This CP is applicable to all Certificates issued by the State Certificate Authority.

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

1.4.2 Prohibited Certificate Uses

Any use of the State of Illinois certificate used in any illegal activities or illegal gains is prohibited and if detected the certificate shall be revoked.

1.4.3 Appropriated Certificate Usage per Assurance Level

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are intended as guidance only and are not binding.

Assurance Level	Appropriate Certificate Uses
SHA1-Level-1	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This assurance level is associated with SHA-1 certificates.
SHA1-Level-2	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. At this level, the assurance of identity is of fairly high importance. This assurance level is associated with SHA-1 certificates.
SHA1-Level-3	This level is relevant to environments where threats to data are higher, the consequences of the failure of security services are high, and the assurance of identity is highly important. This may include very high value transactions or high levels of fraud risk. This assurance level is associated with SHA-1 certificates.
SHA1-Level-4	This level is appropriate for those environments where the threats to data are high, the consequences of the failure of security services are high, and the assurance of identity is

	vital. This may include very high value transactions or high levels of fraud risk. This assurance level is associated with SHA-1 certificates.
SHA1-MEDI Single-Use	This assurance level is associated with SHA-1 certificates and is no longer issued by the State of Illinois
SHA256-Level-1	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This assurance level is associated with SHA-256 certificates.
SHA256-Level-2	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. At this level, the assurance of identity is of fairly high importance. This assurance level is associated with SHA-256 certificates.
SHA-256-Level-3	This level is relevant to environments where threats to data are higher, the consequences of the failure of security services are high, and the assurance of identity is highly important. This may include very high value transactions or high levels of fraud risk. This assurance level is associated with SHA-256 certificates.
SHA-256-Level-4	This level is appropriate for those environments where the threats to data are high, the consequences of the failure of security services are high, and the assurance of identity is vital. This may include very high value transactions or high levels of fraud risk. This assurance level is associated with SHA-256 certificates.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The State of Illinois Policy Authority is responsible for this CP.

1.5.2 Contact Person

Inquiries, suggested changes, or notices regarding this Certificate Policy shall be directed to the PA Chairperson. The Chairperson's contact information is retained on a Memorandum for Record (MFR) and maintained by the Operational

Authority (OA). The OA may be reached via contact information located at http://www.illinois.gov/bccs/services/catalog/security/PKI/Pages/default.aspx.

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

The State of Illinois Certification Practices Statement must conform to this Certificate Policy.

This Certificate Policy is administered by the PA. The Policy Authority is responsible for compliance of the Certification Practices Statement (CPS) with this CP. This shall be done via a vote and approval process on all proposed changes.
In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.5.4 CPS Approval Procedures

The State Policy Authority (PA) approves this Policy, the CPS, and any subsequent changes.

The failure of the State to enforce at any time any of the provisions of this CP, the CPS, a Subscriber Agreement, or a Relying Party Agreement or the failure to require at any time performance by any other party of any of the provisions of this CP, the CPS, a Subscriber Agreement, or a Relying Party Agreement shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of the State to enforce each and every such provision thereafter. The express waiver by the State of any provision, condition, or requirement of this CP, the CPS, a Subscriber Agreement, or a Relying Party Agreement shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

The State of Illinois CA shall submit their CPS and the results of their compliance audit to the appropriate authority (See Section 1.5.3) for approval.

1.6 DEFINITIONS AND ACRONYMS

See Sections 11 and 12.

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

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

2.1 REPOSITORIES

The State of Illinois Operational Authority is responsible for operation of repositories to support their PKI operations.

Entities who cross-certify with the Illinois PKI shall ensure interoperability with the Illinois PKI repository.

The CA software contains an internal database, which immediately publishes information to a public LDAP repository that supports the State PKI and maintains availability, reliability, and sufficient protections for its contents.

2.1.1 Illinois PKI Repository Obligations

The Illinois PKI Operational Authority may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol,

2.2 PUBLICATION OF CERTIFICATION INFORMATION

This CP shall be published electronically and can be located at http://www.illinois.gov/bccs/services/catalog/security/PKI/Documents/SOI_CP_V3.9.pdf .

The following PKI information shall be published in the State Directory:

- All encryption public key certificates issued by the Certificate Authority (CA) to digital certificate users;
- All revocations of digital certificate user public key certificates performed by the CA;
- All revocations of cross-certification certificates issued by the CA.

Subscribers and Relying Parties shall periodically check the State web site for notice of intended modifications to this Certificate Policy document.

2.2.1 Publication of Certificates and Certificate Status

The Illinois PKI Operational Authority shall publish all CA certificates issued by Illinois PKI and all CRLs issued by the Illinois PKI in the Illinois PKI repository.

At a minimum, the Illinois PKI repositories shall contain all CA certificates issued by or to the Entity PKI and CRLs issued by the Illinois PKI.

For the Illinois PKI , mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week,

with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually not to include scheduled maintenance or upgrades.

Entity CAs being considered for cross certification shall be designed to comply with this requirement.

2.2.2 Publication of CA Information

This CP shall be published electronically and can be located at http://www.illinois.gov/bccs/services/catalog/security/PKI/Documents/SOI_CP_V3.9.pdf.

The Illinois CPS will be published; a redacted version of the CPS will be publicly available athttp://www.illinois.gov/bccs/services/catalog/security/PKI/Documents/CPS%20v3-3%20Final%20Redacted.pdf.

2.2.3 Interoperability

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes are recommended.

2.3 FREQUENCY OF PUBLICATION

Changes to items within this Policy that in the judgment of the Policy Authority shall have no/minimal impact on the users using Certificates and Certificate Revocation Lists issued by this Certificate Authority may be made with no change to the Policy version number and no notification to the users.

Changes to the Certificate Policy which, in the judgment of the Policy Authority may have significant impact on the users using Certificates and Certificate Revocation Lists issued by this Certificate Authority, shall undergo a review and comment period of 60 days. The State Policy Authority shall review all comments and respond individually or with further changes as appropriate. If the Policy Authority decides not to make any further changes after the 60 day review period the initially-proposed modified document shall be published in the Repository.

In order to allow entities to modify their procedures as needed, all changes to this Policy shall become effective 30 days after final publication on the State Repository. It shall be the responsibility of Subscribers and Relying Parties to periodically check the Repository for notice of final publication of this Policy.

Use of or reliance on a Certificate after the 30-day period (regardless of when the Certificate was issued) shall be deemed acceptance of the modified terms.

Certificates shall be published in the Directory immediately as they are issued.

CRLs shall be published in the Directory as they are issued (following the timeline described in Section 4.9.7).

2.4 ACCESS CONTROLS ON REPOSITORIES

The State of Illinois will make public certificates and CRL's issued by Illinois PKI available to all relying parties. Obtaining such information is the sole responsibility of the relying party.

The State of Illinois Operational Authority shall protect any information not intended for public dissemination or modification. Public keys and certificate status information in the State of Illinois repository shall be publicly available through the Internet. The use of certificates to access information in Agency repositories shall be determined by the Agency pursuant to its authorizing and controlling statutes.

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The Illinois PKI shall only generate and sign certificates that contain a non-null subject Distinguished Name (DN). Certificates issued by the Illinois PKI may also include alternative name forms.

All certificates, CA's, RA's and entities, shall include a non-NULL subject DN. The subject alternative name is non-critical.

Each End Entity must have a clearly distinguishable and unique X.500 Distinguished Name (DN) in the Certificate subject name field in accordance with IETF RFC 2026.

This Policy does not allow for the utilization of pseudonymous names in certificates.

3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by the Illinois PKI must identify the person or object to which they are assigned.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading.

In the case of device entities, the DN shall include a meaningful description of the device in addition to another form of distinguishable information such as the RDN for the individual administering the device.

Since the Illinois PKI serves most State Governmental entities, including local, municipal, city, and county governments, and since the majority of Illinois PKI users are citizens with no formal attachment to these entities, it is impossible to use a DIT structure based on organizational structure.

3.1.3 Anonymity or Pseudonymity of Subscribers

The Illinois PKI shall not issue anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Entity CAs must specify rules for interpreting names in subscriber certificates in the Entity CP or a referenced certificate profile.

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 IETF rfc822Name (email address).

3.1.5 Uniqueness of Names

Name uniqueness must be enforced by the Illinois PKI.

The Illinois Operational Authority is responsible for ensuring name uniqueness in certificates issued by the Illinois PKI.

The common name (cn) shall be a combination of first name(s) and surname. Middle initials and other identifiers may also be used.

The DN must be unique for all End Entities of the CA. For each End Entity additional numbers or letters may be appended to ensure the DN's uniqueness.

3.1.6 Recognition, Authentication, & Role of Trademarks

The issuance of a Certificate is neither designed nor intended to recognize, authenticate, verify or validate any trademark, service mark, copyright, or any other intellectual property rights in the name of any Subscriber. The Policy Authority (PA) and the Operational Authority (OA) do not certify or validate any intellectual property rights in the name of any Subscriber, expressly disclaim any such certification or validation, and make no endorsements, guarantees or warranties, express or implied, concerning any such intellectual property rights. The Policy Authority (PA) and the Operational Authority (OA) have no control over the name of any Subscriber and shall not be liable under any theory, legal or equitable, for any claims or damages relating to the name of any Subscriber, such damages including, without limitation, direct, indirect, special, incidental, statutory, reliance or consequential damages.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

In the case where a key is generated by the CA or RA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, then proof of possession is not required.

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 shall safeguard their .certificate and password and that the Certificate Authority (CA) shall 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 shall be digitally signed using the signature private key itself.

For the decryption private key, this key shall be 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 Certificate Authority (CA) does not issue Certificates to organizations.

3.2.3 Authentication of Individual Identity

An application for an individual to be a Subscriber may be made by the individual with the exception of bulk applications as described in section 4.1.

Identification and authentication of the prospective Subscriber must be in accordance with the procedures specified in the State Certification Practice Statement.

The Registration Authority (RA) or Local Registration Authority (LRA) shall keep a record of the type and details of the identification used.

The Illinois Operational Authority and RAs/LRAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required under local law. The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten or digital signature and performed in the presence of an LRA or a licensed notary public.

The Illinois PKI does not allow proxy identification/registration of a human subscriber.

Assurance Level	Identification Requirements
SHA1-Level-1	Identity may be established by comparison of user supplied identity information with a trusted information

	source; or by attestation of a Registration Authority (LRA) or other Trusted Agent.
SHA1-Level-2	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D.
SHA1-Level-3	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D. Approval subject to completion of a background check.
SHA1-Level-4	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D. Approval subject to completion of a background check. Private keys shall be secured using a biometric device
SHA1-MEDI Single Use	This assurance level is associated with SHA-1 certificates and is no longer issued by the State of Illinois
SHA256-Level-1	Identity may be established by comparison of user supplied identity information with a trusted information source; or by attestation of a Registration Authority (LRA) or other Trusted Agent.
SHA256-Level-2	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D.
SHA256-Level-3	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D. Approval subject to completion of a background check.
SHA256-Level-4	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D. Approval subject to completion of a background check. Private keys shall be secured using a biometric device

All certificates and requests/upgrades are performed within 30 days.

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*

The Illinois PKI does not issue group certificates.

3.2.3.3 *Authentication of Devices*

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Contact information to enable the CA or RA to communicate with the sponsor when required

During the certificate generation process, the device public keys are received and are bound to the identity created by the certificate. An application for a device or a software application to be a Subscriber shall be sponsored by an individual who represents the organization that is accountable for the device or application. The Registration Authority (RA) or Local Registration Authority (LRA), as defined in section 5.2.1 must authenticate and register the device, commiserate with the assurance level required as part of the process of authenticating the device or application. Both the authentication of the sponsoring individual and the authentication of the device or application shall follow the procedures described in this CP and the corresponding CPS.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

For cross-certification, the State of Illinois Policy Authority shall validate the representative's authorization to act in the name of the organization.

3.2.6 Criteria for Interoperation

The State of Illinois Operational Authority shall determine the criteria for cross-certification with the State of Illinois.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

The Registration Authority (RA) sets keys for automatic renewal/update as required.

3.3.1 Identification and Authentication for Routine Re-key

Routine rekey occurs prior to key expiration as described in 6.3.2 Usage Periods for Public and Private Keys. Subscribers may update certificates automatically unless the certificate has been revoked or previously updated – except that the

Subscriber's identity must be re-established through the existing registration process at least once every nine years. For automatic update, the subscriber shall be authenticated through the current private signature key. Any time that automatic rekey is blocked; the Subscriber's identity must be re-established through the existing registration process.

3.3.1.1 *Routine Re-key – Device or Application*

Certificates issued to devices and applications shall be automatically renewed when the key validity period expires.

3.3.2 Identification and Authentication for Re-key after Revocation

For Subscribers whose Certificates have been revoked, recovery after revocation shall not be permitted until the Subscriber's identity is re-established through the existing registration process.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated.
Revocation of an Individual's certificate can be requested by the CA, RA the local Registration Authority (LRA) for the Subscriber's organization, a State agency, or by the Subscriber.

Revocation of a certificate issued to a device or application may be requested by the individual who sponsored the application for the certificate or another individual authenticated as representing the organization accountable for the device or application.

The Registration Authority (RA) and LRAs shall permit Subscribers to request revocation of a Certificate in which the requestor is identified as the Subject in the certificate. RA and LRAs shall adhere to the procedures identified in the State CPS for authentication of revocation requests.

4. CERTIFICATE LIFE-CYCLE

This section describes operational requirements imposed by this Policy on the Certificate Authority (CA), Registration Authorities (RAs), Registration Authorities (LRAs) and End Entities. It includes handling of Certificate revocations, audit logs, and transaction archives.

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 occurred when someone had undergone a face-to-face registration and activation codes have been generated, but the recipient never activated their certificate. This situation is handled as stipulated in Section 4.4.1.1 of the CPS.

4.1 APPLICATION

This section specifies requirements for initial application for certificate issuance.

The Registration Authority (RA) and appropriate Local Registration Authorities (LRAs) shall accept certificate applications from state employees or individuals who need to conduct electronic business with the State of Illinois through three primary 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 SHA1-Level-1 or SHA256-Level-1 certificate as described in section 3.2.3.

