JNET
5 Technology Park
Harrisburg State Hospital Grounds
Harrisburg, PA 17110

Phone: 717 705 0760
Fax: 717 783 6955
E-mail: jnet@state.pa.us

Commonwealth of Pennsylvania
JNET

Certificate Practice Statement

Table of Contents

COMMONWEALTH OF PENNSYLVANIA JNET CERTIFICATE PRACTICE STATEMENT: USER CERTIFICATES - DRAFT

Revision History

Version	Date	Description	Author
1.0		Initial Version	Mahesh Rengaswamy
2.0	April 23, 2004	Updated to conform with IETF RFC 3647; Updated for new CA implementation; Updated to conform to VeriSign CPS v2.2	Darrell Candis
2.1	July 20,2004	Updated to Include SSL (server certificate) practices	Darrell Candis

1. Introduction

1.1 Overview

JNET is a common secure platform for sharing criminal justice information. Former Governor Tom Ridge of the Commonwealth of Pennsylvania established the JNET Mission as stated below:

> To enhance public safety through the integration of criminal justice information throughout the Commonwealth of Pennsylvania by adopting business practices which promote cost effectiveness, information sharing and timely and appropriate access to information while recognizing the independence of each agency.

The mission statement identified the significance of information sharing and stresses the access to information authorized by an individual's job function. Numerous technology options are present to achieve this goal. Public Key Infrastructure (PKI) refers to the set of security services and processes that enable the use of public key cryptography, X.509 digital certificates and digital signatures. PKI as a business practice addresses the processes of authentication, authorization, data integrity and non-repudiation, each of which speaks directly to the mission statement.

JNET comprises 16 Commonwealth agencies and numerous counties, federal and local government agencies that participate in information sharing by making it available to a community of criminal justice workers who use this information as part of their daily job functions. It is critical for this sensitive information to be available to the criminal justice community in a timely and secure manner.

JNET users authenticate to the myriad services and systems made available via a common yet secure web infrastructure. In the JNET security framework, a user must present a digital certificate (which identifies the user in much the same way that a drivers license identifies an individual) in order to authenticate to a JNET web server and gain access to JNET resources. Through use of public key technology provided by the PKI, all data transmitted between the browser client and the servers are encrypted, ensuring data confidentiality.

Public key technology and digital signatures are also used to digitally sign e-mail messages (ensuring non-repudiation) and enable secure transmission of e-mail messages (thus providing for data integrity).

JNET utilizes the VeriSign Trust Network (VTN) Managed Public Key Infrastructure (MPKI) service for its digital certificate services. Since VeriSign is the manager of the JNET Root CA, VeriSign's own CP and CPS directly affect JNET and its ability to ensure a trust model with VeriSign. Throughout this CPS, the VeriSign CP and CPS will be referenced as well as included as an attachment to this document. It is important to note that JNET uses VeriSign class 3 digital certificates. References to class 1 and 2 certificates in the VeriSign CP and CPS are not applicable. The current version of the VeriSign CPS as of this writing is version 2.2. The VeriSign CPS is still based on the

obsolete IETF RFC 2527. Therefore, there are significant format differences between the JNET CPS and the VeriSign CPS.

This Certification Practice Statement (CPS) describes the JNET Certification Authority (CA) and the actual procedures it follows in creating and managing digital certificates under the JNET Certificate Policy. This CPS shall apply to all certificates issued in support of applications, e-mail, and news under the Commonwealth of Pennsylvania Justice Network (JNET). Version 1.0 of this CPS has been effective since December 31, 1999 and has since been updated to conform with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practice Statement Framework, November 2003, which supersedes the obsolete RFC 2527.

1.2 Document Name and Identification

The JNET Certificate Policy does not yet posses an OID (Object Identifier) that has been registered with the National Institute of Standards and Technology (NIST). An effort is currently underway to address these issues and this section of the CP will be updated accordingly.

1.3 PKI Participants

Certificates issued under JNET will be used for identification and authentication to the JNET applications, web servers, mail servers, and VPN servers. These certificates will also be used to secure communications and transactions (using Secure Sockets Layer (SSL)) between the client and server as well as between the servers, support secure e-mail (using S/MIME), and digitally sign e-mail messages.

The following sections introduce the JNET CA and roles involved in issuing certificates and managing the certificate life cycle process.

1.3.1 Certificate Authorities

The JNET Certification Authority (CA) will generate, sign, and issue digital certificates to support the JNET transactions described above. The JNET Office will serve as the JNET CA Controller/Administrator and as such is responsible for the management, day-to-day operations, and distribution of the JNET CA responsibilities. In this role, the JNET Office will oversee the issuance and revocation of all JNET certificates, the operation of equipment used in managing certificates, the activities of the JNET Registrars, and the collection and maintenance of records. Specifically, the JNET CA Controller/Administrator shall ensure that the following functions are performed in accordance with the stipulations of this policy:

- Certificate generation and revocation
    - Certificates will be generated and revoked in accordance with the VeriSign CP and CPS.
    - The VeriSign KMS manual explains the technical process used to perform this operation.

- Posting certificates and certificate revocation lists (CRLs) to the JNET directory
    - The JNET PKI Design Document details the process by which certificates and CRLs are written to the JNET directory
- Performance of daily and/or weekly backups
    - These procedures are governed by the Standard Operating Procedures of the JNET Operations team.
- Administrative functions such as compromise reporting and system and records maintenance
    - The VeriSign KMS manual contains procedures on performing these functions.
- Programming and management of any hardware cryptographic modules
    - This work is to be performed by VeriSign.

Note that oversight responsibilities should not be confused with control over all of the above functions since separation of duties is required for the trustworthy operation of the JNET CA. Trained and vetted personnel should perform actual operational duties. During system audits and assessments, the CA Controller/Administrator shall be available to external auditors to facilitate their review.

1.3.2 Registration Authorities

The JNET Registrar acts as the Registration Authority and is responsible for the registration/enrollment of users to JNET. The JNET Office acts as the Registration Authority for SSL and IPSec certificate requests. In this role, the Registrar will:

- Inspect the information in the JNET User Access Request Form and verify that the requested access level is consistent with the responsibilities of the user,
    - The JNET Registration Policies and Procedures document contains specific information regarding all registrar roles and responsibilities.
- Ensure that any collateral authorizations (e.g., CLEAN certification) needed to grant particular access levels to users are available,
    - The JNET Registration Policies and Procedures document contains specific information regarding all registrar roles and responsibilities.
- Create and maintain user entries in the JNET Directory,
    - The JNET Registrar Gateway Instructions document contains all information regarding the performance of this function.
- Generate and distribute the authentication code (via a secure, out-of-band method) to the end entities so that they may enroll and retrieve the certificates, and

- The JNET Registrar Gateway Instructions document contains all information regarding the performance of this function.

- Maintain records of the registration/enrollment actions and provide the appropriate records and/or reports to the JNET Office upon request for archive and audit purposes.

- (Placeholder for SSL / IPSec)

The Registrar is also responsible for validating and coordinating the certificate revocation and key recovery requests with the JNET Office. The JNET Help Desk performs this function, and may be reached at 717-783-5164.

Registrars are assigned to specific agencies and/or counties according to user population size and resource availability. Registrar responsibilities may be delegated to one or more individuals per agency or county. The business requirements of a particular agency or county determine the number of registrars assigned.

1.3.3 End Entities

a) Users

JNET users are individuals affiliated with Commonwealth of Pennsylvania Agencies, Counties and municipalities and Federal bodies recognized and approved by the JNET Steering Committee as needing access to criminal justice information through JNET and such information is required as part of the individuals day-to-day business function. These users are issued digital certificates by JNET and can access JNET resources by presenting this digital credential.

Users are required to follow the requirements as outlined in the JNET User Access Request Form.

b) Operators

Operators are responsible for the day-to-day operations and maintenance of the servers and infrastructure needed to support the JNET CA. Operators include contractor staff supporting the JNET hub as well as agency staff or contractors supporting JNET servers located at the various agencies. The CP requires the individuals in these roles to operate the JNET CA in a lawful and responsible manner to support the JNET operations and mechanisms for safeguarding the information and system resources.

c) Applications / Servers

Applications and servers operating within JNET shall also hold certificates for the purpose of authenticating to user clients or other servers and applications. The individuals operating these systems shall also follow the CP and ensure their systems operate in a consistent manner.

