pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enrollment, Identity Proofing and Vetting

ITP Number GEN-SEC013D	***Effective Date*** September 7, 2006
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 Enrollment, Identity Proofing and Vetting policy that was established in ITP-SEC013 - *Identity Protection and Access Management Architectural Standard-Identity Management Services*. Identity cards, which can be used as access credentials to many commonwealth assets, are not issued until the card recipient's identity is assured. User identity provisioning is the process of creating user accounts and enabling access to all needed applications and services. The commonwealth provisioning process involves user enrollment, identity vetting (background checks) and proofing of identity credentials.

When the number of end users within an organization is large, the provisioning process becomes very tedious and expensive. Automating these routine, tedious tasks brings in huge benefits to the end users, as well as to the organization as a whole. GEN-SEC013B - *Directory Services Architecture* describes the policy and architecture for a commonwealth enterprise directory and shared directory services. GEN-SEC013C - *Access Management and Control,* describes the policy and architecture for a shared authentication service for identities in this directory. This supporting documentation describes the architecture for a shared provisioning service to create and manage these directory accounts.

1.1 Organization

This document provides the following information:

- Section 2 defines the provisioning architecture, and a shared user-account provisioning service for those agencies that choose to use it.
- Section 3 discusses delegation and management of approvers.
- Section 4 describes the provisioning principles, including proofing levels, reconciliation back to authoritative sources, and logging/auditing.
- Section 5 discusses security issues, especially administrative access and privacy concerns.
- Section 6 presents an overview of a recommended governance and administration structure.

- References and acronym definitions are provided in GEN-SEC013A - *Identity Protection and Access Management Glossary*.

2. Provisioning Architecture

IPAM defines several components for implementing Commonwealth Identity Management, including a Shared Identity Information Store, a Shared Security Architecture, PIV Card Management and Integration (including PKI), as well as Identity Proofing, Synchronization, and Identity Life Cycle Management. This document describes the Commonwealth Identity Life Cycle Management Architecture, which includes a shared user-account provisioning service for those agencies which do not wish to implement their own.

The shared provisioning service has many similarities to the identity synchronization service described in GEN-SEC013B. From the point of view of Commonwealth of Pennsylvania Enterprise Directory (CoPED), both services establish users and corresponding CoPED accounts, so both follow the scenarios defined in Section 4.3 of GEN-SEC013B for new and existing user account creation at an agency, especially with respect to finding and linking to existing CoPED accounts. Refer to GEN-SEC013B for those scenarios since they are not repeated in this document. *Figure 1 – Provisioning Architecture: Shared Provisioning* presents an overview of the Commonwealth-shared provisioning service.