In person applications may 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 shall be accepted by the RA from appropriate LRAs in accordance with procedures developed on a case by case basis. These procedures shall comply with all requirements of this Certificate Policy and shall 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 shall 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.

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

For the Illinois CA, the certificate application shall be submitted to the Illinois Operational Authority by an authorized representative of the Illinois CMS Director's office.

The Registration Authority (RA) shall accept certificate applications submitted on behalf of hardware devices and software applications or processes that are owned by the State of Illinois or operated by an external entity for the purpose of inter-operating with or operating on behalf of the State. Applications shall be accepted from State employees or Local Registration Authorities (LRAs) holding currently valid Certificates issued by this Certificate Authority (CA) and shall be signed by the appropriate LRA or the agency Director, if no agency LRA is available. The application must include appropriate identification information for the device, a description of the device, the name of the person responsible for maintaining the device, and the purpose that the certificate shall serve if issued. For certificates issued to external entities, the application must also include the name of the State agency employee who is responsible for the ongoing relationship with the external entity, which requires the certificate.

4.1.2 Application for a Cross Certificate

Entities applying for cross-certification are responsible for providing accurate information on their certificate applications. Upon issuance, each certificate issued by the Illinois PKI shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Entity.

For Illinois and cross-certified CAs, all communications among PKI authorities supporting the certificate application and issuance process shall be authenticated and protected from modification.

The Policy Authority (PA) shall develop the necessary procedures to apply for a cross-certificate.

An application for a cross-certificate does not obligate the Policy Authority (PA) to authorize a cross-certificate. The Policy Authority (PA) shall review any CA's request for cross-certification and approve or deny the request according to established procedures.

A Certificate Authority (CA) requesting cross-certification shall include with application:

- Its Certificate Policy
- An external audit report validating the assurance level stated in the CP
- The public verification key generated by the CA
- A statement describing how the proposed cross-certification shall benefit the State of Illinois and its citizens

4.2 CERTIFICATE APPLICATION PROCESSING

Information in certificate applications must be verified as accurate before certificates are issued. Illinois CPs shall specify procedures to verify information in certificate applications for cross – certifying entities.

4.2.1 Performing Identification and Authentication Functions

For the Illinois PKI, the identification and authentication of the applicant shall be performed by the Illinois Operational Authority.

For Illinois CAs, the identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in Section 3.2 of this CP. The Illinois CP identifies the components of the Illinois PKI (e.g., CA or RA or LRA repository) that are responsible for authenticating the Subscriber's identity.

4.2.2 Approval or Rejection of Certificate Applications

For the Illinois PKI, the Illinois Policy Authority may approve or reject a certificate application.

4.2.3 Time to Process Certificate Applications

Certificate applications originating from individuals with an Illinois drivers license or State Id card may apply for their certificates online, in which case the certificate shall normally be issued within 1-5 minutes. Out of State certificate applicants must have an application form notarized and sent to the OA for processing. In this case, the certificate applications shall be processed within 48 hours of receipt.

4.3 ISSUANCE

The issuance and publication of a Certificate by the Certificate Authority (CA) indicates a complete and final approval of the certificate application by the CA. A self-signed root CA certificate is securely delivered to the subscriber using PKIX-CMP protocol during the certificate issuance process.

4.3.1 CA Actions during Certificate Issuance

The Illinois Operational Authority verifies the source of a certificate request before issuance.

The issuance and publication of a Certificate by the Certificate Authority (CA) indicates a complete and final approval of the certificate application by the CA. A self-signed root CA certificate is securely delivered to the subscriber using PKIX-CMP protocol during the certificate issuance process.

4.3.2 Notification to Subscriber of Certificate Issuance

Refer to section 4.4.

4.4 CERTIFICATE ACCEPTANCE

As part of the certificate issuance process, a Subscriber shall explicitly indicate acceptance or rejection of the Certificates to the Certificate Authority (CA) and shall expressly acknowledge to the Registration Authority (RA) or Local Registration Authority (LRA) prior to delivery that it shall adhere to this Policy, both as Subscriber and as Relying Party.

As part of the certificate verification process, a Relying Party must agree to be bound by the terms of the Relying Party Agreement, and must expressly acknowledge and accept the terms of the same prior to being afforded access to any certificate validity information.

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.

4.4.2 Publication of the Certificate by the CA

As specified in 2.2.1, all CA certificates shall be published in the State of Illinois repository.

4.4.3 Notification of Certificate Issuance by the CA to other entities

If the Illinois PKI should issue any other CA certificate which extends its trust model, any existing cross-certified members shall be notified of other entities holding other cross certified pairs.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

All levels of assurance shall protect their private keys from access by other parties 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.

4.5.2 Relying Party Public key and Certificate Usage

End entities that rely on Certificates shall:

- Verify that the State issued certificate is within the validity period specified within the certificate;
- Verify certificates through appropriate means including a) revocation status checking through use of Certificate Revocation Lists (CRLs).
- Trust and make use of certificates only if the validity of the certificate is established between the relying party and the certificate subject. And Relying parties shall rely on a valid Certificate for purposes of verifying the digital signature only if prior to reliance, the Relying Party shall:

    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 shall not be reflected in the Certificate itself, but must be verified by consulting the most recent certificate revocation list.

Illinois PKI -issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. The Illinois PKI issues CRLs specifying the current status of all expired Illinois PKI certificates (note that expired certificates roll off of the CRL after one issuance cycle). It is recommended that relying parties process and comply with this information whenever using Illinois PKI issued certificates in a transaction.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key.

The Illinois CA doesn’t support certificate renewal in accordance with the FPKI definition.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

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

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. This certificate becomes part of the certificate's key history. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

The Illinois PKI subscribers shall identify themselves for the purpose of re-keying as required in Section 3.3.1.

After certificate rekey, the old certificate (the one in key history) may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

The Illinois PKI will issue new cross-certificates to Principal CAs when a currently recognized Principal CA has generated a new key pair and a valid and unexpired MOA exists between the Illinois Policy Authority.

4.7.2 Who may request certification of a new public key

The Illinois PKI Operational Authority may request certification of a new public key for currently cross-certified Entity Principal CAs.

For Illinois or cross certified CAs that support re-keys, such requests shall only be accepted from the subject of the certificate or PKI sponsors. Additionally, CAs and RAs may initiate re-key of a subscriber's certificates without a corresponding request.

4.7.3 Processing certificate Re-keying requests

Before performing re-key, the Illinois PKI Operational Authority shall identify and authenticate Principal CAs by performing the identification processes defined in Section 3.2 or Section 3.3.

The validity period associated with the new certificate must not extend beyond the period of the MOA.

For Entity CAs, see Sections 3.2 and 3.3.

4.7.4 Notification of new certificate issuance to Subscriber

The Illinois PKI Operational Authority shall notify Entity CAs upon issuance of new cross-certificates.

For Entity CAs, no stipulation.

For subscriber certificates, 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.

For Entity CAs, no stipulation.

4.7.6 Publication of the Re-keyed certificate by the CA

As specified in 2.2.1, all CA certificates shall be published in the Illinois PKI or Entity repositories.

4.7.7 Notification of certificate issuance by the CA to other Entities

The Illinois PKI Operational Authority shall inform the FPKIPA of any cross-certificate issuance.

For Entity CAs, no stipulation.

4.8 MODIFICATION

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, an Entity CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.

After certificate modification, the old certificate that resides in key history may or may not be revoked, but must not be further re-keyed, or modified.

4.8.1 Circumstance for Certificate Modification

A certificate may be modified in the case of an email address change, a distinguished name change, or any other change approved by the OA.

4.8.2 Who may request Certificate Modification

Either CAs or end-entities may request certificate modification

4.8.3 Processing Certificate Modification Requests

The Illinois PKI Operational Authority shall perform certificate modification at the direction of the FPKI PA. The Illinois PKI Operational Authority may also perform certificate modification at the request of the Entity CA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.
- Email address
- Distinguished name changes

The validity period associated with the new certificate must not extend beyond the period of the MOA.

For Illinois CAs, proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.

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

4.9 CERTIFICATE REVOCATION & SUSPENSION

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

The State of Illinois CA shall publish CRLs for all certificates for all assurance levels.

4.9.1 Circumstances for Revocation

A Certificate shall be revoked when the Subscriber no longer wants or requires a certificate, or when the Public Key password, token or profile associated with the certificate is compromised or suspected of being compromised. Certificates may also be revoked by the Certificate Authority (CA) upon failure of the Subscriber to meet its obligations under this Policy or any other agreement, regulation, or law that may be in force. Subscribers shall request revocation promptly following detection or suspicion of a compromise or any other event necessitating revocation. The Registration Authority (RA) or Local Registration Authority (LRA) may originate a certificate revocation if knowledge or suspicion of compromise is obtained. The rationale for such a revocation shall be documented, signed by at least one of the CA personnel, and archived.

A Certificate holder's encryption and/or verification certificate is revoked when the certificates are no longer trusted for any reason. Some of the specific reasons for loss of trust in certificates include, but are not limited to:

- Compromise or suspected compromise of private keys and/or user passwords and profile;
- Failure of the subscriber to meet their obligations under this CP and CPS;
- Failure to prove continued ownership of the private keys;
- Request by the Subscriber;
- Receipt of a certified copy of subscriber’s death certificate;
- When information on a certificate changes or becomes obsolete; or
- If the issuing CA determines that the Certificate was not properly issued in accordance with the Certificate Policy.

Agency staff may see indications that a particular certificate cannot be trusted through the course of conducting electronic transactions that involve a particular certificate; however, change in employment status with the agency is NOT by itself a justification for revocation of a certificate.

For the Illinois CAs, a certificate shall be revoked when the binding between the subject and the subject’s public key defined within a certificate is no longer considered valid. There are other circumstances under which certificates issued by the Illinois CA will be revoked:

- When the Operational Authority receives an authenticated request from a previously designated official of the Entity responsible for the certificate.

- When the Illinois PKI Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the Illinois PKI. Under such circumstances, the following individuals may authorize immediate certificate revocation:
    - Chair, Illinois PKI Policy Authority, or
    - Other personnel as designated by the Chair, Illinois PKI Policy Authority.

The Illinois PKI Policy Authority shall meet as soon as practicable to review the emergency revocation.

Illinois CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Revocation of an Individual's certificate may be requested by the Certificate Authority (CA), the Local Registration Authority (LRA) for the Subscriber's organization, a State agency, or by the Subscriber.

An Illinois PKI certificate may be revoked upon direction of the State PKI Policy Authority or upon an authenticated request by a designated official of the Entity responsible for the Principal CA (such official or officials shall be identified in the MOA as authorized to make such a request).

Entity CAs that implement certificate revocation shall, at a minimum, accept revocation requests from subscribers. Requests for certificate revocation from other parties may be supported by Entity CAs. Note that an Entity Principal CA may always revoke the certificate it has issued to the Illinois PKI without any State PKI Policy Authority action.

4.9.3 Procedure for Revocation Request

In the event a revocation request is initiated by an entity other than the Subscriber, the Subscriber shall be afforded reasonable notice and opportunity for hearing. Where the risk to the security and integrity of a private key suggest a reasonable likelihood of irreparable harm absent immediate revocation, a certificate may be revoked without prior notice and opportunity for hearing, provided the subscriber is afforded reasonable notice and opportunity for hearing following Certificate revocation.

- A revocation request may be generated electronically. The request shall be signed with the Subscriber's private signing key and sent to the Registration Authority (RA) or Local Registration Authority (LRA). Alternatively, the Subscriber may notify the RA or LRA in writing.

- All revocation requests and the resulting actions taken by the RA or LRA shall be archived.

- The CA notifies Relying Parties by posting revoked certificates to a CRL in the public Directory. Revocation shall be effective upon publication of the CRL.

- When a certificate is revoked by the CA, a revocation reason shall be included in the CRL entry for the revoked certificate.

- Revoked certificates shall be included on all new publications of the CRL until the certificates expire

Upon receipt of a revocation request involving an Illinois PKI -issued certificate, the Illinois PKI Operational Authority shall authenticate the request. The Illinois PKI Operational Authority may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the Illinois PKI Operational Authority shall revoke the certificate. The Illinois PKI Operational Authority shall give prompt oral or electronic notification to previously designated officials in all entities having a Principal CA with which the Illinois PKI interoperates.

Illinois CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the user to export the signature private key;
- the Subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified.

Revocation requests shall be processed within 18 hours from time of receipt by the RA.

In the case of key compromise, Illinois PKI subscribers (e.g., Entity CAs) are required to request revocation within one hour. For all other reasons, Illinois PKI subscribers are required to request revocation within 24 hours.

4.9.5 Time within which CA must Process the Revocation Request

The Illinois PKI and Entity CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published. CRL's are automatically reissued after a revocation.

4.9.6 Revocation Checking Requirements for Relying Parties

Certificates may be stored locally in the Relying Party's Public Key application but, before use, the status of the certificate shall be checked against a CRL less than twenty-four (24) hours old.

4.9.7 CRL Issuance Frequency

CRLs shall be published immediately upon revocation of a Certificate or at least every 24 hours.

Compromise procedures and a Disaster Recovery Plan for the CA, Registration Authority (RA) and Local Registration Authorities (LRAs) are in place in accordance with the procedures specified by the CA, giving priority to certificate status information. These procedures can be found in the document entitled "State of Illinois Central Management Services Public Key Infrastructure Recovery Activation Plan."

For this CP, CRL issuance encompasses both CRL generation and publication.

For the Illinois PKI, the interval between CRLs shall not exceed 24 hours.

4.9.8 Maximum Latency of CRLs

For the Illinois PKI, CRL's are pushed immediately after generation.

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 other methods are permitted or used.

4.9.12 Special Requirements Related To Key Compromise

In the event of a subscriber key compromise or suspected compromise, the Certificate shall be revoked and a new CRL immediately published. For CA certificates, not applicable.

4.9.13 Circumstances for Suspension

Not Supported. Suspension shall not be used by the Illinois PKI.

4.9.14 Who can Request Suspension

Not supported.

4.9.15 Procedure for Suspension Request

Not supported.