1.4 Certificate Usage

Certificates issued under this policy and the associated public/private key pairs shall only be used for their intended purpose within JNET. This certificate policy applies to all

certificates issued to JNET end entities. JNET end entities include users, operators, and applications/servers using or supporting JNET.

JNET issued certificates may only be used for the following purposes:

- Authentication to JNET authorized and approved web sites
    - Subscriber may either install his/her digital certificate in his/her JNET supported browser or JNET approved roaming certificate solution.
- Authentication and encryption within the JNET secure email system.
    - The authentication/signing certificate will be used for authentication into the mail system.
    - The encryption certificate will be used to encrypt all messages.
- Authentication and access to the JNET VPN Service.
    - The authentication/signing certificate will be used for authentication into the JNET VPN Service.
- Authentication and encryption between messaging servers.
    - The authentication/signing certificate will be used for authentication of channels between messaging servers.
    - The encryption certificate will be used to encrypt all messages.
- Authentication and access to approved Commonwealth of Pennsylvania computer systems
    - There is no current stipulation for certificate usage with Commonwealth computer systems. The CPS will be updated at a later date when such a stipulation becomes available.

1.5 Policy Administration

1.5.1 Specification administration organization

The JNET Office and the JNET Steering Committee will address issues relating to this CPS and will approve modifications and additions as they see fit.

1.5.2 Contact Person

This policy was approved by the JNET Steering Committee and is maintained by the JNET Office. For issues related to this CPS, contact:

JNET Office
5 Technology Park

Harrisburg State Hospital Grounds
Harrisburg PA 17110
Phone: 717 705 0760
Fax: 717 783 6955
E-mail: jnet@state.pa.us

1.5.3 Person determining CPS suitability for the policy

The JNET Steering Committee and associated Security Subcommittee oversee the provision of this CPS and decide the applicability of the CP.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Agency	A term used to identify all Commonwealth agencies participating in JNET.
CA	Certification Authority
CMA	Certificate Manufacturing Authority
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
IETF	Internet Engineering Task Force
ISO	International Organization for Standards
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
URL	Uniform Resource Locater
WWW	World Wide Web

1.6.2 Definitions

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	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Commonwealth of Pennsylvania.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
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. [ABA footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
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”]
Authentication	The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.
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.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this Policy, the term "Certificate" refers to certificates that expressly reference the OID of this policy in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation
Certificate Management Authority	A Certification Authority or a Registration Authority
Certificate Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a certificate based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
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 maintained by a CA of its issued certificates that were revoked prior to the stated expiration dates.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certification Path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.™
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.
Component Private Key	Private Key associated with a function of the certificate issuing equipment, as opposed to being associated with an operator or administrator
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 many 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 CAs
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 Replying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
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.
End Entity	Relying Parties and Subscribers
Firewall	Gateway that limits access between networks in accordance with local security policy [NS4009]

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.
Identification	The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) Establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) Establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems. Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an IS 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.
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 communication.
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 (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the JNET CA and an Agency allowing interoperability between the JNET and the Agency.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
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.

National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves crypto logic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
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]
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
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 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.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
Participant	An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.
PKI Disclosure Statement (PDS)	An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law and agency policy.
Private Key	(1) The signing 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 signing 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 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.
PKI Disclosure Statement (PDS)	An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
Registration Authority (RA)	An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.]
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.

Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.
Relying Party Agreement (RPA)	An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.
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	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke (a certificate)	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between the two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying the digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and who activities are constrained by that other CA (See Superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity; (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.
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).
System Equipment Configuration	A comprehensive accounting of all systems hardware and software types and settings.
System High	The highest security level supported by an IS. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an IS in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted agents do not have automated interfaces with Certification Authorities.
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 knows an “trust anchors”.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to perform their internal functions; and (4) adhere to generally accepted security procedures.
Two-person Control	Continuous surveillance and control of positive control material at all times by 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.
Validation	The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.
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. [FIPS140-1]

2. Publication and Repository Responsibilities

2.1 Obligations

2.1.1 CA obligations

The JNET CA will:

- Issue, post, update, and revoke certificates;

  • Procedures for performing these functions are included in the JNET PKI Design Document, the VeriSign KMS manual and the VeriSign CPS.

- Implement this CPS and update as appropriate to ensure that it reflects actual CA practices;

  • This CPS will be implemented upon its completion.

- Monitor and maintain conformance with the JNET Certificate Policy; and

  • Yearly review to and update to be carried out by the JNET Office in conjunction and approval of the JNET Steering Committee.

- Maintain and enforce access controls and separation of privileges on all JNET CA resources.

  • The JNET Office is charged with ensuring that administrative certificates are kept separate and assigned to two, named JNET management staff, who must be Commonwealth of Pennsylvania employees.

2.1.2 RA obligations

JNET does not currently have a registration authority; a registrar performs this function. The JNET Registrar is responsible for registering users. In addition to registering users, the JNET registrar is responsible for:

- Completing and signing the JNET Registrar Agreement;
- Forwarding the JNET Registrar Agreement to the JNET Office;
- Completing Registrar training;

- Maintaining JNET Sponsor Agreements so you can validate the sponsor's signature(s) and contact him/her if there are any registration issues;
- Acting as the Agency/County point of contact with respect to user registration issues;
- Assisting users with scheduling appropriate JNET Training;
- Reporting violations of JNET Policy and Procedures to the Agency/County JTAC, MTAC, or the JNET Office;
- Managing the digital certificate renewal process in the Agency/County;
- Initiating key recovery;
- Deleting a user from the JNET directory in the case of certificate revocation, or when employees retire, transfer out, or separate from the organization;

- Acting as the Agency/County JNET records keeping repository by;
  - Maintaining a JNET user file that contains the user's JNET Access Request Forms and associated correspondence pertaining to JNET access,
  - Maintaining these user records for three years after the user leaves the organization or relinquishes access to JNET, and
  - Reviewing records on a yearly basis and destroying inactive records that are three years old or older;
  - Forwarding Criminal History Access Request(s) to the JTAC; and
  - Notifying the JNET Office of any circumstance that might affect the user's enrollment status (Arrests, Retirements, Transfers, Separations, etc.).

2.1.3 Subscriber obligations

JNET users and operators will be responsible for the appropriate handling and safeguarding of their private keys, use of the JNET environment, use and safeguarding of information obtained from JNET resources, and the reliability of the information they provide or communicate through JNET.

End entities are obligated to:

- Accurately represent themselves in all communications with the JNET CA and Registrar;

- Protect their private keys at all times, in accordance with JNET Certificate Policy, the JNET Security Policy, local procedures, and as stipulated in the certificate acceptance agreements;

- Notify, in a timely manner, the JNET CA of suspicion that their private keys have been compromised or lost. Such notification will be made directly, or indirectly through mechanisms consistent with this CPS;

- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.

Individuals or entities that fail to fulfill their obligations as set forth in this CPS and the JNET Certificate Policy will have their access privileges revoked and may be subject to disciplinary action, termination, or legal action.

2.1.4 Relying party obligations

Parties who rely upon the certificates issued by the JNET CA are obligated to:

- Use the certificate for lawful work-related activities; and

- Check each certificate for validity prior to reliance using procedures described in the X.509 standard.

The JNET CA will report any unlawful or unauthorized actions it detects related to the use of certificates issued by the JNET CA. Individuals or entities that fail to check the validity of JNET certificates prior to each reliance will have no claim against JNET in the event of a dispute, and may jeopardize any claims against the subject of the certificate.

2.1.5 Repository obligations

The JNET CA will use and maintain a directory (subsequently referred to as the JNET Directory) for the propagation of certificates, CRLs, and other access control information. The Directory will be accessible to all JNET users using the lightweight directory access protocol (LDAP), but will implement enough controls to prevent unauthorized modifications and interception of communications. The Registrars are responsible for the creation and maintenance of user entries in the JNET Directory. These entries will also contain location, identification, access privileges, and group membership information used by servers and other JNET relying parties. The creation of a directory entry with all the required identification and authentication information will be a prerequisite for issuing certificates to new end entities.