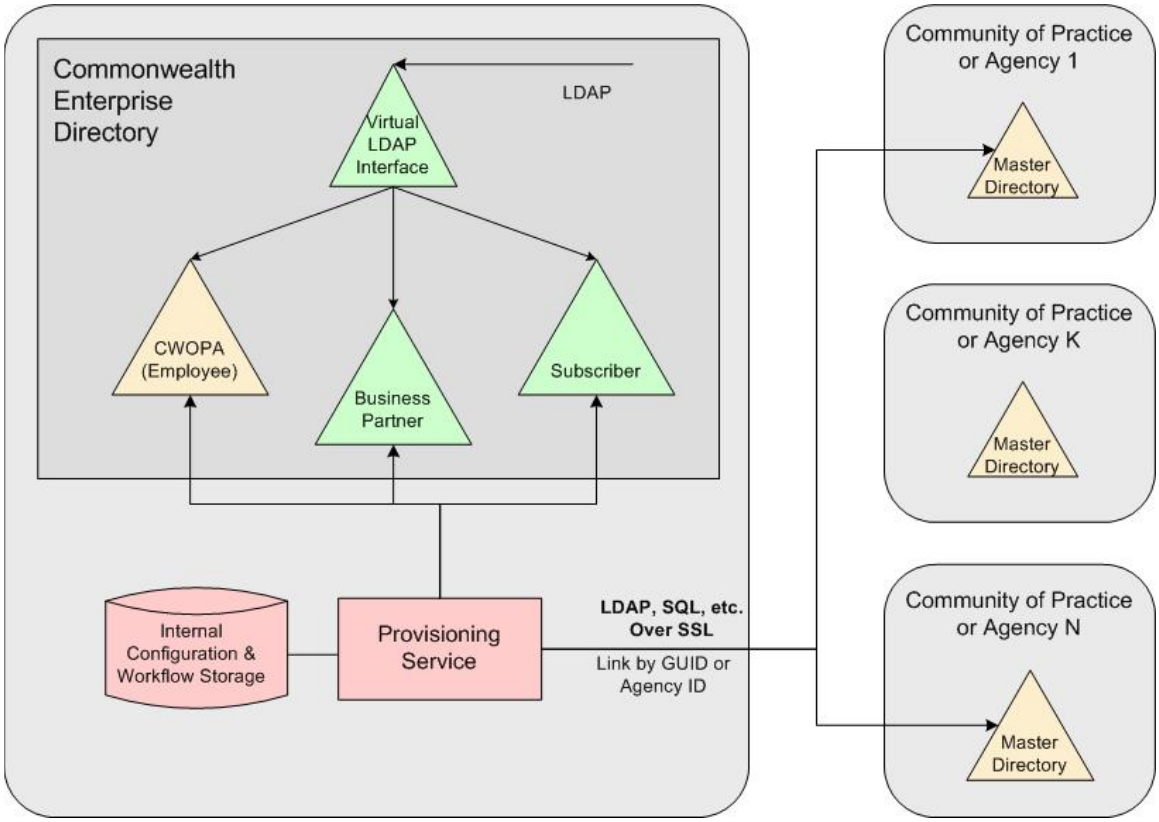

Figure 1 – Provisioning Architecture: Shared Provisioning

The determination of authoritative sources described in Section 5 of GEN-SEC013B also applies equally to the provisioning processes; this is explored more fully in Section 4.2.

Each agency may leverage separate instances of the shared service provisioning technology to populate users into its local identity stores (including the agency master directory) and to manage those identities. By leveraging this technology, the agency can typically save money on the initial (and ongoing) cost of the product, gain architectural insight from the work of the IPAM

Architecture Team, and share the benefits of the expertise gained from the commonwealth's deployment of these shared services.

2.1 Sponsors

A sponsor is an agency that uses the shared provisioning service to provision identities into its identity stores. The sponsor retains responsibility for vetting the user's identity before the provisioning service creates the user's accounts.

2.2 Senior Contact Official

Agencies using the shared provisioning service are also required to appoint and maintain a Senior Contact Official. The Senior Contact Official is responsible for approving all top-level delegations as described in Section 3.2.

2.3 Mixed Architecture

The Commonwealth Identity Life Cycle Management Architecture is mixed. It is based on a distributed structure, wherein each agency has its own processes and procedures for establishing users. It adds to the distributed structure a shared provisioning service for those agencies that do not internally implement all of the functionality of a provisioning service. The two subsections below describe each of these halves of the whole architecture.

2.3.1 Distributed Architecture

The Commonwealth Identity Life Cycle Management Architecture is primarily distributed. Each agency follows its own processes and procedural requirements for establishing users. These processes and procedures should include, but are not limited to:

- Vetting user identities;
- Creating user accounts in local identity stores, and aggregating them into an agency master directory;
- Assigning authentication credentials;
- Assigning application entitlements, often by assigning roles;
- Approving separately any or all of the above steps, by one or more groups of approvers, some of whom may be delegated;
- Notifying the users of their account creation;
- Logging/auditing to ensure that regulations are followed; and
- Managing anomaly situations via escalation.

Section 4 *Provisioning Principles* defines process standards with respect to the vetting of user identities and the resulting assigned Assurance Levels. Once users are thus established and their accounts created, the shared synchronization service described in GEN-SEC013B loads the users' identity information into CoPED. Depending on the configuration defined by the agencies, the shared synchronization service may also share identity information with other agency master directories.

2.3.2 Commonwealth Shared Provisioning Service

As noted above, the primary Commonwealth Identity Lifecycle Management processes reside with the agencies. Not every agency has the wherewithal or desire, however, to implement all of the required steps listed above in Section 2.3.1 *Distributed Architecture*. For those that do not, the commonwealth provides a shared provisioning service.

A provisioning service normally provides several functions. When leveraging the CoPA shared provisioning service, an agency may take advantage of:

- Workflow processes to assure that the agency has vetted and approved the user whose account(s) will be created;
- Creation of user identity accounts to CoPED or agency master directories;
- Assignment and management of appropriate authentication credentials;
- Assignment and management of appropriate commonwealth roles, such as First Responder, Citizen, and Resident. See Section 2.4.4 *Assigning Enterprise Roles and Entitlements*;
- User notification;
- Logging/auditing to ensure that regulations are followed;
- Escalation procedures; and
- Delegation procedures.

