pennsylvania
OFFICE OF ADMINISTRATION

# Information Technology Policy

## *Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Services*

| **ITP Number**<br>ITP-SEC013 | **Effective Date**<br>June 22, 2006 |
|---|---|
| **Category**<br>Security | **Supersedes**<br>--- |
| **Contact**<br>RA-ITCentral@pa.gov | **Scheduled Review**<br>Annual |

**STATUS 03/14/2019: This ITP is undergoing internal review and revisions. Please contact RA-CISO@pa.gov for information regarding this policy.**

## 1. Purpose

The purpose of this Information Technology Policy (ITP) and its addenda is to define and establish policy governing the architectural framework for commonwealth Identity and Access Management Services. Technical standards are found in ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards*.

The approach determined by the IPAM team is comprised of the following distinct components:

- *Enterprise Directory Services* – Provides for consolidation, synchronization and aggregation of shared identity information for retrieval and user authentication;
- *Access Management and Control* – Provides standards and policies for accessing commonwealth facilities and information systems;
- *Enrollment, Identity Proofing and Vetting* – Outlines the processes for
- validating and verifying an individual's identity for the purpose of establishing credentials, such as log-in identifications and identity cards;
- *Specification for a Commonwealth Personal Identity Verification (PIV) Card* – Establishes the physical and logical composition of the Commonwealth PIV card, (magnetic strip, smart chip, photograph);
- *Identity Card Production, Personalization and Issuance* – Outlines the standards for creating, delivering, and activating an individual's unique identity card; and
- *Enterprise Public Key Infrastructure (PKI*) – Provides the standards for use of PKI security mechanisms (cryptography) to verify established identities, support digital signatures and encrypt sensitive data.

## 2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

## 3. Background

Early in 2004 the commonwealth embarked on an initiative to improve identity protection and access management across the enterprise. These efforts included several initiatives to define and collect identity management-related business requirements from a representative set of agencies. An interagency Identity Protection and Access Management (IPAM) team comprised of a governance structure, advisory board, and technical architecture group, was assembled to:

- Establish the commonwealth approach and technical architecture to identity management.

- Align this approach and technical architecture to federal initiatives with respect to commonwealth employees, business partners, and other constituent groups.

Critical business drivers include:

- The need for a standardized Employee/First Responder credentialing system that is compatible with that of the federal government.
- The need for enhanced physical and logical security in the wake of heightened terrorist activities.
- The need for identity token interoperability between and among municipal, state, and federal entities.
- The need for a commonwealth identity management system that adheres to federal standards (such as National Institute of Standards and Technology (NIST) publications).

## 4. Definitions

A comprehensive list of terms and definitions is presented in APP-SEC013A - *IPAM Glossary.*

## 5. Objective

The objective of this policy is to establish the architectural framework for the commonwealth's Identity and Access Management services.

## 6. Policy

Agencies undertaking new identity management implementations or projects related to the implementation of a shared security infrastructure, identity card technology, or other topics covered under the IPAM scope are to adhere to the standards and best practices set forth in this ITP and in ITP-SEC014. Organizations with existing identity management implementations are strongly encouraged to migrate to the standards and practices defined in these ITPs as soon as operationally feasible. All major revisions to non-compliant implementations are to be reviewed as part of the IT Procurement Review Process to determine if the investment warrants a change in standards at that time. Agencies are directed to submit proposed projects, with supporting business case, to the Enterprise Information Security Office for review by the IPAM Architecture Team.

<u>Enterprise Directory Services</u>

Numerous commonwealth applications store and retrieve identity-related information, including user credentials, in various data repositories generically referred to as identity stores. Proliferation of directory-centric applications tends to result in the creation and administration of increasing numbers of disparate identity stores across the enterprise. These identity stores may contain different sets of identity attributes, with different sources and refresh dates and little or no governance over the consistency or accuracy of these stores. This can not only lead to interoperability challenges among the agencies, as well as with business partners, other states, and federal agencies such as Homeland Security and federal law enforcement organizations.

This policy establishes a shared identity information store, the Commonwealth of Pennsylvania Enterprise Directory (CoPED), to support identity authentication and to provide each of the agencies a secure, well-governed, common repository for identity attributes. Commonwealth agencies are directed to utilize CoPED as the identity directory for their identity centric applications, and their access security applications in particular.