Revoked certificates will be removed from the Directory so that an application that fails to check the CRL will be unable to grant access based on a revoked certificate. Revoked certificates are still escrowed by VeriSign for recovery purposes.

2.2 Publication and Repository

2.2.1 Publication of CA information

The JNET Office is responsible for ensuring that the CP and CPS will be published to the secure JNET web site and, optionally, to the JNET public web site. Both documents are to be posted in their entirety, unless otherwise stipulated by the JNET Steering Committee. In addition, both the current VeriSign CP and CPS must also be posted to both the secure and public sites. All documents are to appear with other JNET related documentation of each web site. Updates or modifications to the CP or the CPS must be submitted within one week for final approval.

The CP and CPS are considered controlled documents, in that they may only be modified at the direction of JNET management and/or the JNET Steering Committee. Both documents are to be published only in PDF format. Other documents referenced in the CP and CPS are not required to be published on the JNET web sites.

2.2.2 Frequency of publication

All documents referenced in section 2.2.1 will be published on an as-needed basis, based on the frequency of updates.

2.2.3 Access controls

No access control will be imposed on read access to this CPS including past versions. Access is restricted to JNET CA issued certificates and the JNET directory. The JNET CRL is publicly accessible, and is hosted in two locations. Commonwealth MAN users will have access to the JNET CRL via the JNET directory. External, non Commonwealth MAN users may access the JNET CRL via VeriSign. Currently, JNET has a publicly accessible OCSP service that is hosted by VeriSign. Both internal and external Commonwealth MAN subscribers may access this OCSP responder.

---

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The three types of end entities that will be certified under JNET are users, operators, and applications/servers. This section describes the procedures used to authenticate certificate applicants prior to the issuance of their certificates. It also describes how parties requesting renewal or revocation of certificates are authenticated.

3.1.1 Types of names

X.500 distinguished names (DN) will be used to uniquely identify the subjects (owners) of JNET certificates. The DN for an end entity certificate is formed using the following components:

- Common name (e.g., cn=John Smith)
- User ID (e.g., uid=john.smith)
- E-mail (e.g., e=john.smith@jnet.state.pa.us)
- Organizational unit (i.e., ou=Pennsylvania Justice Network)
- Organization (i.e., o=Commonwealth of Pennsylvania)

The DN for a server certificate is formed using the following components:

- Common name (e.g., cn=www.jnet.state.pa.us)
- Organization (i.e., o=Commonwealth of Pennsylvania)
- State (i.e., st=Pennsylvania)
- Country (i.e., c=US)

The DN for an IPSec certificate is formed using the following components:

- Common name (e.g., cn=www.jnet.state.pa.us)
- Organization (i.e., o=Commonwealth of Pennsylvania)
- State (i.e., st=Pennsylvania)
- Country (i.e., c=US)
- FQDN (Fully Qualified Domain Name) (i.e. fqdn=vpn.jnet.state.pa.us)

3.1.2 Need for names to be meaningful and unique

The DN assigned to JNET entities shall be meaningful in that they reflect the various groupings established by the JNET Directory structure. The Distinguished Name for user certificates will always be the user's first name, followed by a period, and then followed by their last name. In the event of a duplicate existing name, the user's middle initial will be appended to the user's first name. Additional letters from a user's middle name will be appended to the user's first name until uniqueness is achieved. The initials “NMN” will be used in the absence of a middle name. Common names will also follow this standard, with the exception that no period be used between the first and last names. This stipulation does not apply to SSL and IPSec certificates.

3.1.3 Rules for allowing anonymous or pseudonymous subscribers

No subscriber may be anonymous, nor use a pseudonym. The only case where an anonymous subscriber is allowed is in the creation of test accounts. Such test accounts are to be used for test purposes only, and never for production purposes. The usage of these test subscriber accounts must be closely monitored and managed. The JNET Configuration Manager is solely responsible for the issuance and management of test accounts. Test accounts will only be valid for a maximum of 30 days, or as long as required.

3.1.4 Recognition, authentication and role of trademarks

The JNET CA shall not be obligated to research trademarks or resolve trademark disputes. VeriSign retains all rights to its registered trademarks and brand names, and is responsible for resolving any such conflicts it deems appropriate.

3.2 Initial identity Validation

3.2.1 Method to prove possession of private key

In all cases where the users generate key pairs and remain in exclusive control of the private keys, they shall prove possession of such private keys corresponding to the public keys submitted for certification. Refer to Section 3.1.7, page 37 of the VeriSign CPS for further information. However, when smart cards are being used, a user must present the smart card that contains the private keys.

3.2.2 Authentication of organization identity

The identity of an organization (agency) is verified by the JNET Office, which must perform a site visit. An agency is required to submit a letter requesting access to JNET to the JNET Executive Director. The agency must then receive approval from the JNET Steering Committee before being allowed to participate in JNET.

3.2.3 Authentication of individual identity

Initial certification of JNET users and operators requires that a Sponsor submit a JNET Access Request Form to a JNET Registrar on the user's behalf. User Sponsors shall hold their own JNET certificates and be recognized as sponsors by a Registrar. By submitting a JNET Access Request Form, the Sponsor corroborates the identity of the user and the level of access requested. This corroboration is critical to the integrity of the JNET certificate issuance process. Sponsors shall be held responsible for any misrepresentations. Sponsors are required to submit and agree to a Sponsor Agreement Form and Registrars are required to submit and agree to a Registrar Agreement Form. The sponsor's identity is verified in person by the registrar, while the registrar's identity is verified by the agency point of contact.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Subscriber Re-key Request

Routine re-key and renewal of certificates shall occur once every two years for all non-revoked certificates, applicable for subscriber and server certificates. Re-key and renewal mean that certificate holders will generate two new public-private key pairs and obtain the corresponding new certificates. Notifications shall be sent to each subscriber 30 days prior to the expiration of the existing keys/certificates, indicating the need to initiate the renewal process and providing the renewal instructions. Authentication of routine re-key and renewal requests shall be based on the existing keys/certificates, plus the use of an authentication code. Once the new key pairs are generated and the new certificates are installed, old keys and certificates shall not be used for other than verification and/or

decrypting of historical data. The user will access https://certificate.jnet.state.pa.us in order to submit request. Complete user documentation is located at https://www.jnet.state.pa.us.

3.3.2 CA Re-key Request

Any CA re-key request will be initiated by designated JNET Office management staff. These persons must be in possession of CA administration certificates. In addition, these personnel must proceed with the re-key request as prescribed by the VeriSign CPS, Section 3.2.

3.3.2 RA Re-key Request

Any RA re-key request will be initiated by designated JNET Office management staff. Refer to VeriSign CPS Section 4.1.1 for specific instructions.

3.4 Identification and Authentication for Revocation Requests

Revocation requests must be authenticated; see Section 4.4. Requests to self-revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. Alternative authentication methods may be used for out-of-band revocation requests. Authorized persons can request revocation of certificates as deemed necessary. Certificate revocation requested would be accepted from authorized individuals in cases where employee status change occurs.

3.4.1 CA Revocation Request

A CA revocation request can only be made if compromise of the CA certificate is suspected. This request can only me made by JNET senior management, which must include the executive director. At least two senior managers are required to submit the request. The request must be submitted to VeriSign according to Section 3.4 of the VeriSign CPS. Additional instructions will be provided by VeriSign as required.

3.4.2 RA Revocation Request

When a certificate is revoked for administrative reasons such that they do not pose a threat to the integrity of JNET, a Registrar may initiate the changes necessary to the information in the JNET Directory if in possession of all the pertinent information. Once a person's certificate is revoked for reasons other than administrative tasks, the Registrar should notify the JNET Office of the incident and delete the person from the JNET Directory. Otherwise the procedure for initial certification shall be followed.

If a certificate is revoked for reasons outside of administrative issues (loss of password, forgotten password, duplicate attempts to enroll etc), the certificate shall not be renewed.