Although the shared service executes the workflow process, it is up to the agency to perform the actual identity vetting process, and to indicate at what point in the workflow it is completed. Although not totally independent, agencies may generally select which of the listed processes to adopt when using the shared provisioning service.

When an agency wants to enroll a user, that agency executes the shared provisioning service on its behalf, using the configuration settings it has established. These settings define how the service creates the user's account; how it determines the user's credentials, role, and access entitlements; whether the user is to be notified once the account is created and with what message; and the details on the workflow process followed for this user. These are all detailed in the following sections.

2.4 Creating and Managing User Accounts

The main reason for any provisioning service is to provide a mechanism to create and then manage users' accounts in connected identity stores. The IPAM shared provisioning service creates user accounts in CoPED. If the agency desires, the shared provisioning service also creates the users' accounts in the sponsoring agency master directory. The provisioning service does not create and manage accounts across all connected master directories, because the metadirectory already performs that service.

The subsections below detail certain aspects of the account creation (and management) process.

2.4.1 CoPED GUID Integration

The CoPED Global Unique Identifier (GUID) is defined in GEN-SEC013B. It is created by the metadirectory when first synchronizing a user's identity object to CoPED. When the shared provisioning service creates a user account in CoPED, it communicates the creation to the metadirectory to ensure that a unique CoPED GUID is defined for the user.

If the shared provisioning service, operating on behalf of an agency, creates a user account in that agency's master directory, it communicates the creation to the metadirectory to ensure that a unique CoPED GUID is defined for the user as part of the synchronization process to copy the user object to CoPED.

2.4.2 PIV Provisioning Integration

One of the key IPAM architecture drivers is the requirement to create Personal Identity Verification (PIV) Cards for commonwealth employees and first responders that are interoperable with the federal and other state governments' identity infrastructures. When a user who requires a PIV Card is provisioned, the shared provisioning service communicates with the PIV Card issuer to request issuance of the card. This request includes the data elements required by the provider, including:

- Name (FIRST, MI, LAST);
- Individual affiliation;
- Organizational affiliation;
- Expiration date (of the card, but the certificate expiration date can be no later than the card expiration date); and
- Agency Card Serial Number would leverage the CoPED GUID.

The PIV Card enables generation of a cryptographic key pair, and stores the private key locally on the card without export capabilities. The public key is exported in an X.509 certificate, which is returned to the provisioning service to store a copy in CoPED. The PIV Card is discussed in detail in the GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification (PIV) Card*.

2.4.3 Credential Management

As part of the creation and management of users' accounts in CoPED, the shared provisioning service creates and manages the users' authentication credentials. Depending on the assurance level required, these credentials may include UserID and password, digital certificates, or other credentials that may be determined in the future. Users who require PIV Cards receive a combination of data to be stored on the PIV Card with additional federally specified data (see Section 2.4.2 above for PIV integration).

2.4.3.1 Passwords

The shared provisioning service includes password management capability to enhance users' experience on the commonwealth's site and to reduce the cost for the commonwealth to maintain these credentials. Two key features are required to accomplish this. The first feature is password management, which provides self-service password functions, including change of passwords at expiration, resetting passwords, and recovering from lost passwords (getting a new password by answering challenge questions). The second feature is password synchronization, which intercepts password change events and distributes them automatically to the connected systems.

2.4.3.2 Certificates

The shared provisioning service does not issue or manage digital certificates. These are issued and managed by the PKI Shared Service Provider (SSP). When appropriate, however, the shared provisioning service interacts with the SSP to request issuance, re-issuance, or revocation of a digital certificate. The SSP provides the private key certificate to the user as defined in the *X.509 Certificate Policy (CP) for the Commonwealth of Pennsylvania Enterprise Public Key Infrastructure,* which defines in detail the commonwealth's PKI model, and in the *Certification Practice Statement* (CPS) issued by the SSP under the CP. The SSP also returns the public key certificate to the shared provisioning service to store in CoPED.

2.4.4 Assigning Enterprise Roles and Entitlements

As described in GEN-SEC013B, the CoPED schema includes a place to store enterprise-wide access rights, which are embodied in a limited set of commonwealth roles (such as First Responder, Citizen, and Resident). When the shared provisioning service creates or modifies a user account in CoPED, it assigns appropriate commonwealth roles using the criteria defined by EISO. Although most enterprise-wide entitlements (authorization permissions) are determined by the commonwealth roles, certain other entitlements may also be granted if approved by EISO; see the governance description in Section 6.

2.4.5 User Notification

Although not required, it is good practice to notify users when their accounts have been provisioned. The shared provisioning service provides a sponsoring agency with the capability to notify a user of the provisioning results if the user has supplied e-mail addresses. The shared provisioning service uses the notification template defined during the integration process by the sponsoring agency for its notification message.

