THIRD PARTY REVIEW

State of Illinois
Public Key Infrastructure (PKI)

Department of Central Management Services
Bureau of Communication and
Computer Services

September 2004

TABLE OF CONTENTS

Report Digest i

Report on Public Key Infrastructure 1

Report Summary 3

Definitions 6

Report Introduction 9

Department's Description of Controls 10

Auditor's Description of Tests and Operating Effectiveness 12

Subsequent Events 21

Appendix A – Entities with PKI Applications 22

Appendix B – Entities with Local Registration Authorities 23

This Page Intentionally Left Blank

REPORT DIGEST

STATE OF ILLINOIS PUBLIC KEY INFRASTRUCTURE (PKI)

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW

Release Date:
September, 2004

State of Illinois
Office of the Auditor General
WILLIAM G. HOLLAND
AUDITOR GENERAL

To obtain a copy of the
Report contact:
Office of the Auditor General
Iles Park Plaza
740 E. Ash Street
Springfield, IL 62703
(217) 782-6046 or TTY (888) 261-2887

This Report Digest is also available on
the worldwide web at
http://www.state.il.us/auditor

INTRODUCTION

The Department of Central Management Services (Department) operates a Public Key Infrastructure (PKI) to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies.

The purpose of a PKI is to manage keys and certificates, which are used for identification, entitlements, verification, and privacy. A PKI achieves its purpose across a wide variety of applications through the use of encryption and digital signature services.

The State of Illinois Certificate Authority conducted a Cross-Certification with the Federal Bridge Certificate Authority (FBCA) on December 19, 2003. The Cross-Certification will allow State agencies to conduct business with federal agencies in a trusted manner.

We reviewed controls over the Department’s Public Key Infrastructure environment primarily during the period from November 12, 2003 to March 5, 2004. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary to evaluate the controls.

We raised several questions during the audit concerning the Department’s roles and responsibilities with PKI and the requirements outlined in the Electronic Commerce Security Act (5 ILCS 175) and the Administrative Code (14 Ill. Adm. Code Part 100). We recommended the Department clarify its roles and responsibilities through a formal, written Attorney General opinion.

The Department concurred with the recommendation.

AUDITORS' OPINION

Procedures were generally sufficient to provide reasonable, but not absolute, assurance that relevant control objectives were achieved.

WILLIAM G. HOLLAND, Auditor General

AGENCY DIRECTOR/DEPUTY DIRECTOR

Director: Michael Rumman
Deputy Director/Bureau Chief: Jay Carlson

To view an online version of the complete report, go to
http://www.state.il.us/auditor/special.htm

This Page Intentionally Left Blank

SPRINGFIELD OFFICE:
ILES PARK PLAZA
740 EAST ASH • 62703-3154
PHONE: 217/782-6046
FAX: 217/785-8222 • TTY: 888/261-2887

CHICAGO OFFICE:
MICHAEL A. BILANDIC BLDG. • SUITE S-900
160 NORTH LASALLE • 60601-3103
PHONE: 312/814-4000
FAX: 312/814-4006

OFFICE OF THE AUDITOR GENERAL
WILLIAM G. HOLLAND

AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General
State of Illinois

We have examined the accompanying description of controls related to the State of Illinois, Department of Central Management Services, Public Key Infrastructure used in the issuance and usage of digital certificates. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's controls; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily; and (3) such controls had been placed in operation as of March 5, 2004. Our review was primarily performed between November 12, 2003 and March 5, 2004. Management of the Department specified the control objectives. Our examination was performed in accordance with the Illinois State Auditing Act, applicable generally accepted auditing standards, and "Government Auditing Standards" issued by the Comptroller General of the United States. We included those procedures considered necessary under the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the Public Key Infrastructure presents fairly, in all material respects, the relevant aspects of the Department's controls that had been placed in operation as of March 5, 2004. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the body of the report, to obtain evidence about their effectiveness in meeting the control objectives, during the period from November 12, 2003 through March 5, 2004. The specific controls and the nature, timing, extent, and results of the tests are listed in the body of the report. In our opinion, the controls that were tested, as described in the body of the report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the body of the report were achieved during the period from November 12, 2003 through March 5, 2004.

The relative effectiveness and significance of specific controls at the Department and their effect on assessments of control risk are dependent on their interaction with the controls and other factors present.