4.9.16 Limits on Suspension Period

Not supported.

4.10 CERTIFICATE STATUS SERVICES

Not supported.

4.10.1 Operational Characteristics

Not supported.

4.10.2 Service Availability

Not supported.

4.10.3 Optional Features

Not supported.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW & RECOVERY

The State of Illinois shall maintain key history per CA application, but not for key escrow purposes. CA private keys are never escrowed. Subscriber key history is maintained to provide for key recovery (refer to section 5.6). No keys in the Illinois PKI are escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

This section outlines the physical, procedural, and personnel security controls required of the Certificate Authority (CA), Registration Authority (RA), Local Registration Authority (LRA) and Subscribers to protect their operations.

5.1 PHYSICAL CONTROLS

Physical security controls shall be implemented at all times to prevent unauthorized access to the Certificate Authority (CA) hardware and software. This includes the CA host computer and any external cryptographic hardware module or token.

5.1.1 Site Location & Construction

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

The Certificate Authority (CA) host computer shall be in a secure space with access control and IP based monitoring systems. Access to the CA host computer shall be limited to those personnel performing one of the roles described in this Policy. Access shall be controlled through the use of electronic access controls, mechanical combination locksets, or deadbolts. The secure space shall be monitored in accordance with procedures outlined in the CPS.

5.1.2 Physical Access

Access to the Certificate Authority (CA) host computer shall be limited to those personnel performing one of the roles described in this Policy. Access shall be controlled through the use of electronic access controls, mechanical combination locksets, or deadbolts.

5.1.2.1 *Physical Access for CA Equipment*

When the PKI system was first installed, the entire procedure was audited, videotaped, and scripted in the Root Key Generation Ceremony script. During this ceremony, software versions were examined and verified, hardware platforms were validated, and the entire environment was scrutinized to ensure integrity. This was the basis of the establishment of the secure environment. All future updates/changes to the environment are done in accordance with the CPS.

The Illinois CA equipment (including remote workstations) shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the FIPS 199 moderate level of threat in the equipment environment as determined by the State of Illinois. The Illinois CA operates at a high level of assurance.

The physical security requirements pertaining to CAs that issue Illinois SHA1-Level-1 and SHA256-Level-1 certificates are:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers

In addition to those requirements, the following requirements shall apply to CAs that issue Federal Medium, Medium Hardware, or High assurance certificates (Illinois SHA1-Level-2/3/4 and SHA256-Level-2/3/4):

- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer system

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the Illinois CA equipment or remote workstations used to administer the CA operating at the SHA1-Level-1 and SHA256-Level-1 assurance level or higher shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

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

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

5.1.2.2 *Physical Access for RA Equipment*

RA/LRA equipment shall be protected from unauthorized access; the RA/LRA shall implement physical access controls to reduce the risk of equipment tampering. These security mechanisms shall be commensurate with the moderate level of threat in the RA equipment environment.

The Registration Authority (RA) and Local Registration Authorities (LRAs) shall implement at a minimum the following controls:

- The RA computers shall have the boot-lock feature turned on and enable the password protected screen saver feature, and computers shall not be left unattended when the Private Key is in the unlocked state (i.e. when the password has been entered);
- The RA and LRA shall physically protect any password that allows access to keys. Passwords should be memorized and not written down. If a password must be written down, it shall be stored in a locked file cabinet or container accessible only to the RA or LRA;
- If a private key is stored encrypted on a diskette or other unsecured medium, such diskette or other medium shall be stored in a locked file cabinet or container when not in use; and
- LRAs shall not leave their computers unattended when the Private Key is in an unlocked state (i.e., when the password has been entered).
- Any RA or LRA computer that contains private keys encrypted on a hard drive must be secured.

5.1.2.3 *Physical Access for CSS Equipment*

Not applicable.

5.1.2.4 *Physical Security Controls for Subscribers*

Each Subscriber shall physically protect any password that allows entry into the Subscriber's Certificate Authority (CA) Client application. Passwords should be memorized and not written down. If a password must be written down, it shall be securely stored such that only the Subscriber has access to it. Subscribers shall not leave their computers unattended when the Private Key is in an unlocked state (i.e., when the password has been entered).

5.1.3 Power and Air Conditioning

Primary or main electrical power to the facility shall be provided by City, Water, Light & Power, a municipal-owned power company within the city of Springfield, Illinois. Two separate electrical power lines provide service to the building. These electrical trunk lines are located in separate underground trenches that have access into the structure. These electrical feeds are capable of providing an electrical service load up to the capacity of four thousand (4kW) amperes. An uninterruptible Power Supply (UPS) is also in place consisting of both batteries and generators.

The air conditioning for the main computer floor of the CCF building shall be provided via eighteen Liebert Air conditioning units, which is distributed among five 30-ton and thirteen 20-ton units. The approximate age of these air conditioning units is two years and is based upon an installation date of in 2004. These units work in conjunction with three 300-ton York centrifugal chiller systems located on the first floor maintenance area of the facility with a mounted cooling tower. Both the cooling tower and centrifugal chillers are approximately 4 years old. The cooling system is rotated into service on a tri-monthly schedule. Each unit, in itself, is capable of providing all the necessary cooling requirements for the entire computer facility. The configuration of this system is a high availability solution with redundant capabilities that provides the ability to recover and provide cooling services from a two-failure event. These systems are maintained by an annual State contract, where services are provided by a local contracting Customer.

The Illinois CAs shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.) In addition, the Illinois CA directories (containing Illinois issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power. Entity CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1.

5.1.4 Water Exposures

The Illinois PKI environment shall be fully protected from water damage. The State Data Center facility is fully equipped with protection from water damage as described in section 5.1.4 of the CPS.

5.1.5 Fire Prevention & Protection

The Illinois PKI environment shall be fully protected from fire damage. The State Data Center facility is fully equipped with protection from fire damage as described in section 5.1.5 of the CPS.

5.1.6 Media Storage

Illinois CA media shall be stored so as to protect it from accidental damage. Sensitive Illinois CA media shall be stored so as to protect it from unauthorized physical access.

Archived and media records shall be transferred to separate physical media external to the Certificate Authority (CA) host system and CA application.

5.1.7 Waste Disposal

Any documents containing sensitive information as provided under this Certificate Policy (CP) shall be shredded prior to disposal. Any sensitive media will be destroyed when no longer needed.

5.1.8 Off-Site backup

For the Illinois CAs operating at the SHA1-Level-4 and SHA256-Level-4 assurance level or lower, full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the Illinois CA equipment. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational Illinois CA.

5.2 PROCEDURAL CONTROLS

Responsibilities at the Certificate Authority (CA) host computer may be shared by multiple individuals assigned to multiple roles. Each account on the CA host computer and/or within the CA application should have limited capabilities commensurate with the role of the account holder. Two or more persons are required to perform the following tasks:

- Adding and deleting Security Administrators.
- Changing the Security Administrator's password.
- CA Master Key updates.

A single person may be assigned to perform all Local Registration Authority (LRA) tasks.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the FBCA or an Entity CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of six roles.

1. *Administrator*
    - System Administrator- authorized to install, configure, and maintain the CA; establish and maintain user accounts; authorized to perform system backup, recovery and maintenance.
    - CA Administrator-authorized to maintain the operational functions of the CA utilizing administration software.
    - *Directory Administrator*-Responsible for the maintenance and operation of the repository used by the PKI environment

2. *First Officer* – authorized to request or approve certificates or certificate revocations.
3. *Auditor* – authorized to maintain audit logs.
4. *Master User*- configures profiles and audit parameters; and generates component keys. Controls key functions of the PKI software; recovers First Officer password.
5. *Local Registration Authority*-Authorized to perform face-to-face verifications for identification necessary for certificate issuance/upgrade.
6. *Bulk Operations Administrator*-Authorized to perform bulk load operations for certificate creation.

Some roles may be combined. The roles required for each level of assurance are identified in Section 5.2.4.

The following subsections provide a detailed description of the responsibilities for each role.

5.2.1.1 *Administrator (CA, System, and Directory)*

System Administrator

The System administrator role is responsible for:

- Installation, configuration, and maintenance of the CA hardware and software;
- Establishing and maintaining CA system accounts;

System Administrators do not issue certificates to subscribers.

The System Administrator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

The System Administrator role is also known as the Operator role.

CA Administrator

The CA (security) Administrator role is responsible for:

- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.
- CA Administrators can issue certificates to subscribers.

The CA Administrator role is responsible for the overall maintenance of the running and operation of the CA as it pertains to certificate creation and usage.

Directory Administrator

The Directory Administrator is responsible for the availability and maintenance of the PKI repository, including the following functions:

- Creating searchbases
- Creating shadow agreements
- Monitoring the performance of the directory

5.2.1.2 *First Officer*

The First Officer role is responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 *Auditor*

- Refer to the Certification Practices Statement.

5.2.1.4 *Master User*

Master Users perform functions relating to CA “master commands”. Examples include, but are not limited to:

- resetting the First Officer’s password
- recovering the Informix database
- Setting CA system parameters using the Master shell

Some master user commands require multiple master users to perform.

5.2.1.5 *Local Registration Authority*

Local Registration Authorities are authorized to perform face-to-face verifications for identification necessary for certificate issuance/upgrade. They also serve as the main point of contact for operational matters for the OA.

5.2.1.6 *Bulk Operations Administrator*

This role can process bulk files for certificate creation (normally out-of-State registrations) only. This role has no administrative authority.

5.2.2 Number of Persons Required per Task

All Security Administrators operations shall need one Security Administrator authorization. Certain functions, such as activation of the Certificate Authority (CA) Private Key, shall be protected by multi-person controls. In the State PKI the following operations need two Master User authorizations:

- adding and deleting Security Administrators;
- Changing a Security Administrator's password;
- CA Master Key updates.

The Illinois CA requires two or more persons for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.

5.2.3 Identification and Authentication for Each Role

The Certificate Authority (CA) administrative interfaces are used by PKI entities with special privileges, to perform the CA and Registration Authority (RA) functions in the State PKI. These roles and associated privileges are described below:

At the State, there are three Master Users. Their PKI Master User passwords are documented and stored in a safe approved by the State Operational Authority (OA). The Master Users have authority to:

- Maintain Certificate Authority (CA) software services and database.
- Recover Security Administrator and Security Administrator Backup in the event they have forgotten their passwords.
- Recover the RA services, in the event its profile becomes damaged.
- Backup, re-encrypt and restore from backup as necessary, the Certificate Authority (CA) database.

In the Certificate Authority (CA) context, the State personnel who specify the State CA's security policies are Security Administrators. The Security Administrator created during the installation of the Certificate Authority (CA) software is the 'First Officer'. The First Officer, drawing from selected State personnel, creates additional Security Administrators. The main role of the Security Administrators is to set and administer the State's security policy as it applies to all PKI Subscribers. Security Administrators use the Certificate Authority (CA) management interface and have the following privileges:

- Set the security policy for the CA, and alter it.
- Add, delete and deactivate other Security Administrators, Local Registration Authorities, Directory Administrators and Subscribers.
- Authorize sensitive operations, such as adding and deleting Security Administrators and Certificate Authority Administrators.
- Process audit logs.
- All Certificate Authority Administrator privileges.

In the Certificate Authority (CA) software context, the State personnel and any others who are RA's have Administrator privileges. These are:

- Add, delete and suspend Subscribers.
- Manage key recovery for Subscribers.
- Revoke Subscriber Certificates.
- Change Subscriber DNs.

The State Certificate Authority (CA) hardware staff performs the role of System Administrator and has root access to the CA operating system. The Operation Authority shall perform routine self-assessments of security controls.

In the event that the PKI disaster recovery plan is activated, at least 1 master user or OA member shall be present during the recovery process. Sensitive material, such as the Certificate Authority (CA) private signing key, shall remain in the possession of one of these persons at all times until it's activation at the disaster recovery site.

5.2.4 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

In the Illinois PKI, for all assurance levels, Individual personnel shall be specifically designated to the seven roles defined in Section 5.2.1 above. Individuals may assume only one of the CA Administrator and Auditor roles. Individuals designated as First Officer or CA Administrator may not assume the

System Administrator/Operator role. An auditor may not assume any other role. The CA and RA software and hardware shall identify and authenticate its users and shall enforce these roles.

5.3 PERSONNEL CONTROLS

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

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

Certificate Authority (CA) and Registration Authority (RA) personnel shall:

- Be appointed by the PA;
- Be an employee or other authorized individual not subject to frequent re-assignment or extended periods of absence.

The Illinois PKI shall identify at least one individual or group responsible and accountable for the operation of any Illinois CA.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For the Illinois PKI operated in the U.S., all trusted roles are required to be held by U.S. citizens. For PKIs operated at high assurance level, each person filling a trusted role must satisfy at least one of the following:

- The person shall be a citizen of the country where the CA is located; or
- All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity.
- For RA personnel only, in addition to the above, the person may be a citizen of the country where the RA is located.

5.3.2 Background Check Procedures

All individuals fulfilling Trusted Roles within the State must submit to a background investigation, which involves checking the Illinois State Police LEADS system. A previously conducted background check will be accepted as long as it is no more than 2 years old at the time of applying to become an LRA.

A previously conducted background check shall be accepted as long as it is no more than 2 years old at the time of applying to become an LRA.

5.3.3 Training Requirements

Certificate Authority (CA) and Registration Authority (RA) personnel shall receive proper and continuous training in relation to their assigned duties. All training is documented.

All personnel performing duties with respect to the operation of the Illinois CA shall receive comprehensive training in all operational duties they are expected to perform, including disaster recovery and business continuity procedures.

In addition, personnel performing duties with respect to the operation of the Illinois CA shall receive comprehensive training, or demonstrate competence, in the following areas:

- CA/RA security principles and mechanisms;
- All PKI software versions in use on the CA system.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency & Requirements

All Operational Authority members shall receive proper and continuous training in relation to their assigned duties.