2.5 Workflow

Workflow is one key feature that distinguishes the shared provisioning service from the metadirectory providing the shared identity synchronization service. While the rules governing metadirectory data synchronization can be quite complex, the metadirectory is only a back-end process moving data among identity stores. In contrast, the provisioning service interacts with administrators, managers, and other approvers to allow human intervention and management of the process at each step. The provisioning service can also interact with administrators who manage offline resources (such as office locations or telephones) and track completion status accordingly.

The provisioning workflow begins when a sponsor initiates a request to establish a user and create appropriate accounts, manage an existing user's account, or disable an existing user's account. The steps the workflow then processes is determined by the sponsoring agency, the initiating event, and often the data entered or retrieved during the process. The operations listed below are the available steps the agency uses to define the workflow:

- Validate and store request information.
- Request manual approval from an authorized approver.
- Request manual confirmation of offline identity vetting (document inspection, background check); see supporting document, GEN-SEC014D - *Product Standards for Directory, Meta-directory, and Virtual Directory Products for Commonwealth of Pennsylvania Enterprise Directory (CoPED)*.
- Include digital signature with manual approval or confirmation.
- Collect related user data from a connected directory (CoPED or agency master directory).
- Create or modify the user account in the provisioning service's internal data store.
- Create or modify the user account in a connected directory.
- Disable the user account in a connected directory (or possibly many or all connected directories).
- Assign authentication credentials to the user account.
- Communicate with the PKI SSP to request a digital certificate for the user, and store a copy of the issued public key certificate in CoPED.

- Assign one or more enterprise roles to the user account, and possibly assign additional entitlements.
- Notify the resource administrator or other interested parties to create or modify a resource account for the user, set the user's resource entitlements, or manually provision a physical or other offline resource to the user.
- Notify resource administrators or other interested parties that one or more users have had entitlements assigned (added, modified, or deleted).
- Notify managers or other interested parties that user accounts have been created, modified, or disabled, for their managed users.
- Notify users that their accounts have been created, modified, or disabled, or that they have had resource entitlements assigned (added, modified, or deleted).
- Log actions to the audit or tracking database (see Section 4.3, *Logging and Auditing*).

Notifications are typically by e-mail. The sponsoring agency may also decide to issue certain types of notifications in other ways (for example, by delivering a file of names to be added to an off-line resource, or by generating a physical letter to be mailed).

2.6 Standards

The shared provisioning service follows all standards listed in STD-SEC013A - *IPAM Glossary,* as appropriate. In particular, all access to CoPED (to publish users or for attribute modification or gathering) uses the Lightweight Directory Access Protocol (LDAP) v3. Access to the connected agency master directories uses the standard access protocol most appropriate for each store, which is ADSI for Active Directory, LDAP v3 for other directories, or SQL for databases.

The shared provisioning service also supports SPML (the Services Provisioning Markup Language from OASIS), which allows it to interoperate programmatically with other local provisioning systems at the agencies.

3. Delegation Model

This chapter discusses the issues involved when delegating authority within the shared provisioning service's workflows. This includes both the original delegation by the sponsoring agency to specified individuals for approval authority within the workflows (which is permanent until manually changed by the system administrators) and the ability of any approving managers to delegate their own authority, in whole or in part, for a period of time up to one year. All delegation activities are logged to the system audit or tracking database to maintain a record of who has had authority within the workflows at all times.

3.1 Managers

The system administrators and agency administrators may delegate user management functions to business managers who are responsible for a set of users. This initial delegation is determined by the defined sponsoring agency contact official, who is accountable for the delegated functionality. The delegated functions may include:

- Defining the user from an entry form so the user's account can be provisioned.
- Approving a user's request for an account which was created by self-registration.
- Specification (or request) of certain access roles.
- Disabling of, or requesting deletion of, the user's account or some access defined for that account.

Managers, in turn, may choose to delegate their user account creation and approval authority to certain other individuals, giving them responsibility for these tasks for a specified period of time. Depending on the sponsoring agency and application, these individuals may be the manager's subordinates, the manager's peers, a specified list of people (for example, shared administrative assistants), or some combination of these. Each such delegation has a maximum term limit of one year (the manager can specify a shorter time). The manager may re-specify the same person as delegate for another year. There is no limitation on the number of times the delegation may be re-specified.