The description of controls at the Department is as of March 5, 2004, and information about tests of the operating effectiveness of specified controls covers the period from November 12, 2003 through March 5, 2004. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the Department is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the Public Key Infrastructure, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended for the information and use of the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, Department management, existing users of the Illinois Public Key Infrastructure, and the Federal Bridge Certification Authority. However, this report is a matter of public record and its distribution is not limited.

William J. Sampias, CISA
Director, Information Systems Audits

March 5, 2004

REPORT SUMMARY

The objectives of the audit were to:

- Audit the general description of systems/services presented, and the relevant policies outlined in the Certificate Policy (CP) and Certification Practice Statement (CPS) supporting the specified Certification Authority (CA);
- Audit and assess the suitability, existence and effective operation of the security and internal controls over the State of Illinois' procedures for CA root and primary key pair generation and associated key management life-cycle controls; and
- Audit and assess the suitability and existence of the CA environment controls over the establishment of the specified CA, which has been implemented for on-going certification services.

The scope of the audit has been focused on security features and controls, practices, and procedures that are in place with the State of Illinois' processing and management environments to meet management's established control objectives.

This audit addressed specific controls over the organization and operation of the State of Illinois' CA facility located in Springfield, Illinois.

The Department of Central Management Services (Department) operates a Public Key Infrastructure (PKI) to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies.

The purpose of a PKI is to manage keys and certificates, which are used for identification, entitlements, verification, and privacy. By managing keys and certificates through a PKI, an organization establishes and maintains a secure and trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

The Department's control procedures and the degree of compliance with the procedures were sufficient to provide reasonable, but not absolute, assurance that relevant control objectives were achieved.

We identified one issue regarding compliance with the Electronic Commerce Security Act. This issue came to our attention during our testing of the Department's Description of Controls and warrants additional emphasis.

<u>Compliance with the Electronic Commerce Security Act</u>

We raised several questions during the audit concerning the Department's roles and responsibilities with PKI and the requirements outlined in the Electronic Commerce Security Act (5 ILCS 175) and the Administrative Code (14 Ill. Adm. Code Part 100). We believe the importance of the questions raised and the lack of clarity in the governing statute and rules require action by the Department to ensure its program is operating in accordance with the law. As a result, we have developed the following issue and recommendation.

Section 25-105 of the Electronic Commerce Security Act sets forth certain authorities and responsibilities for the Department of Central Management Services. These include:

- The Department may adopt rules setting forth minimum security requirements for the use of electronic records and electronic signatures by State agencies (subsection (a));
- The Department shall specify appropriate minimum security requirements to be implemented and followed by State agencies for (1) the generation, use and storage of key pairs, (2) the issuance, acceptance, use, suspension and revocation of certificates, and (3) the use of digital signatures (subsection (b));
- The Department has the authority to specify the rules, procedures, and policies whereby State agencies may issue or contract for the issuance of certificates (subsection (c)); and
- The Department may specify appropriate minimum standards and requirements that must be satisfied by a certification authority before its services are used by any State agency for the issuance, publication, revocation, and suspension of certificates to such agency, or its employees or agents (for official use), or the certificates it issues will be accepted for purposes of verifying digitally signed electronic records sent to any State agency by any person.

Section 25-105 (c) gives each State agency the authority to issue digital certificates to its employees and agents and persons conducting business or other transactions with the State agency, thereby acting as a certification authority. Section 10-135 of the Electronic Commerce Security Act provides that the Secretary of State may certify a security procedure as a “qualified security procedure” for purposes of establishing a record as a secure electronic record and a signature as a secure electronic signature. Subsection (e) of Section 10-135 further states “[t]he Secretary of State shall have exclusive authority to certify security procedures under this Section.”
Section 15-115 of the Act states the “Secretary of State may adopt rules applicable to **both** the public and private sectors for the purpose of defining when a certificate is considered sufficiently trustworthy. . .such that a digital signature verified by reference to such a certificate will be considered a qualified security procedure (emphasis added). . .” While the Secretary of State has adopted rules governing the approval and operation of certification authorities [14 Ill.Adm.Code Part 100], legal counsel for the Secretary of State has indicated that its rules are intended to apply to private agencies, not State entities, offering electronic commerce security services in Illinois.