Documentation shall be maintained identifying all personnel receiving training and the level of training completed.
Individuals responsible for PKI roles shall be aware of changes in the Illinois PKI operations.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency & Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

If the Certificate Authority (CA) or Operational Authority (OA) determines that a Person or Entity has engaged in an action that is not authorized under the CP, the CPS, or the administrative rules pertaining to the State of Illinois Public Key Infrastructure (PKI), the Person or Entity shall be advised of the unauthorized action and the corrective action that must be taken. If the unauthorized action warrants the revocation or suspension of a Certificate, the process for revoking or suspending the Certificate provided under the PKI administrative rules shall be commenced.

5.3.7 Independent Contractor Requirements

All contractor personnel required for on-site support during the in-service phase of the Certificate Authority (CA) shall be escorted.
Contractor personnel employed to perform functions pertaining to the Illinois PKI shall meet the contractual requirements set forth by the State of Illinois Procurement practices and the CP.

5.3.8 Documentation Supplied To Personnel

Illinois law (5 ILCS 175-Electronic Commerce and Security Act) requires that a copy of this CP and a redacted version of an applicable CPS be available in electronic format from the State. Suggested changes may be submitted to the contact person specified in Section 1.5.2 of this CP. A copy of the CP and CPS is available to all trusted roles and other operational documentation. All documentation, procedures, and other processes necessary to perform the required job functions and to ensure the safe and proper operations of the Illinois PKI shall be provided to all trusted roles.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the Illinois PKI. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention period for archive*, Section 5.5.2.

5.4.1 Types of Events Recorded

All significant events shall be recorded in the Certificate Authority (CA) audit logs in accordance with the procedures specified in the CPS. Logbooks, paper forms, and other physical mechanisms are used where automated collection of events is not possible.
A message from any source received by the Illinois PKI requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- A success or failure indicator, where appropriate
- The identity of the entity and/or operator (of the Illinois CA) that caused the event,

Detailed audit requirements are listed in the table below according to the level of assurance. The Illinois Root CA shall record the events identified in the table for High Assurance.

All security auditing capabilities of the Illinois CA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

*= denotes that the information is found on the CA server in location /authdata/CA1/log/Audit.*date* - otherwise in stated location

Auditable Event	**SHA1-Level-1 and SHA256-Level-1**	**SHA1-Level-2 and SHA256-Level-2**	**SHA1-Level-3 and SHA256-Level-3**	**SHA1-Level-4 and SHA256-Level-4**
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Obtaining a third-party time-stamp		X	X	X
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role *		X	X	X
The value of *maximum authentication attempts* is changed *		X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login *		X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts*		X	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics*		X	X	X
LOCAL DATA ENTRY				

Auditable Event	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256-Level-4
All security-relevant data that is entered in the system		X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system*		X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X
KEY GENERATION				
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)*	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys*	X	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes*	X	X	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted public keys, including additions and deletions*	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication*			X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)*	X	X	X	X

Auditable Event	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256-Level-4
CERTIFICATE REGISTRATION				
All certificate requests - * *and in cabinet in PKI office*	X	X	X	X
CERTIFICATE REVOCATION				
All certificate revocation requests – *in cabinet in PKI office*		X	X	X
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request – *in cabinet in PKI office*		X	X	X
CA CONFIGURATION				
Any security-relevant changes to the configuration of the CA *		X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted *	X	X	X	X
The access control privileges of a user account or a role are modified *	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile *	X	X	X	X
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile *		X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the certificate revocation list profile *		X	X	X
MISCELLANEOUS				

Auditable Event	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256-Level-4
Appointment of an individual to a Trusted Role – *in cabinet in PKI office*	X	X	X	X
Designation of personnel for multiparty control – *in cabinet in PKI office*			X	X
Installation of the Operating System –*Remedy change Management*		X	X	X
Installation of the CA –*Remedy change Management*		X	X	X
Installing hardware cryptographic modules –*Remedy change Management*			X	X
Removing hardware cryptographic modules –*Remedy change Management*			X	X
Destruction of cryptographic modules		X	X	X
System Startup *		X	X	X
Logon Attempts to CA Applications – *on Roaming servers: C:\Program files\Entrust\RoamingServer\logs*		X	X	X
Receipt of Hardware/Software – *Remedy change Management*			X	X
Attempts to set passwords *		X	X	X
Attempts to modify passwords *		X	X	X
Backing up CA internal database *		X	X	X
Restoring CA internal database *		X	X	X
File manipulation (e.g., creation, renaming, moving)			X	X
Posting of any material to a repository *			X	X

Auditable Event	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256-Level-4
Access to CA internal database *			X	X
All certificate compromise notification requests – *in cabinet in PKI office*		X	X	X
Loading tokens with certificates			X	X
Shipment of Tokens			X	X
Zeroizing tokens		X	X	X
Re-key of the CA *	X	X	X	X
Configuration changes to the CA server involving: –*Remedy change Management*				
- Hardware		X	X	X
- Software		X	X	X
- Operating System		X	X	X
- Patches		X	X	X
- Security Profiles			X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing CA – *Sign in sheet in PKI server room*			X	X
Access to the CA server – *Sign in sheet in PKI server room*			X	X
Known or suspected violations of physical security –*incident report at BCCS Security desk*		X	X	X
ANOMALIES				
Software Error conditions - */var/adm/messages***.***		X	X	X
Software check integrity failures *		X	X	X
Receipt of improper messages			X	X

Auditable Event	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256-Level-4
Misrouted messages			X	X
Network attacks (suspected or confirmed) –*Cisco Intrusion Prevention systems on the device and S:TechSafeGuards\CRTS\CIRT and /var/adm/messages.**		X	X	X
Equipment failure – *Lights out port and /var/adm/messages.**	X	X	X	X
Electrical power outages – *Daily report kept in Property Management Office*			X	X
Uninterruptible Power Supply (UPS) failure			X	X
Obvious and significant network service or access failures			X	X
Violations of Certificate Policy – *in cabinet in PKI office*	X	X	X	X
Violations of Certification Practice Statement – *in cabinet in PKI office*	X	X	X	X
Resetting Operating System clock - */var/adm/messages.* and /var/db/ntp.drift*		X	X	X

5.4.2 Frequency of Processing Log

For all assurance levels, audit logs shall be reviewed at least once every week in accordance with the procedures specified by the CPS. Identified issues shall be investigated and processed and out of date logs may be purged after being archived.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained and archived in accordance with the procedures specified in the CPS.
Audit logs shall be retained on-site until reviewed, as well as being retained in the manner described below. The individual who removes audit logs from the Illinois

CA system shall be an official different from the individuals who, in combination, command the Illinois CA private signature key.

5.4.4 Protection of Audit Logs

Access to audit logs shall be protected by a combination of physical and logical security controls in accordance with the procedures specified in the CPS.
Illinois CA system configuration and procedures must be implemented together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.
- Logs are monitored to assure there are no changes by the System Administrator

The entity performing audit log archive need not have modified access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the CA equipment.

5.4.5 Audit Log Backup Procedures

Audit log files shall be backed-up weekly and the backup media shall be stored locally. A consolidated copy of the audit log files shall be sent to a secure off-site storage facility in accordance with procedures specified in the CPS.
Audit logs and audit summaries shall be backed up at least weekly. A copy of the audit log shall be sent off-site on a monthly basis.

5.4.6 Audit Collection System (internal vs. external)

The audit trail accumulation system is internal to the Certificate Authority (CA) software system.

The audit log collection system may or may not be external to the Illinois CA system. Automated audit processes shall be invoked at system (or application) startup, and cease only at system (or application) shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Illinois PKI Operational Authority Administrator (or comparable Entity authority) shall determine whether to suspend Illinois PKI operation (or Entity CA operation respectively) until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

The Certificate Authority (CA) and the Registration Authority application shall notify the CA personnel of any critical security error or discrepancy as it is logged in accordance with procedures specified in the CPS.

5.4.8 Vulnerability Assessments

The Operational Authority (OA) shall review system and application logs in accordance with Section 5.4.2.

For the Illinois CA, personnel shall perform routine assessments for evidence of malicious activity.

5.5 RECORDS ARCHIVE

The Illinois PKI shall comply with their respective records retention policies in accordance with whatever laws apply to the State of Illinois.

5.5.1 Types of Events Archived

The Certificate Authority (CA) shall archive all sensitive events, lists, certificates, keys, records, reports, and agreements in accordance with the procedures specified in the CPS.
Illinois CA archive records shall be sufficiently detailed as to verify that the Illinois CA was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the Illinois CA.

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

Data To Be Archived	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256 -Level-4
CA accreditation (if applicable)	X	X	X	X
Certificate Policy	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
Other agreements concerning operations of the CA	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X

Data To Be Archived	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256 -Level-4
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data as per Section 3.2.3		X	X	X
Documentation of receipt and acceptance of certificates (if applicable)		X	X	X
Subscriber Agreements		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of CA Re-key	X	X	X	X
All CRLs issued and/or published		X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents		X	X	X
Compliance Auditor reports		X	X	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys	X	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	X	X
All changes to the trusted public keys, including additions and deletions	X	X	X	X

Data To Be Archived	SHA1-Level-1 and SHA256-Level-1	SHA1-Level-2 and SHA256-Level-2	SHA1-Level-3 and SHA256-Level-3	SHA1-Level-4 and SHA256 -Level-4
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
The approval or rejection of a certificate status change request		X	X	X
Appointment of an individual to a Trusted role	X	X	X	X
Destruction of cryptographic modules		X	X	X
All certificate compromise notifications		X	X	X
Remedial action taken as a result of violations of physical security		X	X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practices Statement	X	X	X	X

5.5.2 Retention Period for Archive

All sensitive events, lists, certificates, keys, records, reports, and agreements archived shall be retained in accordance with the procedures specified in the CPS.
The minimum retention periods for archive data are identified below. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

This minimum retention period for these records is intended only to facilitate the operation of the Illinois CA.

CA Assurance Level	Minimum Retention Period
SHA1-Level-1 and SHA256-Level-1	7 Years & 6 Months
SHA1-Level-2 and SHA256-Level-2	7 Years & 6 Months
SHA1-Level-3 and SHA256-Level-3	10 Years & 6 Months
SHA1-Level-4 and SHA256-Level-4	20 Years & 6 Months

5.5.3 Protection of Archive

The archive media shall be protected either by physical security, or a combination of physical security and cryptographic protection. Additionally, the archive media shall be provided adequate protection from environmental threats such as temperature, humidity, and magnetism. No unauthorized user shall be permitted to write to, modify, or delete the archive.
No unauthorized user shall be permitted to write to or delete the archive. For the Illinois CA, archived records may be moved to another medium when authorized by the Illinois Operational Authority Administrator. The contents of the archive shall not be released except in accordance with Sections 9.3 & 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the Illinois CA itself.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the OA with direction given by the PA
Applications required to process the archive data shall also be maintained for a period determined by the Illinois PKI Policy Authority.

5.5.4 Archive Backup Procedures

Certificates, CRLs, and keys shall be backed-up and stored locally. A copy of these items shall be made and sent to a secure archive facility in accordance with the procedures specified in the CPS.

For discrepancy and compromise reports and cross-certification agreements, a copy of the document shall be made as it is received and sent to a secure archive facility. Original copies shall be kept locally.

5.5.5 Requirements for Time-Stamping of Records

Time and date stamping of audit logs and archive records is an inherent automatic function of the Certificate Authority (CA)software. The CPS shall describe how time synchronization between the system clocks used for time stamping is performed.

5.5.6 Archive Collection System (internal or external)

All sensitive events, lists, certificates, keys, records, reports, and agreements shall be archived according to the procedures specified in the CPS.

Archived records shall be transferred to separate physical media external to the Certificate Authority (CA) host system and CA application.

5.5.7 Procedures to Obtain & Verify Archive Information

Procedures to create, verify, package, transmit and store Certificate Authority (CA) archive information shall be documented in the CPS.

The contents of the archive shall not be released except as determined by the Illinois PKI Policy Authority for the State of Illinois or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected. The Certificate Authority (CA) does not escrow or archive Subscriber's private keys; however, the Subscriber's profile can be recovered, creating a new set of keys and a new password that controls access to those keys. This process can only be completed by three different CA personnel and shall only occur under one of the following three circumstances:

The Illinois CA supports link certificates as inherent in the application software. Link certificates are special certificates created during a CA key update or rollover, and provide the "link" between the new CA certificate and the previous version used for verification.

5.6.1 Recovery at Subscriber Request

A Subscriber may request that the Subscriber's own profile be recovered if the Subscriber is no longer able to access his/her private keys because the password has been lost or the electronic file has been corrupted. The Subscriber must provide proof of identity through secured shared secrets or other authentication prior to recovery of the Subscriber's profile.

5.6.2 Involuntary Recovery at State Agency Request

- A State Agency may request involuntary recovery of a Subscriber's private encryption keys if that person is or has recently been employed by the State of Illinois, the Agency has reason to believe that data necessary to agency operations has been encrypted using the Subscriber's keys, and the Agency is unable to contact the Subscriber or the Subscriber is unable or unwilling to decrypt the data.
- The Agency's request shall be made in writing to the PA, describing why the Subscriber's private encryption key is necessary to Agency operations and specifying what use shall be made of the key. The request shall be signed by

the Director of the Agency. The Subscriber's keys shall not be recovered until said request is reviewed by the Policy Authority (PA) or those designated by the Policy Authority (PA) to review such requests.

- Prior to recovering the Subscriber's profile, the Certificate Authority (CA) shall alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate shall be recovered and the profile shall be delivered to the Agency Local Registration Authority (LRA) on physical media. The LRA shall sign for receipt of the profile, shall supervise all Agency use of the recovered key for the purposes described in the approved request and shall certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate shall 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 3.3.2 "Identification and authentication for Rekey after Revocation" to be re-authenticated and issued a new Certificate.

5.6.3 Involuntary Recovery by Court Order

- The Policy Authority (PA) and Operational Authority (OA) shall comply with court orders to recover a Subscriber's keys.
- Prior to recovering the Subscriber's profile, the Certificate Authority (CA) shall alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate shall be recovered and the profile shall be delivered to the Agency LRA on physical media. The LRA shall sign for receipt of the profile, shall supervise all Agency use of the recovered key for the purposes described in the approved request and shall certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate shall be revoked following the procedures in Section 4.9 "Certificate Suspension and Revocation."
- A Subscriber whose profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 3.3.2 "Identification and authentication for Rekey After Revocation" to be re-authenticated and issued a new Certificate.