The term manager, as used here, may also apply to someone who is managing access for external individuals not associated with a business partner organization. Although not strictly the manager of those individuals, the manager is the person to whom the management of those users' accounts is delegated by the sponsoring agency, and who then can delegate all or some of that authority as described above. For example, a school district clerk may be delegated the authority to manage the accounts for all the parents of the school district.

3.2 Delegation Management

The shared provisioning service provides for system administrators to define a set of user managers for each sponsoring agency, to whom specific administrative rights are delegated. These rights and the initial set of users are defined during the integration process by the sponsoring agency, approved by the responsible sponsoring agency senior contact official, and implemented when the agency begins using the service. These top-level user managers and their assigned rights are maintained by the system administration team.

In addition, as described above, these user managers may delegate some subset of their capabilities to other users, as allowed by the sponsoring agency. The provisioning system provides online forms for the managers to use to select a delegated user, select which authority to delegate, select the time period for the delegation, and enter a comment explaining why the

delegation occurred. The provisioning system delegates the manager's entitlements, and then logs this information to the system audit or tracking database (see Section 4.3). The manager may manually remove this delegation at any time, or let the delegation automatically expire when the selected time period ends.

Managers receive notification when any of their delegations are about to expire. The default warning period is one week, but can be set to any time by the sponsoring agency. If appropriate, the manager is provided with links to either renew the delegation for additional time up to one year, or to remove the delegation immediately.

Each manager action is logged to the system audit or tracking database. Renewal or immediate removal requires comments. Delegation expiration with no action is also logged.

3.3 User Self-Service

In addition to delegating authorization authority to managers and their assistants, it is possible to delegate both the initial user account creation request as well as much of the day-to-day user management functions back to the affected user. To allow a sponsoring agency to do this, the shared provisioning service provides two types of self-service functionality.

The first type of self-service functionality allows a user who wants access to one or more online functions but who does not currently have a user account to complete an online registration form supplied by the sponsoring agency. This submission then serves as the initiating event for a user account creation workflow. This workflow then processes the request based on the configuration defined by the sponsoring agency, and once approvals and other required steps are completed, it creates the user's account in CoPED or the agency master directory.

The second type of self-service functionality allows the user to manage a subset of the attributes in his or her CoPED account. Since most of the user's attributes are defined by agency or commonwealth processes, the available attributes for self-service modification are limited to basic contact information and requests for additional services or access rights (similar to self-registration requests in that workflows are initiated, although no new user account is created).

The shared provisioning service also provides self-service password management, as described previously in Section 2.4.3.1.

3.4 Anomaly Management

When administrative authority and approvals are delegated to users rather than a dedicated administration team, procedures are to be included to allow for continued successful operation when anomalies occur. These anomalies include temporary absence or termination of one or more approvers, failure to respond to an approval request within a specified period of time, conflicting responses to a parallel approval request, and duplicate registration (or other workflow process) requests which are often the result of a failure to respond to an earlier approval request.

This section describes the procedures to manage these anomalies. In these procedures, notifications or requests are often forwarded to the defined sponsoring agency senior contact official defined in Section 2.1.

3.4.1 Temporary Self-Delegation

Managers who are unavailable to perform their assigned functions are to delegate those functions temporarily to another approved user as defined by the sponsoring agency. This is the same delegation function as described previously in Section 3.2; the manager merely sets a shorter time period to correspond to the temporary absence. In this case, the manager may ignore the end-of-delegation-period notification and allows the delegation to expire.

3.4.2 Manager Termination

If a user manager with responsibilities delegated from another manager is terminated, the delegating manager is to use the delegation management functions to remove the terminating manager's delegation immediately and, as appropriate, re-assign the delegation to another user manager. If the responsibilities were delegated from the administration team on direction of the sponsoring agency, it is up to the defined sponsoring agency contact official to notify the administration team of the termination and reassignment of responsibilities.

In the event that a user manager with delegated responsibilities is terminated (his or her CoPED account is terminated and disabled) without having those responsibilities reassigned to another manager, any workflow requiring approval from the terminated manager must recognize this and follow a defined escalation procedure. If an escalation procedure is not defined, the workflow will send an error notification to the administration team, which then contacts the defined sponsoring agency contact official to reassign a user manager for these responsibilities.

3.4.3 Escalation Policies and Procedures

The shared provisioning service's workflow engine includes escalation capabilities, which allow a sponsoring agency to define policies and procedures to follow when no response is received to a request (generally an approval request) within a specified response time. Depending on the agency's business requirements, the policies may include one or more rules such as:

- Forward the request to a defined alternate responder (this should be the normal rule for most agencies and most processes) and notify the manager who delegated responsibility to the original responder.
- Notify the subject user of the current status and of the progress made to date.
- Notify the defined sponsoring agency contact official, who will decide whether and how to manage the delay or to request additional delegations through the standard official administration channel.
- Automatically deny or approve the request.
- Notify the defined sponsoring agency contact official, as above, and continue such notifications if a response isn't sent after an additional specified time increment. This rule may be repeated a number of times, with different rules triggered depending on which repetition expired.
- Do nothing.