The Department is acting as a certification authority, using a security procedure known as Public Key Infrastructure (PKI). PKI is recognized as a qualified security procedure when operated in accordance with requirements set forth in Secretary of State rules at 14 Ill.Adm.Code 100.40 (a). However, the Department does not follow all requirements of the Secretary of State’s rules pertaining to the approval and operation of certification authorities in the State of Illinois. Further, while the Department has published its “Certificate Policy for Digital Signature and Encryption Applications,” it has not adopted rules in accordance with the Illinois Administrative

Procedure Act. Finally, the Department has made its certification services available to non-State entities.

Recommendation

The Department of Central Management Services should clarify through a formal, written Attorney General opinion:

1) whether its security procedures need to be certified by the Secretary of State to constitute "qualified" security procedures under the Act;
2) whether, when acting as a certification authority, the Department or any other State agency needs to meet requirements set forth in the Secretary of State's administrative rules at 14 Ill.Adm.Code Part 100;
3) whether the Department's certification procedures need to be promulgated and adopted in the form of rules under the Administrative Procedure Act; and
4) whether the Department or any other State agency may offer digital certificates to non-State entities and, if so, under what circumstances (e.g., only for the purpose of doing business with the State).

Department Response

We concur with your recommendations. We will pursue an opinion from the Attorney General on the issue of compliance with the Electronic Commerce Security Act. As noted in the "Subsequent Events" section of the audit report, CMS has placed a sanitized version of the CPS on the State PKI Web page.

The Department response was provided on August 10, 2004, by Jay Carlson, Deputy Director/Bureau Chief, Bureau of Communication and Computer Services of the Department of Central Management Services.

STATE OF ILLINOIS
PUBLIC KEY INFRASTRUCTURE
DEFINITIONS

Access Control: Physical and/or electronic (logical) means that are used to ensure that only authorized entities can gain access to information, computer systems, or communication systems.

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.

Certificate: A digital representation of information that binds the user's identification with the user's public key in a trusted manner. At a minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Certification Authority (CA): A trusted entity authorized to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate (e.g., control of the registration process, the identification and authentication process, the certificate manufacturing process and publication, revocation, renewal and archival of certificates).

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. The CP is a public document that outlines the certificate policies of the CA.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in managing and issuing certificates in relation to a specific Certificate Policy.

Certificate Revocation List (CRL): A computer-generated record that identifies certificates that have been revoked or suspended prior to their expiration dates.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate: A certificate used to establish a trust relationship between two Certification Authorities**.**

Cryptography: The art and science of keeping information secure. It deals with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages.

Data Recovery: The mechanisms and processes that allow authorized parties to recover the plain text data when the decryption key has been lost or is otherwise unavailable.

Decryption: The process of transforming encrypted text or data (called cipher text) into original text or data (called plain text).

Digital Signatures: "Digital signature" or "digitally signed" refers to a transformation of a message using a cryptosystem such that a person who has the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made.

Directory: A repository or database of certificates, CRLs, and other information that is available online to users.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

Federal Information Processing Standard (FIPS): Technical standards issued by the National Institute of Standards and Technology (NIST).

Integrity (Data Integrity): Protection and assurance against unauthorized modification or destruction of information.

Key: Any piece of information, usually a number contained in a certain minimum number of bits, needed or used to encrypt or decrypt a message.

Local Registration Authority (LRA): A type of Registration Authority with responsibility for a local community.

Logical Access Control: Refers to an automated system that controls an individual's ability to access one or more computer system resources such as a workstation, a network, an application, or a database.

Non-Repudiation: Strong and substantial evidence of the identity of the signer of a message, of the time and context of a message, and of message integrity, sufficient to prevent a party from successfully denying the origin, submission, or delivery of the message and sufficient to validate the integrity of its contents.

Operational Authority (OA): Entity responsible for ensuring the Certification Authority operates in accordance with the CP and CPS.

Policy Authority: Responsible for ensuring that both the security policy and the practices that are employed in issuing certificates are consistent with the policies described in the Certificate Policy.

Private Key: The part of a key pair to be safeguarded by the owner. A private key is used to generate a digital signature. Private keys are used to decrypt information, including key encryption keys during key exchange. It is computationally infeasible to determine a private key given the associated public key.

Public Key: The part of a key pair that is made public, usually by posting it to a directory. A public key can be either a signature key or exchange key. The signer's public signature key is used to verify a digital signature.

Public Key Infrastructure (PKI): Framework established to issue, maintain, and revoke public key certificates.

Registration Authority (RA): Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.