5.7 COMPROMISE & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The members of the Illinois Policy Authority shall be notified by the Illinois CA if any of the following incidents occur:

- suspected or detected compromise of the Illinois systems;
- successful physical or electronic attempts to penetrate Illinois systems;
- successful denial of service attacks on Illinois components;

- any incident preventing the Illinois PKI from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The Illinois Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the Illinois CPS.

The Illinois CA shall provide notice as required by the applicable MOA.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

Compromise procedures and a Disaster Recovery Plan for the CA, Registration Authority (RA) and Local Registration Authorities (LRAs) are in place in accordance with the procedures specified by the CA, giving priority to certificate status information. These procedures can be found in the document entitled "State of Illinois Central Management Services Public Key Infrastructure Recovery Activation Plan."
When computing resources, software, and/or data are corrupted, the Illinois CAs shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored
- If the CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in 4.9.7, Table 1.
- If the CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity (CA) Private Key Compromise Procedures

If the State Certificate Authority (CA) private key is compromised, the corresponding public key and CA Certificate shall be revoked
If the Illinois CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The Illinois PKI Policy Authority and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;
- A new Illinois CA key pair shall be generated by the Illinois CA in accordance with procedures set forth in the Illinois CPS; and
- New Illinois CA certificates shall be issued to Entities also in accordance with the Illinois CPS.

If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4.

The Illinois Operational Authority or Entity CA governing body shall also investigate and report to the Illinois Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

All operations shall be covered by a Business Continuity Plan that provides for a smooth transition to alternate equipment and/or facilities in case of equipment failure or facility damage.
The Illinois directory system shall be deployed so as to provide 24 hour, 365 day per year availability. The Illinois Operational Authority shall implement features to provide high levels of directory reliability.

The Illinois Operational Authority shall operate a cold backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. The Illinois operations shall be designed to restore full service within 72 hours of primary system failure.

The Illinois Operational Authority shall at the earliest feasible time securely advise the Illinois Policy Authority and all of its member entities in the event of a disaster where the Illinois CA installation is physically damaged and all copies of the Illinois CA signature keys are destroyed.

Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of Illinois operation with new certificates.

5.8 CA & RA TERMINATION

All operations shall be covered by a Business Continuity Plan that provides for a smooth transition to alternate equipment and/or facilities in case of equipment failure or facility damage.

In the event of a CA key compromise, the CA certificate shall be revoked.

In the event of termination of the Illinois operation, certificates signed by the Illinois shall be revoked and the Illinois Policy Authority shall advise entities that have entered into MOAs with the Illinois Policy Authority that Illinois operation has terminated so they may revoke certificates they have issued to the Illinois. Prior to Illinois termination, the Illinois Operational Authority shall provide all archived data to an archival facility.

Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the Illinois CA is terminated.

In the event that an Illinois CA terminates operation, the Illinois PA shall provide notice to any affiliated party prior to termination.

6. TECHNICAL SECURITY CONTROLS

The Client system and data shall be secured in accordance with the policies described herein.

6.1 KEY PAIR GENERATION & INSTALLATION

6.1.1 Key Pair Generation

Most PKI users shall have the digital signature key pair generated in software. Some PKI users may have hardware tokens, which generate this key pair. The keys generated by the State Certificate Authority (CA) shall be generated in software with the exception of the CA private signing key which shall be generated on the Hardware Security Module.

6.1.1.1 *CA Key Pair Generation*

Cryptographic keying material used to sign certificates, CRLs or status information by the Illinois CA shall be generated in FIPS 140-2 Level 3 validated cryptographic modules. Cryptographic keying material used to sign certificates, CRLs or status information by Entity CAs shall be generated in FIPS 140 validated cryptographic modules or modules validated under equivalent international standards.

For the Illinois CA, the modules shall meet or exceed FIPS 140-2 Level 3 for all assurance levels. Multiparty control is required for CA key pair generation for the Illinois CA.
CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

For all assurance levels, an independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.1.1.2 *Subscriber Key Pair Generation*

All End Entities shall be issued dual key pairs with separate keys for authentication/signing & confidentiality/encryption. Some device certificates may be issued with a single key pair instead of a dual key pair.

Each End Entity must generate its own signature key pair. Signature keys for SHA1-Level-1 (2.16.840.114273.1.1.1.1 or 2.16.840.114273.1.1.1.2) may be

generated in either hardware or software. Signature keys for SHA1-Level-2 software (2.16.840.114273.1.1.1.3) or SHA1-Level-3 software (2.16.840.114273.1.1.1.5) shall be generated in software. Signature keys for SHA1-Level-2 hardware (2.16.840.114273.1.1.1.4) or SHA1-Level-3 hardware (2.16.840.114273.1.1.1.6) shall be generated in hardware. SHA1-Level-4 (2.16.840.114273.1.1.1.7) certificates shall be generated in hardware only.

Signature keys for SHA256-Level-1 (2.16.840.1.114273.3.1.1.1 or 2.16.840.1.114273.3.1.1.2) may be generated in either hardware or software. Signature keys for SHA256-Level-2 software (2.16.840.1.114273.3.1.1.3) or SHA256-Level-3 software (2.16.840.1.114273.3.1.1.5) shall be generated in software. Signature keys for SHA256-Level-2 hardware (2.16.840.1.114273.3.1.1.4) or SHA256-Level-3 hardware (2.16.840.1.114273.3.1.1.6) shall be generated in hardware. SHA256-Level-4 (2.16.840.1.114273.3.1.1.7) certificates shall be generated in hardware only.

For each level of assurance the Certificate OID shall identify whether the private key was generated in hardware or software.

The encryption key pair is generated by the Certificate Authority (CA) and transmitted to the End Entity during the PKIX protocol session.

Level of Assurance	**Key Generation Medium**
SHA1-Level 1 2.16.840.114273.1.1.1.1	Software – Desktop or Repository
2.16.840.114273.1.1.1.2	Hardware token
SHA1-Level 2 2.16.840.114273.1.1.1.3	Software – Desktop or Repository
2.16.840.114273.1.1.1.4	Hardware token
SHA1-Level 3 2.16.840.114273.1.1.1.5	Software – Desktop or Repository
2.16.840.114273.1.1.1.6	Hardware token
SHA1-Level 4 2.16.840.114273.1.1.1.7	Hardware token only (biometric)

SHA256-Level-1 2.16.840.1.114273.3.1.1.1	Software – Desktop or Repository
2.16.840.1.114273.3.1.1.2	Hardware token
SHA256-Level-2 2.16.840.1.114273.3.1.1.3	Software – Desktop or Repository
2.16.840.1.114273.3.1.1.4	Hardware token
SHA256-Level-3 2.16.840.1.114273.3.1.1.5	Software – Desktop or Repository
2.16.840.1.114273.3.1.1.6	Hardware token
SHA-256-Level-4 2.16.840.1.114273.3.1.1.7	Hardware token only (biometric)

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation shall be performed using a FIPS 140-2 approved mechanism. For all assurance levels, subscriber key generation shall be performed using a validated FIPS 140-2 hardware cryptographic module.

6.1.2 Private Key Delivery to Subscriber

The encryption key pair is generated by the Certificate Authority (CA) and transmitted to the End Entity during the PKIX protocol session.
If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

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

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.

- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
    - For shared key applications and network devices, see also Section 3.2.

The Illinois CA must maintain a record of the subscriber acknowledgement of receipt of the hardware token.

6.1.3 Public Key Delivery to Certificate Issuer

The encryption key pair shall be created by the Certificate Authority (CA) software, and a copy of the public encryption key shall be placed in the Directory and delivery of the encryption public key to the Certificate issuer is required. The signature verification public key shall be delivered securely to the Certificate Authority (CA) using the PKIX protocol.

For CAs operating at all assurance levels, the following requirements apply:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance.
- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The Certificate Authority (CA) verification public key shall be delivered in a CA Certificate to users using the PKIX protocol. Authenticity and integrity protection shall be based on a MAC key derived from the authorization code.
When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-) certificate obtained from the issuer(s) of the current CA certificate(s).

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

CA Certificates are signed with the issuing CA's current private key, so secure distribution is not required.

6.1.5 Key Sizes

All signature key pairs generated within the Certificate Authority (CA) shall be at least 2048 bit RSA or, where the DSS is used, as stipulated in FIPS PUB 186.

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.

For CAs that distributes self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA. Those CAs that distribute self-signed certificates and whose key pairs were generated before September 13, 2005 may be 1024 bits for RSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Beginning 12/08/2012, all valid certificates shall be signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after December 8th, 2012 shall be generated using, at a minimum, SHA-256.

RSA signatures on CRLs that are issued on or after January 1, 2012, but before January 1, 2014 that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256.

For Medium assurance, signatures on certificates and CRLs asserting certificate policy OIDs that identify the use of SHA-1 may be generated using SHA-1 until December 31, 2013. CAs that issue end entity certificates generated using, at a minimum, SHA 224 bits after December 31, 2010 must not issue end entity certificates signed with SHA 1.

For Medium … Assurance, Signatures on certificates and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1.

Certificates issued to OCSP responders that include SHA-1 certificates may be signed using SHA-1 until December 31, 2013.

Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

After December 31, 2010, for Medium and High Assurance, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is provided to an OCSP client shall have been signed before the OCSP responder received the request from the client)

- End-entity certificates shall contain public keys that are at least 1024 bit for RSA for Federal inter-operability. End-entity certificates that include a keyUsage extension that only asserts the *digitalSignature* bit that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.

- Beginning 01/01/2011, all valid end-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

- Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

The Illinois CA shall not issue a cross-certificate with a validity period extending beyond 12/31/2010 to any Entity Principal CA unless all of the following conditions apply:

- Certificates that expire after 12/31/2010 are signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA.
- End-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit that expire on or after 12/31/2010 contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- End-entity certificates that do not include a keyUsage extension that expire on or after 12/31/2010 contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent

for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010.

The State of Illinois does not currently use TLS. SSL certificates are provided by Entrust.net Certificate Services.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186 Key Usage Purposes (as per X.509 v3 key usage field).

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Certificates issued by the State Certificate Authority (CA) shall contain the key Usage Certificate extension restricting the purpose to which the Certificate can be applied.

The digital signature key pair shall be used to provide authentication, integrity and support for non-repudiation services.

The encryption key pair shall be used to protect a symmetric key used to encrypt data, and as such provides confidentiality services.

The State CA signing key shall be used to sign Certificates, CRLs and ARLs issued by that CA.

The PKIX session keys shall be used to provide secure communications for key management operations.
Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both,(MEDIUM HW ALSO) except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate.

The Illinois CA issued certificates and CA certificates issued by Entity CAs shall set two key usage bits: *cRLSign* and/or *keyCertSign*.
Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits. Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates to be used for key agreement shall set the *keyAgreement* bit.

For all assurance levels, device certificates may include a single key pair for use with encryption and signature in support of legacy applications. Such certificates

shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the certificate at a future time.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

Certificate Authority (CA) cryptographic operations shall be performed by either hardware or software cryptographic module rated to at least FIPS 140-2 Level 3.

Registration Authority (RA) and Local Registration Authority (LRA) cryptographic operations shall be performed by either hardware or software cryptographic module validated to at least FIPS 140-2 Level 1.

Registration Authority (RA) and Local Registration Authority (LRA) personnel responsible for issuing hardware tokens shall themselves be certified for and use a hardware device that is at least equivalent to the hardware device being issued.

Subscriber cryptographic operations shall be performed by either hardware or software cryptographic module validated to at least FIPS 140-2 Level 1.

The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA & CSS	Subscriber	RA
SHA1-Level-1 Software	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1	Level-3 Software
SHA1-Level-1 Hardware	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1 (Hardware)	Level-3 Software
SHA1-Level-2 Software	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1 (Software)	Level-3 Software
SHA1-Level-2 Hardware	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
SHA1-Level-3 (Software)	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1 (Software)	FIPS 140-2 Level 2 (Hardware)
SHA1-Level-3	FIPS 140-2 Level 3	FIPS 140-2	FIPS 140-2 Level 2

(Hardware)	(Hardware)	Level 2 (Hardware)	(Hardware)
SHA1-Level-4	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
SHA256-Level-1 Software	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1	SHA256-Level-3 Software
SHA256-Level-1 Hardware	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1 (Hardware)	SHA256-Level-3 Software
SHA256 Level-2 Software	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1 (Software)	SHA256-Level-3 Software
SHA256-Level-2 Hardware	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
SHA256-Level-3 (Software)	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 1 (Software)	FIPS 140-2 Level 2 (Hardware)
SHA256-Level-3 (Hardware)	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
SHA256-Level-4	FIPS 140-2 Level 3 (Hardware)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

6.2.2 Private Key Multi-Person Control

The simultaneous intervention of two or more persons is required for operations on the CA's private signing key as referred to in section 5.2.2 of this policy.

Other actions require one-person control.

6.2.3 Private Key Escrow

Private signature keys shall not be escrowed or archived.

6.2.3.1 *Escrow of Illinois CA private signature key*

Under no circumstances shall an Illinois CA signature key used to sign certificates or CRLs be escrowed.

6.2.3.2 *Escrow of CA encryption keys*

Illinois CA encryption keys shall not be escrowed.

6.2.3.3 *Escrow of Subscriber private signature keys*

Subscriber private signature keys shall not be escrowed.

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

Subscriber private dual use keys shall not be escrowed.

6.2.4 Private Key Backup

Subscriber private signature keys may be backed up or copied but must be held in the Subscriber's exclusive control. Keys generated for roaming certificates shall be stored in encrypted form on the directory operated by the CA, accessible only by the Subscriber utilizing the Subscriber's activation data.

Private signature keys shall not be escrowed or archived.

6.2.4.1 *Backup of Illinois CA Private Signature Key*

Illinois CA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.

Backup of Illinois CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, Illinois CA private signature keys shall be backed up under multi-person control.