3.4.3 Subscriber Revocation Request

JNET subscribers must request revocation through their designated registrar. The registrar must validate the identify of the subscriber making the request by either: requiring in-person revocation requests; contacting a second party to confirm the identity of the subscriber making the request.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

A Sponsor shall submit a JNET Access Request Form to a Registrar, on behalf of the applicant, to request issuance of a user certificate to gain access to JNET. The JNET Access Request Form is submitted to the registrar of the sponsor's agency. The registrar is then responsible for approving the request and entering the subscriber's profile information into the JNET directory. Application/server administrators or owners shall submit requests for server certificates directly to the JNET Office. The JNET Office will then request a server certificate from VeriSign. Section 4.1.1 of the VeriSign CPS contains additional information regarding the certificate application process.

4.2 Certificate Application Processing

Certificate application processing time will vary depending on each agency. Subscribers require a background check before being granted access to JNET. Additionally, subscribers requiring criminal history access must have a current CLEAN certification before being given such access in JNET. The registrar is required for ensuring that the background check and/or the CLEAN certification are verified before entering the subscriber's profile information into the JNET directory. Upon approval, the JNET Access Request Form must be sent to the JNET Office. Section 4.1.1 of the VeriSign CPS contains additional information regarding the certificate application process.

4.3 Certificate Issuance

Upon successful completion of the identification and authentication process (in accordance with the JNET Certificate Policy) and upon approval of the JNET Access Request Form, the Registrar shall generate an enrollment memo that can be used by the applicant to enroll and retrieve the certificate. The enrollment memo is generated as the result of the subscriber's profile being created in the JNET directory. The Registrar shall notify the applicant of the authentication code via a secure, out-of-band method (enrollment memo) and provide instructions to enroll, retrieve, and install the certificate in a JNET supported web browser.

Agencies participating in JNET may employ enrollment agents who perform the enrollment in proxy for the users. In such a scenario the Registrar will communicate the enrollment information with the enrollment agents.

The subscriber enrolls for their digital certificates at https://certificate.jnet.state.pa.us. The instructions for enrollment are also located at this site.

4.4 Certificate Acceptance

Acceptance is the action by a subscriber that triggers the subscriber's duties and potential liability. A subscriber is responsible for the following:

- Attend JNET user training; Follow all instructions in the JNET Access Request Form (JNET User Security Agreement);
- Adhere to all published JNET security standards and policies.

4.5 Key Pair and Certificate Usage

Certificates issued by the JNET CA may be used in the following ways.

- Access and authentication to JNET and JNET related web sites and systems.
- Access and authentication to approved Commonwealth web sites and systems.
- Access and authentication to the JNET VPN Service.
- Access, authentication, signing and encryption of email within the JNET email system or other Commonwealth approved email system.
- Authentication and encryption between messaging servers.

4.6 Certificate Renewal

Subscriber certificates may be renewed under the following circumstances:

- A subscriber may renew his/her certificate within 30 days of certificate expiration. The subscriber will notified of pending certificate expiration by their registrar and by accessing the JNET web site. The URL for renewal is https://certificate.jnet.state.pa.us.
- A subscriber may only renew a certificate if the certificate has not been suspended, revoked or compromised.
- Only active subscribers are allowed to renew a certificate.
- Under no circumstance will a subscriber certificate be automatically renewed.
- The CA will publish any renewed certificate and provide notifications in accordance with the VeriSign CPS Section 4.3.
- The subscriber will be notified by the RA (registrar) upon approval of their certificate renewal request.

4.7 Certificate Re-Key

Refer to Section 3.3 of this CPS for information regarding certificate re-key policies.

4.8 Certificate Modification

Under no circumstances will a subscriber's digital certificate be modified. Whenever a subscriber requires a modification, that subscriber will submit a request to their designated registrar to have their digital certificate revoked. The registrar will revoke the subscriber's certificate, and then update the subscriber's profile in the JNET registrar gateway (JNET directory). The registrar will then notify the subscriber when the process has been completed and re-enrollment is allowed. The subscriber will then be required to enroll for a new digital certificate, using their new information. The subscriber will follow the procedures identified in Section 4.3 of this CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

A certificate will be revoked under the following circumstances:

- Identifying information or attributes in the user certificate changes before the certificate expires;
- The certificate subject can be shown to have violated the stipulations of JNET CP, or the CPS of the JNET CA who issued the certificate;
- Compromise of one or both of the private keys is suspected (in dual key-pair situation);
- The user no longer requires access to JNET because of a change in responsibilities or separation;
- The user is under investigation; or
- Refer to Section 4.4.1 of the VeriSign CPS for additional circumstances regarding revocation.

4.9.2 Who can request revocation

The subscriber of the certificate(s), a supervisor of the certificate holder, a Human Resources representative, a JNET Steering Committee member, the subscriber's sponsor or registrar, or the JNET Office may originate certificate revocation requests.

The holder of a certificate shall request revocation immediately upon detecting key compromise and provide as much detail as possible.

Section 4.4.2.1 of the VeriSign CPS contains additional stipulations.

4.9.3 Procedure for revocation request

Authorized parties, as identified in Section 4.9.2, may request revocation of the subscriber's certificate(s) using any format that identifies the certificate to be revoked, provides the reason for revocation, and allows the request to be authenticated (e.g., digitally or manually signed).

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. A record of the revocation request shall be maintained for audit purposes.

The reporting chain goes from the party detecting the compromise to the supervisor of the certificate holder, the Registrar, and the JNET Office, except when one of these parties is involved in the key compromise.

This process is currently under review by the JNET Office. A later revision of the CPS will be released that includes the new revocation request process.

Refer to Section 4.4.3 of the VeriSign CPS for additional stipulations.

4.9.4 Revocation request grace period

The certificate shall be revoked within 48 hours of the submission of a certificate revocation request to the JNET Office. All certificate revocation actions shall be logged and archived for audit purposes. Refer to Section 4.4.4 of the VeriSign CPS for additional stipulations.

4.9.5 Circumstances for suspension

This policy stipulates that JNET certificates shall not be suspended. Refer to VeriSign CPS Section 4.4.5 for additional stipulations.

4.9.6 Who can request suspension

This CPS stipulates that JNET certificates shall not be suspended.

4.9.7 Procedure for suspension request

This CPS stipulates that JNET certificates shall not be suspended.

4.9.8 Limits on suspension period

This CPS stipulates that JNET certificates shall not be suspended.

4.9.9 CRL issuance frequency

The CRL shall be downloaded from the JNET CA and applied to the JNET directory at least every 24 hours.

4.9.10 CRL checking requirements

JNET provides two CRL distribution points:

- production - http://jnetcrl.jnet.state.pa.us/latestCRL.crl,
- test - http://jnetcrl.test.jnet.state.pa.us/latestCRL.crl.

JNET web servers may use either CRL, OCSP or the JNET directory for certificate validation as appropriate.

4.9.11 On-line revocation/status checking availability

See VeriSign CPS Section 4.4.11. JNET may host an OCSP responder at a later date. This CPS will be updated to reflect any such change. The OCSP responder is located at: Pilot – http://pilot-ocsp.verisign.com; Production – http://onsite-ocsp.verisign.com.

4.9.12 On-line revocation checking requirements

Please refer to Section 4.9.10 of this CPS.

4.9.13 Other forms of revocation advertisements available

The JNET directory will contain the public key of the subscriber. A web server may use a hash/CRC verification to determine certificate validity in addition to other validating information such as valid date.

4.9.14 Checking requirements for other forms of revocation advertisements

In the event of a server being unable to utilize either CRL or OCSP, the JNET directory will be used to verify the validity of a subscriber's certificate. The JNET directory is updated as certificate status is changed.

4.10 Certificate Status Services

4.10.1 CRL

The CRL is defined in each subscriber's certificate. A CRL will be published from the VeriSign KMS to the JNET directory at least once every 24 hours. User certificates include the URL for the CRL, which can only be accessed from within the Commonwealth MAN.

4.10.2 OCSP

OCSP services are hosted at VeriSign. Currently, access to the Internet is required to utilize OCSP. A Commonwealth MAN internal OCSP responder is planned for implementation in the future. This CPS will be updated to reflect such a change.

4.10.3 Thumbprint match / JNET directory

Web servers utilizing either a NSAPI or ISAPI filter may use the JNET directory to validate a user's certificate. The user's public key is compared to the public key stored in the directory. The two public keys must match in order for the user to be validated. In addition, date verification of the certificate must take place.