Relying Party: A recipient of a certificate signed by the CA who acts in reliance on those Certificates and/or digital signatures verified using that certificate.

Statement on Auditing Standards (SAS) 70: SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit represents that a service organization has been through an in-depth audit of the control processes which generally include information technology and related processes. SAS 70 audits are also referred to as third party reviews.

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.

Trust: The confidence the user of a system has that the system does perform its required functions and does not perform any unwanted functions.

Token: A device (e.g., floppy disk, Common Access Card, smart card, PC Card, Universal Serial Bus device, etc.) that is used to protect and transport the private keys of a user.

STATE OF ILLINOIS
PUBLIC KEY INFRASTRUCTURE
INTRODUCTION

The Electronic Commerce Security Act (5 ILCS 175) allows the State "to facilitate and promote electronic commerce, by eliminating barriers resulting from uncertainties over writing and signature requirements, and promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce."

The State of Illinois has created a Public Key Infrastructure (PKI) to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies. During fiscal year 2000, the State of Illinois, Department of Central Management Services (Department) contracted with Entrust, Inc.

The purpose of a PKI is to manage keys and certificates, which are used for identification, entitlements, verification, and privacy. By managing keys and certificates through a PKI, an organization establishes and maintains a secure and trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

In January 2001 the Department's Certification Authority (CA) conducted the root key generation and in February 2001 completed the production environment rebuild and key transfer. The CA Operational System Ceremony was a formal procedure, designed to ensure the non-refutability of the integrity of the CA configuration once it became operational. As of February 2004, there were approximately 30,000 users and 14 active applications (see Appendix A for a list of the entities with active applications).

The Certificate Policy for Digital Signature and Encryption Applications has been established and defines all certificate policies of the PKI system. The CP is available, via the Internet:
http://www.illinois.gov/pki/.

A Policy Authority (PA) comprised of individuals representing constitutional offices, State agencies, universities, and local governments has been established. The Policy Authority is responsible for ensuring that both the security policy and the practices employed in issuing certificates are consistent with the policies described in the Certificate Policy.

The State of Illinois CA conducted a Cross-Certification with the Federal Bridge Certificate Authority (FBCA) on December 19, 2003. This process allowed the State to establish a "mutual cross-certification" trust with the FBCA. The Cross-Certification with the FBCA will allow State agencies to conduct business with federal agencies in a trusted manner.

STATE OF ILLINOIS
PUBLIC KEY INFRASTRUCTURE
DESCRIPTION OF CONTROLS

The following Description of Controls section (pages 10 and 11) consists of text provided by the Department of Central Management Services.

The State of Illinois, Department of Central Management Services operates as a Certification Authority (CA) known as State of Illinois Public Key Infrastructure. The CA provides the following certification authority services:

- Subscriber key management services;
- Subscriber registration;
- Certificate renewal;
- Certificate rekey;
- Certificate issuance;
- Certificate distribution;
- Certificate revocation; and
- Certificate status information processing.

The Director of the Department of Central Management Services is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Management has assessed the following controls over its CA operations:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices.

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated; and
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles.

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - The continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

Control Objective: Management should ensure appropriate policies and procedures exist to effectively control the administration of the PKI environment.

Tests Performed: We compared the Certificate Policy (CP) and the Certification Practice Statement (CPS) to the Internet Engineering Task Force framework, *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework (RFC 2527).* The framework provides a comprehensive list of topics that could be potentially covered in either of the documents.

Results: The CP and CPS generally complied with RFC 2527. However, the CP and CPS should be continuously updated to reflect the current environment.

Tests Performed: We reviewed the change control procedures over the CP and the CPS.

Results: Changes to the CP are published for comment for a period of 60 days. At the end of the 60 days the Policy Authority (PA) will approve the changes and publish the CP on the website. The changes to the CP will go into effect 30 days after publication. Changes to the CPS will be made after 30 days notice to the community. All changes to the CP or CPS must be approved by the PA.

Control Objective: Management should ensure that roles and responsibilities are communicated and in accordance with the policies.

Tests Performed: We reviewed the controls and the responsibilities of the Policy Authority, Operational Authority, Certificate Authority, Registration Authority, Local Registration Authority, Relying Party and the Subscriber.