- The Enterprise Directory Service policy is detailed in GEN-SEC013B - *Directory Services Architecture.*
- Best practices for implementing the Directory Services are found in BPD- SEC013H - *Directory Services Implementation Guide.*

- Technology standards for CoPED are named in STD-SEC014A - *IPAM Technical Architectural Standards - Identity Management Services.*
- The Enterprise Directory Product Standards are named in STD-SEC014D - *Product Standard for Directory, Meta-directory, and Virtual Directory Products for Commonwealth of Pennsylvania Enterprise Directory (CoPED).*
- The core identity attributes stored in CoPED are listed in OPD-SEC014F - *Commonwealth of Pennsylvania Enterprise Directory (CoPED) Schema.*

Access Management and Control

Inappropriate or fraudulent access to state-owned physical and logical assets (e.g., facilities and information systems) exposes the commonwealth to significant risk from malicious intruders. A variety of access control systems have been installed across the enterprise to protect these assets and an even larger variety of access mechanisms have been established to utilize them – from security tokens, to biometric readers, manned guard posts, Personal Identification Number (PIN) pads and Smart Card readers. As access control requirements vary, the complexity and total cost of access management increases for the enterprise. A common standard for access management and Access Control System (ACS) products ensures reliable and cost-effective access management and control for agencies across the enterprise.

This policy establishes minimum standards for Access Management and establishes a shared authentication service for access to commonwealth logical resources.

- Commonwealth Access Management and Control policy is set forth in GEN- SEC013C - *Access Management and Control.*
- Standards for Web Single Sign-On products are named in STD-SEC014B – *Web Single Sign-On Standard.*
- Web access security standards are named in ITP-SEC003, *Enterprise Security Auditing and Monitoring - Internet Access Control and Content Filtering (IACCF) Standard.*
- Standards for provisioning system users are named in STD-SEC014E – *Product Standards for Provisioning and Password Reset Technology.*
  The commonwealth's electronic signature policy is explained in ITP-SEC006 - *Commonwealth of Pennsylvania Electronic Signature Policy* and the Commonwealth's Public Key Encryption policy is presented in GEN-SEC013G -*Public Key Infrastructure.*
- Minimum Standards for User IDs and Passwords are found in ITP-SEC007 -*Minimum Standards for User IDs and Passwords.*

Enrollment, Identity Proofing and Vetting

The NIST published Federal Information Processing Standard 201-1 (FIPS 201) to define specifications around a reliable, verifiable government-wide Personal Identity Verification (PIV) process to enable authorized physical and logical access to federally-controlled facilities and information systems.

Seeking to ensure commonwealth interoperability, its ability to share data and PIV card compatibility with federal organizations and other states, the IPAM enrollment, identity proofing and vetting policies conform to these federal standards.

- Policy defining the commonwealth standard PIV card credentialing process is found in GEN-SEC013D - *Enrollment, Identity Proofing and Vetting.*

Specification for a Commonwealth PIV Card

This ITP establishes new standards for the Commonwealth PIV card. The goal of the new PIV

card is to improve security, increase efficiency, reduce identity fraud, and protect personal privacy by establishing the standard for a secure and reliable form of commonwealth-issued identification credential. "Secure and reliable" refers to an identification credential that (a) is issued based on sound criteria for verifying an individual's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established in accordance with an official accreditation process. The standardized and accredited identity framework defined by this policy enables the commonwealth to establish reliable levels of trust for its identity credentials internally, and also with other states and federal agencies.

The Commonwealth PIV Card's physical topology, appearance, and other characteristics are balanced by the need to have the Commonwealth PIV Card commonly recognized as a nationally accepted state identification card, unique to Pennsylvania, but still having the flexibility necessary to support individual department and agency requirements. A common look for Commonwealth PIV Cards is important in meeting the objectives of improved security and interoperability, as they are to be both easily recognized by law enforcement officials and compatible with nationally accepted card reader technologies. In support of these objectives, consistent placement of printed components and integrated technology is necessary. Additionally, the card's construction is to be of durable, tamper-proof materials that defy counterfeiting or attempts to alter the information on the card.

This IPAM policy prescribes physical characteristics of the Commonwealth PIV Card that comply with FIPS 201, the International Organization for Standardization (ISO)/International Electro-technical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443].

- Standards governing PIV Card layout and embedded data attributes are found in GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification (PIV) Card.*
- For approved providers of qualified card stock, refer to the General Services Administration (GSA) FIPS 201 Approved Products List (APL).