4.11 End of Subscription

A subscriber may end his/her subscription to the JNET CA service either voluntarily or involuntarily. Voluntary actions may include, but are not limited to:

- Job, role or responsibility change
- Unwillingness to comply with the JNET User Access Agreement
- Willful job termination

Involuntary actions may include, but are not limited to:

- Certificate expiration
- Involuntary job termination
- Termination of the JNET PKI Service
- Misuse of digital certificate(s)

The subscriber must contact his/her designated registrar or the JNET Office to have their certificates revoked and their access terminated.

4.12 Key Escrow and Recovery

This process is currently under review by the JNET Office. This CPS will be updated to include the new process.

4.13 Security Audit Procedures

This Section describes event logging and audit requirements for the maintenance of a secure operations environment for the JNET CA. Periodic reviews of the audit logs as well as full audits shall be used to detect security breaches, identify potential problems, and suggest modifications and enhancements to the CA infrastructure, the CA's practices and procedures as defined in the CPS.

4.13.1 Types of event recorded

Refer to Section 4.5.1 of the VeriSign CPS. In addition, JNET maintains and retains audit logs for access to web servers and applications.

4.13.2 Frequency of processing log

The audit log shall be consolidated and inspected on a weekly basis. Refer to Section 4.5.2 of the VeriSign CPS for additional stipulations.

4.13.3 Retention period for audit log

Audit logs shall be retained for seven years. Refer to Section 4.5.3 of the VeriSign CPS for additional stipulations.

4.13.4 Protection of audit log

All JNET audit logs have restricted access. The CA and RA audit logs may only be accessed, read-only, by the administrative key holders (designated JNET Office senior management) and JNET personnel responsible for ensuring audit compliance. Access to system housing logs is restricted to designated operational personnel only.

4.13.5 Audit log backup procedures

The audit log backup procedures will follow standard JNET backup procedures.

4.13.6 Audit collection system (internal vs. external)

The audit collection system shall be internal to the operations of the JNET CA. Refer to Section 4.5.6 of the VeriSign CPS for additional information.

4.13.7 Notification to event-causing subject

The JNET Office will be notified of any events that disrupt the normal functioning of the CA. JNET Office management is responsible for determining any appropriate course of action. Refer to Section 4.5.7 of the VeriSign CPS for additional stipulations.

4.13.8 Vulnerability assessments

The JNET CA equipment must be hosted in a secure environment that can be subject to vulnerability assessments on a periodic basis. The JNET Office is responsible for conducting a CA system vulnerability assessment on a yearly basis. There is no JNET stipulation for VeriSign to conduct vulnerability assessments of systems hosted at VeriSign.

4.13.9 Viewing Audit Logs

The JNET Office shall designate a policy manager who is responsible for viewing audit logs. In addition, this position is responsible for coordinating any internal and external audits. External agencies may review JNET audit logs on an as-needed basis, including the Office of Administration (OA); the Pennsylvania State Police (PSP), and any agency contributing data to JNET.

5. Facilities, Management, and Operational Controls

5.1 Physical Security Controls

This section details requirements for the operation of the physical equipment and facilities maintained and operated by the JNET Office.

5.1.1 Site location and construction

The JNET CA and related hardware will be housed in Commonwealth approved computing facilities. The VeriSign CPS Section 5.1.1 has additional stipulations regarding its facilities.

5.1.2 Physical access

The following is the list of physical access controls that must be in place.

- Data center must have restricted access.
- Data center should be monitored for suspicious activity on a 24x7 basis.
- CA and related hardware must be kept in a locked cabinet.
- The number of personnel given access to the CA cabinet must be restricted to as few personnel as possible.
- A log must be kept that records any physical access to the CA or the cabinet in which it is stored.
- All standing security standards and measures for the data center will be followed and adhered to.
- Refer to Section 5.1.2 of the VeriSign CPS for additional stipulations.
- Smart cards are required to login to the CA.

The JNET Office, in coordination with appropriate authorities, must investigate any breach to physical security.

5.1.3 Power and air conditioning

No stipulation. Existing standards and procedures for the Commonwealth data center will be followed. The JNET Office will execute the JNET Contingency Plan as necessary. Refer to Section 5.1.3 of the VeriSign CPS for additional stipulations.

5.1.4 Water exposures

No stipulation. Existing standards and procedures for the Commonwealth data center will be followed. The JNET Office will execute the JNET Contingency Plan as necessary. Refer to Section 5.1.4 of the VeriSign CPS for additional stipulations.

5.1.5 Fire prevention and protection

No stipulation. Existing standards and procedures for the Commonwealth data center will be followed. The JNET Office will execute the JNET Contingency Plan as necessary. Refer to Section 5.1.5 of the VeriSign CPS for additional stipulations.

5.1.6 Media storage

The storage and management of media follow the stipulations as prescribed by JNET backup, recovery and disaster recovery documents. Refer to Section 5.1.6 of the VeriSign CPS for additional stipulations.

5.1.7 Waste disposal

Normal office waste shall be removed or destroyed in accordance with local policy. Media used to collect or transmit information discussed in section 2.8 shall be destroyed, such that the information is unrecoverable, prior to disposal. Refer to Section 5.1.7 of the VeriSign CPS for additional stipulations.

5.1.8 Off-site backup

Existing standards and procedures for off-site backup media storage will be followed for the CA. The JNET Office will execute the JNET Contingency Plan as necessary. Refer to Section 5.1.8 of the VeriSign CPS for additional stipulations.

5.2 Procedural Controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be careful and above reproach as described in the next section. The functions performed in these roles form the basis of trust in the entire JNET CA.

The following is a list of trusted roles.

- Sponsor
- Registrar
- Certification Authority (CA) Controller/Administrator
- JNET Senior Manager

Whenever appropriate, separation of duties shall be implemented for all operations potentially impacting system integrity. The JNET CA Controller/Administrator shall maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and shall make them available during compliance audits. Refer to Section 5.2.1 of the VeriSign CPS for additional stipulations.

5.2.2 Number of persons required per task

To best ensure the integrity of the CMA equipment and operation, it is recommended that wherever possible a separate individual be identified for each trusted role. The separation provides a set of checks and balances over the CMA operation. At least two persons must be present when conducting CA related security or maintenance functions. Under no circumstance will a single individual be allowed to affect any changes, or allowed access to the CA. Separation of roles will be defined by the JNET Operations Manager, as appropriate.

Under no circumstances shall the incumbent of a CMA role perform its own auditor function. Refer to Section 5.2.2 of the VeriSign CPS for additional stipulations.

5.2.3 Identification and authentication for each role

The JNET Office is required to verify the identity of each person assigned to each trusted role. Each person's identity is to be verified based on the process defined in Section 3.2.3 of this CPS. In addition, refer to Section 5.2.3 of the VeriSign CPS for additional stipulations.

5.3 Personnel Security Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The personnel selected to perform setup, upgrade, operations, and maintenance of the JNET CA equipment and granted access to JNET CA data shall be vetted for their integrity, reliability, and trustworthiness according to the regulations of the Commonwealth of Pennsylvania and associated agencies such as the Pennsylvania State Police. These requirements shall also apply to JNET Registrars and their support personnel. Refer to Section 5.3.1 of the VeriSign CPS for additional stipulations.

5.3.2 Background check procedures

JNET follows the processes and procedures as identified in the following documents: Commonwealth OIT document I-series ITBs: Security, Privacy, and Business Continuity Planning: Section I.1.6 Minimum Contractor / Vendor Background Policy; and the Criminal History Background Check. Refer to Section 5.3.2 of the VeriSign CPS for additional stipulations.

5.3.3 Training requirements

Training requirements are under review by the JNET Office. This CPS will be updated to include the new requirements when available. Refer to Section 5.3.3 of the VeriSign CPS for additional stipulations

5.3.4 Retraining frequency and requirements

These requirements are under review by the JNET Office. This CPS will be updated to include the new requirements when available. Refer to Section 5.3.4 of the VeriSign CPS for additional stipulations

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

The JNET Misuse Investigation Procedures will be followed in all cases of unauthorized actions. Refer to Section 5.3.6 of the VeriSign CPS for additional stipulations

5.3.7 Contracting personnel requirements

Contract employees will be subject to the requirements as stipulated in Section 5.3.7 of this CPS.