At least one copy of the Illinois CA private signature key shall be stored off site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

6.2.4.2 Backup of subscriber private signature key

At the SHA1-Level-2 or SHA256-Level-2 hardware assurance levels, SHA1-Level-3 or SHA256-Level-3 hardware assurance levels, or SHA1-Level-4 or SHA256-Level-4 assurance levels, Subscriber private signature keys may not be backed up or copied.

For assurance SHA1-Level-1 or SHA256-Level-1, SHA1-Level-2 or SHA256-Level-2 software, and SHA1-Level-3 or SHA256-Level-3 software, Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control.

Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.3 Backup of Subscriber Key Management Private Keys

Backed up subscriber private key management keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.4 Backup of CSS Private Key

No stipulation.

6.2.5 Private Key Archival

Private signature keys shall not be escrowed or archived.

All hardware cryptographic modules shall be removed and stored in a secure location when not in use.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Certificate Authority (CA) cryptographic operations shall be performed by either hardware or software cryptographic module rated to at least FIPS 140-2 Level 3.

CA signing private keys are generated and stored on the Hardware Security Module and most Subscriber signing private keys are generated in software, within the cryptographic module. In the case of hardware tokens, the token may or may not produce the private signing key at the end-entity. If the hardware token is a storage only device, the private signing key is generated in software and injected onto the device encrypted. Subject End Entity decryption private keys come from the Certificate Authority (CA) , in an encrypted format, and are entered into the cryptographic module encrypted. In all cases, private keys are stored encrypted in the cryptographic module. In both the software and hardware token cases, they are decrypted only at the time at which they are actually being used.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary. The CA private key may be exported only to perform CA key backup.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Keys

The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For both software and hardware token cases, private keys are activated at the time the subject login to the relevant Certificate Authority (CA)component occurs.

For the Illinois CAs at all assurance levels, CA signing key activation requires multiparty control as specified in Section 5.2.2.

6.2.9 Methods of Deactivating Private Keys

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. CA Hardware cryptographic modules shall be removed and stored in a secure container when not in use

The private keys remain active for the period of login. The login period is ended either by the subject logging out from the PKI client application or automatically after a preset period of time configured in Certificate Authority (CA). The preset timer is controlled from the Certificate Authority (CA) software by the Security Administrator.

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles shall destroy CA, RA private signature keys when they are no longer needed. Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

The Certificate Authority (CA) utilizes a Hardware Security Module, which is FIPS 140-2 level 3 certified.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

The user encryption public key Certificates and verification public key Certificates are backed up in the Certificate Authority (CA)database. The complete encryption key pair history and verification public key history for all users, including history of status changes such as revocation date and reason, are archived in this database.

All public keys shall be archived in accordance with the records archival practices described in Section 5.5 (and its sub-sections) of this CP.

6.3.2 Certificate Operational Periods/Key Usage Periods

The Certificate Authority's (CA) RSA-2048 private signing key used to create certificates shall be valid until December 31st, 2031. All CA keys (private and public) shall be retained in archive in accordance with the procedures in the CPS. The State of Illinois CA must not issue subscriber certificates that extend beyond the expiration date of their own certificate and public keys.
When the State of Illinois issues self-signed certificates for use as trust anchors it shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years.

For Registration Authorities (RAs), Local Registration Authorities (LRAs) and Subscribers, a private signing key shall be valid for up to 25 months, and certificates issued for the public signature verification key shall be valid for no more than the period required for retention in archive in accordance with the procedures in the CPS. The lifetime of the associated public keys shall not exceed eight years. Encryption certificates shall be valid for up to 36 months. The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1. Subscriber key management certificates have a maximum lifetime of three years; use of subscriber key management private keys is unrestricted.

6.4 ACTIVATION DATA

Passwords for Registration Authorities (RAs) and Local Registration Authority (LRAs) shall expire after 5 weeks. Passwords for Subscribers shall expire after 52 weeks. The user must create a new password on the first login after expiration.

6.4.1 Activation Data Generation & Installation

The activation data used to unlock Illinois CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

The Illinois PKI uses a PIN as a password to activate the CA private key. At a minimum, the PINs shall be changed upon CA re-key.

Passwords are required by all entities logging on to PKI components. The Certificate Authority (CA) applies a stringent set of rules to each password to ensure it is secure. Some of the rules on password selection are:

- It must have at least eight characters;
- It must have at least one upper-case letter or digit;
- It must have at least one lower-case letter;
- It must not contain many occurrences of the same character;
- It must not be the same as the entity's profile name;

- It must not contain a long substring of the entity's profile name;
- Passwords for Registration Authorities (RAs) and Local Registration Authorities (LRAs) shall expire after 5 weeks;
- Passwords for subscribers shall expire after 52 weeks.

6.4.2 Activation Data Protection

Active Registration Authority (RA), Local Registration Authority (LRA) and Subscriber private keys shall be protected from unauthorized use by encryption keyed with either a password or token.

Extra steps are taken to protect passwords. Once chosen, the password is put through numerous hashing iterations, producing a password token. Only the password token is stored in a user's client profile. Original passwords are never stored.

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

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

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

6.4.3 Other Aspects of Activation Data

In addition, for the Security Administrators and Certificate Authority Administrators, their user-names and password check values are stored in the Certificate Authority (CA) database.

6.5 COMPUTER SECURITY CONTROLS

The Certificate Authority (CA) hardware and software shall be dedicated to performing one task. There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the CA operation. Any network ports or services that are not necessary to the operation of the CA services are disabled. The CA software verifies configuration via check-sum upon start-up to detect unauthorized modification to the CA software or configuration. Configuration changes are documented in audit logs. A formal configuration methodology shall be used for installation and ongoing maintenance of the CA system.

CA access control records shall be maintained and audited periodically. Maintenance and service personnel shall be escorted and supervised according to procedures outlined in the CPS.

All updates to the Certificate Authority and Master Directory computers shall first be applied and tested on test platforms before being applied to the production computers. Proper change management procedures shall be followed when updating the production systems.

6.5.1 Specific Computer Security Technical Requirements

The Certificate Authority (CA) host computers shall include the following functionality provided either by the operating system, or through a combination of operating system, CA application, and physical safeguards:

- Access control to CA services and roles;
- CA workstation is physically secured;
- Access to the Certificate Authority (CA) database and audit trails is restricted;
- Enforced separation of duties for CA roles;
- Identification and authentication of CA roles and associated identities;
- Object re-use for CA random access memory;
- Use of cryptography for session communication and database security;
- Key management plan integral to CA design;
- Archival of CA and history and audit data;
- Audit of security related events;
- Self-test of security related CA services;
- Trusted path for identification of CA roles and associated identities; and
- Recovery mechanisms for keys and the CA application. This functionality is active and logged in the appropriate logs.

For Entity CAs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Entity CA and its ancillary parts shall include the following functionality:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For Certificate Status Servers, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.
- No stipulation for status servers

For remote workstations used to administer the CA, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see section 5.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

6.5.2 Computer Security Rating

No stipulation.

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

The Certificate Authority (CA) uses COTS software and as such the vendor is responsible for the software development function work performed.

For all assurance levels, the System Development Controls for RA functionally are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.
- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.

- Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not parts of the CA operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the Illinois CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the Illinois CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the Illinois CA system. The Illinois CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.
Any new software received shall first be installed and tested on an existing test environment before being put into production. The process of putting a new version of software or application into production shall follow existing change management procedures.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Certificate Authority (CA) application and Repository shall be protected through use of a firewall configured to allow only the protocols and commands required for CA services. The CA, directories, servers, and remote workstations used to administer the CA shall employ appropriate network security controls as described in section 6.7 of the CPS.

The Illinois shadow Directories shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup).

Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

6.8 TIME STAMPING

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

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

7.1 CERTIFICATE PROFILE

All Certificates shall be issued in the *X.509 version 3* Format and shall include the State Policy identifier within the *Certificate Policies* field. The Certificate profiles for Certificates authorized by the State are set forth in this Policy.

7.1.1 Version Numbers

All Certificates shall be issued in the X.509 version 3 Format and shall include the State Policy identifier within the Certificate Policies field. The Certificate profiles for Certificates authorized by the State are set forth in this Policy. The Illinois CA shall issue X.509 v3 certificates (populate version field with integer "2"). CRLs shall be issued in the X.509 version 2 Format. The CRL profile for CRLs issued pursuant to this Policy is as discussed in Section 7.2.

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various Certificate Authorities and communities. This Policy shall follow Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile, except as modified by the CPS. Whenever private extensions are used, they shall be identified in a CPS. Private extensions shall be interoperable in their intended community of use, and shall be marked as non-critical.

A number of X.509 version 3 Certificate extensions are included in Certificates issued by this CA. These are outlined below. The X.509 version 3 Certificate extensions which are never present in Certificates issued by this Certificate Authority (CA) are also outlined below.

The following fields of the X.509 version 3 Certificate format are used in this PKI:

X.509 v3 Certificate Extension	Critical/Non Critical	Optional	Notes
SubjectAltName	Non critical	Optional	• GeneralName – choices [0], [3] and [5] are not implemented.
AuthorityKeyIdentifier	Non critical	Not optional	• only element [0] (authorityKeyIdentifier) is filled in • contains a 20 byte hash of the subjectPublicKeyInfo

X.509 v3 Certificate Extension	Critical/Non Critical	Optional	Notes
			in the CA Certificate
SubjectKeyIdentifier	Non critical	Not optional	• contains a 20 byte hash of the subjectPublicKeyInfo in the Certificate
BasicConstraints	Non critical	Not optional	• only the cA Boolean is used
CRLDistributionPoints	Non critical	Not optional	• ***if interworking with earlier*** Certificate Authority (CA)***software releases is required - set to non critical otherwise set to critical*** • Both the distribution point distinguished name and the complete URL address is included in the extension. The URL is used by relying parties outside of the State of Illinois environment.
KeyUsage	Critical	Not optional	
CertificatePolicies	Non critical	Not optional	• only policyIdentifier element is supported with up to 10 OIDs • policyQualifiers not supported

The following X.509 version 3 Certificate extensions are not used in this PKI:

- name constraints
- policy constraints
- issuer alternative name
- subject Directory attributes

The proprietary Netscape extension “NetscapeCertType” is present in the Certificate Authority (CA) root certificate (marked as non-critical).

For the Illinois PKI, the use of certificate extensions shall follow [RFC 3280] and shall be compatible with [FPKI-Prof] for all assurance levels.

The Illinois PKI CA certificates shall not include any critical private extensions.

7.1.3 Algorithm Object Identifiers

Certificates under this Policy shall use the following OIDs for identifying the algorithm for which the subject key was generated:

- ID-DSA – {ISO(1) MEMBER-BODY(2) US(840) X9-57(10040) X9CM(4) 1}
- RSAENCRYPTION- {ISO(1) MEMBER-BODY(2) US(840) RSADSI(113549) PKCS(1) PKCS-1(1) 1}
- DHPUBLICNUMBER- {ISO(1) MEMBER-BODY(2) US(840) ANSI-X942(10046) NUMBER-TYPE(2) 1}

Certificates issued by the Illinois CAs shall identify the signature algorithm using one of the following OIDs:

id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Certificates issued by the Illinois CAs shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

If elliptic curve cryptography is ever implemented in Illinois, the parameters shall be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }

ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4 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). Distinguished names shall be composed of standard attribute types, such as those identified in [RFC1422] or [RFC3280].

7.1.5 Name Constraints

Name constraints are not used in this PKI.

7.1.6 Certificate Policy Object Identifier

Multiple certificate policies (i.e. assurance levels) are asserted by the Illinois CA and are identified in Section 1.2 of this CP.

7.1.7 Usage of Policy Constraints Extension

Policy constraints are not used in this PKI.

7.1.8 Policy Qualifiers Syntax & Semantics

Policy qualifiers are not used in this PKI.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The Illinois CA does not mark the certificate policies extension as critical.

7.2 CRL PROFILE

. The Illinois CRL profile is as follows in accordance with (FPKI – Prof).

7.2.1 Version Numbers

The Illinois PKI issues CRLs in the X.509 version 2 format.

7.2.2 CRL Entry Extensions

The only Certificate extension which may be identified as critical in Certificates issued by this Certificate Authority (CA) is the cRLDistributionPoints extension. The CRL or ARL shall always be retrieved by either using the directory entry indicated in the certificate, or by using the URL indicated in the certificate, unless a current copy of that CRL or ARL is cached by PKI desktop software.

A number of X.509 version 2 CRL and CRL entry extensions are used in this PKI. CRL extensions shall conform to [FPKI-Prof]. The following CRL and CRL entry extensions are used in this PKI:

X.509 v2 CRL Extension	Critical/Non Critical	Optional	Notes
AuthorityKeyIdentifier	Non critical	Not optional	• only element [0] (authorityKeyIdentifier) is filled in • contains a 20 byte hash of the subjectPublicKeyInfo in the CA Certificate
CRLNumber	Non critical	Not optional	• Incremented each time a particular CRL/ARL is changed
IssuingDistributionPoint	Critical	Not optional	• element [0] (distributionPoint) includes the full DN of the distribution point

			• element [1] (onlyContainsUserCerts) is included for CRLs • element [2] (onlyContainsCACerts) is included for ARLs • element [1] and [2] are never present together in the same revocation list • elements [3] and [4] are not used

7.3 OCSP PROFILE

No Stipulation

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

The Illinois PKI Operational Authority shall have a compliance audit mechanism in place to ensure that the requirements of this CP and the Illinois CPS are being implemented and enforced.

This specification does not impose a requirement for any particular assessment methodology.

The purpose of such audit shall be to verify that the Certificate Authority has a system in place to attest to the quality of the Certificate Authority Services that it provides and to ensure that this system complies with the requirements of this CP and the associated CPS.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The Illinois CA, and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, and Medium Assurance, and at least once every two years for Basic Assurance. Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.

The Certificate Authority (CA) shall undergo a compliance audit prior to initial approval as a CA to demonstrate compliance with State Policies and this CP and the CPS. Subsequent compliance audits shall be required every twelve months, or whenever substantive changes are made to the CP or the CPS.

The auditing of the Root Key Generation Ceremony shall be considered the initial audit for the purposes of this Certificate Policy.

