pennsylvania
OFFICE OF ADMINISTRATION

INFORMATION TECHNOLOGY

Information Technology Policy

Public Key Infrastructure

ITP Number GEN-SEC013G	***Effective Date*** January 25, 2008
Category Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

1. Introduction/Executive Summary

The purpose of this document is to define the Commonwealth's Public Key Infrastructure (PKI) as established in ITP-SEC013, *Identity Protection and Access Management Architectural Standard-Identity Management Services.*

The *Electronic Transactions Act (Act)* (73 P. S. § 2260.101 *et seq*.), provides legal recognition of electronic signatures, records and transactions. Section 5 of the Act requires all agencies under the Governor's jurisdiction to comply with Office of Administration standards relating to the rules for acceptance and use of electronic signatures, records and transactions by commonwealth agencies.

PKI is an integrated set of policies, procedures, hardware, and software used to create, manage, use and rely on X.509 PKI certificates, which convey the public keys used in public key cryptography. X.509 PKI certificates identify an individual, organization, or device as the subject of the PKI certificate and bind that subject to a particular public/private key pair for strong authentication. Different PKI certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes. The commonwealth PKI provides services supporting the use of public key cryptography for strong authentication, confidentiality, integrity and non-repudiation of communications between the commonwealth and its employees, business partners, and subscribers. This includes virtual private networks (VPNs), digital signatures, access to commonwealth resources, and personal identity verification (PIV) cards. This ITP describes the commonwealth policies governing these uses.

Refer to the commonwealth Certificate Policy (CP) for specifics concerning the PKI components, the Certification Practice Statement (CPS), and more guidance for the many uses of PKI certificates.

1.1 Organization

After this Introduction, this document provides the following information:

- Section 2 establishes the general policy governing the commonwealth's PKI;
- Section 3 provides policy for general usage of the PKI, which utilizes two Certificate Authority solutions;
  - Commonwealth internally hosted Certificate Authority; and
  - External shared service provider Certificate Authority;
- Section 4 explains the commonwealth PKI certificate revocation and renewal policy;

- Section 5 covers governance and administration policy; and
- References and acronym definitions are provided in GEN SEC013A - *Identity Protection and Asset Management (IPAM) Glossary*.

2. General Policy

The commonwealth policy for PKI certificates conforms to the X.509 standard. X.509 refers to the Internet Engineering Task Force (IETF) PKIX Certificate and Certificate Revocation List (CRL) Profile of the X.509 v3 certificate standard, as specified in RFC 3280.

2.1 Certificate Policy (CP)

The commonwealth PKIs adhere to the enterprise Certificate Policy (CP). The enterprise CP follows the outline established by RFC3647. The CP is published to the Certificate Authority and is available for public access.

Commonwealth PKIs adhere to Certificate Practice Statements (CPS). The CPS is not published to the Certificate Authority for public access. Agencies may request special access when necessary for coordination with vendors and other business partners as appropriate.

2.2 Certificate Authority (CA)

The X.509 system establishes an entity known as a Certificate Authority (CA) specifically to issue digital certificates for use by other parties. The CA issues a PKI certificate binding a public key to a particular *Distinguished Name* according to the X.500 directory services standard. This public key is paired with its asymmetric private key to confirm authenticity of the associated entity. The CA provides certificate confirmation and validation to the recipients of PKI certified messages. It also provides a CRL to track revoked and expired certificates for its users.

The commonwealth hosts its own internal CA to provide a cost-effective solution for issuing digital certificates for authentication to commonwealth systems. Because access to the internal CA, corresponding key storage and revocation list, is limited to systems on the commonwealth network, the internal CA cannot be used for transactions with entities outside the commonwealth infrastructure. The internal CA does not archive or escrow the keys and certificates, which further constrain its acceptable uses.

Acceptable uses for the Internal CA include, but are not limited to:

- Authentication to the commonwealth VPN;
- Authentication to the commonwealth wireless network; and
- Two-factor authentications to commonwealth systems, services or software applications.

Prohibited uses for the internal CA include, but are not limited to:

- Encrypting e-mail;
- Authenticating the commonwealth to a county or business-partner system; and
- Digital signing of any type.

For applications requiring digital signatures or encryption, or for authentication to external entities, use of the external CA as established in STD-SEC014C - *Product Standards for Public Key Infrastructure / Shared Service Provider,* is required.