3.4.4 Duplicate Requests

The shared provisioning service normally recognizes duplicate requests. This may occur when a user self-registers but is not approved, and therefore is not granted an account within what the user perceives as a reasonable length of time; the user may then assume that the first registration was lost and re-registers. The provisioning system recognizes the suspected duplication and indicates to the user that the initial registration is still pending, with its current status.

3.4.5 Emergency Override

There are times when workflows are interrupted, usually from a failure by a user manager to respond to an approval request within the specified time. If the escalation policies and procedures identified in Section 3.4.3 are not sufficient to resolve the issue, the sponsoring agency can specify that the shared provisioning service's administration team has the ability to override the request and allow the workflow to continue. In this case, the action is not only logged to the system audit or tracking database, but is also immediately e-mailed to the defined sponsoring agency contact official so immediate action can be taken if the override is inappropriate.

In addition to overriding interrupted workflows, the shared provisioning service's administration team has the ability to manually execute or override workflow steps when directed by the EISO. In each case, (as with the interrupted workflows), the action is both logged to the system audit or tracking database and also immediately e-mailed to the defined sponsoring agency contact official so immediate action can be taken if the override is inappropriate.

4. Provisioning Principles

This chapter describes the principles of the shared provisioning service.

4.1 Assurance Levels

Typically, agencies will provision users into their local Master Directories, and let the Enterprise Data Synchronization Service add them to CoPED. Included with the other user attributes will be the identity code of the sponsoring/proofing agency and the identity's Assurance Level. The Assurance Level is a value indicating the degree of confidence that the user is who he or she claims to be, and is based on the quality of the identification credentials presented and the depth of the identity vetting process used. The minimum identity proofing requirements for each of the four Assurance Levels are in Table I, *Identity Proofing Requirements* below. Commonwealth employees and first responders are typically vetted to an Assurance Level of 200.

An explanation of the roles of Registrar and Enrolling Official is provided in SEC013F *Identity Card Production, Personalization and Issuance.*

Table I. Identity Proofing Requirements

Assurance Level	Minimum Requirements
100 (None)	No specific requirements at this level. This level indicates there is no assurance of identity other than the recipient's word.

200 (Low)	In-Person: Requires possession of a valid current primary government photo ID that contains applicant's picture, and either address of record or nationality (driver's license or passport). Registrar or Enrolling Official: • Inspect Photo-ID, compare picture to applicant, record ID number, address and date of birth. If ID appears valid and photo matches applicant then: a) if ID confirms the address of record, then authorize issuance of the credentials and send notification of same to that address; b) if ID does not confirm address of record, issue credentials in a manner that will confirm the applicants address. For instance, the agency may choose to mail the credential to the address of record in an envelope stamped "if not at this address, return to sender." Remote Delivery Channel: Requires possession of a valid government ID number (a driver's license or passport) and a financial account number (checking account, savings account, loan or credit card) with method of confirmation (bank contact, credit check). Registrar or Enrolling Official: • Inspects both ID number and account number supplied by applicant. Verify information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirm that: name, date of birth, address, and other personal information in records are for the most part, consistent with the application and sufficient to uniquely identify the individual. • Initiate address confirmation and notification: a) Send notice to the address of record confirmed by the records check; or b) Issue credentials in a manner that confirms the address of record supplied by the applicant; or c) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at the number or e-mail address indicated by the applicant's records.

300 (Moderate)	<u>In-Person</u>: Requires possession of a verified current primary government photo ID that contains applicant's picture, and either address of record or nationality (driver's license or passport). Registrar or Enrolling Official: • Inspect Photo-ID and verify via the issuing organization or through credit bureaus or similar databases. Confirm that name, date of birth, address, and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and date of birth. If ID is valid and photo matches applicant then: a) if ID confirms address of record, authorize or issue credentials and send notice to address of record; b) if ID does not confirm address of record, issue credentials in a manner that confirms address of record. <u>Remote:</u> Requires possession of a valid government ID (driver's license or passport) number and a financial account number (checking account, savings account, loan or credit card) with confirmation via records of either number. Registrar or Enrolling Official is to: • Verify information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirm that: name, date of birth, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. • Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant (return receipt requested); or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number indicated in the applicant's records, and record the call.

