pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Technology Standards

ITP Number ITP-SEC014	**Effective Date** June 22, 2006
Category Security	**Supersedes** ---
Contact RA-ITCentral@pa.gov	**Scheduled Review** 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 addendums is to establish and define the technical standards for commonwealth Identity and Access Management Services. Policy governing the architectural framework for IPAM is found in ITP-SEC013 - *IPAM Architectural Standard – Identity Management Services*.

Technology standards for the following areas have been defined:

- Identity Management Services
- Web Single Sign-On
- A federally approved Shared Service Provider (SSP) for KPI/Cryptographic Key Management
- Directory Service Technologies comprised of Enterprise Directory, Meta- Directory (for synchronization), and Virtual Directory
- Access Control Systems
- Personal Identity Verification (PIV) Card Stock Providers
- PIV Card Personalization and Production
- PIV Card Management Systems

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.

As business needs change, agencies are encouraged to make recommendations to their IPAM Architecture Team members regarding suggested modifications to this ITP. Agencies not currently represented on the IPAM Architecture Team may either seek representation or submit/present their recommendations to the team.

All new projects related to the implementation of a shared security infrastructure, identity card technology or other topics covered under the IPAM scope are required to follow current standards and best practices defined by this policy. All agencies will direct proposed projects, with supporting business case, to the IPAM Architecture Team for review and approval.

3. Background

Early in 2004 the Commonwealth of Pennsylvania launched enterprise-wide efforts addressing identity protection and access management. These efforts included several initiatives to define and collect related business requirements from a representative set of commonwealth 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 the federal initiative with respect to commonwealth employees, business partners, and other constituent groups.

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 technology standards 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 required to use the standards and best practices defined by the IPAM ITPs. Major revisions to existing implementations not using the current standards will be reviewed as part of the IT Procurement Review Process to determine if the investment warrants a change in standards at that time. All organizations having existing identity management implementations are strongly encouraged to migrate to the standards and practices defined by IPAM as soon as operationally feasible.

In order to ensure interoperability with federal and other jurisdictions, the commonwealth has adopted Federal Information Processing Standard (FIPS) 201. All related procurements will be made from the Federal General Services Administration (GSA) Schedule 70 approved products list.

Note: In cases where the commonwealth has explicitly designated a standard (e.g., VeriSign for digital certificates), the designated standard will take precedence over the GSA products list.

IPAM terms and expressions are listed in APP-SEC013A, *IPAM Glossary*.

<u>Product Standards for Identity Management Directories and Services</u>

Numerous commonwealth applications store and retrieve identity-related information, including user credentials, in various data repositories generically referred to as identity stores. GEN SEC013B - *Directory Services Architecture* establishes the Commonwealth of Pennsylvania Enterprise Directory (CoPED) to provide the various agencies and Communities of Practice with shared identity services and technologies to support their identity-centric auditing, reporting and application needs. The tools and standards to manage identities and to store identity data are available and recommended for agency use. These are named in STD-SEC014A - *IPAM Technical Architectural Standards - Identity Management Services,* and STD-SEC014D - *Product Standard for Directory, Meta-directory, and Virtual Directory Products for Commonwealth of Pennsylvania Enterprise Directory (CoPED).*

<u>Product Standard for Web Single Sign-On</u>

A goal of Web services is to incorporate multiple Web-enabled applications into a seamless, well-integrated Web experience for the user. Ideally, the user will feel as though all Web activities in a session are part of a single application. One factor required to achieve this is to eliminate the user's requirement to log into each secured application. Web Single Sign-on

technology accomplishes this, and the commonwealth product standard is named in STD-SEC014B - *Web Single Sign-On Standard.*

Service Provider Standard for Public Key Infrastructure/Shared Service Provider
The commonwealth's Public Key Infrastructure (PKI) is described in the Commonwealth Certificate Policy (CP), Certification Practice Statement (CPS), and ITP-SEC013 - *IPAM Architectural Standard.* The commonwealth relies on a federally certified SSP as its Certificate Authority (CA) for Private/Public Key and revocation list management. Approved providers are named in STD-SEC014C - *Product Standards for Public Key Infrastructure / Shared Service Provider.*

Product Standard for Commonwealth Access Control Systems
The Access Control System (ACS) provides the interface for a user's access token (such as a PIV Card), cross-checks the credential with the access authorization data store, and releases the asset's security mechanism to allow ingress to authorized users. The ACS is to be compatible with the access token used. Consult the FIPS 201 approved products list that is available through the General Services Administration (GSA) Schedule 70 for approved ACS devices.

Service Provider Standard for PIV Card Stock
FIPS 201 stipulates minimum requirements of PIV card stock to ensure appropriate durability and tamper proofing characteristics. To ensure these requirements are met, approved vendors for card stock are named in the FIPS 201 approved products list and are available through the GSA Schedule 70.

Product and Service Provider Standard for PIV Card Personalization and Production Stations
Agencies have two options for how to personalize PIV Card stock with the cardholder's personal information. They may collect the personal information and send it to an accredited service provider to place on the card, or they may acquire and use their PIV Card Personalization and Issuing Stations. Approved service providers and personalization stations are named in the FIPS 201 approved products list and are available through the GSA Schedule 70.

Product Standard for Commonwealth Card Management Systems
The PIV Card Management System tracks the entire life cycle of the PIV Card from its issue to revocation. It automates coordination with card stock and personalization service providers, identifies applicants who are already cardholders, and ensures that no two cards carry the same card number. Approved Card Management Systems are listed in the FIPS 201 approved products list and are available through the GSA Schedule 70.

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*
- 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 Standard 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 - *CoPA Enterprise Directory Schema*
- STD-SEC014G - *Web Services Security Standard*
- STD-SEC014H - *IPAM Technical Architectural Standards – Federal Standards Related to FIPS 201*
- STD-SEC014I - *Product Standards for Personal Identity Verification (PIV) Card Management System (CMS) Provider*
- ITP-SEC013 - *IPAM Architectural Standard – Identity Management Services*
- APP-SEC013A - *IPAM Glossary*
- GEN-SEC013B - *Directory Services Architecture*
- FIPS 201 - *FIPS 201 Approved Products List*

8. Authority

Executive Order 2016-06 - *Enterprise Information Technology Governance*

9. 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	06/22/2006	Base Policy	N/A
Revision	04/16/2008	Policy Refresh	N/A
Revision	04/02/2014	ITP Reformat	N/A