Subsequent audits shall be conducted either by an independent auditor contracted by the Department of Central Management Services, or in conjunction with the annual IT compliance audit of the Department of Central Management Services Bureau of Communication & Computer Services.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the Illinois PKI compliance auditor must be thoroughly familiar with requirements which the Illinois PKI Policy Authority imposes on the issuance and management of Illinois PKI certificates. Likewise, the Illinois CA compliance auditor must be thoroughly familiar with the requirements which Illinois imposes on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

Annual audits are performed by independent auditors selected by the State of Illinois. Auditors must demonstrate competence in the field of compliance audits and must regularly perform such compliance audits as a primary responsibility.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

For both the Illinois PKI and Entity CAs, the compliance auditor either shall be a private firm, that is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement.

Annual audits shall be performed either by third party independent auditors contracted specifically for the purpose of auditing the State's PKI operations, or by auditors employed by the State of Illinois who are independent of the Operational Authority (OA)or Policy Authority (PA).

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of an Entity PKI shall be to verify that an entity subject to the requirements of an Entity CP is complying with the requirements of those documents, as well as any MOAs between the Entity PKI and applicable State law (Illinois Commerce and Security Act: 5 ILCS 175 and associated administrative rules).

The annual audit investigates the operations of the Certificate Authority (CA) and Registration Authority (RA) functions of the State PKI to ensure their compliance with this CP and the CPS. Some areas of focus for these audits are:

- **Identification & Authentication**

  Initial Registration
  Routine Rekey
  Rekey after Revocation
  Revocation Request

- **Operational Requirements**

  Certificate Application
  Certificate Issuance
  Certificate Acceptance
  Key Recovery
  Certificate Suspension/Revocation
  Computer Security Audit Procedures

Records Archival
CA key Changeover
Compromise and Disaster Recovery
CA Termination

- **Physical, Procedural & Personnel Security**

  Physical Security Controls
  Procedural Controls
  Personnel Security Controls

- **Technical Security Controls**

  Key Pair Generation & Installation
  Private Key Protection
  Other Aspects of Key Pair Management
  Activation Data
  Computer Security Controls
  Lifecycle Security Controls
  Network Security Controls
  Cryptographic Module Engineering Controls

- **Certificate & CRL Profiles**

  Certificate Profile
  CRL Profile

- **Specification Administration**

  Contact Information
  Specification Change Procedures
  Publication and Notification Procedures
  Approval Procedures

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the Entity compliance auditor finds a discrepancy between how the Entity CA is designed or is being operated or maintained, and the requirements of the Entity CP, any applicable MOAs, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall document the discrepancy;
- The compliance auditor shall notify the responsible party promptly;
- The Entity PKI shall determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any

relevant MOA provisions. The Entity PKI shall proceed to make such notifications and take such actions without delay.

If a deficiency is identified by the auditor, the State Policy Authority (PA) shall, based upon the findings of the auditor, determine which of the following actions shall be taken:

a.) Continue to operate as usual;
b.) Continue to operate but with limitations on rights; or
c.) Suspend operation

If action a) or b) is taken the State Policy Authority (PA) and Operational Authority (OA) are responsible for ensuring that corrective actions are taken within a reasonable time frame. At that time, or earlier if agreed by the PA and auditor, the audit team shall reassess. If, upon reassessment, corrective actions have not been taken, the PA shall determine if more severe action (e.g. action c) above) is required.

If action c) is taken all certificates issued by the CA, including end-user certificates are revoked prior to suspension of the service. The State PA and OA are responsible for reporting the status of corrective action to the auditors on a weekly basis. The PA and auditor together shall determine when the re-assessment is to occur. Upon reassessment, if the deficiencies are deemed to have been corrected, the Certificate Authority (CA) shall resume service and new certificates shall be issued to Certificate users.

8.6 COMMUNICATION OF RESULTS

Results of the annual audit are provided to the State PA, The State of Illinois Department of Central Management Services' Chief Security Officer, as well as the Auditor General. The State Policy Authority (PA) with input from the auditor shall determine if Certificate users need to be informed of any action as a result of the audit. The State PA shall communicate to Certificate users via the internet at http://www.illinois.gov/bccs/services/catalog/security/PKI/Pages/default.aspx.

On an annual basis, the State of Illinois PKI PA shall submit an audit compliance package to the Federal PKI Policy Authority. This package shall be prepared in accordance with the "Compliance Audit Requirements" document and includes an assertion from the State of Illinois PKI PA that all PKI components have been audited - including any components that may be separately managed and operated. The report package shall identify the versions of the CP and CPS used in the assessment.

9. OTHER BUSINESS & LEGAL MATTERS

9.1 FEES

No direct fees shall be assessed by the Certificate Authority (CA) or OA.

In cross-certification agreements with business partner organizations, the costs are 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, shall be addressed in the specific cross-certification agreement itself and are outside the scope of this CP.

9.1.1 Certificate Issuance/Renewal Fees

The Certificate Authority (CA) shall issue, renew, and revoke Subscribers certificates at no cost.

9.1.2 Certificate Access Fees

The Certificate Authority (CA) shall 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 shall not impose fees for certificate revocation or status services.

9.1.4 Fees for other Services

The Certificate Authority (CA) shall not impose fees for access to policy information.

9.1.5 Refund Policy

Because no fees shall be charged for certificate services, as specified in this CP, there is no need to provide for refunds.

9.2 FINANCIAL RESPONSIBILITY

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers and Relying Parties relating to any transactions in which such Subscribers or Relying Parties participate and which use the Certificates or any services provided by the State in relation to the Certificates. The State makes no representations and gives no warranties and conditions regarding the financial efficacy of any transaction completed utilizing a Certificate or any services provided by the State in relation to the Certificates and the State shall have no liability except as explicitly set forth herein in respect to the use of or reliance on a Certificate or any services provided by the State in relation to the Certificates.

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 Certificate Authority (CA), Registration Authority (RA), or any Local Registration Authority (LRA) shall not disclose certificate or certificate-related information to any third party except when:

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

Any requests for disclosure of information must be signed and submitted to the CA. The Certificate Authority (CA) shall communicate all such requests to the Policy Authority (PA).

9.3.1 Scope of Confidential Information

The Subscriber's private signing key must be kept confidential by the Subscriber. The Certificate Authority (CA) and Registration Authority (RA) are not provided any access to those keys.

The Subscriber's private encryption key must be kept confidential by the Subscriber; however, the Certificate Authority (CA) may recover private encryption keys for subscribers as described in Section 4.7 "Certificate Re-Key".

Personal information held by the Certificate Authority (CA), other than that which is explicitly published as part of a certificate, CRL, certificate policy, or this document is considered confidential and shall not be released unless required by law.

Shared secret information shall be encrypted, hashed, stored securely, or otherwise physically protected.

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;
- Is protected by the CA in such a way as to insure the integrity of said personal information.

9.3.2 Information not within the scope of Confidential Information

Information included in public certificates and CRLs issued by the Certificate Authority (CA) are not considered confidential. Information in this Certificate Policy is not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

It is the responsibility of the Illinois OA to protect confidential information.

The revocation reason code given during certificate revocation is not confidential and may be shared with all users and Relying Parties. However, no other details concerning a revocation may be disclosed.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information treated as Private

No stipulation.

9.4.3 Information not deemed Private

No stipulation

9.4.4 Responsibility to Protect Private Information

Sensitive information is stored securely, and is released only in accordance with other stipulations in Section 9.4.7.

9.4.5 Notice and Consent to use Private Information

Any notice to be given by a Subscriber, or Relying Party under this CP, the CPS, a Subscriber Agreement, or a Relying Party Agreement shall be given in writing to the address specified below by prepaid receipted mail, facsimile, or overnight courier, and shall be effective as follows (i) in the case of facsimile or courier, on the next Business Day, and (ii) in the case of receipted mail, five (5) Business Days following the date of deposit in the mail. Any notice to be given by the State under this CP, the CPS, any Subscriber Agreement, or any Relying Party Agreement shall be given by email or to the last address for the Subscriber on file with the State. In the event of notice by email, the notice shall become effective on the next Business Day. In the event of notice to the last address on file with the State, notice shall become effective as specified in (i) or (ii), depending on the means of notice utilized.

Notice address for the State:
State of Illinois Digital Certificate Authority
Department of Central Management Services
201 W. Adams
Springfield Illinois 62704-1874

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

- The Policy Authority (PA) and Operational Authority (OA) shall comply with court orders to recover a Subscriber's keys.
- Prior to recovering the Subscriber's profile, the Certificate Authority (CA) shall alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate shall be recovered and the profile shall be delivered to the Agency Local Registration Authority (LRA) on physical media. The LRA shall sign for receipt of the profile, shall supervise all Agency use of the recovered key for the purposes described in the approved request and shall certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate shall 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 3.3.2 "Identification and authentication for Rekey After Revocation" to be re-authenticated and issued a new Certificate.

9.4.7 Other Information Disclosure Circumstances

Unless otherwise provided by law, information identified under a subpoena issued by a civil court, tribunal, officer or other authority with jurisdiction over a civil proceeding may be released by the Operational Authority (OA) upon sufficient service of the subpoena. If a subpoena seeks information that is confidential under this CP, the Operational Authority shall take all reasonable steps to secure a protective order from the authority with jurisdiction over the civil proceeding that provides the maximum protection possible for the confidential information under the circumstances.

Information pertaining to a Subscriber that is confidential under this CP may be disclosed to the Subscriber if the Subscriber submits a written request identifying the particular information to be disclosed and provides sufficient authentication of identify as required under Section 3.2.3 of this CP. The information shall be provided to the Subscriber by means no less secure than registered mail, restricted delivery, unless the Subscriber agrees in writing to a less secure means. The Subscriber may be required to pay the costs related to disclosing the information.

9.5 INTELLECTUAL PROPERTY RIGHTS

Certificates and CRLs issued by the Certificate Authority (CA) are the property of the State.

This CP is the property of the State.

The Distinguished Names (DNs) used to represent entities within the CA domain in the Directory and in certificates issued to End-Entities within that domain all

include a relative distinguished name (RDN) for the State and as such are the property of the State.

With respect to the CA system, the Software, including any related copyright, trademark, and patent rights, is owned by the CA software vendor and shall remain the sole and exclusive property of the CA software vendor.

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in a Certificate.

The State OIDs are the property of the State, which may be used only by the CAs in accordance with the provisions of this Policy. Any other use of the above without the express written permission of the State is expressly prohibited.

The State retains all of its right, title, and interest (including all intellectual property rights), in, to and under all the Certificates, except for any information which is supplied by a Subscriber and which is included in a Certificate, which shall remain the property of the Subscriber. All Subscribers grant to the State a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under this CP, the Subscriber's Subscriber Agreement, and any Relying Party Agreements. The State shall be entitled to transfer, convey, or assign this license in conjunction with any transfer, conveyance, or assignment by the State as contemplated in Section 9.16.2. The State grants to Subscribers and Relying Parties a non-exclusive, non-transferable right to use, copy, and distribute the Certificates, subject to such Certificates being used as contemplated under the State Certificate Policy, the CPS, the Subscriber's Agreement, and any Relying Party Agreements, and further provided that such the Certificates are reproduced fully and accurately and are not published in any publicly available database, repository or Directory without the express written permission of the State.

The State shall grant permission to reproduce this CP provided that (i) the copyright notice on the first page of this CP is retained on any copies of this CP, and (ii) this CP is reproduced fully and accurately. The State retains all right, title, and interest, in, to and under this CP, including all intellectual property rights therein.

In no event shall the State be liable to any Subscribers or Relying Parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition, or any other violation of any patent, trademark, copyright, trade secret, or any other intellectual property or other right arising from or relating to the use of the Certificate or in the use of any services provided by the State in relation to any Certificate.

9.6 REPRESENTATIONS & WARRANTIES

Refer to section 9.6.1 and 9.6.2

9.6.1 CA Representations and Warranties

As the Certificate Authority (CA) and Registration Authority (RA) functions are provided by the State, the liability issues related to both functions are combined in this CP. Nothing in this Certificate Policy shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on the State by virtue of any contract or obligation that is otherwise determined by applicable law. The State shall have no liability to any subscriber, relying party and any other entity for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of a Certificate or any services provided by the State. Use of any Certificate is limited by the terms of this CP and the CPS. This CP also contains limited warranties and disclaimers of representations, warranties, and conditions.

The Certificate Authority (CA) shall:

- Provide CA services with a maximum available application target of 100% and allowing for normal maintenance, and in accordance with the policies and processes described in this Certificate Policy and the Certification Practice Statement. In the event of a major disaster, service could be interrupted.
- Issue certificates to Subscribers, in accordance with the certificate policies referenced herein as well as the procedures and practices described in the Certification Practice Statement;
- Revoke certificates which are issued by this CA, upon receipt of a valid request to do so from either the subscriber who is the subject of the certificate to be revoked, a Registration Authority (RA), Local Registration Authorities (LRA) or the CA itself, as required by the Certificate Policy;
- Issue and publish CRLs on a regular schedule as required by the Certificate Policy;
- Notify Subscribers that certificates have been issued to them or that their certificate has been revoked; and
- Notify others (e.g. Relying Parties) of certificate issuance/revocation by provision of access to certificates, CRLs in the State PKI repository.
- Securely notify all cross-certified CA's of CA private key update.

9.6.2 RA Representations and Warranties

As the Certificate Authority (CA) and Registration Authority (RA) functions are provided by the State, the liability issues related to both functions are combined in this CP.

Nothing in this Certificate Policy shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on the State by virtue of any contract or obligation that is otherwise determined by applicable law.

The State shall have no liability to any subscriber, relying party and any other entity for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of a Certificate or any services provided by the State. Use of any Certificate is limited by the terms of this CP and the CPS. This CP also contains limited warranties and disclaimers of representations, warranties, and conditions.

The Registration Authority (RA) or Local Registration Authorities (LRA shall verify the accuracy and authenticity of the information provided by Subscribers to the RA or LRA at the time of application for a certificate. Pursuant to the terms of a valid Subscriber Agreement, the RA or LRA may make use of the State employment records to verify the data by comparing the application information with information in the State databases. The RA shall provide this verification on behalf of the CA.