400 (High)	In-Person: Requires in-person appearance and verification of two independent ID documents or accounts, one of which is to be current primary government picture ID that contains applicant's picture, and either address of record or nationality (driver's license or passport), and a new recording of a biometric of the applicant at the time of application. Registrar or Enrolling Official: • *Primary Photo ID:* Inspect photo-ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and date of birth. • *Secondary Government ID or financial account:* a) Inspect photo-ID and if apparently valid, compare picture to applicant, record ID number, address, and date of birth; or b) Verify financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that: name, date of birth, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. • *Record Current Biometric* Record a current biometric (photograph or fingerprints) to ensure that applicant cannot repudiate application. • *Confirm Address* Issue credentials in a manner that confirms address of record. • *Conduct appropriate background check if required.* Remote: Not an option. Level 400 identity proofing is to be in person.

If the user being vetted already has an identity account in CoPED, then the provisioning system incorporates the new sponsoring agency identity code into a running list of sponsors for that user. The user's Assurance Level and vetting process code only changes if the Assurance Level from the new sponsor is higher than the user's currently stored Level.

This processing is similar to that performed by the metadirectory; see Section 4 of GEN-SEC013B for a detailed explanation of the synchronization service.

4.2 Authoritative Sources

Effective management of user attributes is critical to the provisioning process and requires strict adherence to the authoritative source policy for:

- Creation of each class of user account
- Deletion or disabling of each class of user account
- Creation of each attribute, for each class of user account
- Modification of each attribute, for each class of user account
- Deletion of each attribute, for each class of user account

Section 5.1 of GEN-SEC013B provides a detailed discussion of this topic.

4.2.1 Reconciliation Policy

While metadirectory products are backend processes designed to move data among identity stores without human intervention, provisioning systems are designed for user interaction and serve as user management systems. Reconciliation is the process by which provisioning systems verify that provisioned users' attributes are not being changed in local agency identity stores, unless those local stores are authoritative for the changed attribute or the changes have gone through the appropriate user management process. Reconciliation can also include writing CoPED attribute values back to a local agency master directory if the local values have been inappropriately changed.

The provisioning system follows a permissive model when deciding whether to write CoPED attribute values back to a local agency master directory when the local values have been inappropriately changed. When the agency is integrated with the shared provisioning service, by default the non-authoritative attributes in its master directory will be overwritten by the reconciliation process. The agency may optionally choose, however, that certain attributes are not to be overwritten during reconciliation, so that any data mismatches between the agency master directory and CoPED for those attributes will be preserved.

4.3 Logging and Auditing

Since the provisioning process is critical to ensuring who has access to which resources, it is important to not only log all events but also to maintain an audit trail of all provisioning actions. To enable this data to be usefully searched, the audit trail is to be written to a relational database rather than flat files. As noted in Section 3, all delegation events are also written to the audit trail, since it is as equally important to know who is granting access as it is to know who has access.

Also, since these audit logs are critical to verifying the secure operation of the IPAM infrastructure, security methods are required to ensure that the integrity of the logs themselves. The methods employed depend on the provisioning product selected, but should meet the requirements of ITP-INF001 - *Database Management Systems*. Treat the logs as records to be maintained as defined in the INF-series ITPs. These may include such methods as:

- Digitally signing each entry to resist entry tampering.
- WORM (Write Once Read Many) media to resist erasure.
- Database access security.
- Mutually authenticated SSL channel to write entries.

5. Security Issues

The security for any government directory, and for its data loading processes, warrants careful examination. This is especially true for CoPED and its provisioning processes because it is a core component of the access control systems. GEN-SEC013B describes the security requirements on CoPED itself. The Shared Provisioning Service is to also provide security configuration and encryption that adhere to existing commonwealth protocols and policy for securing mission-critical data systems, including physical access restrictions. This section discusses these issues.

5.1 Administrative Access Control

GEN-SEC013B states that access to CoPED is programmatic by approved commonwealth (including agency) applications. The shared provisioning service is one of those applications, and therefore strictly limits access by administrators to the provisioning configuration as well.

As noted in GEN-SEC013B, the guiding principle of compliance for attribute selection (especially meeting the privacy requirements of existing laws, regulations, and standards governing the use of personally identifiable attributes) limits the storage of private data but does not eliminate it. Although the provisioning service is not itself an LDAP-accessible directory, it does include an internal data store that holds a current view of the identity data being collected and published about each user. Access to that internal data store is limited in the same way as administrative access directly to CoPED: configuration data is restricted to only appropriate maintenance personnel, and access to collected identity data is restricted to an approved data administrators group and protected by appropriate Access Control Lists (or equivalent, based on the product features).