Results: The PA is responsible for the creation, approval, and implementation of the CP and CPS. The State's PA is comprised of individuals representing constitutional offices, State agencies, universities, and local governments, which are current users. As of February 2004 there were six agencies represented. The PA should meet at least quarterly to ensure that it is fulfilling its mission.

The Operational Authority (OA), under the direction of the Director of the Department, is responsible for ensuring the Certificate Authority operates in accordance with the CP and CPS.

The Certificate Authority (CA) "ensures the trustworthiness of Subscriber's electronic identities, issues and signs certificates." Additionally, the CA revokes certificates and publishes certificate status through certificate revocation lists. Also, the CA may cross-certify with other CAs when authorized by the PA.

The Registration Authority (RA) is responsible for the procedures and process of Subscriber's submitting applications for certificates. The RA must identify and authenticate the individual applying for the certificate, approve or reject the application, and revoke the certificate when necessary.

The Local Registration Authority (LRA) is a subset of the RA. The LRAs are responsible for the identification and authentication of information on Subscriber applications for their agency. Each participating State agency, university and local government "may appoint an LRA to be responsible for the identification and authentication of Subscribers and its constituency in accordance with the CP." As of November 2003 there were 33 LRAs representing 20 State agencies, universities, and local governments (See Appendix B for a complete list of entities with an LRA).

The End-Entities (Subscribers) consist of State employees, individuals conducting business with the State, hardware and software devices and/or applications. Subscribers are generally required to:

- Use certificates to encrypt information;
- Make true representation of information submitted in the application;
- Use certificates in accordance with the CP;
- Preserve integrity of private keys;
- Protect passwords;
- Review all certificate information and accept/reject certificate upon issuance;
- Inform RA/LRA within 48 hours of information changes; and
- Inform RA/LRA within eight hours of private key compromise.

The specific requirements are communicated to the Subscriber via the Subscriber Agreement.

The Relying Party is a "recipient of a certificate signed by the State CA who acts in reliance on those certificates and/or digital signatures verified using the certificate." Additionally, Relying Parties must agree to abide by the terms of the CP and CPS. Currently, there are no Relying Parties.

Control Objective: Management should ensure compliance with relevant governmental and external requirements.

Tests Performed: We reviewed governmental and external requirements for compliance.

Results: As outlined in the Report Summary section, we raised several questions during the audit concerning the Department's roles and responsibilities with PKI and the requirements outlined in the Electronic Commerce Security Act (5 ILCS 175) and the Administrative Code (14 Ill. Adm. Code Part 100). We recommend the Department clarify through a formal, written Attorney

General opinion whether they are complying with all necessary provisions of the Act and Administrative Code.

We also noted that Section 15-305 of the Electronic Commerce Security Act requires "(a) For each certificate issued by a certification authority with the intention that it will be relied upon by third parties to verify digital signatures created by subscribers, a certification authority must publish or otherwise make available to the subscriber and all such relying parties:

(1) its certification practice statement, if any,. . ."

The Department has published its CP; however it has not published or otherwise made available its CPS. The Department classified the CPS as confidential as they believe it contains privileged information that is inappropriate for public disclosure. We recommend the Department take reasonable steps to publish the CPS, or non-confidential parts thereof, in compliance with the Act.

The CP states, "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 Subscription Agreements and all Relying Party Agreements. Any dispute in respect to this CP, any Subscription 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 CP states "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 the CP and the CPS. The CP also contains limited warranties and disclaimers of representations, warranties and conditions."

All information submitted to the CA by the Subscriber is to remain confidential, unless otherwise required by law. All information is maintained in locked cabinets in locked offices. Only the Acting Security Officer, Acting CA Administrator, and the Acting Directory Administrator have access to cabinets. The CA, RA or LRA will not disclose information to any third party unless required to by a court order, CP, or the certificate holder. During the fiscal year there were no requests for confidential information.

The CP requires the CA to undergo a compliance audit prior to initial approval as a CA to demonstrate compliance with State policies, the CP, and the CPS. Additionally, compliance audits are to be conducted annually, or whenever substantive changes are made to the CP or the CPS. The initial audit was conducted by Deloitte & Touche LLP during the root key of the CA, in January 2001. Deloitte & Touche LLP conducted SAS 70 audits in 2002 and 2003 and presented the Department with an unqualified opinion in both audits. The March 15, 2003 report stated:

> *In our opinion, the control objectives included in the accompanying description were sufficient to meet the stated objectives of the indicated systems/services, the described control procedures were suitably designed to provide reasonable assurance that the control objectives described therein were achieved, and they operated effectively during the period of March 1, 2002 to February 28, 2003*.