Each LRA shall verify the accuracy and authenticity of the information provided by the Subscribers to the LRA at the time of application for a certificate. The Certificate Authority (CA) may, but is not required to, verify the accuracy and authenticity of information provided by Subscribers through an LRA.

When an agency or entity is implementing Level-4 or SHA256-Level-4 (biometric) certificates, the Policy Authority may authorize a trusted individual within the agency or entity to validate the background checks received before the Level-4 or SHA256-Level-4 certificate is created. This individual should possess a Level-3 or SHA256-Level-3 certificate, and must be a Local Registration Authority (LRA).

9.6.2.1 *Disclaimers*

Provided that the State has substantially complied with the certificate policy, and the certificate practices statement, the State shall not be liable for any loss which:

(1) Is incurred by the subscriber of a certificate issued by the State, or any other person, or
(2) Is caused by reliance upon a certificate issued by the State, upon a digital signature verifiable with reference to a public key listed in a certificate, or upon information represented in such certificate, or repository.

In addition to the foregoing, the State specifically disclaims liability for loss or damages:

- Incurred between the time a certificate is revoked and the next scheduled issuance of a CRL;
- Due to unauthorized use of certificates issued by the CA, and use of certificates beyond the prescribed use defined by the Certificate Policy under which the certificate was issued;

- Caused by fraudulent or negligent use of certificates and/or CRLs issued by the CA;
- Due to disclosure of personal information contained within certificates and revocation lists;
- Due to erroneous authentication of user identity; and,
- Due to losses incurred if not notified of revoked certificates.

The State makes no representations and gives no warranties or conditions, whether express, implied, statutory, by usage of trade, or otherwise and the State specifically disclaims any and all representations, warranties and conditions of merchantability, non-infringement of copyright or patent rights of others, title, satisfactory equality, or fitness for a particular purpose.

9.6.2.2 *Loss Limitations*

In no event shall the State or any State employee, Director or Agent, incur any liability arising out of or relating to any digital certificate or any services provided by the State in respect to Certificates whether issued by the State of Illinois Certificate Authority (CA) or another. This limitation shall apply regardless of the number of transactions, digital signatures, or causes of action arising out of related to such Certificate or any services provided regarding any such Certificate. The foregoing limitations shall apply to any claim whatsoever, whether based in contract, tort, or any other theory of liability and shall be applicable to subscribers, relying parties and any other person relying upon, issuing, or applying for a Certificate from the State of Illinois or any other CA under this Certificate Policy.

In no event shall the State, or any State employee, Director, or Agent be liable for any incidental, special, punitive, exemplary, indirect, reliance, or consequential damages (including without limitation, damages for loss of business, loss of business opportunities, loss of good will, loss of profits, business interruption, loss of data, lost savings or other similar losses) whether arising out of theories of contract, tort, or any other theory of liability.

9.6.2.3 *Other Exclusions*

Without limitation, the State shall not be liable to any Subscribers, Relying Parties, other CAs, or any other person, entity or organization for any losses, costs, expenses, liabilities, damages, claims or settlement amounts arising out of or relating to use of a Certificate or any services provided by the State in respect to the Certificates if:

- The Certificate was issued as a result of errors, misrepresentations, or other acts or omissions of a Subscriber or of any other person, entity, or organization;
- The Certificate has expired or has been revoked;
- The Certificate has been modified or otherwise altered;
- The Subscriber has violated the Certificate Policy, Certification Practice Statement, or its Subscriber Agreement or a Relying Party is

in violation of the Certificate Policy, Certification Practice Statement or its Relying Party Agreement;

- The Private Key associated with the Certificate has been compromised; or
- The Certificate is used other than as permitted by this Certificate Policy and the associated Certification Practice Statement or is used in contravention of applicable law.

In no event shall the State be liable for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to its refusal to issue a Certificate.

In no event shall the State be liable to any Subscriber, Relying Party, other CA, or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to any proceeding or allegation that a Certificate or any contents of a Certificate infringe, misappropriate, dilute, unfairly compete with, or otherwise violate any patent, trademark, copyright, trade secret, or any other intellectual property right or other right of any person, entity, or organization in any jurisdiction.

9.6.2.4 *Hazardous Activities*

The Certificates and the services provided by the State under this Certificate Policy and the associated Certificate Practice Statement are not designed, manufactured or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including but not limited to the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines. The State specifically disclaims any and all representations and warranties with respect to such hazardous activities or uses, whether express, implied, statutory, by usage of trade, or otherwise.

9.6.3 Subscriber Representations and Warranties

Subscribers shall:

- Make true representation at all times to the CA, the Registration Authority (RA) and the appropriate Local Registration Authorities (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.

For the Level-4 of SHA256-Level-4 Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber shall be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers at all assurance Levels shall agree to the following:

- Accurately represent themselves in all communications.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their subscriber agreements and local procedures.
- Promptly notify the Illinois PKI upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS. (http://www.illinois.gov/bccs/services/catalog/security/PKI/Pages/default.aspx)
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

9.6.4 Relying Parties Representations and Warranties

None

9.6.5 Representations and Warranties of other Participants

None

9.7 DISCLAIMERS OF WARRANTIES

Nothing contained in the State Certificate Policy, Certification Practice Statement or in any Subscriber Agreement, or any Relying Party Agreement shall be deemed to constitute either the State, or any of its subcontractors, agents, suppliers, employees, or directors the partner, agent, trustee, or legal representative of any Subscriber, Relying Party or any other third party or to create any fiduciary relationship between the State and any Subscriber, Relying Party or any other third party, for any purpose whatsoever. Nothing in this CP or in any Subscriber Agreement or any Relying Party Agreement shall confer on any Subscriber, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the State.

9.8 LIMITATIONS OF LIABILITY

As the Certificate Authority (CA) and Registration Authority (RA) functions are provided by the State, the liability issues related to both functions are combined in this CP.

Nothing in this Certificate Policy shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on the State by virtue of any contract or obligation that is otherwise determined by applicable law.

The State shall have no liability to any subscriber, relying party and any other entity for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of a Certificate or any services provided by the State. Use of any Certificate is limited by the terms of this CP and the CPS. This CP also contains limited warranties and disclaimers of representations, warranties, and conditions.

9.9 INDEMNITIES

Refer to section 9.9.1 and 9.9.2

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 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 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 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.

9.10 TERM & TERMINATION

9.10.1 Term

Refer to section 9.12.2

9.10.2 Termination

Termination of this CP is at the discretion of the Illinois Policy Authority.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

Sections 2 (Repositories), 9.6 (Representations and Warranties), 9.2 (Financial Responsibility), 9.14 (Governing Law), 9.3 (Confidentiality), 9.5 (Intellectual Property Rights), 4.4 Certificate Acceptance), 4.9 (Certificate Revocation and Suspension), 9.12 (Amendments), 1.5.4 (CPS Approval Procedures) shall survive termination or expiration of this CP, any Subscriber Agreements, and any Relying Party Agreements. All references to sections which survive termination of this CP, any Subscriber Agreements, and any Relying Party Agreements, shall include all subsections beneath such Section. All payment obligations shall survive any termination or expiration of this CP, any Subscriber Agreements, and any Relying Party Agreements.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

The Illinois PKI PA shall establish appropriate procedures for communications with Entity CAs via contracts or memoranda of agreement as applicable.

For all other communications, no stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Changes to items within this Policy that in the judgment of the Policy Authority shall have no/minimal impact on the users using Certificates and Certificate Revocation Lists issued by this Certificate Authority may be made with no change to the Policy version number and no notification to the users.

9.12.2 Notification Mechanism and Period

Changes to the Certificate Policy which, in the judgment of the Policy Authority may have significant impact on the users using Certificates and Certificate Revocation Lists issued by this Certificate Authority, shall undergo a review and comment period of 60 days. The State Policy Authority shall review all comments and respond individually or with further changes as appropriate. If the Policy Authority decides not to make any further changes after the 60 day review period the initially-proposed modified document shall be published in the Repository.

In order to allow entities to modify their procedures as needed, all changes to this Policy shall become effective 30 days after final publication on the State Repository. It shall be the responsibility of Subscribers and Relying Parties to periodically check the Repository for notice of final publication of this Policy.

Use of or reliance on a Certificate after the 30-day period (regardless of when the Certificate was issued) shall be deemed acceptance of the modified terms.

9.12.3 Circumstances under which OID must be changed

No stipulation

9.13 DISPUTE RESOLUTION PROVISIONS

Within the Certificate Authority (CA) domain, disputes between Certificate users, one of which acts in the role of a subscriber and the other which acts in the role of a relying party, or between Certificate users and the CA or the RA, shall initially be reported to the Policy Authority (PA) for resolution. Such reports should be sent in writing to the address listed in Section 1.5.2.

Decisions regarding DN composition and resolution of any disputes regarding name composition or name forms shall be made by the PA.

9.14 GOVERNING LAW

The laws of the State of Illinois, excluding its conflict of laws, rules and any applicable treaties, shall govern the construction, validity, interpretation, enforceability and performance of this CP, all Subscriber Agreements and all Relying Party Agreements. Any dispute in respect to this CP, any Subscriber

Agreement, any Relying Party Agreement, or in respect to the Certificates or any services provided by the State in respect to the Certificates, shall be brought in the Illinois Court of Claims, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes. The Illinois PKI provides electronic signatures that comply with the Federal E-Sign Act and the State of Illinois' Electronic Commerce Security Act (5 ILCS 175).

9.15 COMPLIANCE WITH APPLICABLE LAW

The Illinois CA shall comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

All references in this CP to "Sections" refer to the sections of this CP. As used in this CP, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine and all terms used in the singular shall be deemed to include the plural, and vice versa, as the context may require. The words "hereof," "herein" and "hereunder" and other words of similar import refer to this CP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP. The words "include" and "including" when used herein is not intended to be exclusive and mean, respectively, "include, without limitation," and "including, without limitation."

9.16.2 Assignment

The Certificates and the rights granted under this CP, the CPS, any Subscriber Agreement, or any Relying Party Agreement are personal to the Subscriber to whom a Certificate was issued, and to the person, entity, or organization which entered into the Subscriber Agreement or Relying Party Agreement with the State, and cannot be assigned, sold, transferred, or otherwise disposed of, whether voluntarily, involuntarily, by operation of law, or otherwise, without the prior written consent of the State. Any attempted assignment or transfer without such consent shall be void and shall automatically terminate such Subscriber's or Relying Party's rights under this CP, the CPS, any Subscriber Agreement, or any Relying Party Agreement.

The State may assign, sell, transfer, or otherwise dispose of this CP, any Subscriber Agreement, or any Relying Party Agreement together with all of its rights and obligations under this CP, the CPS, any Subscriber Agreements, and any Relying Party Agreements (i) to an affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets of the business of the State to which this CP, the Subscriber Agreements, and Relying Party Agreements relate. Subject to the foregoing limits, this Agreement shall be binding upon and

shall inure to the benefit of permitted successors and assigns of the State, Subscribers, and Relying Parties, as the case may be.

9.16.3 Severability

Whenever possible, each provision of this CP, any Subscriber Agreements, and any Relying Party Agreements shall be interpreted in such manner as to be effective and valid under applicable law. If the application of any provision of this CP, any Subscriber Agreements, or any Relying Party Agreements or any portion thereof to any particular facts or circumstances shall be held to be invalid or unenforceable by a court of competent jurisdiction, then (i) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of this CP, any Subscriber Agreements, or any Relying Party Agreements shall not in any way be affected or impaired thereby, and (ii) such provision shall be enforced to the maximum extent possible so as to effect its intent and it shall be reformed without further action to the extent necessary to make such provision valid and enforceable.

For greater certainty, it is expressly understood and agreed that every provision of this CP, any subscriber agreements, or any relying party agreements that deal with (i) limitation of liability or damages, or (ii) disclaimers of representations, warranties, conditions, or liabilities, is expressly intended to be severable from any other provisions of this CP, any subscriber agreements, or any relying party agreements and shall be so interpreted and enforced.

Any and all legal actions in respect to a dispute which is related to a Certificate or any services provided in respect to a Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the Certificate, whichever is sooner. If any action in respect to a dispute which is related to a Certificate or any service or services provided in respect to a Certificate is not commenced prior such time, any party seeking to institute such action shall be barred from commencing or proceeding with such action.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The State shall not be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or comply with the terms of this CP, any Subscriber Agreement, or any or settlement amounts arising out of or related to delays in performance or from failure to perform Relying Party Agreement due to any causes beyond its reasonable control, which causes include, without limitation, acts of God, so-called "hackers," "crackers" or other computer intruders, or the public enemy, riots and insurrections, acts of terrorism, war, accidents, fire, strikes and other labor difficulties, embargoes, judicial action, lack

of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.

9.17 OTHER PROVISIONS

This CP, the CPS, all Subscriber and Relying Party Agreements state all of the rights and obligations of the State and any Subscriber or Relying Party in respect to the subject matter hereof and thereof and such rights and obligations shall not be augmented or derogated by any prior agreements, communications or understandings of any nature whatsoever whether oral or written. The rights and obligations of the State may not be modified or waived orally and may be modified only in a writing signed or authenticated by a duly authorized representative the State.

In the event of a conflict between the provisions of this CP and the CPS, and any express written agreement between the State and a Subscriber or Relying Party, with respect to a Certificate or any services provided by the State with respect to the Certificates, the terms described in the CP and the CPS shall take precedence. In the event of a conflict between the provisions of this CP and CPS and a cross-certification agreement executed between the Policy Authority (PA) and the entity responsible for another CA, the terms of the cross-certification agreement shall take precedence.

10. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

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-E Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC

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 & ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FPKI OA	Federal Public Key Infrastructure Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Entity and the FPKIPA allowing interoperation between the FBCA and Entity Principal CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply

URL	Uniform Resource Locator
U.S.C.	United States Code
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	An agent of the State PKI CA. The Operational Authority is

(OA)	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.
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.
Remote workstation	Any workstation or computer which is used to connect to, manage or manipulate PKI hardware at a remote (i.e., off-site) location.
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]