The provisioning server is to be located in the application layer, so that it can access both the data store maintained in the data layer (CoPED) and external agency master directories. This location provides the provisioning server with firewall protection from casual access (both Internet and internal). Once accessed, the internal administrative access control policy is rigorously enforced in accordance with *FIPS 201* and *NIST SP 800-73* stipulations, federal and commonwealth legislation pertaining to the storage and handling of private information, and existing commonwealth network and information security standards and protocols.

The shared provisioning service runs in the security context of a specific account, which can be the same account as used by the metadirectory. It also accesses the connected master directories in the context of accounts specified for each connected directory. These accounts are to be locked down, denying access by normal users (e.g., for Windows, deny log-on locally, as a batch job, over the network, or Terminal Services) using X.509 certificates to authenticate, or creating long and hard random passwords and periodically changing those passwords.

5.2 Authentication

As noted in Section 2, the shared provisioning service connects to a number of master directories belonging to agencies. When communicating with each remote master directory, the provisioning server and directory mutually authenticate to ensure the provisioning service collects its data from (and potentially returns data to) the proper system.

5.3 Encryption

In addition to authenticating to remote systems, the provisioning service protects the identity data being transmitted between systems by requiring SSL for all traffic. This is primarily for remote traffic to agency master directories not co-located in the data layer; it is also to be used between systems within the data layer to further reduce the risk from exchanging sensitive data.

To ensure the security of any sensitive data at rest in the provisioning system's internal data store, such data is encrypted in place as discussed in Section 6.2 of GEN-SEC013B.

6. Governance and Administration

Ongoing governance for suggested modifications to the Shared Provisioning Service is provided by the Office of Administration/Office for Information Technology/Enterprise Information

Security Office (OA/OIT/EISO), with oversight and approval provided by the ETSC. Once modifications (including new functionality or integrations) are approved by the ETSC, they are to be designed and implemented by a designated administrative group. It is recommended that this be the same group that performs day-to-day operational oversight and management of the provisioning service.

During the detailed design and implementation of their use of the provisioning services, as well as during updates to those uses, any sponsoring agencies using the shared provisioning service is to work with EISO to define the detailed integration parameters. As noted previously in Section 2.1, the defined sponsoring agency senior contact official is responsible for approving the integration details before they are implemented. These integration parameters include:

- Definition of the approval workflow, including request validation (see Section 2.5).
- Specification of a user account creation template for creating user accounts in the agency master directory (see Section 2.4).
- Delegation and escalation procedures (see Sections 3.2 and 3.4.3).
- Delegation expiration warning time (see Section 3.2).
- Authentication credentials to be provided (see Section 2.4.3).
- Roles to be assigned and criteria for assigning each (see Section 2.4.4).
- E-mail notification cases and templates (see Sections 2.4.5 and 2.5).
- Contact officials (positions rather than names) for delegation approvals and anomalies (see Section 3.4, *Anomaly Management*).

As noted in *FIPS-201-1* (version 5, page 17), "To ensure the privacy of applicants, [the Commonwealth] shall...Assign an individual to the role of senior [Commonwealth] official for privacy… The individual serving in this role may not assume any other operational role in the PIV system." This senior privacy official reviews all requests for additional attribute data to be stored in CoPED to ensure that inappropriate private data is not added. This official also identifies stored attributes that require encryption or special access control (ACLs or equivalent) to protect their sensitivity. This official works in concert with the agency privacy officers defined in ITP-PRV002 - *Electronic Information Privacy Officer*.

Under the Commonwealth's Core Security Model, each agency retains control and execution of fine-grained authorization for its Web sites and applications.

7. Related ITPs/Other References

- ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Services*
- APP-SEC013A - *Identity Protection and Access Management (IPAM) Glossary*
- GEN-SEC013B - *Directory Services Architecture*
- GEN-SEC013C - *Access Management and Control*
- GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification (PIV) Card*
- GEN-SEC013F - *Identity Card Production, Personalization and Issuance*

- ITP-INF001 - *Database Management Systems*
- ITP-PRV002 - *Electronic Information Privacy Officer*

- STD-SEC014D - *Product Standards for Directory, Meta-directory, and Virtual Directory Products for Commonwealth of Pennsylvania Enterprise Directory (CoPED)*

8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

9. 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	9/7/2006	Base Policy
Revision	6/22/2009	Refreshed document
	4/2/2014	ITP Reformat