Logically, the external CA is a single root CA, although physically it may actually consist of more than one CA entity, as determined by the commonwealth's Shared Service Provider. The external CA is to be used for all communications with entities external to the commonwealth, and for any permanent signing or encrypting.

All commonwealth PKI certificates are to be issued using either an internal CA or an external CA.

2.3 Registration Authority

Each CA delegates the actual registration and certificate delivery to one or more associated Registration Authorities (RAs). OA may designate an agency as an RA to register the agency's internal and/or external users. Agencies desiring to act as an RA are directed to consult with the IPAM team at RA-IPAM@state.pa.us.

2.4 Minimum Requirements of the Certificates

For maximum security and compatibility with the Commonwealth of PA Enterprise Directory (CoPED), all PKI certificates shall:

- Have X.500 directory service compliant subject names;
- Be FIPS-140 minimum key specification compliant (according to the most current version of FIPS-140); and
- Have unique certificate names.

PKI Certificates containing private keys are to be stored in a secured container. These include CAPI, Java Key stores, and the secure Commonwealth of Pennsylvania (CoPA) PIV card. All PKI certificate stores are to be password protected.

Other PKI certificate requirements depend on whether they are for users, software applications, or hardware as described in the following subsections.

2.4.1 User Certificates

User certificates are to be used only for transacting official commonwealth business as outlined in the applicable CP. They are issued on an individual basis and are to be used only by that individual and not to be shared with others. Much like a user's password or social security number, the digital certificate, specifically the private key, needs to be protected from disclosure. Specifics of such protection will depend on the media on which the certificate is stored. Practices to safeguard the certificate include, but are not limited to:

- Password protection on the PKI certificate;
- Encryption of the PKI certificate or its storage medium; and
- Locking of the PKI certificate to prevent exporting it to another location.

2.4.2 PIV Cards

The integrated circuit chip (ICC) on the PIV card is a secure container for the certificate. PKI Certificates are not to be exportable from the PIV Card.

2.4.3 Applications/Software

Computer programs and services (including web services) may use PKI certificates to authenticate themselves to other programs and systems.

2.4.4 Hardware (SSL, Servers, Routers)

Workstations and servers may use PKI certificates to authenticate themselves to other systems and computer programs. PKI certificate use on workstation browsers requires that the browser security be set at High Level. This will require the user to enter a password for each browser session.

2.5 Identity Verification and Vetting

Only users formally vetted and registered to CoPED Assurance Levels 200 or higher are to be eligible to obtain a PKI certificate. Level 100 identities (as defined in GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*) include no assurance that the identity is who he/she claims to be.

External CA PKI certificate (those issued by the shared service provider) requests for software or hardware (code signing, messaging) are also only to be granted to components that have been validated and vetted according to the applicable commonwealth certificate policies and the Commonwealth Certificate Practice Statement.

3. General Usage

PKI certificates are to be used only for official commonwealth business. Some common uses are listed below:

3.1 Encryption

There are a number of technologies that are well suited to make use of PKI certificates for encryption. For example:

- Secure Sockets Layer (SSL) for secure internet transmissions. SSL fundamentally requires a public and private key for its encryption;
- VPNs use public wires to connect secure nodes, so public-key encryption is a good choice for encrypting data transmitted in this way;
- Secure Multipurpose Internet Mail Extensions (S/MIME) incorporates public-key encryption into the standard MIME e-mail protocol; and
- Securing confidential information, such as with XML encryption, or for document and file storage systems.

3.2 Certificate Use with Mail

At each agency's discretion, external CA issued PKI certificates may be used to enforce official business mail policy and security matters as appropriate. Examples of appropriate usage include, but are not limited to:

- Correspondence with federal or state governments;
- JNET correspondence; and,
- Correspondence that includes sensitive information warranting a moderate to high security level as explained in Section 7 of GEN-SEC013C - *Access Management and Control.*

3.3 VPNs

The commonwealth CA will issue PKI certificates to be used for remote access VPNs, both to authenticate the users accessing the VPN and to set up the encrypted SSL session.

3.4 Digital Signatures

PKI digital signatures are an approved option for electronic document signing. Appropriate usage of PKI for digital signatures is explained in the ITP-SEC006.

3.5 Authentication

Various logical containers, such as the integrated circuit chip on a commonwealth issued PIV card or the PKI certificate store on a server, may hold external CA-issued PKI certificates for authentication to physical and logical resources.

4. Certificate Revocation and Renewal

All PKI certificates are to have an expiration period, and are no longer valid once the expiration period has passed. The maximum term for PKI certificates is five years. Shorter terms may be used according to individual circumstances and security requirements.