Control Objective: Management should maintain controls to provide assurance that subscriber information is properly authenticated.

Tests Performed: We reviewed the registration process.

Results: State employees and businesses/individuals conducting electronic business with the State may submit a certificate application. The State has three registration processes: web registration, face-to-face registration, and bulk registration.

In-State Subscribers

Available on the State's Homepage is an application for Subscribers to complete to obtain a digital identity. The Subscriber is required to read the State of Illinois Digital Certificate Subscriber Agreement and agree to the terms. Once agreed to, the Subscriber completes the State of Illinois Digital Identification Application. The information on the application is to be taken from the Subscriber's State of Illinois Driver's License or Identification Card. Once the application is completed, it is then automatically verified to a trusted source. If verification is approved, a Subscriber profile is created. We verified the process by successfully registering Auditor General staff through the web registration model.

Out-of-State Subscribers

Out-of-State Subscribers requesting digital identities are required to complete and have notarized a State of Illinois Digital Identification Application. The Application is then mailed to the Department. Each application is reviewed for completeness and indication of notarization.

The information from the application is then entered into a bulk operation. Once all applications are manually input, the batch is run, producing the reference code and authentication code, which are returned to the Subscriber. We reviewed 25 out-of-State applications for completeness and notarization, noting no exceptions.

The Subscribers, both in-State and out-of-State, are provided Level I assurance. Face-to-face applications are submitted in person to the RA or an authorized LRA. The Subscriber is asked to complete the web registration process then submit a completed State of Illinois Digital Identification Application in person with two credentials, one of which must be a Secretary of State issued photo ID. Face-to-face registration can provide three levels of assurance: Level II, Level III, and Level IV. Level II is provided to all face-to-face registers, Level III is provided to individuals completing the face-to-face registration process and submitting to a background check. Level IV is provided to those individuals completing the Level III process, in addition to using biometric devices to secure their private keys. No Level IV certificates have been distributed. We reviewed 16 Level II applications for completeness, noting no exceptions. We also reviewed 10 Level III applications for completeness, documentation of background checks, and completed LRA agreements, noting no exceptions.

Bulk applications for State agency staff or other definable groups of individuals will be accepted by the RA from appropriate LRAs in accordance with procedures developed on a case-by-case basis. The bulk registration process provides a Level I assurance.

Control Objective: Management should ensure certificates are issued and maintained in order to ensure integrity.

Tests Performed: We reviewed certificates, revocation procedures, and Certificate Revocation Listings.

Results: Names for Certificate issuers and subjects are of the X.500 Distinguished Name (DN) forms in accordance with RFC 2459 (Internet Engineering Task Force framework, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459)*). The DN is commonly known and is a combination of first name and surname. Each DN must be unique in order for no two individuals to be assigned the same DN. The DN is the complete name of the Directory entry that uniquely identifies a person or entity.

The CP does not allow for the utilization of pseudonymous names in certificates. The PA will settle disputes relating to DN forms. To date no disputes have occurred.

The CP states, “a certificate holder's encryption and/or verification certificate is revoked when the certificates are no longer trusted, for any reason.” If someone initiates a request other than the Subscriber, the Subscriber will be notified and an opportunity for a hearing will be offered. In the event of a key compromise, the key will be immediately revoked without notice to the Subscriber. The Subscriber may submit a request electronically, by signing the request with the private key and sending it to the RA or LRA. In addition, the Subscriber may submit the request in writing. During the audit period two certificates had been revoked: one for key compromise, the other due to the death of the Subscriber. We reviewed the request for revocation relating to the key compromise, noting the RA had revoked the certificate within one hour of receipt of the request.

If the request is due to key compromise, suspected compromise or Subscriber’s dismissal, the request must be placed within eight hours. If the request is for any other reason, the request must be placed within 48 hours. All requests will be processed within eight hours of the request and published on the Certificate Revocation List at least every 24 hours.

The CA is required to provide certificate status information to Subscribers to ensure the validity of certificates. This is conducted by issuing a Certificate Revocation List (CRL). The CRL is a signed and timestamped certificate containing serial numbers of public key certificates that have been revoked, and the reason for revocation. The CRL allows Subscribers access to this information from the Directory to check the trustworthiness of the certificates of other Subscribers they intend on encrypting files for.