<u>Identity Card Production, Personalization and Issuance</u>
This ITP establishes an Identity Life Cycle Management Architecture that defines a consistent, reliable, and federally accepted process for PIV card production, management and issuance. This accredited process ensures the consistent levels of quality and reliability necessary to allow these cards to be used as trusted authentication tokens for access to commonwealth physical and logical assets, and to be used nationally as a federally accepted form of identification.

This ITP also defines a shared user-account provisioning service for agencies that wish to leverage the economies of an enterprise-shared service. This shared provisioning service includes workflow processes that ensure the minimum acceptable standards for account creation, process roles, the assignment and management of appropriate authentication credentials, and escalation and delegation procedures are met.

- The Commonwealth Identity Life Cycle Management Architecture is described in GEN-SEC013F - *Identity Card Production, Personalization and Issuance.*
- Commonwealth standards for card management systems are named in STD- SEC014H - *IPAM Technical Architecture Standards: Federal Standards Related to FIPS 201.*

<u>Enterprise Public Key Infrastructure</u>

A PKI supports the use of digital certificates (such as X.509 v3) and the associated public/private key pair for digital signature, authentication and encryption. The commonwealth PKI policies conform to Federal Bridge specifications for cross certification in accordance with the standards, guidelines and practices of the Federal PKI Policy Authority (FPKI Policy Authority) and of the Federal PKI Steering Committee (FPKISC).

All commonwealth or agency PKI implementations are to conform to the commonwealth certificate policy and utilize a federally certified Shared Service Provider (SSP) to ensure FIPS 201 and Federal Bridge compliance. This SSP operates under a Certification Practice Statement that incorporates the requirements specified in the X.509 v3 Certificate Policy for the commonwealth's enterprise PKI and other certificate policies associated with identity initiatives mandated by the U.S. Federal Government.

- The commonwealth's PKI policy is explained in GEN-SEC013G - *Enterprise Public Key Infrastructure (PKI).*
- The commonwealth standard for PKI Shared Service Provider and PKI Certificate Authority is named in STD-SEC014C - *Product Standards for Public Key Infrastructure/Shared Service Provider.*

## 7. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- APP-SEC013A - *Identity Protection and Access Management (IPAM) Glossary*
- GEN-SEC013B - *Directory Services Architecture*
- GEN-SEC013C - *Access Management and Control*
- GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*
- GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification (PIV) Card*
- GEN-SEC013F - *Identity Card Production, Personalization and Issuance*
- GEN-SEC013G - *Public Key Infrastructure (PKI)*
- BPD-SEC013H - *Directory Services Implementation Guide*
- BPD-SEC013I - *Federal ID Assurance Standards*
- BPD-SEC013J - *Authentication via the PIV Card*
- ITP-SEC003 - *Enterprise Security Auditing and Monitoring - Internet Access Control and Content Filtering (IACCF) Standard*
- ITP-SEC006 - *Commonwealth of Pennsylvania Electronic Signature Policy*
- ITP-SEC007 - *Minimum Standards for User IDs and Passwords*
- ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards*
- STD-SEC014A- *IPAM Technical Architectural Standards – Identity Management Services*
- STD-SEC014B - *Web Single Sign-on Standard*
- STD-SEC014C - *Product Standards for Public Key Infrastructure/Shared Service Provider*
- STD-SEC014D - *Product Standards for Directory, Meta-directory, and Virtual Directory Products for Commonwealth of Pennsylvania Enterprise Directory (CoPED)*
- STD-SEC014E - *Product Standards for Provisioning and Password Reset Technology*

- OPD-SEC014F - *Commonwealth of Pennsylvania Enterprise Directory (CoPED) Schema*
- STD-SEC014G - *Web Services Security Standard*
- STD-SEC014H - IPAM Technical Architectural Standards – Federal Standards Related to FIPS 201

## 8. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

## 9. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

## 10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

| Version | Date | Purpose of Revision | Redline |
|---|---|---|---|
| Original | 6/22/2006 | Base Policy | N/A |
| Revision | 9/25/2009 | Added NIST published Federal Information Processing Standard 201-1 information to Enrollment, Identity Proofing and Vetting Section of Policy; refreshed document | N/A |
| Revision | 4/2/2014 | ITP Reformat | N/A |