PKI certificates may also be revoked. Agencies are responsible for notifying CAs when PIV Cards or PKI certificates need to be revoked. A list of possible reasons for revocation appears near the end of this Section 4. In the case of an expired PKI certificate, the date of expiration is included as a part of the PKI certificate itself and can be checked upon presentation of the PKI certificate. The revocation status of a PKI certificate, however, is not inherent in the PKI certificate itself, and is to be determined from external sources.

There are two mechanisms by which an agency may determine the revocation status of a certificate:

- CRL – FIPS 201 requires approved CAs to publish a list of all revoked PKI certificates at least once every 18 hours. All revoked PKI certificates are to be maintained on the CRL at least until their expiration dates. Because there is no requirement to update the CRL more frequently, the information contained in the CRL could be as much as eighteen hours old. In time-sensitive situations this can pose a real security risk.
- Online Certificate Status Protocol (OCSP) – FIPS 201 requires every CA that issues PIV Card authentication certificates to operate an OCSP server that provides the status for every PIV Card authentication certificate the CA issues. This mechanism allows users to query the CA database for the current status of a PKI certificate. Because the response is generally closer to real-time, and does not require the user to download lengthy revocation lists, the response is much more reliable and there is far less chance of missing a revoked PKI certificate. Agencies are strongly encouraged to implement OCSP over CRL unless there is a high degree of confidence that timing will never be an issue.

A subject (such as user, application, and hardware) may have its PKI certificate revoked under any of the following conditions:

- any information on the PKI certificate changes;
- subject’s association with the commonwealth is terminated;
- subject’s PIV card is revoked;
- subject’s agency affiliation changes;
- private key associated with either the subject or the CA is compromised;
- subject’s function is eliminated (typically evoked for retired applications or Web servers);
- user fails to maintain obligations set forth in policy statements;
- as per other agency or enterprise security policies outside this document and;
- upon request from an official who is authorized to make such decisions.

Subjects authorized for renewal are required to renew their PKI certificates before they expire. Users are to be notified in advance of pending expirations, and PIV cardholders may apply for renewal starting six weeks prior to the expiration date. Subject identities are to be revalidated prior to renewal.

5. Process and Governance

Key details of the commonwealth's PKI governance model are detailed below. Commonwealth agencies and business units are directed to consult with OA/OIT/EISO when PKI certificate services are required.

5.1 Root Authority

As defined in Section 2.2, *Certificate Authority*, the commonwealth has two independent CAs, one for internal use and one available for external use. Each CA is to have a single commonwealth owned root authority; the internal is administered by OA, and the external is administered by a federally-approved Shared Service Provider (SSP) with which the commonwealth has contracted. This SSP is named in STD-SEC014C - *Product Standards for PKI/SSP*. The SSP solution requires the commonwealth to be an intermediary CA, and prescribes adherence to its CP and all particular constraints therein.

Any approved agency CA is to attach to one of the commonwealth root CAs as a sub-CA.

All root keys are to be delivered by way of encrypted on-line exchange.

5.2 Escrow Agents (External CA Governance/Administration)

Escrow agents are commonwealth representatives who are authorized to request a copy of the private key of another subject within the commonwealth, and to archive that copy. This may be done for information recovery purposes, or agency business purposes such as fraud detection or employee turnover. Consult the VeriSign certificate policy at http://www.verisign.com/log-in/index.html for details.

5.3 Compliance Audit

Each CA is to be audited periodically as defined by its CP. Audits will be coordinated with and reviewed by the Identity Protection and Asset Management (IPAM) governance body.

5.4 Records Archival

Archive periods are dependent on the nature of the document being archived. Reference the appropriate archival policy; and if using PKI for encryption or document signing, ensure that the digital certificates are appropriately escrowed.

Refer to the VeriSign certificate policy for details on external certificate escrow and archive practices. Additional contractual agreements may be necessary to ensure compliance with specific agency archival requirements.

8. Related ITPs/Other References

- ITP-SEC013 - IPAM Architectural Standard-Identity Management Services
- GEN-SEC013C - Access Management and Control
- ITP-SEC006 - Commonwealth of Pennsylvania Electronic Signature Policy
- STD-SEC014C - Product Standards for Public Key Infrastructure / Shared Service Provider

9. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	1/25/2008	Base Policy
Revision	6/22/2009	Refreshed document
	4/2/2014	ITP Reformat