In order for the system to operate more efficiently, the CRL has been partitioned into 70+ unique distribution points. Each certificate issued includes the DN of the CRL Distribution Point. This allows Subscribers to check the current CRL when working on-line. The checking of the CRL is done automatically by the software. The State CA issues CRLs on a 24-hour interval, 7 days a week. Additionally, each time a certificate is revoked the CRL is updated and forced out.

The Authority Revocation List (ARL) is a signed, timestamped list of the serial numbers of CA public key certificates that have been revoked. ARLs are issued in 24-hour intervals, 7 days a week.

Revocation of a certificate containing a public key can occur for a number of reasons. However, the compromise of the CA Private Key is the most serious type of compromise in security. In the event the State CA Public Key must be revoked, all affected entities will be notified. In the event the State CA Private Key is compromised; the public key and CA certificate will be revoked. In the event the CA ceases operation all entities will be notified.

Since the creation of the State's CA none of the above events have occurred.

Control Objective: Management should record and review system activities.

Tests Performed: We reviewed the Department's process to record and review audit logs.

Results: Audit logs record all activities that occur within the system. Such activities include:

- Successful and failed attempts to initialize end-users, remove, enable, disable, update, and recover users, their keys and certificates;
- Successful and failed attempts to create, remove, login as, set, revoke privileges of, create, update and recover keys and certificates for the RA and LRAs;
- Failed interactions with the Directory including any failed connection attempts, read and write operations by the RA; and
- All events related to Certificate revocation, security policy modification and validation, the RA software startup and stop, database backup, Certificate and Certificate chain validation, attribute Certificate management, user upgrade, DN change, database and audit trail management, Certificate life-cycle management and other miscellaneous events.

Audit logs permit the CA to investigate events and provide evidence needed to support corrective action. Additionally, the audit log system is internal to the RA software system. Audit logs provide evidence that certain events took place at certain times. The audit logs are automatically timestamped and recorded. The Acting Security Officer and the Acting Directory Administrator review audit logs weekly.

All sensitive events, audit logs, lists, certificates, keys, records, reports, agreements, and correspondence are archived for five years. The Authority database is encrypted, protected by the master keys, and archived for 30 years. All records archived are maintained at two off-site locations.

Control Objective: Management should ensure that the environment is always protected against outside elements to safeguard its integrity.

Tests Performed: We reviewed the physical and logical security over the environment.

Results: The CA is housed at the Central Computer Facility (CCF). The CCF facility was built with pre-cast concrete, has a steel structure, and the shell is noncombustible. The CCF is a secure building that requires monitoring 24 hours a day, 7 days a week, by security guards, surveillance cameras, card readers, and alarms. Access doors remain locked at all times with access restricted by the card readers.

The Department has implemented logical security controls to protect its environment.

Control Objective: Management should ensure established policies and procedures are in place for the authorization of changes.

Tests Performed: We reviewed the Department's change control process.

Results: Changes to the environment follow the Department's change control procedures. All changes are required to be tested in the test environment before being put into production.

The Department does not develop software relating to the PKI environment. All software development is conducted by Entrust. Entrust is evaluated by third parties and has received FIPS 140-1 validation, Common Criteria certification and the WebTrust Seal for CAs.

Control Objectives: Management should ensure that all secret and private keys and activation data are protected, and utilized solely by authorized individuals.

Tests Performed: We reviewed the controls over the keys and data.

Results: The CA, using hardware and software cryptographic modules that comply with the Federal Information Processing Standards and Publication (FIPS) 140-1, creates the Subscriber's encryption and decryption key pairs.

The CA creates the encryption key pair and the corresponding encryption public key certificate. A copy of the encryption public key certificate is stored on the Authority database and the encryption public key is put in the user's Directory entry.

The Subscriber's signing key pairs, encryption key pairs, and the CA signing key pairs utilize Rivest-Shimar-Adleman (RSA) with Secure Hashing Algorithm-1 (SHA-1), with a minimum length of 1024 bits.

The Subscriber's private signing key is never backed up, but Subscribers may make a copy of their profile, which will contain a copy of their private signing key. The Authority database and the CA signing key are encrypted and protected by the master keys. Backups of the CA signing key are maintained on Luna CA3 tokens and stored at the off-site location.