5.3.8 Documentation supplied to personnel

Documentation sufficient to define duties and procedures for each role shall be provided for reference to the personnel filling that role. JNET management is responsible for ensuring that all documentation is available to staff in a convenient manner. Refer to Section 5.3.8 of the VeriSign CPS for additional stipulations

5.3.9 Need for separation of privileges

No single individual shall have sole access or control over any function or process relating to the operation and maintenance of the JNET CA. The control over key material and JNET CA hardware cryptographic modules shall be split among two or more individuals. These individuals will be Commonwealth employees, preferably JNET management. Any such access by these trusted individuals will be logged.

5.4 Audit Logging Procedures

All subscriber and system auditing requirements and procedures are governed by the JNET Auditing Requirements document.

5.5 Records Archival

JNET CA archive records shall be detailed enough to establish the validity of a signature and the proper operation of the CA at some point in time. At a minimum, the following data shall be archived.

Data that shall be recorded for archive at the initialization of the CA equipment:

- CA system equipment configuration files,

- Results of CA assessments and/or audits accreditation (if necessary),
- Certification Practice Statement, and
- Any contractual agreements to which the CA is bound.
- Data that shall be recorded for archive during CA operation:
- Modifications or updates to any of the above data items;
- All certificates and CRLs (or other revocation information) as issued or published;
- Weekly audit logs;
- Identity verification logs; and
- Other data for verifying archive contents.

5.5.1 Types of event recorded

All events including issuance of certificates and revocation of certificates shall be recorded for future examination. Refer to VeriSign CPS Section 4.6.1 for additional stipulations.

5.5.2 Retention period for archive

Archive records shall be kept for a period of seven years. Refer to VeriSign CPS Section 4.6.2 for additional stipulations.

5.5.3 Protection of archive

The JNET Operations Manager is ultimately responsible for ensuring that the staff tasked with performing archiving operations adheres to the stipulations stated in this CPS. No one person should be granted access to perform any modifications to archived records. Refer to VeriSign CPS Section 4.6.3 for additional stipulations.

5.5.4 Archive backup procedures

Standard backup procedures will be followed to backup archive. Refer to VeriSign CPS Section 4.6.4 for additional stipulations.

5.5.5 Requirements for time-stamping of records

Refer to VeriSign CPS Section 4.6.5 for stipulations.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Refer to Section 5.6.3 of this CPS.

5.5.8 Viewing archived records (1.0)

Archived records shall be available to previously identified internal and external auditors upon their request. Archived records shall also be available for the verification of specific operations upon request to the JNET Office. This request must be made in writing, and the requesting party must demonstrate need-to-know before being granted access to the records. The custodian of the archive shall retrieve the pertinent records and only make available those needed to complete the verification.

5.6 Key changeover

The JNET CA uses its original signing (private) key for creating certificates; however, parties relying on JNET certificates employ the CA's certificate for the life of the user certificate beyond that signing. The JNET CA will not issue certificates that extend beyond the expiration dates of its own certificate and public keys.

All subscriber certificates will have a lifetime of two years. One month prior to the end of that period, a notification shall be sent to holders of valid unexpired JNET certificates. This notification will be made to the user via the JNET web site and via email, as available.

Refer to VeriSign CPS Section 4.7 for additional stipulations.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Reporting and Handling Procedures

All incidents of compromise will be treated as misuse. All misuse procedures are detailed in the JNET Misuse Investigation Procedures document.

5.7.2 Recovery Procedures for Computing Resources, Software, and/or Data corruption

In case of such a disaster, the JNET Disaster Recovery plan will be employed to implement procedures to reinstate the JNET CA equipment.

5.7.3 Recovery Procedures for Entity Key compromise

In case of compromise of the JNET CA private key the cause must be immediately assessed to avoid repetition of the compromise and to ensure that the recovery process will not have to be repeated for the same reason. The stipulations identified in the VeriSign CPS Section 4.8.3 will be followed. In addition, new certificates will be issued to subscribers and a new CA certificate will be distributed.

Although the priority shall be continuity of service, an investigation to the causes, motives, and effects of the compromise shall be completed. This investigation shall begin as soon as possible even if the recovery is not complete. The findings of the investigation shall be reported to the JNET Office who would be responsible to react appropriately with technical or procedural remedies, legal action, and/or prosecution.

5.7.4 Business Continuity and Disaster Recovery

The JNET Disaster Recovery and Business Continuity Plan will be followed. Refer to VeriSign CPS Section 4.8.2 for additional stipulations.

5.8 CA Termination

In case termination of the JNET CA is necessary it will be handled in a way consistent with Section 5.7 above. If the termination is for convenience, contract expiration, re-organization, or other non-security related reason, then certificates may continue to be considered valid at the discretion of the program or relying party (who shall be made aware of the termination with a minimum two weeks). In this case, provision must be made for compromise recovery, audit, archive, and data recovery material, either by transferring the current agreements to the new CA, or by the program otherwise upholding the current contractual agreements or making new arrangements.

After termination, records shall be turned over to the JNET Steering Committee. The Committee shall identify the stakeholders (agencies and/or counties) that will receive the archived records. Refer to VeriSign CPS Section 4.9 for additional stipulations.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation and Installation

Private keys must not appear in clear text form outside the module in which it was generated. Keys may only be extracted in encrypted form for the following purposes:

- Delivery to their owners,
- For storage by an emergency key recovery mechanism, or
- For delivery to an authorized official in response to a validated emergency key recovery request.

Subscribers use a dual key pair configuration. The authentication key pair is generated by using a client side CSR. The CSR may be in the form of a web browser, operating system container, or smart card. The encryption key pair is generated by the VeriSign KMS (key management server). Refer to VeriSign CPS Section 6.1.1 for additional stipulations.

6.1.2 Private key delivery to entity

If the private key for an entity is not generated within the boundaries of the entity's cryptographic module, it shall be delivered to the entity in encrypted form. A protected data structure (such as defined in PKCS#12) shall be used to hold during transmission. This encrypted file must be password protected. This password must be communicated out-of-band, or in a manner that differs from the distribution of the key(s). Refer to VeriSign CPS Section 6.1.2 for additional stipulations.

6.1.3 Public key delivery to certificate issuer

Refer to VeriSign CPS Section 6.1.3 for stipulations. Other delivery methods may be used, but require the identity of the sender to be verified.

6.1.4 CA public key delivery to users

The JNET CA shall ensure the authenticated and secure delivery of its certificate to all JNET clients and servers. The public key is delivered to the subscriber at the completion of a successful enrollment, or may be delivered to the subscriber by their designated registrar. In addition, the CA public key may be downloaded from https://certificate.jnet.state.pa.us. Refer to VeriSign CPS Section 6.1.4 for additional stipulations.

6.1.5 Key sizes

The JNET CA shall support the largest key size available to both servers and clients within JNET for the selected public key algorithm. The key size shall be at least 1024 bits (classified as medium security key by VeriSign). This value is to be predefined in the

enrollment pages until additional key sizes are required. Key sizes of 2048 may be used, when supported by officially supported JNET web browsers. Refer to VeriSign CPS Section 6.1.5 for additional stipulations.

6.1.6 Public key parameters generation

Required public key parameters shall be generated consistently with the applicable algorithm standards.

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

Keys associated with the current CP shall be certified for use in signing and encrypting. The JNET CA requires the usage of dual key pairs for all subscribers. One key pair is used for digital signatures and authentication, while the other key is used for encryption. Refer to VeriSign CPS Section 6.1.9 for additional stipulations.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Standards for cryptographic module

The relevant standard for cryptographic modules is [FIPS1401]. Cryptographic modules for user clients shall be validated FIPS 140-1 level 1 or higher. Cryptographic modules for servers shall be validated FIPS 140-1 level 1 or higher. The cryptographic module for the JNET CA shall be validated FIPS 140-1 level 2 or higher.

All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plain text. Refer to VeriSign CPS Section 6.1.1 for additional stipulations.

This CPS stipulates that the JNET CA must conform to FIPS 140-2 within the 2005 calendar year. This CPS must then be updated to reflect the upgrade.

6.2.2 Private key (2 out of 3) multi-person control

Multi-person control requires that more than one individual independently authorize themselves to the system to enable the operations of the JNET CA. This mechanism prevents any single party from gaining access to the certificate-signing key.

JNET CA signature keys may only be backed up under two-person control. The parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits. Refer to VeriSign CPS Section 6.2.2 for additional stipulations.

6.2.3 Encryption Private key escrow

User encryption private keys will be escrowed to provide key recovery for private keys. However, the private keys being escrowed must be encrypted until such time it is recovered. The private keys being escrowed shall also be under multi-person control. The CA (KMS) automatically escrows all private keys into a directory stored on the KMS. This

repository is encrypted, as are the keys themselves. Refer to VeriSign CPS Section 6.2.3 for additional stipulations.

6.2.4 Private key backup

The JNET CA, Registrars, and servers shall backup their private keys as contingency in case of destruction, corruption, or failure of the original. Subscribers may have one copy of their private key(s) on their hard disk and another on a removable medium stored in a safe, cool, dry, location away from magnetic fields. All copies of the private key(s) shall remain encrypted, and password protected while not in use. Refer to VeriSign CPS Section 6.2.4 for additional stipulations.

6.2.5 Private key archival

Refer to VeriSign CPS Section 6.2.5 for stipulations.

6.2.6 Private key entry into cryptographic module

Refer to VeriSign CPS Section 6.2.6 for stipulations.

6.2.7 Private key storage

A private key may be stored in a module only if encrypted. Plaintext storage is not allowed under any circumstances.

6.2.8 Method of activating private key

Pass-phrases, PINs, or biometrics may be used to activate the private key in a cryptographic module. Activation data generation requirements are specified in Section 6.4.1 of this CPS. Entry of activation data shall be protected from disclosure (e.g., the data should not be displayed while it is entered).

6.2.9 Method of deactivating private key

Refer to VeriSign CPS Section 6.2.8 for stipulations.

6.2.10 Method of destroying private key

Refer to VeriSign CPS Section 6.2.9 for stipulations.

6.2.11 Crypto Module Capabilities

Refer to JNET CP Section 6.2.11. Refer to VeriSign CPS Section 6.2.1 for additional stipulations.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Refer to VeriSign CPS Section 6.3.1 for stipulations.

6.3.2 Usage periods for the public and private keys

The key usage periods for keying material are described in Section 3.2 of this CPS. Refer to VeriSign CPS Section 6.3.2 for additional stipulations.

6.4 Activation Data

6.4.1 Activation data generation and installation

Refer to VeriSign CPS Section 6.4.1 for stipulations. Subscribers using a JNET provided roaming PKI service must use two factor authentication mechanisms for the protection of their private key(s).

6.4.2 Activation data protection

Refer to VeriSign CPS Section 6.4.1 for stipulations. Subscribers using a JNET provided roaming PKI service must use two factor authentication mechanisms for the protection of their private key(s).

6.5 Computer Security Controls

Security features in the JNET CA equipment shall be active and properly configured to prevent and detect unauthorized access, modification, or compromise. Activity logs shall be reviewed with the frequency specified in Section 4.13. Audits shall be carried out as described in Section 4.13.

6.5.1 Specific computer security technical requirements

JNET follows the stipulations as outlined in Section 6.5.1 of the VeriSign CPS.

6.5.2 Computer security rating

CA equipment used for High Confidence assurance infrastructures shall be hosted on platforms using operating systems that have been evaluated to at least a C2 [TCSEC] or E2/F-C2 [ITSEC] rating. Refer to VeriSign CPS Section 6.5.2 for additional stipulations.

6.6 Life Cycle Technical Controls

The JNET CA equipment shall be dedicated to the management of JNET certificates and the administration of public-private key pairs. The JNET CA equipment shall not have installed applications or component software that are not part of the CA configuration. Equipment updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel.

6.6.1 System development controls

All system development will follow the JNET Development Methodology. Refer to VeriSign CPS Section 6.6.1 for additional stipulations.

6.6.2 Security management controls

Security management controls will adhere to the JNET System Security Policy. Additional controls may be specified in the CPS, as required. Refer to VeriSign CPS Section 6.6.2 for additional stipulations.

6.6.3 Life cycle security ratings

Refer to VeriSign CPS Section 6.6.3 for stipulations.

6.7 Network Security Controls

JNET CA equipment is only permitted to access the following network devices/services: VeriSign, the JNET directory, the JNET RA and JNET backup services. No other network access is permitted without the expressed consent and approval of the JNET Office. An appropriately configured and maintained firewall, or equivalent controlled access device, shall protect all connectivity to JNET CA equipment. Refer to VeriSign CPS Section 6.7 for additional stipulations.

6.8 Time-stamping

Time-stamping services will be implemented at a future date. This CPS will be revised to address time stamping.

7. Certificate, CRL, and OCSP Profile

7.1 Certificate Profile

The JNET CA shall issue and manage public key certificates defined in accordance with version 3 of the ITU X.509 Certificate Format. The JNET CA shall generate and post Certificate Revocation Lists (CRL) in accordance with version 3 of the ITU X.509 Certificate Format as a management tool to report unexpired certificate no longer deemed accurate or valid.

7.1.1 Version number(s)

This policy exclusively uses X.509 Version 3 certificates as indicated in Section above. Refer to VeriSign CPS Section 7.1.1 for additional stipulations.

7.1.2 Certificate extensions

Refer to VeriSign CPS Section 7.1.2 for stipulations.

7.1.3 Algorithm object identifiers

Refer to VeriSign CPS Section 7.1.3 for stipulations.

7.1.4 Name forms

In general, the Distinguished Name (DN) will be used on all JNET certificates. Any name form defining GeneralName in [ISO9594-8] may be used, in accordance with the required profile (Section 7.1). Use of alternate name forms shall be defined in a CPS, along with any applicable name constraints.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy Object Identifier

The JNET CP will be submitted for review and an application for an OID will be submitted to CSOR. The details of this will be presented in a future version of the JNET CP. Refer to VeriSign CPS Section 7.1.6 for additional stipulations.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Refer to VeriSign CPS Section 7.1.8 for stipulations.

7.1.9 Processing semantics for the critical certificate policy extension

This policy does not require the certificatePolicies extension to be critical. Entities relying on certificates that do not process this extension do so at risk.

7.2 CRL Profile

7.2.1 Version number(s)

The CRL version number will follow the standards as stipulated in IETF RFC 3280. Refer to VeriSign CPS Section 7.2 for additional stipulations.

7.2.2 CRL and CRL entry extensions

The CRL will follow the standards as stipulated in IETF RFC 3280. Refer to VeriSign CPS Section 7.2 for additional stipulations.

7.3 OCSP Profile

The OCSP Profile will follow the standards are specified in IETF RFC 2560.

8. Compliance Audit and Other Assessment

8.1 Specification change procedures

Every three years the JNET Steering Committee and JNET Office shall review this CPS and determine whether major changes are warranted. Minor changes will result in the creation of an addendum to the current CPS. Minor changes include, but are not limited to: URL changes; responsibility reassignment; address changes; referring document changes. Major changes will result in the publishing of a new CPS. Major revisions may include: installation of a new CA; new releases of VeriSign CP and/or CPS; changes to IETF documents. Any resulting changes will result in a newly published CPS. The new CPS will obsolete any previous CPS, making any such CPS invalid. Refer to VeriSign CPS Section 8.1 for additional stipulations.

8.2 Publication and notification policies

The JNET office shall publish minor changes in an addendum to this policy next to the location for this CPS. Major changes will result in a new CPS that will replace the old one. The old CPS will be archived. The JNET Office will notify subscribers via the official JNET web site to any changes made to the CPS. Refer to VeriSign CPS Section 8.2 for additional stipulations.

8.3 CPS approval procedures

An internal audit shall be conducted by the JNET Office and submitted to the JNET Steering Committee every six months. An external independent audit shall take place once a year. The Steering Committee shall, using the results from these audits, evaluate and approve the CPS, and any resulting changes, on an annual basis.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

There is no stipulation for any fees at this time. The JNET Steering Committee may pursue such action at its discretion. This CPS will be updated to reflect any such change.