Private keys are activated at the time the Subscriber logs in to the software. Authentication will occur by means of an ID/password or PIN. The private keys will remain active for the time in which the Subscriber is logged in.

Passwords have specific requirements and once passwords are accepted, they are put through a hashing iteration to produce a password token. The token is then stored in the Subscriber's profile. Original passwords are never stored. We reviewed the password policy, noting they comply.

Passwords for the RA and LRAs expire after five weeks. Subscriber passwords expire after 52 weeks. The password for the Security Officer expires after 12 weeks. Once private keys are no longer required, they are overwritten with zeros.

The key lifetimes for certificates are as follows:

Encryption public key	36 months
Verification public key	36 months
Signing private key	25 months
CA private signing key	20 years
Subscriber certificate	3 years

Subscriber private keys may only be utilized during the validity period of the corresponding certificate. Public keys on expired certificates may be utilized to validate signatures on documents during their lifetime.

The State CA creates certificates in order for Subscribers to obtain another's public key. In order for trust to be given, the "CA employs a digital signature to cryptographically sign certificates and provide assurance that the information within the certificate is correct." Certificate fields identify the CA, the Subscriber, version number of the certificate, Subscriber's public key, validity period, and serial number of the certificate along with the algorithm utilized. The CA may add certificate extensions in order to provide additional information. Extensions provide methods of increasing information the certificate contains in order to complete the certificate process. We noted the State CA issues certificates that comply with X.509 standards.

The State CA utilizes CRLs to revoke certificates. The CRLs are stored in the Directory and are checked to verify that certificates have not been revoked. CRL fields identify the CA, the date of the current CRL, the date the next CRL will be generated, and revoked certificates. The CRL may contain additional information through CRL extensions. The extensions provide information about specific entries or extensions. The State CRLs are issued in the x.509 version 2 format.

Control Objective: Management should maintain a written plan for the restoration of critical applications.

Tests Performed: We reviewed the disaster recovery plan.

Results: The Policy Authority has developed a disaster recovery plan: the State of Illinois-Public Key Infrastructure-Information Processing, Recovery Activation Plan (Plan), Version 1.4.

According to the Plan "this document details exact, precise instructions and actions required to recover the CMS PKI environment and services."

The Department has arranged for a facility in the Springfield area for providing disaster recovery services. In addition, the Department has contracted with a disaster recovery service provider for out-of-State recovery locations, in the event of a regional disaster. The Department should ensure the Plan reflects the current environment and is tested annually.

Control Objective: Management should ensure that critical resources are backed-up on a regular basis.

Tests Performed: We reviewed the Department's backup process.

Results: Two types of backups are performed: full system backups and incremental backups. A full backup is a copy of the Authority database, its content, and the Directory at the time the backup occurs. An incremental backup is a copy of the changes, only, to the Authority database and its content since the previous backup. Backups are conducted daily and weekly.

SUBSEQUENT EVENTS
(UNAUDITED)

On June 12, 2004 the Department upgraded its PKI environment to the latest versions of the PKI software.

On June 29, 2004 the Department placed a "sanitized" version of the CPS on its website (http://www.illinois.gov/pki/).

APPENDIX A
STATE OF ILLINOIS PUBLIC KEY INFRASTRUCTURE
ENTITIES WITH PKI ENABLED APPLICATIONS
As of February 2004

1. Department on Aging
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Corrections
5. Department of Commerce and Economic Opportunity
6. Department of Employment Security
7. Department of Public Aid
8. Department of Revenue
9. Environmental Protection Agency
10. Illinois Commerce Commission
11. Illinois State Police
12. Pollution Control Board
13. State Employees’ Retirement System
14. City of Chicago - Department of Public Health

APPENDIX B
STATE OF ILLINOIS PUBLIC KEY INFRASTRUCTURE
LIST OF ENTITIES WITH LOCAL REGISTRATION AUTHORITIES (LRAs)
As of November 2003

1. Department on Aging
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Human Services
5. Department of Insurance
6. Department of Public Aid
7. Department of Public Health
8. Department of Revenue
9. Department of Transportation
10. Environmental Protection Agency
11. Illinois Commerce Commission
12. Illinois Industrial Commission
13. Illinois State University
14. Office of Banks and Real Estate
15. Office of the Attorney General
16. Office of the Auditor General
17. Office of the Secretary of State
18. Teachers' Retirement System of the State of Illinois
19. University of Illinois
20. City of Chicago - Department of Public Health