9.1.2 Certificate access fees

The JNET CA shall not impose any certificate access fees on subscribers.

9.1.3 Revocation or status information access fees

The JNET CA may establish a fee structure for certificate validation services. It is not recommended that fees be charged for certificate validation services.

9.1.4 Fees for other services such as policy information

The JNET CA shall not impose any fees for access to this CPS or other related information.

9.1.5 Refund policy

There will be no financial allocation or reimbursement of any kind related to the JNET CA or PKI.

9.2 Financial responsibility

9.2.1 Indemnification by relying parties

This CPS and ensuing CPS lay out the policy and requirements for CAs, repository and RAs. JNET, the Commonwealth of Pennsylvania, VeriSign and the JNET CA providers assume no financial responsibility for improperly used certificates. Refer to VeriSign CPS Section 2.2.4 for additional stipulations.

9.2.2 Fiduciary relationships

Refer to VeriSign CPS Section 2.3.2 for additional stipulations.

9.2.3 Administrative processes

Refer to VeriSign CPS Section 2.3.3 for additional stipulations.

9.3 Confidentiality of Business Information

9.3.1 Types of information to be kept confidential

The following is a list of information that should be considered confidential.

- All user information (name, agency, phone number, etc.)
- Subscriber private key(s)
- Information contained in the JNET directory
- Any stipulations dictated by Commonwealth or federal laws and regulations.
- Any justice related information accessible within JNET

Additional stipulations are specified in Section 2.8.1 in the VeriSign CPS.

9.3.2 Types of information not considered confidential

The only information not considered confidential is the names of: JNET participating agencies; JNET senior management; JNET Steering Committee. In addition, any information published on the JNET public web site and press releases is also not considered confidential. Additional stipulations are specified in Section 2.8.2 in the VeriSign CPS.

9.3.3 Disclosure of certificate revocation/suspension information

Stipulations are specified in Section 2.8.3 in the VeriSign CPS.

9.3.4 Release to law enforcement officials

The JNET CA will not disclose certificate or certificate-related information to any third party, except when:

- Authorized by this CPS;
- Required to be disclosed by law, governmental rule or regulation, or court order; or
- Authorized by the user when necessary to affect an appropriate use of the certificate.

The JNET CA may choose to further define or restrict the user's authority to disclose certificate or certificate-related information. Additional stipulations are specified in Section 2.8.4 in the VeriSign CPS.

9.3.5 Release as part of civil discovery

Stipulations are specified in Section 2.8.5 of the VeriSign CPS.

9.3.6 Disclosure upon owner's request

The owner of a JNET issued certificate cannot disclose any certificate related information without written consent from the JNET Office. Any such request must be submitted in written format. Additional stipulations are specified in Section 2.8.6 of the VeriSign CPS.

9.3.7 Other information release circumstances

No stipulation.

9.4 Privacy of Personal Information

All subscriber information is considered to be sensitive and confidential. Under no circumstance is personal information to be released, unless there is a case concerning misuse.

9.5 Intellectual Property Rights

The information held and maintained by the JNET CA, including certificates, the CA's CPS, system specifications, names, and keys, is the property of the Commonwealth of Pennsylvania. The definition, development, collection, and maintenance of this information are the responsibility of the JNET Office. Additional stipulations are specified in Section 2.9.1 of the VeriSign CPS.

9.6 Representations and Warranties

There are no warranties, either expressed or implied, provided to any subscriber of the JNET CA.

9.7 Disclaimers of Warranties

There are no warranties, either expressed or implied, provided to any subscriber of the JNET CA.

9.8 Limitations of Liability

9.8.1 CA liability

Subscribers will have no claims against the Commonwealth of Pennsylvania or VeriSign, arising from the use of the JNET CA issued certificate. In no event will the Commonwealth of Pennsylvania JNET CA be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the JNET CA or any other CA under this policy. Additional stipulations are specified in Section 2.2.1 of the VeriSign CPS.

9.8.2 RA liability

Stipulations are specified in Section 2.2.2 of the VeriSign CPS.

9.8.3 Subscriber liability

Stipulations are specified in Section 2.2.3 of the VeriSign CPS.

9.9 Indemnities

Under no circumstance will the JNET Office, JNET CA or the Commonwealth of Pennsylvania be held liable for the misuse of a digital certificate by a subscriber. A subscriber is wholly responsible for the usage of their certificate as stipulated in the JNET User Access Agreement.

9.10 Term and Termination

The CP and CPS are to remain active until superseded by newer revisions, or until the termination of the JNET CA. No provision in this CPS may be terminated without review of the JNET Steering Committee.

9.11 Individual Notices and Communications with Participants

A subscriber is obligated to inform his/her RA (registrar) of any changes to their employment status, or any change in status that would affect the usage of his/her digital certificate. A RA (registrar) or sponsor is required to notify the JNET Office in the event of a change in their status, or any change in the status of their approved subscribers. This notification must be provided in written form.

9.12 Amendments

No stipulation.

9.13 Dispute Resolution Procedures

All subscribers must adhere to all rules and standards as defined in this CPS. Any subscriber that does not agree to the terms as outlined in this CPS may have their access and keys revoked by contacting the JNET Office. There will be no other resolutions. Additional stipulations are specified in Section 2.4.3 of the VeriSign CPS.

9.14 Governing Law

The laws and regulations of the Commonwealth of Pennsylvania and any applicable Federal laws of the United States of America shall govern the enforceability, construction,

interpretation, and validity of this CPS. Additional stipulations are specified in Section 2.4.1 of the VeriSign CPS.

9.15 Compliance with Applicable Law

The operation of the JNET CA will be subject to and in compliance with the laws of the Commonwealth of Pennsylvania, the United States of America, and any local applicable laws.

9.16 Miscellaneous Provisions

Should it be determined that one section of this policy is incorrect or invalid, the other sections shall remain in effect until the policy is updated. Requirements for updating this policy are described in Section 8. Responsibilities, requirements, and privileges of this document shall be merged to the newer edition upon release of that newer edition.

9.17 Other Provisions

There are no other provisions at this time.

Appendix A: Bibliographical References

[ABA]	American Bar Association, *Digital Signature Guidelines,* 1996-08-01. `http://www.abanet.org/scitech/ec/isc/dsgfree.html`
[Boeyen]	Sharon Boeyen, "Certificate Policies and Certification Practice Statements," February 1997 (Entrust Technologies White Paper, Version 1.0), Section 1.
[FIPS140-2]	*Federal Information Processing Standard 140-2 - Security Requirements for Cryptographic Modules*, 2001. `http://csrc.nist.gov/publications/fips/index.html`
[ISO9594-8]	International Standard, *Information Technology-Open Systems Interconnection-The Directory: Authentication Framework,* 1997. `ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc`
[NS4009]	NSTISSI 4009, National Information Systems Security Glossary, January 1999
[PKCS12]	PKCS#12 - Personal Information Exchange Syntax Standard, ,April 1997. `http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html`
[PRIVACT]	5 U.S.C. 552a, Privacy Act of 1974. `http://www4.law.cornell.edu/uscode/5/552.html`
[RFC2510]	Internet Engineering Task Force (IETF) RFC, Adams and Farrell. *Certificate Management Protocol,* 1999 March. `http://www.ietf.org/rfc/rfc2510.txt`
[RFC2560]	Internet Engineering Task Force (IETF) RFC, *Internet x.509 Public Key Infrastructure Online Certificate Status Protocol,* 2002 April. `http://www.ietf.org/rfc/rfc2560.txt`

[RFC3280] Internet Engineering Task Force (IETF) RFC, *Internet x.509 Public Key Infrastructure Certificate and Certification Revocation List (CRL) Profile,* 2003 November.

`http://www.ietf.org/rfc/rfc3280.txt`

[RFC3647] Internet Engineering Task Force (IETF) RFC, *Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,* 2003 November.

`http://www.ietf.org/rfc/rfc3647.txt`

[X.509] CCITT (ITU-T) Recommendation X.509 (equivalent to ISO 9594-8), *The Directory: Authentication Framework,* that defines the standard format of a digital certificate